Ángela Barbero (Ed.)

LNCS 5228

Coding Theory and Applications

Second International Castle Meeting, ICMCTA 2008
Castillo de la Mota, Medina del Campo, Spain, September 2008
Proceedings

Springer

Lecture Notes in Computer Science 5228

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Ángela Barbero (Ed.)

Coding Theory and Applications

Second International Castle Meeting, ICMCTA 2008
Castillo de la Mota, Medina del Campo, Spain
September 15-19, 2008
Proceedings

Springer

Volume Editor

Ángela Barbero
Departamento de Matemática Aplicada (U. Valladolid)
E.T.S. Ingenieros Industriales
Paseo del Cauce s/n, 47011
Valladolid, Spain
E-mail: angbar@wmatem.eis.uva.es

Library of Congress Control Number: 2008934288

CR Subject Classification (1998): E.4, I.1, G.2, E.3

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-87447-X Springer Berlin Heidelberg New York
ISBN-13 978-3-540-87447-8 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12519927 06/3180 5 4 3 2 1 0

Preface

It is a pleasure to welcome you to the proceedings of the second International Castle Meeting on Coding Theory and its Applications, held at La Mota Castle in Medina del Campo. The event provided a forum for the exchange of results and ideas, which we hope will foster future collaboration. The first meeting was held in 1999, and, encouraged by that experience, we now intend to hold the meeting every three years.

Springer kindly accepted to publish the proceedings volume you have in your hands in their LNCS series. The topics were selected to cover some of the areas of research in Coding Theory that are currently receiving the most attention. The program consisted of a mixture of invited and submitted talks, with the focus on quality rather than quantity. A total of 34 papers were submitted to the meeting. After a careful review process conducted by the scientific committee aided by external reviewers, we selected 14 of these for inclusion in the current volume, along with 5 invited papers. The program was further augmented by the remaining invited papers in addition to papers on recent results, printed in a separate volume.

We would like to thank everyone who made this meeting possible by helping with the practical and scientific preparations: the organization committee, the scientific committee, the invited speakers, and the many external reviewers who shall remain anonymous. I would especially like to mention the General Advisor of the meeting, Øyvind Ytrehus. Finally I extend my gratitude to all the authors and participants who contributed to this meeting.

We thank the official institutions that sponsored our efforts: the Proyecto Consolider "Ingenio Mathematica" and the University of Valladolid.

This preface would not be complete without a few words about the special environment provided by the castle that gave its name to the meeting. La Mota Castle was built on the remains of a moorish castle from the 12th century. The current architecture is from the 15th century. In those days, the castle was one of the biggest and most important castles in Europe, located in Medina del Campo, one of the main trade centers of the Spanish Empire. The castle has lodged historical characters like Queen Isabel the Catholic and her daughter Joan the Mad, and its dungeons have provided accommodation for other prominent guests like César Borgia (who managed to escape by use of a file and a rope). We are sure such an atmosphere will generate inspiration for future work on the topics of the meeting and in many other directions.

July 2008 Ángela Barbero

Organization

2ICMCTA 2008 was organized by the University of Valladolid and was held in the Castillo de la Mota in Medina del Campo.

Organizing Committee

General Chair	Ángela Barbero (University of Valladolid, Spain)
Co-chair	Juan Tena (University of Valladolid, Spain)
General Advisor	Øyvind Ytrehus (University of Bergen, Norway)
Other members	M. Francisca Blanco (University of Valladolid, Spain)
	Javier Galán (University of Valladolid, Spain)
	Carlos Munuera (University of Valladolid, Spain)
	Daniel Sadornil (University of Cantabria, Spain)

Scientific Committee

Maria Bras-Amorós	University Rovira i Virgili, Spain
Gerard Cohen	ENST Paris, France
Tom Høholdt	Denmark Technological University, Denmark
Ignacio Luengo	Complutense University of Madrid, Spain
Garegin Markarian	Lancaster University, UK
Consuelo Martínez	University of Oviedo, Spain
Matthew Parker	University of Bergen, Norway
Kevin Phelps	Auburn University, USA
Josep Rifá	Autonomous University of Barcelona, Spain
Eirik Rosnes	University of Bergen, Norway
Emina Soljanin	Bell Labs, USA
Faina Solov'eva	University of Novosibirsk, Russia
Ludo Tolhuizen	Philips Research, Eindhoven, The Netherlands
Mercé Villanueva	Autonomous University of Barcelona, Spain
Jos Weber	Technical University of Delft, The Netherlands
Øyvind Ytrehus	University of Bergen, Norway

Sponsoring Institutions

Ingenio Mathematica (project Consolider)
University of Valladolid

Table of Contents

A Diametric Theorem in $\mathbb{Z}_m^n$ for Lee and Related Distances

Rudolf Ahlswede[1] and Faina I. Solov'eva[2]

[1] Universität Bielefeld, Fakultät für Mathematik, Postfach 100131, 33501 Bielefeld, Germany
hollmann@math.uni-bielefeld.de
[2] Sobolev Institute of Mathematics and Novosibirsk State University,
pr. ac. Koptyuga 4, Novosibirsk 630090, Russia
sol@math.nsc.ru

Abstract. We present the diametric theorem for additive anticodes with respect to the Lee distance in $\mathbb{Z}_{2^k}^n$, where $\mathbb{Z}_{2^k}$ is an additive cyclic group of order 2^k. We also investigate optimal anticodes in $\mathbb{Z}_{p^k}^n$ for the homogeneous distance and in $\mathbb{Z}_m^n$ for the Krotov-type distance.

1 Introduction

In this paper we establish the diametric theorem for optimal additive anticodes in $\mathbb{Z}_{2^k}^n$ with respect to the Lee distance, where $\mathbb{Z}_{2^k}$ is any additive cyclic group of order 2^k. We also study additive anticodes for related distances such as the homogeneous distance, see [7], and the Krotov-type distance, see [13].

Farrell [8], see also [15], has introduced the notion of an anticode (n, k, d) as a subspace of $GF(2)^n$ with diameter constraint d (the maximum Hamming distance between codewords) and dimension k. In fact earlier anticodes were used by Solomon and Stiffler [16] to construct good linear codes meeting the Griesmer bound, see also [6]. Such anticodes may contain repeated codewords.

Like in [1] we study anticodes without multiple codewords. The notion of an optimal anticode investigated in the paper is different from the notion in [15], Chapter 17. Let G^n be the direct product of n copies of a finite group G defined on the set $\mathcal{X} = \{0, 1, \ldots, q-1\}$. We investigate

$$AG^n(d) = \max\{|\mathcal{U}| : \mathcal{U} \text{ is a subgroup of } G^n \text{ with } D(\mathcal{U}) \leq d\},$$

where $D(\mathcal{U}) = \max\limits_{u,u' \in \mathcal{U}} d(u, u')$ is the diameter of $\mathcal{U}$, $d(\cdot, \cdot)$ is the Hamming distance for any finite group G, the Lee distance or the homogeneous distance for any cyclic group $\mathbb{Z}_{p^k}$, where p is prime, or a Krotov-type distance for $\mathbb{Z}_m^n$. In [4] the complete solution of the long standing problem of determining

$$\max\{|\mathcal{U}| : \mathcal{U} \subset \mathcal{X}^n \text{ with } D_H(U) \leq d\},$$

for the Hamming distance d, is presented and all extremal anticodes are given. Another diametric theorem in Hamming spaces for group anticodes is established

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 1–10, 2008.

in [1]: for any finite group G, every permitted Hamming distance d, and all $n \geq d$ subgroups of G^n with diameter d have maximal cardinality q^d.

In Section 2 we give necessary definitions and auxiliary results from [1], in Sections 3 and 4 we prove the diametric theorem for $\mathbb{Z}_{2^k}^n$ with respect to the Lee distance, in Section 5 we investigate optimal anticodes in $\mathbb{Z}_{p^k}^n$ endowed with the homogeneous distance, and Section 6 is devoted to optimal anticodes in $\mathbb{Z}_m^n$ for Krotov type distances.

2 Preliminary Definitions and Auxiliary Results

Throughout in what follows we consider groups additive and write the concatenation of words multiplicative, i.e. for $u^n \in \mathbb{Z}_m^n$ we use $u^n = u_1 u_2 \dots u_n$. The all-zero word of length n is denoted by 0^n.

Definition 1. *For any $\mathcal{U} \subset \mathcal{X}^n$ and $\mathcal{S} \subset \mathcal{X}$, where $\mathcal{S} \neq \emptyset$, we define*

$$\mathcal{U}_{\mathcal{S}} = \{u_1 \dots u_{n-1} : u_1 \dots u_{n-1} s \in \mathcal{U} \text{ for all } s \text{ from } \mathcal{S} \\ \text{and } u_1 \dots u_{n-1} s \notin \mathcal{U} \text{ for all } s \text{ from } \mathcal{X} \setminus \mathcal{S}\}.$$

From this definition we have the property

$$\mathcal{U}_{\mathcal{S}} \cap \mathcal{U}_{\mathcal{S}'} = \emptyset \text{ if } \mathcal{S} \neq \mathcal{S}'. \tag{2.1}$$

Definition 2. *For any $\mathcal{U} \subset \mathcal{X}^n$ we define*

$$\mathcal{U}_{(n)} = \{u_n \in \mathcal{X} : \text{ there exists a word } u_1 \dots u_{n-1} \text{ such that } u_1 \dots u_{n-1} u_n \in \mathcal{U}\}.$$

For two sets $\mathcal{U}, \mathcal{V} \subset \mathcal{X}^n$ their cross-diameter is defined as

$$D(\mathcal{U}, \mathcal{V}) = \max_{u \in \mathcal{U}, v \in \mathcal{V}} d(u, v).$$

Let G be any finite Abelian group. Denote by $\mathcal{S}_0$ a subset of G containing 0. Further we will use the following three lemmas, which can be found in [1].

Lemma 1. *For any subgroup $\mathcal{U}$ of G^n (briefly $\mathcal{U} < G^n$) a non-empty subset $\mathcal{U}_{\{0\}} 0$ of $\mathcal{U}$ is its subgroup.*

Lemma 2. (Generalization of Lemma 1) *If $\mathcal{U} < G^n$ then for a non-empty subset $\mathcal{U}_{\mathcal{S}_0} 0$ from $\mathcal{U}$ it is true that $\mathcal{U}_{\mathcal{S}_0} 0 \leq \mathcal{U}$.*

Lemma 3. *If $\mathcal{U}$ is a subgroup of G^n, then*

(i) There is exactly one subset $\mathcal{S}_0$ in G with $\mathcal{U}_{\mathcal{S}_0} \neq \emptyset$;
(ii) The set $\mathcal{S}_0$ is a group;
(iii) The set $\mathcal{U}_{\mathcal{S}_0} \mathcal{S}_0$ is a subgroup of $\mathcal{U}$.

By Lemma 3 we have $\mathcal{U}_{\mathcal{S}_0} \mathcal{S}_0 \leq \mathcal{U}$, so we can decompose a group $\mathcal{U}$ into cosets of the subgroup $\mathcal{U}_{\mathcal{S}_0} \mathcal{S}_0$:

$$\mathcal{U} = \bigcup_{\alpha} (\mathcal{U}_{\mathcal{S}_0} + \alpha)(\mathcal{S}_0 + \psi(\alpha)) \tag{2.2}$$

for suitable ψ.

3 A Diametric Theorem in $\mathbb{Z}_{2^k}^n$ for Lee Distance

Let $\mathbb{Z}_m$ be an additive cyclic group of order m. The Lee weight of $i \in \mathbb{Z}_m$ is defined as

$$w_L(i) = \min\{i, m-i\}.$$

For $u = (u_1, \dots, u_n) \in \mathbb{Z}_m^n$, $w_L(u) = \sum_{i=1}^{n} w_L(u_i)$ and for $u, v \in \mathbb{Z}_m^n$ the Lee distance between u and v is

$$d_L(u,v) = w_L(u-v).$$

Let $\mathcal{U}$ be any subgroup of $\mathbb{Z}_m^n$. The Lee diameter of $\mathcal{U}$ we define as

$$D_L(\mathcal{U}) = \max_{u,v\in\mathcal{U}} d_L(u,v).$$

For any two sets $\mathcal{U}, \mathcal{V} \subset \mathbb{Z}_m^n$ their Lee cross-diameter is

$$D_L(\mathcal{U},\mathcal{V}) = \max_{u\in\mathcal{U}, v\in\mathcal{V}} d_L(u,v).$$

It is well-known that the order of any group is divisible by the order of any of its subgroups.

Let $\mathbb{Z}_m$ be an additive cyclic group, then for any $r|m$ denote by $\left(\frac{m}{r}\right)$ the subgroup of $\mathbb{Z}_m$ generated by the element $\frac{m}{r}$. It can be written in the form

$$\left(\frac{m}{r}\right) = \left\{0, \frac{m}{r}, 2\frac{m}{r}, \dots, (r-1)\frac{m}{r}\right\}$$

and has an order r.

Lemma 4. (Diameter of a subgroup $\left(\frac{m}{r}\right)$ of $\mathbb{Z}_m$) *For any $r|m$ we have*

$$D\left(\left(\frac{m}{r}\right)\right) = \begin{cases} D(\mathbb{Z}_{2^k}) = 2^{k-1} & \textit{if } m = 2^k \textit{ for some } k \geq 1, \\ \lceil \frac{r-1}{2} \rceil \cdot \frac{m}{r} & \textit{otherwise.} \end{cases}$$

Proof. First consider the case $m = 2^k$, $k \geq 1$. Any subgroup of the group $\mathbb{Z}_{2^k}$ is a cyclic group (2^{r-s}) for some $s \in \{0, 1, \dots, k\}$ with the generator 2^{r-s}. It is easy to see that any subgroup (2^{r-s}) contains the element $2^{k-1} \in \mathbb{Z}_{2^k}$. The Lee weight of this element is

$$w_L(2^{k-1}) = \min\{2^{k-1}, 2^k - 2^{k-1}\} = 2^{k-1}.$$

By the definition of the Lee weight we have

$$w_L(2^t) < w_L(2^{k-1})$$

for any $t \neq k-1$. Then

$$D((2^{r-s})) = 2^{k-1} \text{ for any } s \text{ from } \{0, 1, \dots, k\}.$$

Let now m be any integer not equal to a power of 2 and let r be any integer such that $r|m$. By the definition of the subgroup $\left(\frac{m}{r}\right)$ we have

$$\left(\frac{m}{r}\right) = \left\{0, \frac{m}{r}, 2\frac{m}{r}, \ldots, (r-1)\frac{m}{r}\right\}$$

and the order of $\left(\frac{m}{r}\right)$ is $|\left(\frac{m}{r}\right)| = r$. Then we have $r-1$ non-zero elements in $\left(\frac{m}{r}\right)$ distinguished by pairs $i \cdot \frac{m}{r}$ and $(r-1-i)\frac{m}{r}$, such that $w_L(i \cdot \frac{m}{r}) = w_L((r-1-i)\frac{m}{r}) = i \cdot \frac{m}{r}$ for $i = 1, \ldots, \lfloor \frac{r-1}{2} \rfloor$. If r is even we have one maximal element $\lceil \frac{r-1}{2} \rceil \cdot \frac{m}{r}$ with $w_L(\lceil \frac{r-1}{2} \rceil \cdot \frac{m}{r}) = \lceil \frac{r-1}{2} \rceil \cdot \frac{m}{r}$. It is easy to see that $w_L(i \cdot \frac{m}{r}) < w_L(\lceil \frac{r-1}{2} \rceil \cdot \frac{m}{r})$ for any $i < \lceil \frac{r-1}{2} \rceil$ regardless of the parity of r. Therefore $D((\frac{m}{r})) = \lceil \frac{r-1}{2} \rceil \cdot \frac{m}{r}$.

Lemma 4 has the following useful consequences.

Corollary 1. *Let $r = 2l$ be even and $r|m$, then $D\left(\left(\frac{m}{r}\right)\right) = D(\mathbb{Z}_m) = \frac{m}{2}$.*

Corollary 2. *Let $r = 2l+1$ be odd and $r|m$, then $D\left(\left(\frac{m}{r}\right)\right) = \frac{l}{2l+1}m < \frac{m}{2}$.*

Corollary 3. *For any odd r or s such that $r|m$, $s|m$, and $s > r$ we have $D\left(\left(\frac{m}{s}\right)\right) > D\left(\left(\frac{m}{r}\right)\right)$.*

Remark 1. Like for the Hamming distance (see [1]) in the Lee case for $m = 2^k$ all subgroups of $\mathbb{Z}_m$ have the same diameter. This makes the approach via the transformation L introduced in [1] possible.

Lemma 5. *For any odd r and s such that $r|m$, $s|m$ and $s > r$ we have*

$$\frac{\log_2 s}{D\left(\left(\frac{m}{s}\right)\right)} > \frac{\log_2 r}{D\left(\left(\frac{m}{r}\right)\right)}. \tag{3.1}$$

Further, if r is even and the other relations hold again, the inequality also holds. In particular for $s = p^j$, $r = p^i$, $j > i$ it is true

$$\frac{j}{D((p^{k-j}))} > \frac{i}{D((p^{k-i}))}.$$

Proof. By Corollary 2 it suffices to show for any natural number l that

$$\frac{2l+1}{l}\log_2(2l+1) < \frac{2l+3}{l+1}\log_2(2l+3),$$

or that

$$(2l+1)^{\frac{2l+1}{l}} < (2l+3)^{\frac{2l+3}{l+1}},$$

or

$$(2l+1)^{2l^2+3l+1} < (2l+3)^{2l^2+3l},$$

which is equivalent to

$$(2l+1) < \left(\frac{2l+3}{2l+1}\right)^{2l^2+3l} = \left(1 + \frac{2}{2l+1}\right)^{2l^2+3l}.$$

Since $(1+a)^n + 1 + na \geq 1 + na$ sufficient is

$$1 + \frac{2(2l^2+3l)}{2l+1} > 1 + 2l,$$

or, equivalently, $4l^2 + 6l > 4l^2 + 2l$, which is true.

The final statement holds by Corollaries 1 and 2.

Remark 2. In summary, having again the relations $r|m$, $s|m$, and $s > r$, the inequality (3.1) can fail only for r odd and s even. Since in this case $D((\frac{m}{s})) = \frac{m}{2}$, the weakest counterexample could be for $r = 2l+1$ and $s = 2l+2$. Here we have to find l such that

$$\frac{\log_2(2l+2)}{\lceil\frac{2l+1}{2}\rceil\frac{m}{2l+2}} < \frac{\log_2(2l+1)}{\lceil\frac{2l}{2}\rceil\frac{m}{2l+1}}$$

or, equivalently, with

$$2l\log_2(2l+2) < (2l+1)\log_2(2l+1)$$

or with

$$\left(1 + \frac{1}{2l+1}\right)^{2l} < 1 + 2l.$$

Since the term to the left is smaller than e this holds for all $l = 1, 2, \ldots$.

On the other hand for $s = 2l' + 2$, $l' > l$ we have to check whether

$$2l\log_2(2l'+2) < (2l+1)\log_2(2l+1).$$

This fails for $l' \geq l_0'(l)$, suitable.

Remind that by $\mathcal{S}_0$ we denote a subset of $\mathbb{Z}_{2^k}$ containing 0.

Lemma 6. *If for any subgroup $\mathcal{U} < \mathbb{Z}_{2^k}^n$, $k \geq 1$, of diameter d it is true that $|\mathcal{S}_0| \geq 2$, then the transformation*

$$L : \bigcup_{\mathcal{S}} \mathcal{U}_{\mathcal{S}}\mathcal{S} \to \left(\bigcup_{\mathcal{S}} \mathcal{U}_{\mathcal{S}}\right)\mathbb{Z}_{2^k}$$

results in a group of diameter not more than d and not decreased cardinality.

Proof. First we show that the transformation L does not decrease the cardinality. Consider the decomposition (2.2). Every u^{n-1} occuring in some $\mathcal{U}_{\mathcal{S}_0} + \alpha$ has multiplicity

$$|\mathcal{S}_0 + \psi(\alpha)| = |\mathcal{S}_0|$$

and gets by the transformation L the multiplicity $|\mathbb{Z}_{2^k}| \geq |\mathcal{S}_0|$. So the cardinality does not decrease.

Furthermore by (2.2) and Lemma 4 we have

$$D(\mathcal{U}_{\mathcal{S}_0}) = D(\mathcal{U}_{\mathcal{S}_0} + \alpha) \leq d - 2^{k-1}$$

and also

$$D(\mathcal{U}_{\mathcal{S}_0}+\alpha,\mathcal{U}_{\mathcal{S}_0}+\alpha')\le d'-2^{k-1},$$

where $d'\le d$.

Using the transformation L and Lemma 4 we get

$$D\left(\left(\bigcup_{\mathcal{S}}\mathcal{U}_{\mathcal{S}}\right)\cdot\mathbb{Z}_{2^k}\right)\le d-2^{k-1}+2^{k-1}=d.$$

Hence the transformation L is appropriate, i.e. does not decrease the cardinality and does increase the diameter d.

Lemma 7. *If for any subgroup $\mathcal{U}<\mathbb{Z}_{2^k}^n$, $k\ge 1$ of diameter d it is true that $\mathcal{S}_0=\{0\}$, then there exist appropriate transformations of the group $\mathcal{U}$ into another subgroup of $\mathbb{Z}_{2^k}^n$ that do not decrease the cardinality and do not increase the diameter d.*

Proof. For $\mathcal{S}_0=\{0\}$ the decomposition (2.2) transforms into the decomposition

$$\mathcal{U}=\bigcup_{i\in\mathcal{U}_{(n)}}(\mathcal{U}_{\{0\}}+\varphi(i))i, \tag{3.2}$$

where $\mathcal{U}_{(n)}$ is from Definition 2. All cosets $\mathcal{U}_{\{0\}}+\varphi(i)$, $i\in\mathcal{U}_{(n)}$, are disjoint or equal.

We distinguish two cases.

Case 1: Since the set $\mathcal{U}_{\{0\}}$ by Lemma 2 is a subgroup for the case if there exist i,j, $i\ne j$, such that

$$\mathcal{U}_{\{0\}}+\varphi(i)=\mathcal{U}_{\{0\}}+\varphi(j),$$

then $\varphi(i)-\varphi(j)\in\mathcal{U}_{\mathcal{S}_0}$.

Case 1a: If $d_L(i,j)=2^{k-1}$ then

$$D(\mathcal{U}_{\{0\}}+\varphi(i))=D(\mathcal{U}_{\{0\}})=d-2^{k-1}.$$

In this case we use the transformation L, i.e. replace all i by $\mathbb{Z}_{2^k}$.

Case 1b: Let $d(i,j)=2^s<2^{k-1}$. W.l.o.g. we consider the case $\mathcal{U}_{\{0\}}=\mathcal{U}_{\{0\}}+\varphi(i)$, where $d(0,i)=2^s$. Since $\mathcal{U}_{(n)}$ is a subgroup in $\mathbb{Z}_{2^k}$ by Lemma 4 we have $D(\mathcal{U}_{(n)})=2^{k-1}$. Therefore we can find in $\mathcal{U}_{(n)}$ an element 2^{k-1}. Either $\mathcal{U}_{\{0\}}=\mathcal{U}_{\{0\}}+\varphi(2^{k-1})$ or $\mathcal{U}_{\{0\}}\ne\mathcal{U}_{\{0\}}+\varphi(2^{k-1})$ we have $D(\mathcal{U}_{\{0\}})=D(\mathcal{U}_{\{0\}}+\varphi(2^{k-1}))=d-2^{k-1}$.

In both cases we use the transformation L, i.e. replace $\mathcal{U}_{(n)}$ by $\mathbb{Z}_{2^k}$ (the smaller one we replace by $\mathbb{Z}_{2^k}$ not changing the diameter).

Case 2: If $\mathcal{U}_{\{0\}}+\varphi(i)\ne\mathcal{U}_{\{0\}}+\varphi(j)$ for any distinct i,j from $\{0,1,\dots,2^k-1\}$, then we replace all i by 0 and get the subgroup in $\mathbb{Z}_{2^k}^n$ with the same cardinality as the group $\mathcal{U}$ and the diameter does not increase.

From Lemmas 1-4, 6, and 7 we get

Theorem 1. *For any cyclic group $\mathbb{Z}_{2^k}$, $k \geq 1$, with respect to the Lee distance it holds*

$$A\mathbb{Z}_{2^k}^n(d) = |\mathbb{Z}_{2^k}|^{\min\left(n, \lfloor \frac{d}{2^{k-1}} \rfloor\right)} = 2^{k \min\left(n, \lfloor \frac{d}{2^{k-1}} \rfloor\right)}.$$

4 Optimal Direct Products of Cyclic Groups with Specified Lee Diameter

Let us consider maximal direct products of subgroups in $\mathbb{Z}_{p^k}$ with n factors and Lee diameter not exceeding d, $p > 2$. Recall that by Lemma 4

$$D\left(\left(\frac{p^k}{p^s}\right)\right) = D((p^{k-s})) = \lceil \frac{p^s - 1}{2} \rceil \cdot p^{k-s}$$

and write $F_{p^s} = (p^{k-s})$.

Clearly, for $k > s \geq t \geq 1$ it is true that $|F_{p^s}| \cdot |F_{p^t}| = |F_{p^{s+1}}| \cdot |F_{p^{t-1}}|$ and

$$D(F_{p^s}) + D(F_{p^t}) \geq D(F_{p^{s+1}}) + D(F_{p^{t-1}}), \tag{4.1}$$

because this is equivalent with

$$\lceil \frac{p^s - 1}{2} \rceil \frac{p^k}{p^s} + \lceil \frac{p^t - 1}{2} \rceil \frac{p^k}{p^t} \geq \lceil \frac{p^{s+1} - 1}{2} \rceil \frac{p^k}{p^{s+1}} + \lceil \frac{p^{t-1} - 1}{2} \rceil \frac{p^k}{p^{t-1}},$$

which is equivalent to

$$\frac{1}{2} - \frac{1}{2p^s} + \frac{1}{2} - \frac{1}{2p^t} \geq \frac{1}{2} - \frac{1}{2p^{s+1}} + \frac{1}{2} - \frac{1}{2p^{t-1}}$$

or to

$$\frac{1}{p^{s+1}} + \frac{1}{p^{t-1}} \geq \frac{1}{p^s} + \frac{1}{p^t}$$

or

$$p^{t-1} + p^{s+1} \geq p^t + p^s.$$

This is true, because $p^{s+1} > 2p^s > p^s + p^t$.

From (4.1) readily follows

Lemma 8. *For cardinality p^T, $T = ak + t$, $0 \leq t < k$, the group $\prod_1^a F_{p^k} \cdot F_{p^t}$ has the smallest diameter, namely*

$$D\left(\prod_1^a F_{p^k} \cdot F_{p^t}\right) = a\frac{p^k - 1}{2} + \frac{p^t - 1}{2}p^{k-t}.$$

This optimization problem can also be written as the following linear programming problem

$$\begin{aligned} &\text{(a) } d \le \sum_{t=1}^{k} a_t \cdot diam(\mathbb{Z}_{p^t}) \\ &\text{(b) } \max \left\{ \prod_{t=1}^{k} p^{a_t \cdot t} : \text{integers } a_1, a_2, \dots, a_k \text{ satisfy (a)} \right\} \\ \text{or } &\text{(c) } \max \left\{ \sum_{t=1}^{k} a_t \cdot t : \text{integers } a_1, a_2, \dots, a_k \text{ satisfy (a)} \right\}. \end{aligned}$$

The value of t is $f(t) = \frac{t}{diam(\mathbb{Z}_{p^t})}$, which can be seen with Lemma 5 to be monotonically increasing in t.

Therefore it is best to use $\mathbb{Z}_{p^k}$ as often as possible as factor in the subgroup, then $\mathbb{Z}_{p^{k-1}}$ as often as possible (under the constraint (a)) etc.

The result easily generalizes from $m = p^k$, F_{p^s}, F_{p^t}, $s > t$, to $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\mu^{\alpha_\mu}$, $F_S = F_{p_1^{\beta_1} p_2^{\beta_2} \cdots p_\mu^{\beta_\mu}}$, $F_T = F_{p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_\mu^{\gamma_\mu}}$, $S > T$. In the case there exists i such that $\beta_i < \alpha_i, \gamma_i \ge 1$ by taking p_i from T and adding it to S. Obviously for $S' = Sp_i$, and $T' = \frac{T}{p_i}$ we have $|F_S| \cdot |F_T| = |F_{S'}| \cdot |F_{T'}|$ and $D(F_S) + D(F_T) \ge D(F_{S'}) + D(F_{T'})$ because

$$\frac{\lceil \frac{S-1}{2} \rceil}{S} + \frac{\lceil \frac{T-1}{2} \rceil}{T} \ge \frac{\lceil \frac{S'-1}{2} \rceil}{S'} + \frac{\lceil \frac{T'-1}{2} \rceil}{T'}$$

holds, since it is true the inequality

$$\frac{1}{2} - \frac{1}{2S} + \frac{1}{2} - \frac{1}{2T} \ge \frac{1}{2} - \frac{1}{2S'} + \frac{1}{2} - \frac{1}{2T'}$$

as a consequence of $S' + T' \ge S + T$.

5 A Diametric Theorem in $\mathbb{Z}_{p^k}^n$ for Homogeneous Distance

According to [7] the homogeneous weight of $i \in \mathbb{Z}_{p^k}$ is given by

$$w_{hom}(i) = \begin{cases} 0 & \text{if } i = 0, \\ p-1 & \text{if } i \in \mathbb{Z}_{p^k} \setminus (p^{k-1}), \\ p & \text{if } i \in (p^{k-1}) \setminus \{0\}. \end{cases} \tag{5.1}$$

For $u = (u_1, u_2, \dots, u_n) \in \mathbb{Z}_{p^k}^n$, $w_{hom}(u) = \sum_{i=1}^{n} w_{hom}(u_i)$ and for $u, v \in \mathbb{Z}_{p^k}^n$ the homogeneous distance between u and v is $d_{hom}(u, v) = w_{hom}(u - v)$. The homogeneous diameter we define as

$$D_{hom}(\mathcal{U}) = \max_{u,v \in \mathcal{U}} d_{hom}(u, v)$$

and for any two sets $\mathcal{U}, \mathcal{V} \subset \mathbb{Z}_{p^k}^n$ the homogeneous cross-diameter is

$$D_{hom}(\mathcal{U}, \mathcal{V}) = \max_{u \in \mathcal{U}, v \in \mathcal{V}} d_{hom}(u, v).$$

Lemma 4′. (Homogeneous diameter of a subgroup of $\mathbb{Z}_{p^k}$) *For any integer $i \in \{1, 2, \dots, k-1\}$ we have $D_{hom}((p^i)) = D_{hom}(\mathbb{Z}_{p^k}) = p$, where $(p^i) = \{0, p^i, 2p^i, \dots, (p^{k-i} - 1)p^i\}$ has p^{k-i} elements.*

Proof. Since $p^{k-i-1} \leq p^{k-i} - 1$ and $p^{k-i-1}p^i = p^{k-1}$ we have $p^{k-1} \in (p^i)$ for any $i \in \{1, 2, \dots, k-1\}$. Therefore by (5.1)

$$p = D_{hom}((p^i)) \leq D_{hom}(\mathbb{Z}_{p^k}) = p.$$

It is easy to see that both Lemmas 6 and 7 have corresponding Lemmas 6′ and 7′, we just have to replace in the proofs 2^{k-1} by p and note that a subgroup $\mathcal{U} < \mathbb{Z}_{p^k}$ is of the form (p^i) for some i.

Using this and Lemma 4′ we get for

$$A'\mathbb{Z}_{p^k}^n(d) = \max\{|\mathcal{U}| : \mathcal{U} < \mathbb{Z}_{p^k}^n \text{ with } D_{hom}(\mathcal{U}) \leq d\} \text{ the following}$$

Theorem 2. *For any cyclic group* $\mathbb{Z}_{p^k}$*,* $k \geq 1$*, it is true* $A'\mathbb{Z}_{p^k}^n(d) = p^{k \min\left(n, \lfloor \frac{d}{p} \rfloor\right)}$.

6 A Diametric Theorem in $\mathbb{Z}_m^n$, $m = 4l$, for Krotov-Type Distance

For the cyclic group $\mathbb{Z}_m$ the Krotov-type weight $w_K : \mathbb{Z}_m \to \mathbb{R}^+$ is defined by

$$w_K(i) = \begin{cases} 0 & \text{if } i = 0, \\ 1 & \text{if } i \text{ is odd}, \\ 2 & \text{otherwise} \end{cases} \tag{6.1}$$

(see also [13]). For any word $u = (u_1, u_2, \dots, u_n)$ from $\mathbb{Z}_m^n$ we define the Krotov-type weight $w_K(u) = \sum_{i=1}^{k} w_K(u_i)$, distance $d_K(u, v) = w_K(u - v)$, diameter $D_K(\mathcal{U})$, and cross-diameter $D_K(\mathcal{U}, \mathcal{V})$.

As analog to Lemma 4 we get

Lemma 4″. (Diameter of a subgroup of $\mathbb{Z}_m$ for Krotov-type distance) *For any non-trivial* $\mathcal{U} < \mathbb{Z}_m$*,* $m \geq 2$*, we have*

$$D_K\left(\left(\frac{m}{s}\right)\right) = \begin{cases} 1 & \textit{if } s = 2 \textit{ and } \frac{m}{2} \textit{ is odd}, \\ 2 & \textit{otherwise}. \end{cases}$$

The proof easily follows from (6.1) and the fact that any subgroup $(\frac{m}{s})$ has an even element with the one exception if $s = 2$ and $\frac{m}{2}$ is odd. Lemmas 6″, 7″, the analogs to Lemmas 6, 7, are valid for the case $4|m$. Using these facts and Lemma 4″ we get.

Theorem 3. *For any cyclic group* $\mathbb{Z}_m$ *with* $4|m$ *with respect to the Krotov-type distance it is true* $A''\mathbb{Z}_m^n(d) = m^{\min\left(n, \frac{d}{2}\right)}$.

References

1. Ahlswede, R.: Another diametric theorem in Hamming spaces: optimal group anticodes. In: Proc. IEEE Information Theory Workshop, Punta del Este, Uruguay, March 13-17, 2006, pp. 212–216 (2006)

2. Ahlswede, R., Katona, G.: Contributions to the geometry of Hamming spaces. Discrete Mathematics 17, 1–22 (1977)
3. Ahlswede, R., Khachatrian, L.: The complete intersection theorem for systems of finite sets. European J. Combinatorics 18, 125–136 (1997)
4. Ahlswede, R., Khachatrian, L.: The diametric theorem in Hamming spaces -optimal anticodes. Adv. Appl. Math. 20, 429–449 (1998)
5. Ahlswede, R., Khachatrian, L.: A pushing-pulling method: New proofs of intersection theorems. Combinatorica 19, 1–15 (1999)
6. Belov, B.I., Logachev, V.N., Sandimorov, V.P.: Construction of a class of linear binary codes achieving the Varshamov-Griesmer bound. Problemy Peredachi Informatsii 10(3), 36–44 (1974)
7. Constantinescu, I., Heise, W.: A metric for codes over residue class rings of integers. Probl. Inform. Transm. 33(3), 208–213 (1997)
8. Farrell, P.G.: Linear binary anticodes. Electronics Letters 6, 419–421 (1970)
9. Katona, G.: Intersection theorems for systems of finite sets. Acta Math. Acad. Sci. Hung. 15, 329–337 (1964)
10. Kleitman, D.: On a combinatorial conjecture of Erdös. J. Combin. Theory 1, 209–214 (1966)
11. Krotov, D.S.: $\mathbb{Z}_4$-linear perfect codes. Diskr. Analiz Issled. Oper., Ser. 1, 7(4), 78–90 (2000) (in Russian)
12. Krotov, D.S.: $\mathbb{Z}_4$-linear Hadamard and extended perfect codes. Electronic Notes in Discrete Mathematics 6, 107–112 (2001)
13. Krotov, D.S.: On $\mathbb{Z}_{2^k}$-dual binary codes. IEEE Trans. Inform. Theory 53(4), 1532–1537 (2007)
14. MacDonald, J.E.: Design for maximmum minimum-distance error-correcting codes. IBM J. Res. Develop. 4(1), 43–57 (1960)
15. MacWilliams, F.J., Sloane, N.J.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
16. Solomon, G., Stiffler, I.I.: Algebraically punctured cyclic codes. Information and Control 8(2), 170–179 (1965)
17. Venturini, D.: Construction of maximum linear binary codes in the case of large distances. Problems of Cybernetics 16, 231–238 (1966) (in Russian)

Perfect 2-Colorings of Johnson Graphs $J(6,3)$ and $J(7,3)$

Sergey Avgustinovich and Ivan Mogilnykh

Sobolev Institute of Mathematics and Novosibirsk State University,
pr. ac. Koptyuga 4, Novosibirsk 630090, Russia
avgust@math.nsc.ru, ivmog84@gmail.com

Abstract. The problem of the existence of perfect 2-colorings in Johnson graphs $J(6,3)$ and $J(7,3)$ is solved in this paper. Perfect coloring is a generalization of the notion of completely regular codes, given by Delsarte [3]. This problem of existence of such structures is closely related to Delsarte hypothesis about the nonexistence of nontrivial perfect codes in Johnson graphs, the problem of existence of block schemes, the problem of existence of completely regular codes in Johnson graphs and other well-known mathematical problems. Some auxiliary theorems, which can be applied for treatment of perfect colorings in two colors in other graphs, are given in this paper.

1 Introduction

Consider the n-cube $E^n = \{x = (x_1, \ldots, x_n) : x_i \in \{0,1\}\}$. *The Hamming distance* between vectors $x, y \in E^n$ is defined by $d(x,y) = \sum_{i=1}^{n}(x_i \oplus y_i)$, where $\oplus$ denotes addition via modulo 2. *The Hamming weight* of a vector x is the distance from x to the all-zero vector. A vector x in E^n is said to precede a vector y in E^n (notation: $x \preceq y$) if $x_i \leqslant y_i$ for all $i \in \{1, \ldots, n\}$. A face Γ_x corresponding to a vector x in E^n is defined as the set $\{z : z \in E^n, x \preceq z\}$. A collection of k-subsets (referred to as blocks) of an n-set such that any t-subset occurs in λ blocks precisely is called a (λ, n, k, t)-design. A (1,n,k,t)-design is referred to as a Steiner system and is usually denoted by $S(n,k,t)$. Vertices of the Johnson graph $J(n,w)$ are all vectors of weight w in E^n; vertices that are at distance 2 from each other are connected by edges. It is easily checked that the Johnson graph $J(n,w)$ is a regular graph of degree $w(n-w)$. The graph metric in the Johnson graph is called the Johnson metric. For any two vertices x and y of some Johnson graph $d_J(x,y) = d(x,y)/2$ holds, where $d_J(x,y)$ is the Johnson metric between x and y.

By a *perfect m-coloring* of vertices of a graph $G = (V,E)$ (also known as an equatable partition, a graph divisor, a regular partition) with a matrix $A = \{a_{ij}\}_{i,j=1,\ldots,m}$, we mean a map T from the set of vertices V to the set of colors $\{1, 2, \ldots, m\}$ such that the color composition of the neighborhood of any vertex depends only on its color, and the number of vertices of the color j adjacent to a fixed vertex of the color i is a_{ij}. The matrix A is called the matrix of parameters

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 11–19, 2008.

of perfect coloring T. In case $m = 2$ the colors 1 and 2 symbolize white and black colors respectively. In what follows we denote the set of all white vertices by W and the set of all black vertices by B. Perfect colorings were previously studied in [10],[5], [9].

Let us be given a graph $G = (V, E)$. A *sphere of radius* i centered at v is defined as $B_i(v) = \{w \in V : d_G(v, w) \leq i\}$, where the distance d_G is the standard graph metric on G. An arbitrary subset C of a vertex set V is called *a code* in graph G. *The covering radius of a code* C is $\rho_C = max\{d(x, C), x \in V(G)\}$. A subset C of V is called *an e-perfect code* in G if spheres of radius e centered at the vertices of C form a partition of all vertices of G. If C either coincides with V (i.e., $e = 0$) or consists of at most two vertices, such a perfect code is called *trivial.*

In 1973, Delsarte conjectured [3] the nonexistence of nontrivial perfect codes in Johnson graphs. All presently known results confirm the conjecture (see [4],[1],[8]). It is easy to note that to a 1-perfect code in a regular graph of degree (or valence) t, we may assign a perfect 2-coloring. If we suppose such a code to exist and color all code vertices into white color, and all noncode ones – into the black color, we obtain a perfect 2-coloring. So, the problem of existence of perfect 2-colorings in Johnson graphs includes the Delsarte hypothesis.

There are a lot of examples of nonisomorphic 1-perfect codes in E^n. The perfect colorings, that arise from these codes are also nonisomorphic, but they have the matrix of parameters equal. The situation is analogous in Johnson graphs: there are examples of nonisomorphic perfect 2-colorings with the same matrix of parameters. For example, there are two nonisomorphic perfect colorings of $J(6, 3)$ with matrix $\begin{pmatrix} 3 & 6 \\ 4 & 5 \end{pmatrix}$. The purpose of this article is to list all parameters of existing perfect 2-colorings of $J(6, 3)$, $J(7, 3)$ and to validate any matrix by a construction of perfect coloring. In [10] all perfect 2-colorings of $J(n, 2)$ were described, so graphs $J(6, 3)$ and $J(7, 3)$ are graphs for which the problem of existence of perfect 2-colorings was open.

2 Some Properties of Perfect Colorings

Some properties of perfect colorings that will be used in proving the main result of this paper are given in this section.

Proposition 1. *Let T be a perfect coloring of a graph G into two colors with the matrix $A = \{a_{ij}\}_{i,j=1,2}$, then the number of white vertices in G is equal to $|V(G)|a_{21}/(a_{12} + a_{21})$.*

Proof. Let us consider a graph obtained by deleting all edges (u, v) in graph G such that u and v are colored in the same color. The graph obtained is biregular bipartite graph with parts W and B and degrees a_{12} and a_{21}. On the one hand, the number of edges in this graph is equal to $a_{12}|W|$, and on the other hand it is equal to $a_{21}|B|$. Taking into account $|W| + |B| = |V(G)|$, we obtain $|W| = |V(G)|a_{21}/(a_{12} + a_{21})$.

Let G be an arbitrary graph, C be a code in G. The following sets will be referred to as layers of a distance partition (with respect to a code C): $L_0(C) = C$ $L_j(C) = \{y \in V : d_J(y, L_0(C)) = j\}$ for $0 \leq j \leq \rho_C$. Note that $V(G) = \bigcup_{0 \leq j \leq \rho_C} L_j(C)$. This partition will be referred to as *the distance partition of vertices of G with respect to C*. The distance partition with respect to C is called *distance-regular* and code C is called *completely-regular*, if the numbers of vertices from layers $j-1$, j, $j+1$ (these numbers are denoted d_j^-, d_j^0 and d_j^+ respectively) adjacent to a fixed vertex from the layer j depend only on j, but not on a choice of a fixed vertex from layer j. Completely regular codes were previously investigated in [11], [9]. If we color every layer from a distance-regular partition with respect to a completely regular code C into its unique color, then we obtain a perfect coloring in $\rho(C)$ colors. The matrix of parameters of such a perfect coloring is a tridiagonal matrix of the set of numbers d_j^-, d_j^0 and $d_j^+, 0 \leq j \leq \rho(C)$. Also note that any set of vertices of a fixed color (W,B) of any perfect coloring into two colors is a completely regular code with covering radius $\rho = 1$.

Let T be a perfect coloring of a graph G, and C be a code in G. We denote $l_j(C) = |L_j(C) \cap W|$.

Theorem 1. *Let T with a matrix of parameters $A = \{a_{ij}\}_{i,j=1,2}$ be a perfect coloring in two colors of a graph G and C be a completely regular code in G. Then for all $j : 0 \leq j \leq \rho(C)$ we have $l_{j-1}(C)d_{j-1}^+ + l_j(C)(a_{21} - a_{11} + d_j^0) + l_{j+1}(C)d_{j+1}^- = |L_j(C)|a_{21}$.*

Proof. Let R_j be the set of all edges of $J(n,w)$ with one end (of any color) belonging to $L_j(C)$ and the other end white. On one hand, a white one can belong only to one of the layers $L_j(C)$, $L_{j+1}(C)$, or $L_j(C)$, and the other one of any color belongs to $L_j(C)$. Let us write this as follows:

$$|R_j| = l_j(C)d_j^0 + l_{j+1}(C)d_{j+1}^- + l_{j-1}(C)d_{j-1}^+. \tag{2.1}$$

On the other hand we can write it in this way

$$|R_j| = l_j(C)a_{11} + (|L_j(C)| - l_j(C))a_{21}. \tag{2.2}$$

Substituting (2.1) in (2.2), we obtain the desired equality.

A graph G is called *distance regular*, if for any two vertices x and y such that $d_G(x,y) = k$ the number of vertices $z : d_G(z,x) = i, d_G(z,y) = j$ is equal to the $\gamma_{i,j,k}$, that does not depend on a choice of x, y, but only on i, j and k. The graphs $E^n, J(n,w)$ are known to be distance regular [2]. A few examples of completely regular codes in some distance regular graphs are given in following two statements.

Consequence 1. Let G be a distance regular graph, x be an arbitrary vertex of graph G, then

1. The set $\{x\}$ is a completely regular code in G.

2. Let T be a perfect coloring of G into two colors with matrix of parameters $A = \{a_{ij}\}_{i,j=1,2}$, then for any i the number of vertices of white color in $L_i(\{x\})$ is the same for any vertex x from W and for any coloring whose matrix of parameters is $A = \{a_{ij}\}_{i,j=1,2}$.

Proof. 1. It is easy to see that the numbers d_j^-, d_j^0 and d_j^+ in the definition of completely regular code are equal: $\gamma_{j-1,1,j}, \gamma_{j,1,j}$ and $\gamma_{j+1,1,j}$ respectively.

2. Applying the Theorem 1 to completely regular code $\{x\}$, we get the desired property.

Note that these results hold up to the renaming of colors (the word "white" can be replaced by the word "black"). Let us now consider graph $J(n,w)$. In what follows V will denote the vertex set of a graph $J(n,w)$. Let $C = \Gamma_x \cap V$, where x is a vertex of E^n of weight i, $i \leq w$. In this case we will write $L_j(x)$ and $l_j(x)$ instead of $L_j(\Gamma_x \cap V)$ and $l_j(\Gamma_x \cap V)$ in through out of what follows.

Theorem 2.[10] *Let i be an integer such that $0 \leq i \leq w$, x be an arbitrary vector of E^n of weight i. Then $C = \Gamma_x \cap V$ is completely regular code in $J(n,w)$ with the numbers $d_j^+ = (i-j)(n-w-j)$, $d_j^0 = (i-j)j + (w-i+j)(n-w-j)$, $d_j^- = j(w-i+j)$, $L_j(x) = C_i^j C_{n-i}^{w-i+j}, 0 \leq j \leq i$ and $\bigcup_{0 \leq j \leq i} L_j(x)$, $L_0 = C$, is distance regular partition of $J(n,w)$.*

3 Some Constructions of Perfect Colorings of Johnson Graphs

Following constructions of perfect 2-coloring in Johnson graphs (for more of those see [10]) will be required to list all parameters of existing perfect colorings in graphs $J(6,3)$ and $J(7,3)$.

Example 1. Fix a coordinate $i \in \{1,\dots,n\}$. Color in white all vertices of $J(n,w)$ whose ith coordinate is 0, and color in black all vertices with this coordinate equal to 1. We get a perfect coloring with the matrix

$$\begin{pmatrix} w(n-w-1) & w \\ n-w & (w-1)(n-w) \end{pmatrix}.$$

Example 2. Consider an arbitrary $(s,n,w,w-1)$ block scheme in the Johnson graph $J(n,w)$. Color all vertices of the system in white and all the others in black. It is easily seen that the matrix of the obtained perfect coloring has the following form

$$\begin{pmatrix} w(s-1) & w(n-w) - w(s-1) \\ ws & w(n-w) - ws \end{pmatrix}.$$

Example 3. Let us consider a trivial 1-perfect code in $J(6,3)$ that consists of a pair of vertices that are at the Johnson distance 3 from each other. If we color code vertices in white and all others in black, we obtain a perfect coloring with the matrix

$$\begin{pmatrix} 0 & 9 \\ 1 & 8 \end{pmatrix}.$$

4 Eigenvalues of a Graph and Eigenvalues of a Perfect Coloring

To list all parameters of perfect colorings of $J(6,3)$ and $J(7,3)$ the notion of an eigenvalue of a graph and an eigenvalue of a perfect coloring, along with the notion of an antipodal graph and an antipodal perfect coloring are required. These notions with some auxiliary results are presented in the next two sections. The number θ is called an *eigenvalue of a graph* G, if θ is an eigenvalue of the adjacency matrix of this graph. The number θ is called an *eigenvalue of a perfect coloring* T *into two colors with the matrix* A, if θ is an eigenvalue of A. The following theorem demonstrates the connection between the introduced notions.

Theorem 3 [7]**.** *If* T *is a perfect coloring of a graph* G *in* m *colors, then any eigenvalue of* T *is an eigenvalue of* G.

Further we will use the eigenvalues of the Johnson graph (see, for example, [6]):

Theorem 4. *The eigenvalues of* $J(n,w)$ *are precisely the set of numbers:* $\theta_i = (n-w-i)(w-i)-i, 0 \leq i \leq w$.

Statement 2. *Let* T *be a perfect coloring into two colors with the matrix of parameters* $A = \{a_{ij}\}_{i,j=1,2}$ *of a regular graph* G *of valency* r. *Then the numbers* $a_{11} - a_{21}$, r *are eigenvalues of* T *and therefore are eigenvalues of* G .

Proof. The result is obtained by straightforward computation of eigenvalues of A and the application of Theorem 3.

5 Perfect Colorings of the Antipodal Graph into Two Colors

Graph G is called *antipodal*, if for any vertex x of graph G there is exactly one vertex y at the distance, which is equal to the diameter of G. A pair of such vertices is called antipodal. Obviously, the graphs $E^n, J(2w,w)$ are antipodal. Perfect coloring into two colors of a graph G is called *plus-antipodal* (*minus-antipodal*), if any two antipodal vertices are colored in one (two different) color (colors). We give some properties of such colorings:

Statement 3. *Any perfect coloring of the antipodal distance regular graph* G *into two colors is either plus-antipodal or minus-antipodal. The perfect colorings with the identical matrices of parameters are simultaneously plus-antipodal or minus-antipodal.*

Proof. Let d be the diameter of G, x be an arbitrary vertex of graph G. Taking into account that G is antipodal, $L_d(x)$ consists exactly of vertex y such that x and y are antipodal. Then applying Consequence 1 of the Theorem 1, we obtain that the color of vertex y is unambiguously defined by the color of vertex x. Because of arbitrary choice of vertices x, y, the result is proven.

Statement 4. *Let T be a minus-antipodal perfect coloring of a graph G into two colors, then the matrix $A = \{a_{ij}\}_{i,j=1,2}$ is symmetric.*

Proof. Since G is antipodal then its vertex set can be divided into pairs of antipodal vertices, with one of them being white and another one being black. So, the number of vertices of different colors is the same. Applying Statement 1 we obtain $a_{12} = a_{21}$.

6 Perfect Colorings of J(6,3) into Two Colors

From above we have that J(6,3) is antipodal distance regular graph. We will use this fact while proving the following theorem:

Theorem 5. *The only perfect colorings of J(6,3) into two colors are perfect colorings with matrices:*

$$\begin{pmatrix} 0 & 9 \\ 1 & 8 \end{pmatrix}; \begin{pmatrix} 1 & 8 \\ 2 & 7 \end{pmatrix}; \begin{pmatrix} 2 & 7 \\ 3 & 6 \end{pmatrix}; \begin{pmatrix} 3 & 6 \\ 4 & 5 \end{pmatrix}; \begin{pmatrix} 4 & 5 \\ 5 & 4 \end{pmatrix} \tag{6.1}$$

$$\begin{pmatrix} 3 & 6 \\ 6 & 3 \end{pmatrix} \text{ and } \begin{pmatrix} 6 & 3 \\ 3 & 6 \end{pmatrix}, \tag{6.2}$$

with any perfect coloring with the matrix from list (6.1) being plus-antipodal, and from the list (6.2) being minus-antipodal.

Proof. By Statement 3, an arbitrary perfect coloring into two colors of a graph $J(6,3)$ is either plus-anipodal, or minus-antipodal. Let us list all parameters of existing plus-antipodal colorings of $J(6,3)$ into two colors. Consider a perfect coloring from Example 3: two antipodal vertices of $J(6,3)$ form a trivial 1-perfect code in $J(6,3)$, and therefore induce perfect coloring. Due to its structure, this coloring is plus-antipodal. Since the set of vertices of antipodal graph parts on pairs of antipodal vertices, then the set of vertices of $J(6,3)$ parts into 10 perfect codes, each of them inducing plus-antipodal coloring. We can obtain a new coloring from this partition. We arbitrarily divide these 10 perfect codes into two groups and color the group of the smaller size with white color, and other with black. Then we obtain perfect coloring with the matrix

$$\begin{pmatrix} i-1 & 9-i+1 \\ i & 9-i \end{pmatrix},$$

where $i, 1 \leq i \leq 5$ is the number of perfect codes in the group of the smaller size. So we obtain five perfect colorings with parameters from the list (6.1). Note that any such perfect coloring is plus-antipodal due to its construction. It is obvious that this is exactly all plus-antipodal perfect colorings of $J(6,3)$ into two colors.

Now we list all parameters of minus-perfect colorings. By Theorem 4, the set of eigenvalues of $J(6,3)$ is {9,-3,3,-1}. This and Statements 2 and 4, imply that a matrix of arbitrary minus-antipodal perfect coloring of $J(6,3)$ is only one of the matrices from the following list: $\begin{pmatrix} 4 & 5 \\ 5 & 4 \end{pmatrix}$;$\begin{pmatrix} 3 & 6 \\ 6 & 3 \end{pmatrix}$;$\begin{pmatrix} 6 & 3 \\ 3 & 6 \end{pmatrix}$. We have shown the existence of plus-antipodal coloring with the matrix $\begin{pmatrix} 4 & 5 \\ 5 & 4 \end{pmatrix}$, so by Statement 3 there is no minus-antipodal perfect coloring of J(6,3) with this matrix. Because of existence of 2-fold Steiner systems in $J(6,3)$ and according to Examples 1 and 2 perfect colorings with parameters from (6.2) do exist.

7 Perfect Colorings of J(7,3) into Two Colors

As the graph $J(7,3)$ is not antipodal, the methods used in the previous section can not be applied here. The proof of the following theorem is based on the fact that the Johnson graph is distance regular and the application of Theorem 2.

Theorem 5. *The only perfect colorings of $J(7,3)$ into two colors are perfect colorings with matrices:*

$$\begin{pmatrix} 9 & 3 \\ 4 & 8 \end{pmatrix}; \tag{7.1}$$

$$\begin{pmatrix} 0 & 12 \\ 3 & 9 \end{pmatrix}; \begin{pmatrix} 3 & 9 \\ 6 & 6 \end{pmatrix}. \tag{7.2}$$

Proof. According to Example 1 there is the perfect coloring of J(7,3) with matrix (7.1). Also there is a 1-fold and 2-fold Steiner triple systems in $J(7,3)$, therefore, using Example 2 we obtain perfect colorings of $J(7,3)$ with the matrices from the list (7.2). We now show that there is no perfect colorings of J(7,3) with matrices different from listed above. We prove it by contradiction.

Let T be a perfect coloring with the matrix $A = \{a_{ij}\}_{i,j=1,2}$, which is different from (7.1),(7.2). By Theorem 4 the numbers $\theta_0 = 12, \theta_1 = 5, \theta_2 = 0, \theta_3 = -3$ are eigenvalues of $J(7,3)$. By Statement 2 the equality $a_{11} - a_{21} = \theta_k$ holds for some $k \geq 1$.

Let $k = 1$. In this case by Statement 2 we have $a_{21} = a_{11} - 5$. We now use the equations that arise from Theorem 2 while considering distance regular partition with respect to one vertex, say x, of $J(7,3)$. These are:

$$-5l_0 + l_1 = a_{11} - 5;$$

$$12l_0 + 4l_2 = 12(a_{11} - 5);$$

$$6l_1 + l_2 + 9l_3 = 18(a_{11} - 5);$$

$$2l_2 - 2l_3 = 4(a_{11} - 5).$$

Taking into account $L_0 = x$ and depending on the color of the vertex x, we have the following equalities:

$$l_0 = 0, l_1 = a_{11} - 5, l_2 = 3(a_{11} - 5), l_3 = a_{11} - 5$$

and

$$l_1 = 0, l_1 = a_{11}, l_2 = 3(a_{11} - 6), l_3 = a_{11} - 8.$$

Since the number of white colored vertices in any set is a nonnegative integer, we have $a_{11} \geq 8$. In the case $l_0 = 0$ the number of the white vertices on the third layer equals to $a_{11} - 5$, so the number of black vertices on the same layer equals $|L_3| - (a_{11} - 5) = 9 - a_{11}$, which is also nonnegative integer number. In the cases $a_{11} = 8$ and 9, we have, up to the renaming of colors, matrix A equal to (7.1).

Let $k = 2$. Then, using Statement 2, we get $a_{21} = a_{11}$. By Statement 1 the number of white vertices in $J(7,3)$ equals $(a_{11}|V(J(7,3))|)/12 = (a_{11}35)/12$. Integers 35 and 12 being coprime, so we obtain $a_{11} = 12$. Therefore a_{12} equals 0, and, taking into account that $a_{21} = 12$ is nonzero, we get the contradiction.

Let $k = 3$. Then, again using Statement 2 we obtain $a_{11} - a_{21} = -3$. If a_{11} is divisible by 3, then T is, up to the renaming of the colors, a perfect coloring with the one matrix from the list (7.2). If a_{11} is not divisible by 3, then, by Statement 1, the number of white vertices of the graph $J(7,3)$ equals $(a_{11} + 3)/15$ and we get a contradiction.

8 Conclusion

In general the problem of existence of all perfect colorings of Johnson graphs is far from being solved. Particulary, this problem includes the Delsarte conjecture about nonexistence of nontrivial perfect codes in Johnson graphs, along with the question of existence of Steiner systems which is still open. In this paper all parameters of existing perfect colorings in Johnson graphs $J(6,3)$, $J(7,3)$ (the graphs with the smallest parameters for which this problem was open) were listed, some approaches for solving this problem for Johnson graphs were given.

References

[1] Ahlswede, R., Aydinian, H.K., Khachatrian, L.H.: On perfect codes and related concepts. Designs, Codes and Cryptography 22, 221–237 (2001)

[2] Brouwer, A.E., Cohen, A.M., Neumaier, A.: Distance regular graphs. Springer, Berlin (1989)

[3] Delsarte, P.: An algebraic approach to the association schemes of coding theory. Philips Res. Rep. Suppl. 10, 1–97 (1973)

[4] Etzion, T., Schwarz, M.: Perfect constant-weight codes. IEEE Trans. Inform. Theory 50(9), 2156–2165 (2004)

[5] Fon-Der-Flaass, D.G.: Perfect colorings of a hypercube. In: 985th AMS Meeting, Indiana University Bloomington, pp. 31–32 (2003)

[6] Godsil, C.: Association schemes, combinatorics and optimization. University of Waterloo (2005)

[7] Godsil, C., Gordon, R.: Algebraic graph theory. Springer Science+Business Media, LLC (2004)

[8] Gordon, M.D.: Perfect single error-correcting codes in the Johnson scheme. IEEE Trans. Inform. Theory 52(10), 4670–4672 (2006)

[9] Martin, W.J.: Completely regular designs. J. Combin. Designs. 6(4), 261–273 (1998)

[10] Mogilnykh, I.Yu.: On the regularity of perfect 2-colorings of the Johnson graph. Probl. Inform. Transm. 43(4), 271–277 (2007)

[11] Zinoviev, V.A., Rifa, J.: On new completely regular q-ary codes. Probl. Inform. Trans. 43(2), 97–112 (2007)

A Syndrome Formulation of the Interpolation Step in the Guruswami-Sudan Algorithm

P. Beelen and T. Høholdt

DTU-Mathematics, Technical University of Denmark
Kgs. Lyngby, DK-2800, Denmark

1 Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and $C \subset \mathbb{F}_q^n$ a code of length n. If $c \in C$ and $h = (h_1 h_2 \cdots h_n)$ is a row of a parity check matrix of C, then it is clear that $h \cdot c = 0$. Such parity checks can therefore be used to test if a given word $w \in \mathbb{F}_q^n$ is an element of C, but it turns out that the expressions $h \cdot w$ (usually called syndromes of w) can be useful in decoding algorithms as well. The link between decoding and syndromes is an old one. Indeed the first known algorithm for the decoding of Reed-Solomon codes (Peterson's algorithm) uses syndromes. Now let $\mathcal{P} = \{x_1, \ldots, x_n\}$ be a subset of $\mathbb{F}_q$ consisting of n distinct elements. We can see an RS-code of dimension $k \leq n$ as the set of all n-tuples that arise by evaluating all polynomial $f(x)$ of degree less than or equal to $k-1$ in the points $x_1, \ldots, x_n$. The syndromes of a word w that are used in Peterson's decoding algorithm are the following:

$$s_\lambda(w) = \sum_{i=1}^{n} x_i^\lambda w_i.$$

After Sudan's algorithm for list decoding of RS-codes was discovered [13], again a reformulation in terms of certain generalized syndromes turned out to be useful [9]. These generalized syndromes can be seen as syndromes of words $w^e := (w_1^e, \ldots, w_n^e)$. Although the theoretically fastest, currently known decoding algorithms (see [1]) do not use syndromes, it turns out that for many practical parameters, the algorithm in [9] and variations of it is still the most desirable. Although generalized syndromes appear for the first time to describe list decoding algorithms, they can also be used to describe interesting decoding algorithms for RS-codes (see [2]).

All in all, it is clear that the usage of generalized syndromes is an ongoing and fruitful proces. The more general Guruswami-Sudan algorithm [6] for list decoding has not been reformulated in terms of syndromes in full generality, although there are interesting results in case of RS-codes (see [10]). The goal of this paper is to fill this gap in the literature and to clarify previous results. We will do this in complete generality for AG-codes generalizing previous results in [3]. The paper is organized as follows: in Section 2, we describe the Guruswami-Sudan algorithm, in Section 3 we develop the necessary tools and reformulate the Guruswami-Sudan algorithm in terms of syndromes, which is our main result, and in Section 4 we give an example.

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 20–32, 2008.

We will use the following list of notations:

$\mathbb{F}_q$	a finite field with q elements
χ	an algebraic curve defined over a finite field $\mathbb{F}_q$.
g	the genus of χ.
$\mathcal{F}$	the function field of the curve χ with constant field $\mathbb{F}_q$.
$P_1, \ldots, P_n$	rational points on χ.
D	the divisor $P_1 + \cdots + P_n$.
G and A	rational divisors with supports disjoint from $\operatorname{supp} D$.
$\mathrm{Ev}_D\,()$	evaluation map defined by $\mathrm{Ev}_D\,(f) = (f(P_1), \ldots, f(P_n))$.
$C_L(D, G)$	the evaluation code $\mathrm{Ev}_D\,(L(G))$.
$\mathrm{Res}_D()$	residue map defined by $\mathrm{Res}_D(\omega) = (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega))$.
$C_\Omega(D, G)$	the residue code $\mathrm{Res}_D(\Omega(-D + G))$.

As standard references for the theory of algebraic curves and algebraic function fields, we use [12,5]. The last reference is especially useful for checking facts on Hasse-derivatives, which we use in Section 3.

2 List-Decoding Using the Guruswami-Sudan Algorithm

In this section we will describe the Guruswami-Sudan list decoding algorithm for algebraic geometry codes. List decoding was introduced by P. Elias in 1957 [4] and in 1997 M. Sudan presented a list decoder for Reed-Solomon codes [13], which was extended to algebraic geometry codes by Shokrollahi and Wasserman in [11]. These algorithms only gave an improvement for small rates but in 1999 V. Guruswami and M. Sudan [6] generalized the algorithms to cover all rates.

Suppose that we are given a curve χ defined over a finite field $\mathbb{F}_q$ with function field $\mathcal{F}$. We wish to use the AG-code $C_L(D, G)$ and therefore assume that we have received the word $(r_1, \ldots, r_n)$ containing at most τ errors. The Guruswami-Sudan list decoding algorithm works with a divisor A with $\operatorname{supp} A \cap \operatorname{supp} D = \emptyset$ satisfying certain conditions that we describe below and a natural number s.

The idea of the algorithm is to find a nonzero polynomial $Q(y) \in \mathcal{F}[y]$ such that:

(i) $Q(y) = Q_0 + Q_1 y + \cdots + Q_\lambda y^\lambda$ where $Q_i \in L(A - iG), i = 0, \ldots, \lambda$
(ii) $Q(y)$ has a zero of multiplicity s in (P_j, r_j), $j = 1, \ldots, n$

The meaning of (ii) is the following: Let t be a local parameter at P_j then $Q(y) = \sum \mu_{a,b} t^a (y - r_j)^b$. That $Q(y)$ has a zero of multiplicity s in (P_j, r_j) then means that $\mu_{a,b} = 0$ for $a + b < s$.

The conditions on the divisor A are as follows.

(1) $\deg A < s(n-\tau)$
(2) $\deg A > \frac{ns(s+1)}{2(\lambda+1)} + \frac{\lambda \deg G}{2} + g - 1$

It can be seen that if $\tau < n - \frac{n(s+1)}{2(\lambda+1)} - \frac{\lambda \deg G}{2s} - \frac{g}{s}$ then such a divisor A exists.

Lemma 1. *Suppose the transmitted word is generated by $f \in L(G)$ and $Q(y)$ satisfies (i) and (ii) then $Q(f) = 0$.*

Proof. Since $f \in L(G)$ and $Q_i \in L(A - iG)$ we have $f^i Q_i \in L(A)$ and therefore $Q(f) \in L(A)$. We also have that $Q(f(P_j))$ has a zero of multiplicity s in P_j for at least $n - \tau$ j's $\in \{1, 2, \ldots, n\}$ so that $Q(f) \in L(A - sP_{i_1} - \cdots - sP_{i_r})$ with $r \geq n - \tau$. But $\deg(A - sP_{i_1} - \cdots - sP_{i_r}) < 0$ and therefore $Q(f) = 0$. This implies that if the divisor A satisfies condition (1) above then the function f that generated the sent codeword gives a factor $y - f$ in $Q(y)$.

Lemma 2. *If* $\deg A$ *satisfies (2) above then a nonzero $Q(y) \in \mathcal{F}[y]$ exists satisfying (i) and (ii).*

Proof. By selecting bases for the spaces $L(A - iG), i = 0, 1, \ldots, \lambda$ the condition (ii) translates into a system of homogeneous linear equations in $\sum_{i=0}^{\lambda} l(A - iG)$ unknowns. The number of equations is $\frac{n(s+1)s}{2}$ which by (2) is smaller than the number of unknowns, so there is a nonzero solution to the system.

This leads to the following algorithm:

```
Input: A received word $r = (r_1, r_2, \ldots, r_n)$.
    Find a polynomial $Q(y)$ satisfying $(i)$ and $(ii)$.
    Find factors of $Q(y)$ of the form $y - f$ with $f \in L(G)$.
    If no such factors exist Output: Failure.
    Else Output : $\mathrm{Ev}_D(f)$ for those $f$'s where $d(\mathrm{Ev}_D(f), r) \leq \tau$.
```

It can be seen that this list decoding algorithm only improves on $\frac{n - \deg G}{2}$ if $\lambda \geq s$ and

$$n\left(1 - \frac{s+1}{\lambda+1}\right) > \left(\frac{\lambda}{s} - 1\right) \deg G + \frac{2g}{s} + 1$$

and also that for fixed λ the optimal s is

$$\left\lfloor \left[\frac{2(\lambda+1)}{n}\left(\frac{\lambda}{2}\deg G + g\right)\right]^{\frac{1}{2}} \right\rfloor$$

Example 1. In this example, which is taken from [7], we consider the Hermitian curve over $\mathbb{F}_4$ defined by $x_2^2 + x_2 = x_1^3$. We write $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 = \alpha + 1$. Also we write $P_1 = (0,0)$, $P_2 = (0,1)$, $P_3 = (1, \alpha)$, $P_4 = (1, \alpha^2)$, $P_5 = (\alpha, \alpha)$, $P_6 = (\alpha, \alpha^2)$, $P_7 = (\alpha^2, \alpha)$, $P_8 = (\alpha^2, \alpha^2)$, and denote by T_∞ the unique pole of x_1. We now take $D = P_1 + \cdots + P_8$, $G = 4T_\infty$, and $A = 35T_\infty$. If we choose $s = 6$ and $\lambda = 8$, we can correct 2 errors using the list decoder. In order to describe the list-decoding procedure, we need to choose bases for the spaces $L(A - iG)$, whose dimension we denote by l_i. In this case we can for $0 \leq i \leq \lambda$ and $1 \leq j \leq l_i$ choose

$$g_{ij} = \begin{cases} 1 & \text{if } j = 1, \\ x_1 x_2^{(j-2)/3} & \text{if } j \equiv 2 \bmod 3, \\ x_2^{j/3} & \text{if } j \equiv 0 \bmod 3, \\ x_1^2 x_2^{(j-4)/3} & \text{if } j > 1 \text{ and } j \equiv 1 \bmod 3. \end{cases}$$

Suppose that we transmit the all zero word and receive.

$$(\alpha^2, 0, 0, \alpha^2, 0, 0, 0, 0).$$

We now use list decoding for $s = 6$ and $\lambda = 8$. To find an interpolation polynomial we could solve the linear system occurring in the proof of Lemma 2. This system has 168 equations and 171 variables. However, we will see in Section 3 that this approach is not optimal. In Section 4 we will use the results from Section 3 and get that an interpolation polynomial is given by:

$$\begin{aligned} Q(y) = {} & (1 + x_2 + \alpha x_2^2 + \alpha x_1^2 x_2 + \alpha^2 x_1 x_2^2 + \alpha x_2^3 + \alpha^2 x_1^2 x_2^2 + \alpha x_1 x_2^3 + x_2^4 + \\ & \alpha x_1^2 x_2^3 + \alpha^2 x_1 x_2^4 + x_1^2 x_2^4 + \alpha x_1 x_2^5 + \alpha^2 x_1^2 x_2^5 + \alpha x_1 x_2^6 + x_2^7 + \alpha x_1^2 x_2^6 + \\ & x_1 x_2^7 + x_2^8 + x_1^2 x_2^7 + \alpha x_1 x_2^8 + \alpha x_2^9 + \alpha^2 x_1^2 x_2^8 + x_1 x_2^9 + \alpha^2 x_2^{10} + x_1^2 x_2^9) y + \\ & (\alpha^2 + \alpha x_1 + \alpha x_1^2 + x_2^2 + \alpha^2 x_1^2 x_2 + \alpha^2 x_2^3 + x_1^2 x_2^2 + \alpha^2 x_1 x_2^3 + \alpha^2 x_2^5 + x_1^2 x_2^4 + \\ & x_1^2 x_2^4 + \alpha^2 x_2^6 + \alpha x_1^2 x_2^5 + \alpha x_2^7 + \alpha^2 x_1^2 x_2^6 + \alpha x_1 x_2^7 + x_2^8 + \alpha^2 x_1 x_2^8 + \alpha x_2^9) y^2 + \\ & (\alpha^2 + \alpha x_2 + x_1 x_2 + \alpha^2 x_1^2 x_2 + x_1 x_2^2 + \alpha x_2^3 + x_1^2 x_2^2 + \alpha^2 x_2^4 + \alpha^2 x_1^2 x_2^3 + \\ & \alpha x_2^5 + \alpha x_1^2 x_2^4 + \alpha^2 x_1 x_2^5 + \alpha x_2^6 + \alpha^2 x_1^2 x_2^5 + \alpha^2 x_1 x_2^6) y^3 + (\alpha + x_1 + \alpha^2 x_2 + \\ & x_1 x_2 + \alpha x_2^2 + \alpha^2 x_1^2 x_2 + \alpha x_1 x_2^2 + x_2^3 + \alpha x_1 x_2^3 + \alpha x_2^4 + x_1^2 x_2^3) y^4 + (\alpha + \\ & \alpha^2 x_2 + \alpha^2 x_1 x_2 + x_2^2 + x_1^2 x_2 + x_1 x_2^2 + \alpha^2 x_1^2 x_2^2 + \alpha x_1 x_2^3) y^5 + (1 + \alpha^2 x_1 + \\ & \alpha x_2 + \alpha^2 x_1^2 + \alpha^2 x_1 x_2 + x_2^2 + \alpha^2 x_1^2 x_2) y^6 + y^7 + (\alpha^2 + \alpha x_1) y^8. \end{aligned}$$

As we have seen, and we will discuss this further in the next section, the polynomial $Q(y)$ can be found by solving a system of homogenous linear equations.

3 Syndrome Formulation of List Decoding

In this section we will formulate the list decoding algorithm using syndromes. The advantage is that one can eliminate variables from the system of linear equations used to determine the interpolation polynomial. This approach is not new, especially not in case of Reed-Solomon codes, see e.g. [9,10], but we will state a more general result than is known until now, though for Hermitian codes there exists also some relevant literature (see e.g. [3,8]).

As discussed in the previous section, in order to list-decode we need a polynomial $Q(y) = \sum_{i=0}^{\lambda} Q_i y^i$ such that $Q_i \in L(A - iG)$ and such that (P_l, r_l) is a zero of $Q(y)$ of multiplicity s for all i between 1 and n. We denote by $g_{i1}, \ldots, g_{il_i}$ a basis of $L(A - iG)$ and write $Q_i = \sum_{j=1}^{l_i} q_{ij} g_{ij}$. The condition that (P_l, r_l) is a zero of $Q(y)$ of multiplicity s gives rise to $\binom{s+1}{2}$ linear equations in the coefficients q_{ij}. More explicitly, we can do the following: first for any $P_l \in \operatorname{supp} D$ we choose a function $t_l \in \mathcal{F}$ such that $v_{P_l}(t_l) = 1$. Given such a t_l, we can write a function

g that is regular at P_l as a power series in t_l, say $g = \alpha_0 + \alpha_1 t + \cdots + \alpha_a t^a + \cdots$. We have that $\alpha_0 = g(P_l)$. The α_a depend in general on P_l and the choice of $t_l \in \mathcal{F}$. Denoting by $D_{t_l}^{(a)}$ the a-th Hasse-derivative with respect to t_l, we then have that $D_{t_l}^{(a)}(g)(P) = \alpha_a$, so we can describe the power series purely in terms of Hasse-derivatives. We extend the Hasse-derivative to $\mathcal{F}[y]$ by first defining

$$D_y^{(b)} D_{t_l}^{(a)}(gy^j) := \binom{j}{b} D_{t_l}^{(a)}(g) y^{j-b}$$

and then by extending it linearly to $\mathcal{F}[y]$. This definition ensures that if we develop the polynomial $Q(y)$ in a power series in the variables t_l and $y - r_l$, then the coefficient of $t_l^a (y - r_l)^b$ is given exactly by $D_y^{(b)} D_{t_l}^{(a)}(Q(y))(P_l, r_l)$.

By the approximation theorem there exists $t \in \mathcal{F}$ such that $v_P(t) = 1$ for all $P \in \operatorname{supp} D$. We will therefore for convenience assume from now on that $t_l = t$ does not depend on l. The $\binom{s+1}{2}$ equations coming from the condition that (P_l, r_l) is a zero of $Q(y)$ of multiplicity s can now be described as follows:

$$D_y^{(b)} D_t^{(a)}(Q(y))(P_l, r_l) = 0, \text{ for all } a,\ b \text{ with } a + b < s,$$

or equivalently

$$\sum_{i=b}^{\lambda} \binom{i}{b} r_l^{i-b} \sum_{j=1}^{l_i} q_{ij} D_t^{(a)}(g_{ij})(P_l) = 0, \tag{1}$$

for all $\binom{s+1}{2}$ pairs of nonnegative integers (a, b) such that $a + b < s$.

We would like to write these equations in matrix form

$$\mathbf{M} \begin{pmatrix} \mathbf{q}_0 \\ \vdots \\ \mathbf{q}_\lambda \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{2}$$

For $0 \le b \le s-1$ and $b \le i \le \lambda$, we therefore introduce the following $(s-b)n \times l_i$ matrix:

$$\mathbf{M}_i^{(i-b)} := \begin{pmatrix} g_{i1}(P_1) & \ldots & g_{il_i}(P_1) \\ \vdots & & \vdots \\ D_t^{(s-1-b)}(g_{i1})(P_1) & \ldots & D_t^{(s-1-b)}(g_{il_i})(P_1) \\ & & \\ \vdots & & \vdots \\ & & \\ g_{i1}(P_n) & \ldots & g_{il_i}(P_n) \\ \vdots & & \vdots \\ D_t^{(s-1-b)}(g_{i1})(P_n) & \ldots & D_t^{(s-1-b)}(g_{il_i})(P_n) \end{pmatrix} \tag{3}$$

and the $(s-b)n \times (s-b)n$ matrix

$$\mathbf{D}_i^{(b)} := \binom{i+b}{b} \begin{pmatrix} r_1^i & & & & & & \\ & \ddots & & & & & \\ & & r_1^i & & & & \\ & & & \ddots & & & \\ & & & & r_n^i & & \\ & & & & & \ddots & \\ & & & & & & r_n^i \end{pmatrix}, \tag{4}$$

where every element r_l^i is repeated $s-b$ times on the diagonal. Using these definitions, we can then find the matrix $\mathbf{M}$ we are looking for. In other words, if we define $\mathbf{M}$ to be the matrix:

$$\left(\begin{array}{c|c|c|c|c|c} \mathbf{M}_0^{(0)} & \mathbf{D}_1^{(0)}\mathbf{M}_1^{(1)} & \dots & \mathbf{D}_{s-1}^{(0)}\mathbf{M}_{s-1}^{(s-1)} & \dots & \mathbf{D}_{\lambda}^{(0)}\mathbf{M}_{\lambda}^{(\lambda)} \\ \hline \mathbf{0} & \mathbf{M}_1^{(0)} & \dots & \mathbf{D}_{s-2}^{(1)}\mathbf{M}_{s-1}^{(s-2)} & \dots & \mathbf{D}_{\lambda-1}^{(1)}\mathbf{M}_{\lambda}^{(\lambda-1)} \\ \hline \vdots & \ddots & \ddots & \vdots & & \vdots \\ \hline \mathbf{0} & \dots & \mathbf{0} & \mathbf{M}_{s-1}^{(0)} & \dots & \mathbf{D}_{\lambda-s+1}^{(s-1)}\mathbf{M}_{\lambda}^{(\lambda-s+1)} \end{array}\right), \tag{5}$$

then we can reformulate equation (1) as matrix equation (2).

Example 2. In this example we show how to calculate the above equations in case of the Hermitian curve given by the equation $x_2^q + x_2 = x_1^{q+1}$ defined over $\mathbb{F}_{q^2}$. The function $t = x_1^{q^2} - x_1$ is a local parameter for all points on the curve different from T_∞. We will describe how to compute $D_t^{(a)}(f)$ for any function $f \in \mathcal{F}$. In the first place, Hasse derivatives satisfy the Leibniz rule:

$$D_t^{(a)}(fg) = \sum_{i=0}^{a} D_t^{(i)}(f) D_t^{(a-i)}(g)$$

and more general

$$D_t^{(a)}(f_1 \cdots f_m) = \sum_{i_1+\cdots+i_m=a} D_t^{(i_1)}(f_1) \cdots D_t^{(i_m)}(f_m).$$

Using this and the linearity of Hasse derivatives, we see that in order to describe them explicitly, it is enough to be able to calculate $D_t^{(a)}(x_1)$ and $D_t^{(a)}(x_2)$ for all natural numbers a.

We will now show how to calculate $D_t^{(a)}(x_1)$ recursively. We have that $D_t^{(0)}(x_1) = x_1$. Now suppose that $a > 0$ and that we know $D_t^{(\alpha)}(x_1)$ for all α between 0 and $a-1$. Using the equation $t = x_1^{q^2} + x_1$, we find that $D_t^{(a)}(x_1) = D_t^{(a)}(t) - D_t^{(a)}(x_1^{q^2})$. We have that $D_t^{(0)}(t) = t$, $D_t^{(1)}(t) = 1$ and $D_t^{(a)}(t) = 0$ if $a > 1$. Further using the general Leibniz rule, we find that $D_t^{(a)}(x_1^{q^2}) = \sum_{i_1+\cdots i_{q^2}=a} D_t^{i_1}(x_1) \cdots D_t^{(i_{q^2})}(x_1)$. If $i_j = a$ for some j, then remaining indices are zero implying that for this choice of indices we find the term $x_1^{a-1}D_t^{(a)}(x_1)$. By varying j between 1 and q^2, we see that there are exactly q^2 such terms. Thus these terms do not contribute to the sum. This means that $D_t^{(a)}(x_1) = D_t^{(a)}(t - x_1^{q^2})$ can be expressed as polynomial in $D_t^{(\alpha)}(x_1)$ for α varying between 0 and $a-1$.

It remains to show how to calculate $D_t^{(a)}(x_2)$ recursively. In the first place $D_t^{(0)}$ $(x_2) = x_2$ and since $x_2^q + x_2 = x_1^{q+1}$, we also have that $D_t^{(a)}(x_2) = D_t^{(a)}(x_1^{q+1}) - D_t^{(a)}(x_2^q)$. We already know how to calculate $D_t^{(a)}(x_1^{q+1})$ recursively and similarly as above we can express $D_t^{(a)}(x_2^q)$ as a polynomial in $D_t^{(\alpha)}(x_2)$ with α between 0 and $a-1$. For future use, we state some explicit results for $q = 2$:

a	0	1	2	3	4	5
$D_t^{(a)}(x_1)$	x_1	1	0	0	1	0
$D_t^{(a)}(x_2)$	x_2	x_1^2	$x_1 + x_1^4$	1	x_1^8	0

Before continuing our discussion of equation (1), we will establish some facts on the matrices $\mathbf{M}_i^{(0)}$. We will think about them as generator matrices of certain codes that we will define now.

Definition 1. *Let s be a natural number, $D = P_1 + \cdots + P_n$ as before and A be a divisor with support disjoint from* $\operatorname{supp} D$*, but of arbitrary degree. Further, let $t \in \mathcal{F}$ be a local parameter for all $P \in \operatorname{supp} D$ simultaneously. We define*

$$\mathrm{Ev}_P^{(s)} : L(A) \to \mathbb{F}^s$$

$$f \mapsto (f(P), D_t^{(1)}(f)(P), \ldots, D_t^{(s-1)}(f)(P))$$

$$\mathrm{Ev}_D^{(s)} : L(A) \to \mathbb{F}^{sn}$$

$$f \mapsto (\mathrm{Ev}_{P_1}^{(s)}(f), \ldots, \mathrm{Ev}_{P_n}^{(s)}(f))$$

and

$$C_L^{(s)}(D, A) := \mathrm{Ev}_D^{(s)}(L(A)).$$

Note that if $s > 1$, the map $\mathrm{Ev}_P^{(s)}$ depends on the choice of the local parameter t. The point of the above definition is that the columns occurring in the matrix $\mathbf{M}_i^{(0)}$ are codewords in the code $C_L^{(s-i)}(D, A - iG)$. Moreover, we have that

$$\operatorname{rank} \mathbf{M}_i^{(0)} = \dim C_L^{(s-i)}(A - iG). \tag{6}$$

In order to define the analogue of the code $C_\Omega(D, A)$, we consider a differential $\omega \in \Omega(-sD + A)$. Locally at a point $P \in \operatorname{supp} D$, one can then write $\omega = (\beta_s t^{-s} + \cdots + \beta_1 t^{-1} + \cdots)\, dt$. We can calculate β_i using residues, since $\beta_i = \mathrm{res}_P(t^{i-1}\omega)$. This motivates the following definition:

Definition 2. *Let s, D, A and t be as in Definition 1. We define*

$$\mathrm{Res}_P^{(s)} : \Omega(-sD+A) \to \mathbb{F}^s$$

$$\omega \mapsto (\mathrm{res}_P(\omega), \mathrm{res}_P(t\omega), \dots, \mathrm{res}_P(t^{s-1}\omega)),$$

$$\mathrm{Res}_D^{(s)} : \Omega(-sD+A) \to \mathbb{F}^{sn}$$

$$\omega \mapsto (\mathrm{Res}_{P_1}^{(s)}(\omega), \dots, \mathrm{Res}_{P_n}^{(s)}(\omega))$$

and

$$C_\Omega^{(s)}(D, A) := \mathrm{Res}_D^{(s)}(\Omega(-sD+A)).$$

If $s = 1$ it is well known that $C_L^{(s)}(D, A)$ and $C_\Omega^{(s)}(D, A)$ are dual to each other. We will now show that this also holds for arbitrary s. It is important that the choice of local parameter t is fixed when defining these codes.

Proposition 1. *We have that*

1. $\dim C_L^{(s)}(D, A) = l(A) - l(-sD + A)$,
2. $C_\Omega^{(s)}(D, A) = C_L^{(s)}(D, A)^\perp$.

Proof. Let $g \in L(A)$. We have that $\mathrm{Ev}_D^{(s)}(g) = (0, \dots, 0)$ if and only if g has a zero of order at least s in every $P \in \operatorname{supp} D$. This implies that the kernel of $\mathrm{Ev}_D^{(s)}$ is $L(-sD + A)$. This proves the first statement.

Now we prove the second statement. Let $\omega \in \Omega(-sD + A)$ and $g \in L(A)$. Locally at a $P \in \operatorname{supp} D$, we can write $\omega = (\beta_s t^{-s} + \cdots + \beta_1 t^{-1} + \cdots)\,dt$ and $g = \alpha_0 + \alpha_1 t + \cdots + \alpha_{s-1} t^{s-1} + \cdots$. Then $\mathrm{Res}_P^{(s)}(\omega) = (\beta_1, \dots, \beta_s)$ and $\mathrm{Ev}_P^{(s)}(g) = (\alpha_0, \dots, \alpha_{s-1})$. The inner product $\langle \mathrm{Res}_P^{(s)}(\omega), \mathrm{Ev}_P^{(s)}(g)\rangle$ is exactly the coefficient of t^{-1} in the product $g\omega$. Therefore we have that

$$\langle \mathrm{Res}_P^{(s)}(\omega), \mathrm{Ev}_P^{(s)}(g)\rangle = \mathrm{res}_P(g\omega).$$

Also note that $g\omega \in \Omega(-sD)$. All in all, we can deduce that

$$\langle \mathrm{Res}_D^{(s)}(\omega), \mathrm{Ev}_D^{(s)}(g)\rangle = \sum_{i=0}^{n} \mathrm{res}_{P_i}(g\omega) = 0.$$

In the last equality, we used the residue theorem. This implies that $C_\Omega^{(s)}(D, A) \subset C_L^{(s)}(D, A)^\perp$.

The proposition now follows once we prove that

$$\dim C_\Omega^{(s)}(D, A) + \dim C_L^{(s)}(D, A) = sn.$$

However, similarly to the first statement, one can prove that $\dim C_\Omega^{(s)}(D, A) = \dim \Omega(-sD + A) - \dim \Omega(A)$. Therefore we have that

$$\begin{aligned}\dim C_L^{(s)}(D, A) + \dim C_\Omega^{(s)}(D, A) &= l(A) - l(-sD + A) + \\ \dim \Omega(-sD + A) - \dim \Omega(A) &= \deg(A) - \deg(-sD + A) = sn.\end{aligned}$$

We used Riemann-Roch's theorem to obtain the second equality.

Recall that $l_i = l(A - iG)$. For convenience we also define

$$m_i := l(-(s-i)D + A - iG).$$

Combining the above proposition with equation (6), we find that

$$\operatorname{rank} \mathbf{M}_i^{(0)} = l_i - m_i. \tag{7}$$

Note that this implies that $\dim C_L^{(s)}(D, A) = l(A)$ if $\deg A < sn$. This is always the case in the setup of the list decoding algorithm.

Definition 3. *Let A and G be divisors as in the list decoding setup. Let b be an integer between 0 and $s-1$ and $\omega_1, \ldots, \omega_{(s-i)n}$ differential forms such that $\operatorname{Res}_D^{(s-b)}(\omega_i)$ for $1 \leq i \leq \dim C_\Omega^{(s-b)}(D, A-bG)$ is a basis of $C_\Omega^{(s-b)}(D, A-bG)$ and $\operatorname{Res}_D^{(s-b)}(\omega_1)$, $\ldots$, $\operatorname{Res}_D^{(s-b)}(\omega_{(s-b)n})$ is a basis of $\mathbb{F}^{(s-b)n}$. Then we define the $(s-b)n \times (s-b)n$ matrix.*

$$\mathbf{H}_b := \begin{pmatrix} \operatorname{Res}_D^{(s-b)}(\omega_1) \\ \vdots \\ \operatorname{Res}_D^{(s-b)}(\omega_{(s-b)n}) \end{pmatrix}$$

and for $0 \leq b \leq s-1$ and $b \leq i \leq \lambda$, the $(s-b)n \times l_i$ matrix

$$\mathbf{S}_i^{(i-b)} := \mathbf{H}_b \, \mathbf{D}_{i-b}^{(b)} \, \mathbf{M}_i^{(i-b)}.$$

Note that the matrices $\mathbf{H}_b$ are regular. We now obtain the following proposition.

Proposition 2. *The set of equations in (1) is row equivalent to the system*

$$\left(\begin{array}{c|c|c|c|c|c} \mathbf{S}_0^{(0)} & \mathbf{S}_1^{(1)} & \ldots & \mathbf{S}_{s-1}^{(s-1)} & \ldots & \mathbf{S}_\lambda^{(\lambda)} \\ \hline \mathbf{0} & \mathbf{S}_1^{(0)} & \ldots & \mathbf{S}_{s-1}^{(s-2)} & \ldots & \mathbf{S}_\lambda^{(\lambda-1)} \\ \hline \vdots & \ddots & \ddots & \vdots & & \vdots \\ \hline \mathbf{0} & \ldots & \mathbf{0} & \mathbf{S}_{s-1}^{(0)} & \ldots & \mathbf{S}_\lambda^{(\lambda-s+1)} \end{array}\right) \begin{pmatrix} \mathbf{q}_0 \\ \mathbf{q}_1 \\ \vdots \\ \mathbf{q}_\lambda \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{8}$$

Proof. The proposition follows after multiplying the b-th row of matrices in equation (5) with $\mathbf{H}_b$.

The matrices $\mathbf{S}_0^{(0)}$, $\ldots$, $\mathbf{S}_{s-1}^{(0)}$ are independent of the received word $\mathbf{r}$ and by equation (7) we have

$$\operatorname{rank} \mathbf{S}_i^{(0)} = l_i - m_i. \tag{9}$$

If $l_i < (s-i)n$, this reduces to $\operatorname{rank} \mathbf{S}_i^{(0)} = l_i$. Further, we have that if $l_i < (s-i)n$, then $\mathbf{S}_i^{(0)}$ can be written in the form

$$\mathbf{S}_i^{(0)} = \left(\begin{array}{c} \mathbf{0} \\ \hline \mathbf{B}_i^{(0)} \end{array}\right),$$

where $\mathbf{0}$ denotes the $(s-i)n - l_i \times l_i$ zero matrix. The $l_i \times l_i$ matrix $\mathbf{B}_i^{(0)}$ is regular, meaning that with Gaussian elimination, we can eliminate the variables $q_{i1}, \ldots, q_{il_i}$ in all rows different from those of $\mathbf{B}_i^{(0)}$. For $i = 0$ the situation is very simple, since the only rows in system (8) in which the variables $q_{01}, \ldots, q_{0l_0}$ occur, are the rows coming from $\mathbf{B}_0^{(0)}$. If $l_i \geq (s-i)n$, then we can eliminate $\operatorname{rank} \mathbf{S}_i^{(0)} = l_i - m_i$ variables among $q_{i1}, \ldots, q_{il_i}$.

All in all, we can simplify system (8) by eliminating $\sum_{i=0}^{s}(l_i - m_i)$ variables. This means that the remaining

$$\sum_{i=0}^{s} m_i + \sum_{i=s+1}^{\lambda} l_i$$

variables can be found by solving

$$\sum_{i=0}^{s} (\,(s-i)n - l_i + m_i\,)$$

linear equations. This gives an in general significant reduction of the size of the original system.

4 Example

In this section we give a continuation of Example 1. In the formulation from Section 2, we needed to solve a linear system of 168 equations 171 variables in order to find an interpolation polynomial $Q(y)$. We have just seen however that we can reduce the size of the system. First we calculate the rank of the matrices $\mathbf{S}_i^{(0)}$ and find:

i	0	1	2	3	4	5
rank $\mathbf{S}_i^{(0)}$	35	31	27	23	16	8

This means that we can eliminate 140 variables and equations thereby reducing the original system to a system of 28 equations in 31 variables. We can eliminate all 116 variables q_{ij} with $0 \leq i \leq 3$ and $1 \leq j \leq l_i$, since for $i \leq 3$ we have that $l_i < (s-i)n$. For $i = 4$ and $i = 5$, the situation is more complicated, but all we need to do is to compute the matrices $\mathbf{S}_4^{(0)}$ and $\mathbf{S}_5^{(0)}$ explicitly. In order to do this, we need to choose differentials as in Definition 3. Given a b between 0 and s, we can choose a basis for $\Omega(-(s-b)D + A - bG)$ with the desired properties as follows (recall $t = x_1 + x_1^4$):

$$\omega_i = \begin{cases} f_i \, dt/t^{s-b} & \text{if } 1 \leq i < (s-b)n, \\ f_{(s-b)n+1} \, dt/t^{s-b} & \text{if } i = (s-b)n. \end{cases}$$

Using this choice of differential, we can compute all matrices $\mathbf{S}_i^{(0)}$ explicitly. By our choice of bases, they have more structure than we indicated before. In the first place we find that $(\mathbf{B}_i^{(0)})_{pq} = 0$ if $p + q < l_i + 1$ and $(\mathbf{B}_i^{(0)})_{pq} = 1$

if $p+q=l_i+1$. This means that the Gaussian elimination steps needed to eliminate the q_{ij} (with $0 \le i \le 3$ and $1 \le j \le l_i$) are straightforward to do. We also find that the matrix $\mathbf{S}_4^{(0)}$ is equal to

$$\begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0
\end{pmatrix}.$$

Therefore we can eliminate the 16 variables q_{4j} with $1 \le j \le 15$ and $j=17$. We also find that

$$\mathbf{S}_5^{(0)} = \begin{pmatrix}
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&1&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&1\\
0&0&0&0&1&0&0&1&0&0&0&0&0&1&0\\
0&0&0&1&0&0&1&0&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&0&0&0&0&1&0&0&0\\
0&1&0&0&1&0&0&0&0&0&1&0&0&1&0\\
1&0&0&0&0&0&0&0&1&0&0&0&0&0&0
\end{pmatrix},$$

enabling us to eliminate the 8 variables q_{5j} with $1 \le j \le 7$ and $j=9$. What remains is to calculate the remaining 31 variables. Doing the elimination explicitly, we find that the vector consisting of these remaining 31 variables has to be in the kernel of the 28×31 matrix:

$$\left(\begin{array}{c|c} \mathbf{A}_1 & \mathbf{A}_2 \\ \hline \mathbf{A}_3 & \mathbf{A}_4 \end{array}\right),$$

with

$$\mathbf{A}_1 = \begin{pmatrix}
0&0&0&1&\alpha&\alpha&\alpha&0&0&\alpha^2&1&0&1&\alpha^2&1\\
0&0&\alpha^2&\alpha&1&\alpha^2&\alpha^2&0&\alpha&\alpha^2&0&\alpha^2&\alpha^2&0&\alpha\\
0&\alpha^2&0&\alpha^2&0&1&1&\alpha&1&\alpha&0&\alpha^2&0&1&\alpha^2\\
0&0&0&\alpha^2&\alpha&1&\alpha&1&1&\alpha^2&\alpha^2&0&\alpha^2&\alpha&\alpha\\
\alpha^2&0&\alpha^2&1&0&\alpha&\alpha&1&\alpha^2&\alpha&\alpha^2&1&\alpha^2&0&0\\
0&\alpha^2&\alpha&0&\alpha^2&0&\alpha^2&1&\alpha^2&1&0&0&0&1&\alpha^2\\
0&\alpha&0&\alpha&1&1&0&\alpha^2&\alpha&\alpha^2&0&0&0&\alpha^2&0\\
\alpha^2&0&0&1&0&\alpha^2&0&1&\alpha&0&1&0&\alpha&1&1\\
\alpha&0&0&\alpha&\alpha^2&\alpha^2&1&0&1&\alpha&0&0&0&0&0\\
0&\alpha&\alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha&\alpha&1&\alpha^2&0&\alpha&0&\alpha^2&0\\
0&\alpha^2&0&0&0&0&\alpha^2&\alpha^2&0&\alpha^2&\alpha&0&\alpha&1&1\\
0&0&\alpha&\alpha^2&1&\alpha^2&0&1&\alpha^2&0&0&\alpha&0&0&\alpha\\
\alpha^2&\alpha&0&0&\alpha^2&1&\alpha^2&1&\alpha&1&0&\alpha^2&0&\alpha&\alpha^2\\
0&0&0&0&0&0&0&\alpha^2&0&0&0&0&0&0&0
\end{pmatrix},$$

$$\mathbf{A}_2 = \begin{pmatrix}
0 & 1 & 0 & \alpha^2 & \alpha^2 & 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha & \alpha & 0 & 0 & 0 \\
1 & 0 & 0 & \alpha & \alpha^2 & 1 & \alpha^2 & \alpha^2 & 1 & \alpha & 1 & 1 & \alpha^2 & 0 & 0 & 0 \\
0 & 0 & \alpha & 0 & 1 & \alpha & \alpha & 0 & 1 & 1 & 0 & \alpha^2 & \alpha & 0 & 0 & 0 \\
0 & \alpha & 1 & \alpha^2 & \alpha & \alpha & \alpha^2 & 1 & \alpha & \alpha & 1 & 0 & 1 & 0 & 0 & 0 \\
\alpha & 0 & 1 & \alpha & 1 & 0 & 1 & \alpha & \alpha^2 & 0 & 0 & \alpha & \alpha^2 & 0 & 0 & 0 \\
\alpha & 0 & \alpha & 0 & \alpha & 0 & 1 & 0 & \alpha & 0 & 1 & 1 & 1 & 0 & 0 & \alpha \\
0 & 0 & 0 & 0 & \alpha & 0 & \alpha & 0 & \alpha & \alpha & \alpha & \alpha^2 & 0 & 0 & \alpha & 0 \\
\alpha & \alpha^2 & \alpha & \alpha & 0 & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha & 0 & 0 & \alpha \\
\alpha^2 & 0 & \alpha^2 & 0 & \alpha^2 & \alpha^2 & 0 & \alpha^2 & 1 & \alpha & \alpha^2 & \alpha & 1 & \alpha & \alpha & 0 \\
1 & 0 & \alpha^2 & 0 & 1 & 1 & 1 & \alpha & \alpha & \alpha & 1 & 1 & \alpha^2 & 0 & \alpha & \alpha^2 \\
0 & \alpha^2 & 0 & \alpha & \alpha & 1 & \alpha^2 & \alpha & 1 & \alpha^2 & 1 & \alpha^2 & 1 & \alpha & \alpha^2 & \alpha \\
0 & 0 & \alpha & 0 & 0 & 1 & \alpha & \alpha & \alpha^2 & \alpha & \alpha & \alpha & 0 & 0 & \alpha & \alpha \\
0 & 0 & \alpha & 0 & 0 & \alpha & 0 & \alpha^2 & \alpha^2 & 0 & \alpha^2 & \alpha & \alpha^2 & \alpha^2 & \alpha & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha & 0 & 0 & \alpha^2 & 1 & 0 & 0 & 0
\end{pmatrix},$$

$$\mathbf{A}_3 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & 0 & \alpha & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha & 0 & \alpha^2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \alpha^2 & 0 & 0 & \alpha & 0 & \alpha^2 & \alpha & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \alpha^2 & \alpha & 0 & \alpha^2 & \alpha & \alpha^2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \alpha & 0 & \alpha^2 & 0 & \alpha^2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \alpha^2 & 0 & \alpha^2 & \alpha & \alpha^2 & 0 & \alpha & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \alpha & 0 & \alpha & \alpha^2 & 0 & \alpha & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & 0 & 0 & \alpha^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & 0 & \alpha^2 & \alpha & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix},$$

and

$$\mathbf{A}_4 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \alpha & \alpha^2 & 0 & \alpha^2 & \alpha & \alpha & \alpha & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & 1 & 1 & \alpha & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & \alpha & \alpha^2 & 1 & \alpha^2 & 0 & \alpha^2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha & 0 & 1 & \alpha^2 & 1 & \alpha^2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \alpha & 0 & 0 & \alpha^2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \alpha & \alpha & 0 & \alpha^2 & \alpha & 1 & \alpha & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & \alpha^2 & 1 & \alpha^2 & \alpha & 0 & \alpha & 0 & 0 & 0 \\
0 & 0 & \alpha^2 & \alpha & 0 & 0 & \alpha & \alpha^2 & \alpha & \alpha^2 & 1 & 0 & \alpha^2 & 0 & 0 & 0 \\
\alpha^2 & \alpha & 0 & 0 & \alpha & \alpha^2 & \alpha^2 & \alpha^2 & \alpha & 1 & 1 & \alpha^2 & \alpha & 0 & 0 & 0 \\
\alpha & 0 & 0 & 0 & \alpha^2 & 0 & \alpha & \alpha & 1 & \alpha^2 & \alpha & \alpha^2 & \alpha & 0 & 0 & 0 \\
0 & \alpha^2 & \alpha & \alpha^2 & 0 & \alpha & \alpha^2 & \alpha^2 & \alpha & 1 & \alpha^2 & 1 & \alpha^2 & 0 & 0 & 0 \\
0 & \alpha & \alpha^2 & 0 & \alpha & 0 & \alpha & \alpha & 1 & \alpha^2 & \alpha & \alpha^2 & \alpha & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha^2 & \alpha^2 & \alpha & 0 & 0 & 0
\end{pmatrix}.$$

This matrix is much easier to handle than the original 168 × 171 matrix. Its kernel is 5-dimensional and one of the solutions is given by (only nonzero values are given, the rest of the 31 variables are zero):

q_{58}	q_{510}	q_{511}	q_{61}	q_{62}	q_{63}	q_{64}	q_{65}	q_{66}	q_{67}	q_{71}	q_{81}	q_{82}
1	α^2	α	1	α^2	α	α^2	α^2	1	α^2	1	α^2	α

Setting in these 31 values in system (8), we can then calculate the remaining 140 variables immediately and find the interpolation polynomial $Q(y)$ mentioned in Example 1.

References

1. Alekhnovich, M.: Linear diophantine equations over polyomials and soft decoding of Reed-Solomon codes. IEEE Trans. Inform. Theory 51, 2257–2265 (2005)
2. Schmidt, G., Sidorenko, V., Bossert, M.: Decoding Reed-Solomon codes beyond half the minimum distance using shift-register synthesis. In: ISIT 2006, Seattle, USA, July 9–14, pp. 459–463 (2006)
3. Beelen, P., Høholdt, T.: List decoding using syndromes, in Algebraic Geometry and its Applications. In: Chaumine, J., Hirschfeld, J., Rolland, R. (eds.) World Scientific Series on Number Theory and its Applications, vol. 5 (May 2008)
4. Elias, P.: List decoding for noisy channels. In: 1957-IRE WESCON Convention record (now IEEE), pt. 2, pp. 94–104 (1957)
5. Goldschmidt, D.M.: Algebraic functions and projective curves. Springer, Berlin (2003)
6. Guruswami, V., Sudan, M.: Improved decoding of Reed-Solomon and algebraic-geometric codes. IEEE Trans. Inform. Theory 45, 1757–1767 (1999)
7. Nielsen, R.R.: List decoding of linear block codes, Ph.D. thesis, Technical University of Denmark, Copenhagen (2001)
8. O'Sullivan, M.E.: Decoding of Hermitian codes: the key equation and efficient error evaluation. IEEE Trans. Inform. Theory 46, 512–523 (2000)
9. Roth, R.M., Ruckenstein, G.: Efficient decoding of Reed-Solomon codes beyond half the minimum distance. IEEE Trans. Inform. Theory 46, 246–257 (2000)
10. Ruckenstein, G.: Error decoding strategies for algebraic codes, Ph.D. thesis, Israel Institute of Technology, Haifa (2001)
11. Shokrollahi, M.A., Wasserman, H.: List decoding of algebraic-geometric codes. IEEE Trans. Inform. Theory 45, 432–437 (1999)
12. Stichtenoth, H.: Algebraic function fields and codes. Springer, Berlin (1993)
13. Sudan, M.: Decoding of Reed-Solomon codes beyond the error-correcting bound. J. Compl. 13, 180–193 (1997)

How to Know if a Linear Code Is a Group Code?*

José Joaquín Bernal, Ángel del Río, and Juan Jacobo Simón

Departamento de Matemáticas, Universidad de Murcia, España
josejoaquin.bernal@alu.um.es, adelrio@um.es, jsimon@um.es

Abstract. We present an intrinsecal characterization of when a linear code C is a (left) group code, i.e. the ambient space can be identified with a group algebra in which the standard basis is the group basis such that C is a (left) ideal in this group algebra. As application we obtain a class containing properly the class of metacyclic groups such that every group code is an abelian group code. We also use the characterization to describe all the possible group structures on some classes of generalized Reed-Solomon codes.

1 Introduction

In this note $\mathbb{F} = \mathbb{F}_q$ denotes the field with q elements. We consider $\mathbb{F}$ as the alphabet of linear codes and $\mathbb{F}^n$, the n-dimensional vector space, as the ambient space. The standard basis of $\mathbb{F}^n$ is denoted by $E = \{e_1, \dots, e_n\}$. For a group G, we denote by $\mathbb{F}G$ the group algebra over G with coefficients in $\mathbb{F}$.

Recall that a linear code $C \subseteq \mathbb{F}^n$ is said to be cyclic if and only if C is closed under cyclic permutations, that is, $(x_1, \dots, x_n) \in C$ implies $(x_2, \dots, x_n, x_1) \in C$. For $C_n = \langle g \rangle$, the cyclic group of order n, the bijection $\phi : E \to C_n$ given by $\phi(e_i) = g^{i-1}$ extends to an isomorphism of vector spaces $\phi : \mathbb{F}^n \to \mathbb{F}C_n$ and the cyclic codes in $\mathbb{F}^n$ are the subsets C of $\mathbb{F}^n$ such that $\phi(C)$ is an ideal of $\mathbb{F}C_n$.

More generally, if G is a group of order n and $C \subseteq \mathbb{F}^n$ is a linear code then we say that C is a *left G-code* (respectively, a *right G-code*; a *G-code*) if there is a bijection $\phi : E \to G$ such that the linear extension of ϕ to an isomorphism $\phi : \mathbb{F}^n \to \mathbb{F}G$ maps C to a left ideal (respectively, a right ideal; a two-sided ideal) of $\mathbb{F}G$. A *left group code* (respectively, *group code*) is a linear code which is a left G-code (respectively, a G-code) for some group G. A (left) cyclic group code (respectively, abelian group code, solvable group code, etc.) is a linear code which is (left) G-code for some cyclic group (respectively, abelian group, solvable group, etc.). In general, if $\mathcal{G}$ is a class of groups then we say that a linear code is a (left) $\mathcal{G}$ group code if and only if C is a (left) G-code for some G in $\mathcal{G}$.

Note that the cyclic codes of order n are cyclic group codes. However, not every cyclic group code is a cyclic code. For example, the linear code $\{(a, a, b, b) : a, b \in \mathbb{F}\}$ is not a cyclic code but it is a G-code via the map $\phi : \{e_1, \dots, e_4\} \to \langle g \rangle$, given by $\phi(e_1) = 1$, $\phi(e_2) = g^2$, $\phi(e_3) = g$ and $\phi(e_4) = g^3$, where $C_4 = \langle g \rangle$

[*] Research supported by D.G.I. of Spain and Fundación Séneca of Murcia.

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 33–36, 2008.

is a cyclic group of order 4. If one fixes a bijection $\phi : E \to G$ to induce an isomorphism $\phi : \mathbb{F}^n \to \mathbb{F}G$ then the left G-codes are precisely those codes of $\mathbb{F}^n$ which are permutation equivalent to codes of the form $\phi^{-1}(I)$ for I running on the left ideals of $\mathbb{F}G$. In particular, the cyclic group codes are the codes which are permutation equivalent to cyclic codes.

In this note we communicate a criterion to decide when a linear code is a group code in terms of its intrinsical properties in the ambient space, which does not assume an "a priori" group algebra structure on the ambient space. We also include some applications. An extended version of this note with proofs will be disposed soon [BRS].

2 Main Result

Let S_n denote the group of permutations on n symbols, that is the group of bijections of $\mathbb{N}_n = \{1, \dots, n\}$ onto itself. Recall that a subgroup G of S_n is *regular* if and only if it is transitive and has order n. We consider S_n acting by linear transformations on $\mathbb{F}^n$ via the following rule:

$$\sigma(e_i) = e_{\sigma(i)}, \quad (\sigma \in S_n, i \in \mathbb{N}_n).$$

The group of permutation automorphisms of a linear code C is

$$\mathrm{PAut}(C) = \{\sigma \in S_n : \sigma(C) = C\}.$$

For a subgroup H of a group G, let $\mathrm{Cen}_G(H)$ denote the centralizer of H in G.

The following theorem characterizes (left) group codes.

Theorem 1. *Let C be a linear code of length n over a field $\mathbb{F}$ and G a finite group of order n.*

1. *C is a left G-code if and only if G is isomorphic to a transitive subgroup of S_n contained in $\mathrm{PAut}(C)$.*
2. *C is a G-code if and only if G is isomorphic to a transitive subgroup H of S_n such that $H \cup \mathrm{Cen}_{S_n}(H) \subseteq \mathrm{PAut}(C)$.*

Corollary 2. *Let C be a linear code of length n over a field and let $\mathcal{G}$ be a class of groups.*

1. *C is a left $\mathcal{G}$ group code if and only if $\mathrm{PAut}(C)$ contains a regular subgroup of S_n in $\mathcal{G}$.*
2. *C is a $\mathcal{G}$ group code if and only if $\mathrm{PAut}(C)$ contains a regular subgroup H of S_n in $\mathcal{G}$ such that $\mathrm{Cen}_{S_n}(H) \subseteq \mathrm{PAut}(C)$.*

Remark 3. *Theorem 1 should be compare with Proposition III.1 in [PR] which states that a non-necessarily linear binary code C is propelinear if $\mathrm{Iso}(C)$, the group of affine bijections of the ambient space leaving C invariant, contains a regular subgroup acting transitively on C. A code C of length n is propelinear if for every $x \in C$ there is a permutation $\pi_x \in S_n$ such that the map $y \mapsto x + \pi_x(y)$ belongs to $\mathrm{Iso}(C)$ and $\pi_x \circ \pi_y = \pi_{x+\pi_x(y)}$ for every $x, y \in C$.*

3 Application I: Group Codes Versus Abelian Group Codes

Most of the studies on group codes in the literature consider either cyclic codes or abelian group codes. Recently some authors have payed attention to arbitrary group codes (see [KS] for a survey on group codes). Sabin and Lomonaco [EL] proved that if C is a G-code for a split metacyclic group G (i.e. G is a semidirect product of cyclic groups) then C is an abelian group code. As a first application of Theorem 1, we extend this result to a wider class of groups which includes all metacyclic groups. Recall that a group G is metacyclic if it has a normal cyclic subgroup A such that G/A is cyclic.

Theorem 4. *Let G be a group. Assume that G has two abelian subgroups A and B such that every element $g \in G$ can be written as $g = ab$, with $a \in A$ and $b \in B$. If C is a G-code then C is an abelian group code.*

Corollary 5. *If C is a metacyclic group code then C is an abelian group code.*

Theorem 4 provides a family of groups $\mathcal{G}$ such that every two-sided $\mathcal{G}$ code is also an abelian group code. We do not know any example of a group code which is not an abelian group code. For left group codes the situation is completely different. Using a counting argument one can prove that for every non-abelian group G and every prime p not dividing the order of G there is a left G-code over some field of characteristic p which is not an abelian group code. This proof is not constructive. Alternatively the following provides a concrete example.

Example 6. Let $\mathbb{F} = \mathbb{F}_{11}$ be the field with 11 elements. Every 2-dimensional cyclic group code of length 6 over $\mathbb{F}$ is permutation equivalent to one of the following codes:

$$\begin{aligned}
C_1 &= \{(\lambda, \mu, \mu - \lambda, -\lambda, -\mu, \lambda - \mu) \mid \lambda, \mu \in \mathbb{F}\}, \\
C_2 &= \{(\lambda, \mu, -\mu - \lambda, \lambda, \mu, -\mu - \lambda) \mid \lambda, \mu \in \mathbb{F}\}, \\
C_3 &= \{(\lambda, \mu, \lambda, \mu, \lambda, \mu) \mid \lambda, \mu \in \mathbb{F}\}.
\end{aligned}$$

Using this one can easily check that the subspace C of $\mathbb{F}^6$ generated by $u = (2, 5, -7, 2, -7, 5)$ and $v = (4, -3, -1, -4, 1, 3)$ is not an abelian group code. However C is a left S_3-code. Indeed, $A = (1, 2, 3)(4, 5, 6)$ and $B = (1, 4)(2, 6)(3, 5)$ belong to $\mathrm{PAut}(C)$, since $A(u) = 5u + 4v$, $B(u) = u$, $A(v) = 5(v - u)$ and $B(v) = -v$. Moreover $\langle A, B\rangle$ is a regular subgroup of S_6 isomorphic to S_3 and the claim follows from Theorem 1.

4 Application II: Cauchy Codes

Another applications of Theorem 1 involves the family of Cauchy codes (see [D] or [H] for details). Let $\overline{\mathbb{F}}$ denote the projective line over $\mathbb{F}$. We evaluate a homogenous polynomial $F \in \mathbb{F}[X, Y]$ on an element $z \in \overline{\mathbb{F}}$ by setting $F(z) = F(\varphi(z))$, where $\varphi(x) = (x, 1)$ if $x \in \mathbb{F}$ and $\varphi(x) = (1, 0)$ if $x = \infty$. Let $1 \leq k < n$,

$\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}^n$ with $\alpha_i \neq \alpha_j$ for $i \neq j$ and $v = (v_1, \ldots, v_n)$ with $0 \neq v_i \in \mathbb{F}$ for every i. Then the Cauchy codes of length n, dimension k, location vector α and scaling vector v is the following linear code:

$$\mathcal{C}_k(\alpha, v) = \{(v_1 P(\alpha_1), \ldots, v_n P(\alpha_n)) : P \in \mathbb{F}[X,Y]_{k-1}\},$$

where $\mathbb{F}[X,Y]_{k-1}$ denotes the set of polynomials in two variables which are homogeneous of degree $k-1$. Every Cauchy code is MDS and its dual is another Cauchy code. Examples of Cauchy codes are the generalized Reed-Solomon codes.

Using Theorem 1 we obtain criteria to decide when Cauchy codes of some lengths are left group codes. For example, it is well known that the extended Reed-Solomon codes are q-ary elementary abelian group codes (see e.g. [LM]). Next theorem shows that these are the only left group q-ary Cauchy codes of length q and this is also the only possible left group code structure on extended Reed-Solomon codes. (Note that the assumption $2 \leq k \leq q-2$ excludes one-dimensional codes and its dual codes. However this case can be easily treated separately using Theorem 1.)

Theorem 7. *Let C be a q-ary Cauchy code of length q and dimension $2 \leq k \leq q-2$ and let G be a group of order q. Then C is a left G-code if and only if it is permutation equivalent to the parity check extended Reed-Solomon code and G is p-elementary abelian.*

We also use Theorem 1 to give a complete description of the group code structure of all the q-ary Cauchy codes of length $q-1$ or $q-2$. In particular, we prove that if C is a q-ary Cauchy G-code of length $q-1$ then either G is cyclic or q is odd and G is a dihedral group and describe all the Cauchy codes of this type with all its possible group code structures.

References

[BRS] Bernal, J.J., del Río, Á., Simón, J.J.: An intrinsical description of group codes in preparation

[D] Dür, A.: The automorphism groups of Reed-Solomon codes. J. Combin. Theory Ser. A. 44, 69–82 (1987)

[EL] Evans Sabin, R., Lomonaco, S.J.: Metacyclic Error-Correcting Codes. AAECC 6, 191–210 (1995)

[H] Huffman, W.C.: Codes and groups. In: Pless, V.S., Huffman, W.C., Brualdi, R.A. (eds.) Handbook of coding theory, vol. II, pp. 1345–1440. North-Holland, Amsterdam (1998)

[LM] Landrock, P., Manz, O.: Classical codes as ideals in group algebras. Des. Codes Cryptogr. 2, 273–285 (1992)

[KS] Kelarev, A.V., Solé, P.: Error-correcting codes as ideals in group rings. Abelian groups, rings and modules (Perth, 2000), Contemp. Math. 273, 11–18 (2001)

[PR] Phelps, K.T., Rifà, J.: On binary 1-perfect additive codes: Some structural properties. IEEE Trans. Inform. Theory 48, 2587–2592 (2002)

Witness Sets

Gérard Cohen[1], Hugues Randriam[1], and Gilles Zémor[2]

[1] Ecole Nationale Supérieure des Télécommunications,
46 rue Barrault,
75 634 Paris 13, France
cohen@enst.fr, randriam@enst.fr
[2] Institut de Mathématiques de Bordeaux,
Université de Bordeaux, UMR 5251,
351 cours de la Libération,
33405 Talence, France
Gilles.Zemor@math.u-bordeaux1.fr

Abstract. Given a set C of binary n-tuples and $c \in C$, how many bits of c suffice to distinguish it from the other elements in C ? We shed new light on this old combinatorial problem and improve on previously known bounds.

1 Introduction

Let $C \subset \{0,1\}^n$ be a set of distinct binary vectors that we will call a code, and denote by $[n] = \{1, 2, ...n\}$ the set of coordinate positions. It is standard in coding theory to ask for codes (or sets) C such that every codeword $c \in C$ is as different as possible from all the other codewords. The most usual interpretation of this is that every codeword c has a large Hamming distance to all other codewords, and the associated combinatorial question is to determine the maximum size of a code that has a given minimal Hamming distance d. The point of view of the present paper is to consider that "a codeword c is as different as possible from all the other codewords" means that there exists a small subset $W \subset [n]$ of coordinates such that c differs from every other codeword in W. Put differently, it is possible to single out c from all the other codewords by focusing attention on a small subset of coordinates. More precisely, for $x \in \{0,1\}^n$, and $W \subset [n]$ let us define the projection π_W

$$\begin{aligned} \pi_W \ : \{0,1\}^{[n]} &\to \{0,1\}^W \\ x &\mapsto (x_i)_{i \in W} \end{aligned}$$

and let us say that W is a *witness set* (or a witness for short) for $c \in C$ if $\pi_W(c) \neq \pi_W(c')$ for every $c' \in C$, $c \neq c'$. Codes for which every codeword has a small witness set arise in a variety of contexts, in particular in machine learning theory [1,3,4] where a witness set is also called a specifying set or a discriminant: see [5, Ch. 12] for a short survey of known results and also [2] and references therein for a more recent discussion of this topic and some variations.

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 37–45, 2008.

Let us now say that a code has the w-witness property, or is a *w-witness code*, if every one of its codewords has a witness set of size w. Our concern is to study the maximum possible cardinality $f(n, w)$ of a w-witness code of length n. We shall give improved upper and lower bounds on $f(n, w)$ that almost meet.

The paper is organised as follows. Section 2 gives some easy facts for reference. Section 3 is devoted to upper bounds on $f(n, w)$ and introduces our main result, namely Theorem 2. Section 4 is devoted to constant weight w-witness codes, and we derive precise values of the cardinality of optimal codes. Section 5 studies mean values for the number of witness sets of a codeword and the number of codewords that have a given witness set. Section 6 is devoted to constructions of large w-witness codes, sometimes giving improved lower values of $f(n, w)$. Finally, Section 7 concludes with some open problems.

2 Easy and Known Facts

Let us start by mentioning two self-evident facts

- If C is a w-witness code, so is any translate $C + x$,
- $f(n, w)$ is an increasing function of n and w.

Continue with the following example. Let C be the set of all n vectors of length n and weight 1. Then every codeword of C has a witness of size 1, namely its support. Note the dramatic change for the slightly different code $C \cup \{\mathbf{0}\}$. Now the all-zero vector $\mathbf{0}$ has no witness set of size less than n. Bondy [3] shows however that if $|C| \leq n$, then C is a w-witness code with $w \leq |C| - 1$ and furthermore C is a *uniform* w-witness code, meaning that there exists a single subset of $[n]$ of size w that is a witness set for *all* codewords.

We clearly have the upper bound $|C| \leq 2^w$ for uniform w-witness codes. For ordinary w-witness codes however, the best known upper bound is, [5, Proposition 12.2],

$$f(n, w) \leq 2^w \binom{n}{w}. \tag{1}$$

The proof is simple and consists in applying the pigeon-hole principle. A subset of $[n]$ can be a witness set for at most 2^w codewords and there are at most $\binom{n}{w}$ witness sets.

We also have the following lower bound on $f(n, w)$, based on a trivial construction of a w-witness code.

Proposition 1. *We have:* $f(n, w) \geq \binom{n}{w}$.

Proof. Let $C = \binom{[n]}{w}$ be the set of all vectors of weight w. Notice that for all $c \in C$, $W(c) = \mathit{support}(c)$ is a witness set of c.

Note that the problem is essentially solved for $w \geq n/2$; since $f(n, w)$ is increasing with w, we then have:

$2^n \geq f(n, w) \geq f(n, n/2) \geq \binom{n}{n/2} \geq 2^n/(2n)^{1/2}$.

We shall therefore focus in the sequel on the case $w \leq n/2$.

In the next section we improve the upper bound (1) to a quantity that comes close to the lower bound of Proposition 1.

3 An Improved Upper Bound

The key result is the following.

Theorem 1. *Let $g(n,w) = f(n,w)/\binom{n}{w}$. Then, for fixed w, $g(n,w)$ is a decreasing function of n. That is:*

$$n \geq v \geq w \qquad \Rightarrow \qquad g(n,w) \leq g(v,w).$$

Proof. Let C be a binary code of length n having the w-witness property, with maximal cardinality $|C| = f(n,w)$. Fix a choice function $\phi : C \to \binom{[n]}{w}$ such that for any $c \in C$, $\phi(c)$ is a witness for c. For any $V \in \binom{[n]}{v}$, denote by C_V the subset of C formed by the c satisfying $\phi(c) \subset V$. Remark that the projection π_V is injective on C_V, since each element of C_V has a witness in V. Then $\pi_V(C_V)$ also has the w-witness property.

Remark now that if V is uniformly distributed in $\binom{[n]}{v}$ and W is uniformly distributed in $\binom{[n]}{w}$ and independent from V, then for any function $\psi : \binom{[n]}{w} \to \mathbb{R}$ one has

$$E_W(\psi(W)) = E_V(E_W(\psi(W) \,|\, W \subset V)), \tag{2}$$

where we denote by $E_W(\psi(W))$ the mean value (or expectation) of $\psi(W)$ as W varies in $\binom{[n]}{w}$, and so on.

We apply this with $\psi(W) = |\phi^{-1}(W)|$ to find

$$\begin{aligned} g(n,w) &= \binom{n}{w}^{-1} |C| = \binom{n}{w}^{-1} \sum\nolimits_{W \in \binom{[n]}{w}} |\phi^{-1}(W)| \\ &= E_W(\,|\phi^{-1}(W)|\,) \\ &= E_V(E_W(\,|\phi^{-1}(W)| \,|\, W \subset V)) \\ &= E_V\left(\binom{v}{w}^{-1} \sum\nolimits_{W \in \binom{V}{w}} |\phi^{-1}(W)|\right) \\ &= E_V\left(\binom{v}{w}^{-1} |C_V|\right) \\ &= E_V\left(\binom{v}{w}^{-1} |\pi_V(C_V)|\right) \\ &\leq g(v,w) \end{aligned}$$

the last inequality because $\pi_V(C_V)$ is a binary code of length v having the w-witness property.

Remark: It would be interesting to try to improve Theorem 1 using some unexploited aspects of the above proof, such as the fact that the choice function ϕ may be non-unique, or the fact that the last inequality not only holds in mean value, but for all V. For instance, suppose there is a codeword $c \in C$ (with C optimal as in the proof) that admits two distinct witnesses W and W', with $W \not\subset W'$. Let ϕ be a choice function with $\phi(c) = W$, and let ϕ' be the choice function that coincides everywhere with ϕ, except for $\phi'(c) = W'$. Let V contain W' but not W. If we denote by C'_V the subcode obtained as C_V but using ϕ' as choice function, then $C'_V = C_V \cup \{c\}$ (disjoint union), so $|\pi_V(C_V)| = |\pi_V(C'_V)| - 1 < f(v,w)$, and $g(n,w) < g(v,w)$.

Theorem 1 has a number of consequences: the following is straightforward.

Corollary 1. *For fixed w, the limit*

$$\lim_{n\to\infty} g(n,w) = \frac{f(n,w)}{\binom{n}{w}}$$

exists.

The following theorem gives an improved upper bound on $f(n,w)$.

Theorem 2. *For $w \le n/2$, we have the upper bound:*

$$f(n,w) \le 2w^{1/2}\binom{n}{w}.$$

Proof. Choose $v = 2w$ and use $f(v,w) \le 2^v$; then $f(n,w) \le \binom{n}{w} f(2w,w)/\binom{2w}{w}$ and the result follows by Stirling's approximation.

Set $w = \omega n$ and denote by $h(x)$ the binary entropy function

$$h(x) = -x\log_2 x - (1-x)\log_2(1-x).$$

Theorem 2 together with Proposition 1 yield:

Corollary 2. *We have*

$$\begin{aligned} \lim_{n\to\infty} \tfrac{1}{n}\log_2 f(n,\omega n) &= h(\omega) && \textit{for } 0 \le \omega \le 1/2 \\ &= 1 && \textit{for } 1/2 \le \omega \le 1. \end{aligned}$$

4 Constant-Weight Codes

Denote now by $f(n,w,k)$ the maximal size of a w-witness code with codewords of weight k. The following result is proved using a folklore method usually attributed to Bassalygo and Elias, valid when the required property is invariant under some group operation.

Proposition 2. *We have:*

$$\max_k f(n,w,k) \le f(n,w) \le \min_k \frac{f(n,w,k)2^n}{\binom{n}{k}}.$$

Proof. The lower bound is trivial.

For the upper bound, fix k, pick an optimal w-witness code C and consider its 2^n translates by all possible vectors. Every n-tuple, in particular those of weight k, occurs exactly $|C|$ times in the union of the translates; hence there exists a translate (also an optimal w-witness code of size $f(n,w)$ - see the remark at the beginning of Section 2) containing at least the average number $|C|\binom{n}{k}2^{-n}$ of vectors of weight k. Since k was arbitrary, the result follows.

We now deduce from the previous proposition the exact value of the function $f(n,w,k)$ in some cases.

Corollary 3. *For constant-weight codes we have:*

- *If $k \le w \le n/2$ then $f(n,w,k) = \binom{n}{k}$ and an optimal code is given by $S_k(\mathbf{0})$, the Hamming sphere of radius k centered on $\mathbf{0}$.*
- *If $n-k \le w \le n/2$, then $f(n,w,n-k) = \binom{n}{k}$ and an optimal code is given by the sphere $S_k(\mathbf{1})$.*

Proof. If $k \le w \le n/2$, we have the following series of inequalities:

$$\binom{n}{k} \le f(n,k,k) \le f(n,w,k) \le \binom{n}{k}.$$

If $n-k \le w \le n/2$, perform wordwise complementation.

5 Some Mean Values

Let C be a binary code of length n (not necessarily having the w-witness property). Let

$$\mathcal{W}_{C,w} : C \to 2^{\binom{[n]}{w}}, \quad \mathcal{W}_{C,w(}c) = \{W \in \binom{[n]}{w} \ : \ W \text{ is a witness for } c\},$$

and symmetrically,

$$\mathcal{C}_{C,w} : \binom{[n]}{w} \to 2^C, \quad \mathcal{C}_{C,w}(W) = \{c \in C \ : \ W \text{ is a witness for } c\}.$$

Remark that if $C' \subset C$ is a subcode, then $\mathcal{W}_{C',w}(c) \supset \mathcal{W}_{C,w}(c)$ for any $c \in C'$, while $\mathcal{C}_{C',w}(W) \supset (C' \cap \mathcal{C}_{C,w}(W))$ for any $W \in \binom{[n]}{w}$.

Lemma 1. *With these notations, the mean values of $|\mathcal{W}_{C,w}|$ and $|\mathcal{C}_{C,w}|$ are related by*

$$|C|E_c(|\mathcal{W}_{C,w}(c)|) = \binom{n}{w} E_W(|\mathcal{C}_{C,w}(W)|),$$

or equivalently

$$\frac{|C|}{\binom{n}{w}} = \frac{E_W(|\mathcal{C}_{C,w}(W)|)}{E_c(|\mathcal{W}_{C,w}(c)|)}.$$

Proof. Double count the set $\left\{(W,c) \in \binom{[n]}{w} \times C \ : \ W \text{ is a witness for } c\right\}$.

Now let $\gamma(C,w) = E_W(|\mathcal{C}_{C,w}(W)|)$ and let $\gamma^+(n,w)$ be the maximum possible value of $\gamma(C,w)$ for C a binary code of length n, and $\gamma^{++}(n,w)$ be the maximum possible value of $\gamma(C,w)$ for C a binary code of length n having the w-witness property.

Lemma 2. *With these notations, one has $\gamma^+(n,w) = \gamma^{++}(n,w)$.*

Proof. By construction $\gamma^+(n,w) \geq \gamma^{++}(n,w)$. On the other hand, let C be a binary code of length n with $\gamma(C,w) = \gamma^+(n,w)$, and let then C' be the subcode of C formed by the c having at least one witness of size w, *i.e.* $C' = \bigcup_{W\in\binom{[n]}{w}} \mathcal{C}_{C,w}(W)$. Then C' has the w-witness property, and

$$\gamma^{++}(n,w) \geq \gamma(C',w) \geq \gamma(C,w) = \gamma^+(n,w).$$

The technique of the proof of Proposition 1 immediately adapts to give:

Proposition 3. *With these notations, w being fixed, $\gamma^+(n,w)$ is a decreasing function of n. That is:*

$$n \geq v \geq w \qquad \Rightarrow \qquad \gamma^+(n,w) \leq \gamma^+(v,w).$$

Proof. Let C be a binary code of length n with $\gamma(C,w) = \gamma^+(n,w)$. For $V \in \binom{[n]}{v}$, denote by C_V the subset of C formed by the c having at least one witness of size w included in V, *i.e.* $C'_V = \bigcup_{W\in\binom{V}{w}} \mathcal{C}_{C,w}(W)$. Then C'_V has the w-witness property, $\mathcal{C}_{C,w}(W) \subset \mathcal{C}_{C'_V,w}(W)$ for any $W \subset V$, and π_V is injective on C'_V. Using this and (2), one gets:

$$\begin{aligned}
\gamma^+(n,w) &= E_W(|\mathcal{C}_{C,w}(W)|)\\
&= E_V(E_W(\,|\mathcal{C}_{C,w}(W)|\,|\,W\subset V))\\
&\leq E_V(E_W(\,|\mathcal{C}_{C'_V,w}(W)|\,|\,W\subset V))\\
&= E_V(E_W(\,|\mathcal{C}_{\pi_V(C'_V),w}(W)|\,|\,W\subset V))\\
&= E_V(\gamma(\pi_V(C'_V),w))\\
&\leq \gamma^+(v,w).
\end{aligned}$$

6 Constructions

6.1 A Generic Construction

Let $\mathcal{F} \subset \binom{[n]}{\leq w}$ be a set of subsets of $\{1,\ldots,n\}$ all having cardinality at most w.

Let $C_{\mathcal{F}} \subset \{0,1\}^n$ be the set of words having support included in one and only one $W \in \mathcal{F}$. Then:

Proposition 4. *With these notations, $C_{\mathcal{F}}$ has the w-witness property.*

Proof. For each $c \in C_{\mathcal{F}}$, let W_c be the unique $W \in \mathcal{F}$ containing the support of c. Then W_c is a witness for c.

Example 1. For $\mathcal{F} = \binom{[n]}{w}$ we find $C_{\mathcal{F}} = S_w(\mathbf{0})$, and

$$f(n,w) \geq |C_{\mathcal{F}}| = \binom{n}{w}.$$

Example 1'. Suppose $w \geq n/2$. Then for $\mathcal{F} = \binom{[n]}{n/2}$ we find $C_{\mathcal{F}} = S_{n/2}(\mathbf{0})$, and

$$f(n,w) \geq |C_{\mathcal{F}}| = \binom{n}{n/2}$$

(where for ease of notation we write $n/2$ instead of $\lfloor n/2 \rfloor$).

Example 2. For $\mathcal{F} = \{W\}$ with $|W| \leq w$ we find $C_{\mathcal{F}} = \{0,1\}^W$ (where we see $\{0,1\}^W$ as a subset of $\{0,1\}^n$ by extension by 0 on the other coordinates), and

$$f(n,w) \geq |C_{\mathcal{F}}| = 2^w.$$

Exemple 3. Let $\mathcal{F}$ be the set of (supports of) words of a code with constant weight w and minimal distance d (one can suppose d even). Then for all distinct $W, W' \in \mathcal{F}$ one has $|W \cap W'| \leq w - d/2$, so for all $W \in \mathcal{F}$, the code $C_{\mathcal{F}}$ contains all words of weight larger than $w - d/2$ supported in W. This implies:

Corollary 4. *For all d one has*

$$f(n,w) \geq A(n,d,w)B(w,d/2-1)$$

where:

- $A(n,d,w)$ *is the maximal cardinality of a code of length n with minimal distance at least d and constant weight w*
- $B(w,r) = \Sigma_{1 \leq i \leq r}\binom{w}{i}$ *is the cardinality of the ball of radius r in $\{0,1\}^w$.*

For $d = 2$, this construction gives the sphere again. For $d = 4$, this gives $f(n,w) \geq (1+w)A(n,d,w)$. We consider the following special values:

- $n = 4$, $d = 4$, $w = 2$: $A(4,4,2) = 2$
- $n = 8$, $d = 4$, $w = 4$: $A(8,4,4) = 14$
- $n = 12$, $d = 4$, $w = 6$: $A(12,4,6) = 132$

the last two being obtained with $\mathcal{F}$ the Steiner system $S(3,4,8)$ and $S(5,6,12)$ respectively.

The corresponding codes $C_{\mathcal{F}}$ have same cardinality as the sphere ($2 \times 3 = 6$, $14 \times 5 = 70$ and $132 \times 7 = 924$ respectively), but they are not translates of a sphere. Indeed, when C is a (translate of a) sphere with $w = n/2$, one has

$\mathcal{C}_{C,w}(W) = 2$ for any window $W \in \binom{[n]}{w}$. On the other hand, for $C = C_{\mathcal{F}}$ as above, one has by construction $\mathcal{C}_{C,w}(W) = w + 1$ for $W \in \mathcal{F}$.

6.2 Another Construction

Let $D \subset \{0,1\}^w$ be a binary (non-linear) code of length $w > n/2$ and minimal weight at least $2w - n$.

Let C_1 be the code of length n obtained by taking all words of length w that do not belong to D, and completing them with 0 on the last $n - w$ coordinates. Thus $|C_1| = 2^w - |D|$.

Let C_2 be the code of length n formed by the words c of weight exactly w, and such that the projection of c on the first w coordinates belongs to D. Thus if n_k is the number of codewords of weight k in D, one finds $|C_2| = \sum_k n_k \binom{n-w}{w-k}$.

Now let C be the (disjoint!) union of C_1 and C_2. Then C has the w-witness property. Indeed, let $c \in C$. Then if $c \in C_1$, c admits $[w]$ as witness, while if $c \in C_2$, c admits its support as witness.

As an illustration, let D be the sphere of radius $w - t$ in $\{0,1\}^w$, for $t \in \{1, \dots, \frac{n-w}{2}\}$. Then

$$f(n,w) \geq |C| = 2^w + \binom{w}{w-t}\left(\binom{n-w}{t} - 1\right).$$

If w satisfies $2^w > \binom{n}{n/2}$ but $w < n - 1$, this improves on examples 1, 1', and 2 of the last subsection, in that one finds then

$$f(n,w) \geq |C| > \max(\binom{n}{w}, \binom{n}{n/2}, 2^w).$$

On the other hand, remark that $C_1 \subset \{0,1\}^{[w]}$ and $C_2 \subset S_w(\mathbf{0})$, so that $|C| \leq 2^w + \binom{n}{w}$.

7 Conclusion and Open Problems

We have determined the asymptotic size of optimal w-witness codes. A few issues remain open in the non-asymptotic case, among which:

- When is the sphere $S_w(\mathbf{0})$ the/an optimal w-witness code? Do we have $f(n,w) = \binom{n}{w}$ for $w \leq n/2$? In particular do we have $f(2w,w) = \binom{2w}{w}$?
- For $w > n/2$, do we have $f(n,w) \leq \max(\binom{n}{n/2}, 2^w + \binom{n}{w})$?
- Denoting by $f(n,w,\geq d)$ the maximal size of a w-witness code with minimum distance d, can the asymptotics of Proposition 2 be improved to

$$\frac{1}{n}\log_2 f(n, \omega n, \geq \delta n) < h(\omega) \ ?$$

References

1. Anthony, M., Brightwell, G., Cohen, D., Shawe-Taylor, J.: On exact specification by examples. In: 5th Workshop on Computational learning theory, pp. 311–318 (1992)
2. Anthony, M., Hammer, P.: A Boolean Measure of Similarity. Discrete Applied Mathematics 154(16), 2242–2246 (2006)
3. Bondy, J.A.: Induced subsets. J. Combin. Theory (B) 12, 201–202 (1972)
4. Goldman, S.A., Kearns, M.J.: On the complexity of teaching. In: 4th Workshop on Computational learning theory, pp. 303–315 (1991)
5. Jukna, S.: Extremal Combinatorics Springer Texts in Theoretical Computer Science (2001)
6. Kushilevitz, E., Linial, N., Rabinovitch, Y., Saks, M.: Witness sets for families of binary vectors. J. Combin. Theory (A) 73, 376–380 (1996)

On Rank and Kernel of $\mathbb{Z}_4$-Linear Codes[⋆]

C. Fernández-Córdoba, J. Pujol, and M. Villanueva

Department of Information and Communications Engineering,
Universitat Autònoma de Barcelona,
08193-Bellaterra, Spain
{cristina.fernandez,jaume.pujol,merce.villanueva}@autonoma.edu

Abstract. A code $\mathcal{C}$ is a quaternary linear code if $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$. In this paper, the rank and dimension of the kernel for $\mathbb{Z}_4$-linear codes, which are the corresponding binary codes of quaternary linear codes, are studied. The possible values of these two parameters for $\mathbb{Z}_4$-linear codes, giving lower and upper bounds, are established. For each possible rank r between these bounds, the construction of a $\mathbb{Z}_4$-linear code with rank r is given. Equivalently, for each possible dimension of the kernel k, the construction of a $\mathbb{Z}_4$-linear code with dimension of the kernel k is given.

Keywords: Quaternary codes, $\mathbb{Z}_4$-linear codes, rank, kernel.

1 Introduction

Let $\mathbb{Z}_2$ and $\mathbb{Z}_4$ be the ring of integers modulo 2 and modulo 4, respectively. Let $\mathbb{Z}_2^n$ be the set of all binary vectors of length n and let $\mathbb{Z}_4^n$ be the set of all quaternary vectors of length n. Any non-empty subset C of $\mathbb{Z}_2^n$ is a binary code and a subgroup of $\mathbb{Z}_2^n$ is called a *binary linear code* or a $\mathbb{Z}_2$*-linear code*. Equivalently, any non-empty subset $\mathcal{C}$ of $\mathbb{Z}_4^n$ is a quaternary code and a subgroup of $\mathbb{Z}_4^n$ is called a *quaternary linear code*.

The Gray map: $\phi : \mathbb{Z}_4^n \longrightarrow \mathbb{Z}_2^{2n}$, is given by $\phi(v_1, \ldots, v_n) = (\varphi(v_1), \ldots, \varphi(v_n))$ where $\varphi(0) = (0, 0)$, $\varphi(1) = (0, 1)$, $\varphi(2) = (1, 1)$, $\varphi(3) = (1, 0)$. This Gray map is an isometry which transforms Lee distances defined in a quaternary code $\mathcal{C}$ over $\mathbb{Z}_4^n$ to Hamming distances defined in the corresponding binary code $C = \phi(\mathcal{C})$. Note that the length of the binary code C is $N = 2n$.

Let $\mathcal{C}$ be a quaternary linear code. Since $\mathcal{C}$ is a subgroup of $\mathbb{Z}_4^n$, it is isomorphic to an abelian structure $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, $\mathcal{C}$ is of type $2^\gamma 4^\delta$ as a group, it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords and the number of order two codewords in $\mathcal{C}$ is $2^{\gamma+\delta}$. Moreover, the binary image $C = \phi(\mathcal{C})$ of any quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ is called a $\mathbb{Z}_4$*-linear code* of length $N = 2n$ and type $2^\gamma 4^\delta$.

Two binary codes C_1 and C_2 of length n are said to be *isomorphic* if there exists a coordinate permutation π such that $C_2 = \{\pi(c) \mid c \in C_1\}$. They are said to be *equivalent* if there exists a vector $a \in \mathbb{Z}_2^n$ and a coordinate permutation π such that $C_2 = \{a + \pi(c) \mid c \in C_1\}$. Two quaternary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ both

[⋆] This work was supported in part by the Spanish MEC and the European FEDER under Grants MTM2006-03250 and TSI2006-14005-C02-01.

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 46–55, 2008.

of length n and type $2^\gamma 4^\delta$ are said to be *monomially equivalent*, if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. They are said to be *permutation equivalent* if they differ only by a permutation of coordinates (see [9]). Note that if two quaternary linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are monomially equivalent, then, after the Gray map, the corresponding $\mathbb{Z}_4$-linear codes $C_1 = \phi(\mathcal{C}_1)$ and $C_2 = \phi(\mathcal{C}_2)$ are isomorphic as binary codes.

Two structural properties of non-linear binary codes are the rank and dimension of the kernel. The *rank* of a binary code C, $rank(C)$, is simply the dimension of $\langle C\rangle$, which is the linear span of the codewords of C. The *kernel* of a binary code C, $K(C)$, is the set of vectors that leave C invariant under translation, i.e. $K(C) = \{x \in \mathbb{Z}_2^n \mid C + x = C\}$. If C contains the all-zero vector, then $K(C)$ is a binary linear subcode of C. In general, C can be written as the union of cosets of $K(C)$, and $K(C)$ is the largest such linear code for which this is true (see [1]). We will denote the dimension of the kernel of C by $ker(C)$.

The rank and dimension of the kernel have been studied for some families of $\mathbb{Z}_4$-linear codes (see [3], [4], [5], [10], [14]). These two parameters do not always give a full classification of $\mathbb{Z}_4$-linear codes, since two non-equivalent $\mathbb{Z}_4$-linear codes could have the same rank and dimension of the kernel. In spite of that, they can help in classification, since if two $\mathbb{Z}_4$-linear codes have different ranks or dimensions of the kernel, they are non-equivalent. Moreover, in this case the corresponding quaternary linear codes are not monomially equivalent, so these two parameters can also help to distinguish between quaternary linear codes that are not monomially equivalent.

The aim of this paper is the study of the rank and dimension of the kernel of $\mathbb{Z}_4$-linear codes. The paper is organized as follows. In Section 2, we recall some properties related to both quaternary linear and $\mathbb{Z}_4$-linear codes, including the linearity of $\mathbb{Z}_4$-linear codes. In Section 3, we determine all possible values of the rank for $\mathbb{Z}_4$-linear codes and we prove the existence of a $\mathbb{Z}_4$-linear code with rank r for all possible values of r. Equivalently, in Section 4, we establish all possible values of the dimension of the kernel for $\mathbb{Z}_4$-linear codes and we prove the existence of a $\mathbb{Z}_4$-linear code with dimension of the kernel k for all possible values of k. Finally, the conclusions are given in Section 5.

2 Preliminaries

Let $\mathcal{C}$ be a quaternary linear code. Although $\mathcal{C}$ is not a free module, every codeword is uniquely expressible in the form

$$\sum_{i=1}^{\gamma} \lambda_i u_i + \sum_{j=1}^{\delta} \mu_j v_j,$$

where $\lambda_i \in \mathbb{Z}_2$ for $1 \leq i \leq \gamma$, $\mu_j \in \mathbb{Z}_4$ for $1 \leq j \leq \delta$ and u_i, v_j are vectors in $\mathbb{Z}_4^n$ of order two and four, respectively. The vectors u_i, v_j give us a generator matrix $\mathcal{G}$ of size $(\gamma + \delta) \times n$ for the code $\mathcal{C}$. In [8], it was shown that any quaternary linear code of type $2^\gamma 4^\delta$ is permutation equivalent to a quaternary linear code with a canonical generator matrix of the form

$$\mathcal{G}_S = \begin{pmatrix} 2T & 2I_\gamma & \mathbf{0} \\ S & R & I_\delta \end{pmatrix}, \tag{1}$$

where R, T are matrices over $\mathbb{Z}_2$ of size $\delta \times \gamma$ and $\gamma \times (n-\gamma-\delta)$, respectively; and S is a matrix over $\mathbb{Z}_4$ of size $\delta \times (n-\gamma-\delta)$.

The concepts of duality for quaternary linear codes were also studied in [8], where the inner product for any two vectors $u, v \in \mathbb{Z}_4^n$ is defined as

$$u \cdot v = \sum_{i=1}^{n} u_i v_i \in \mathbb{Z}_4.$$

Then, the *dual code* of $\mathcal{C}$, denoted by $\mathcal{C}^\perp$, is defined in the standard way

$$\mathcal{C}^\perp = \{v \in \mathbb{Z}_4^n \mid u \cdot v = 0 \text{ for all } u \in \mathcal{C}\}.$$

The corresponding binary code $\phi(\mathcal{C}^\perp)$ is denoted by $C_\perp$ and called the $\mathbb{Z}_4$-*dual code* of C. Moreover, the additive dual code $\mathcal{C}^\perp$, which is also a quaternary linear code, is of type $2^\gamma 4^{n-\gamma-\delta}$.

The following two lemmas were proved for quaternary vectors and quaternary linear codes, respectively, in [8]. Let $u * v$ denote the component-wise product, for any $u, v \in \mathbb{Z}_4^n$.

Lemma 1 ([8] or [16]). *For all $u, v \in \mathbb{Z}_4^n$, we have*

$$\phi(u+v) = \phi(u) + \phi(v) + \phi(2u * v).$$

Note that if u or v are vectors in $\mathbb{Z}_4^n$ of order two, then $\phi(u+v) = \phi(u) + \phi(v)$.

Lemma 2 ([8] or [16]). *Let $\mathcal{C}$ be a quaternary linear code. The $\mathbb{Z}_4$-linear code $C = \phi(\mathcal{C})$ is a binary linear code if and only if $2u * v \in \mathcal{C}$, for all $u, v \in \mathcal{C}$.*

Note that if $\mathcal{G}$ is a generator matrix of a quaternary linear code $\mathcal{C}$ and $\{u_i\}_{i=1}^{\gamma}$ and $\{v_j\}_{j=0}^{\delta}$ are the row vectors of order two and four in $\mathcal{G}$, respectively, then the $\mathbb{Z}_4$-linear code $C = \phi(\mathcal{C})$ is a binary linear code if and only if $2v_j * v_k \in \mathcal{C}$, for all j, k satisfying $1 \leq j < k \leq \delta$, since the component-wise product is bilinear.

3 Rank of $\mathbb{Z}_4$-Linear Codes

Let $\mathcal{C}$ be a quaternary linear code of length n and type $2^\gamma 4^\delta$ and let $C = \phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code of length $N = 2n$. In this section, we will study the rank of these $\mathbb{Z}_4$-linear codes C. We will show that there exists a $\mathbb{Z}_4$-linear code C with $r = rank(C)$ for any possible value of r.

Lemma 3. *Let $\mathcal{C}$ be a quaternary linear code of type $2^\gamma 4^\delta$ and let $C = \phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code. Let $\mathcal{G}$ be a generator matrix of $\mathcal{C}$ and let $\{u_i\}_{i=1}^{\gamma}$ be the rows of order two and $\{v_j\}_{j=0}^{\delta}$ the rows of order four in $\mathcal{G}$. Then, $\langle C \rangle$ is generated by $\{\phi(u_i)\}_{i=1}^{\gamma}$, $\{\phi(v_j), \phi(2v_j)\}_{j=1}^{\delta}$ and $\{\phi(2v_j * v_k)\}_{1 \leq j < k \leq \delta}$.*

Proof. If $x \in \mathcal{C}$, then x can be expressed as $x = v_{j_1} + \cdots + v_{j_m} + w$, where $\{j_1, \ldots, j_m\} \subseteq \{1, \ldots, \delta\}$ and w is a codeword of order two. By Lemma 1, $\phi(x) = \phi(v_{j_1} + \cdots + v_{j_m}) + \phi(w)$, where $\phi(w)$ is a linear combination of $\{\phi(u_i)\}_{i=1}^{\gamma}$ and $\{\phi(2v_j)\}_{j=1}^{\delta}$, and $\phi(v_{j_1} + \cdots + v_{j_m}) = \phi(v_{j_1}) + \cdots + \phi(v_{j_m}) + \sum_{1 \le k < l \le m} \phi(2v_{j_k} * v_{j_l})$. Therefore, $\phi(x)$ is generated by $\{\phi(u_i)\}_{i=1}^{\gamma}, \{\phi(v_j), \phi(2v_j)\}_{j=1}^{\delta}$ and $\{\phi(2v_j * v_k)\}_{1 \le j < k \le \delta}$. □

Proposition 1. *Let $\mathcal{C}$ be a quaternary linear code of length n and type $2^\gamma 4^\delta$ and let $C = \phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code of length $N = 2n$. Then,*

$$rank(C) \in \{\gamma + 2\delta, \ldots, \min(n + \delta,\ \gamma + 2\delta + \binom{\delta}{2})\}.$$

Let $\mathcal{C}$ be a quaternary linear code of length n and type $2^\gamma 4^\delta$ and let $C = \phi(\mathcal{C})$ with $rank(C) = \gamma + 2\delta + \bar{r}$, where $\bar{r} \in \{0, \ldots, \min(n - \gamma - \delta, \binom{\delta}{2})\}$. Let $\mathcal{G}$ be a generator matrix of $\mathcal{C}$ and let $\{u_i\}_{i=1}^{\gamma}$ be the rows of order two and $\{v_j\}_{j=0}^{\delta}$ the rows of order four in $\mathcal{G}$. By the proof of Proposition 1, the quaternary linear code $\mathcal{S}_{\mathcal{C}}$ generated by $\{u_i\}_{i=1}^{\gamma}$, $\{v_j\}_{j=1}^{\delta}$ and $\{2v_j * v_k\}_{1 \le j < k \le \delta}$ is of type $2^{\gamma + \bar{r}} 4^\delta$ and it is easy to check that $\phi(\mathcal{S}_{\mathcal{C}}) = \langle C \rangle$, by Lemma 3. Therefore, the code $\langle C \rangle$ is both binary linear and $\mathbb{Z}_4$-linear.

For the parameters n, γ, δ given by some families of $\mathbb{Z}_4$-linear codes such as, for example, extended 1-perfect $\mathbb{Z}_4$-linear codes (see [5], [13] or Example 1), the upper bound above is tight. We also know $\mathbb{Z}_4$-linear codes such that the rank is in between these two bounds such as, for example, the Hadamard $\mathbb{Z}_4$-linear codes (see [14] or Example 1).

Example 1. *For any integer $t \ge 3$ and each $\delta \in \{1, \ldots, \lfloor (t+1)/2 \rfloor\}$ there exists a unique (up to isomorphism) extended 1-perfect $\mathbb{Z}_4$-linear code C of length $n = 2^t$, such that the $\mathbb{Z}_4$-dual code of C has $\gamma = t + 1 - 2\delta$ (see [10]). The Hadamard $\mathbb{Z}_4$-linear codes H are the $\mathbb{Z}_4$-dual of the extended 1-perfect $\mathbb{Z}_4$-linear codes.*

The rank of the Hadamard $\mathbb{Z}_4$-linear codes was computed in [14] and the rank of the extended 1-perfect $\mathbb{Z}_4$-linear codes in [5] and [10]. Specifically,

$$rank(H) = \begin{cases} \gamma + 2\delta + \binom{\delta-1}{2} & \text{if } \delta \ge 3 \\ \gamma + 2\delta & \text{if } \delta = 1, 2 \end{cases}$$

and $rank(C) = \bar{\gamma} + 2\bar{\delta} + \delta = n + \bar{\delta}$ (except when $t = 4$ and $\delta = 1$), where $\bar{\gamma} = \gamma$ and $\bar{\delta} = n - \gamma - \delta$. Note that the rank of the extended 1-perfect $\mathbb{Z}_4$-linear codes satisfies the upper bound.

The next point to be solved is how to construct $\mathbb{Z}_4$-linear codes with any rank in the range of possibilities given by Proposition 1.

Lemma 4. *There exists a quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ if and only if*

$$\gamma, \delta \ge 0,\ \ n > 0,\ \ \delta + \gamma \le n. \qquad (2)$$

Proof. Straightforward from matrix (1). □

Theorem 1. *Let n, γ, δ be integer numbers satisfying (2). Then, there exists a $\mathbb{Z}_4$-linear code C of length $N = 2n$ and type $2^\gamma 4^\delta$ with $rank(C) = r$ for any*

$$r \in \{\gamma + 2\delta, \dots, \min(n + \delta,\ \gamma + 2\delta + \binom{\delta}{2})\}.$$

Proof. Let $\mathcal{C}$ be a quaternary linear code of length n and type $2^\gamma 4^\delta$ with generator matrix

$$\mathcal{G} = \begin{pmatrix} 2T & 2I_\gamma & \mathbf{0} \\ S_r & \mathbf{0} & I_\delta \end{pmatrix},$$

where S_r is a matrix over $\mathbb{Z}_4$ of size $\delta \times (n - \gamma - \delta)$, and let $C = \phi(\mathcal{C})$ be its corresponding $\mathbb{Z}_4$-linear code. Let $\{u_i\}_{i=1}^{\gamma}$ and $\{v_j\}_{j=0}^{\delta}$ be the row vectors of order two and four in $\mathcal{G}$, respectively.

By Proposition 1, $rank(C) = r = \gamma + 2\delta + \bar{r}$, where $\bar{r} \in \{0, \dots, \min(n - \gamma - \delta, \binom{\delta}{2})\}$. In the generator matrix $\mathcal{G}$, the Gray map image of the γ row vectors $\{u_i\}_{i=1}^{\gamma}$ and the 2δ row vectors $\{v_j\}_{j=1}^{\delta}$, $\{2v_j\}_{j=1}^{\delta}$ are independent binary vectors over $\mathbb{Z}_2$. For each $\bar{r} \in \{0, \dots, \min(n - \gamma - \delta, \binom{\delta}{2})\}$, we will define S_r in an appropriate way such that $rank(C) = r = \gamma + 2\delta + \bar{r}$.

Let e_k, $1 \le k \le \delta$, denote the column vector of length δ, with a one in the kth coordinate and zeroes elsewhere. For each $\bar{r} \in \{0, \dots, \min(n - \gamma - \delta, \binom{\delta}{2})\}$, we can construct S_r as a quaternary matrix where in $\bar{r}$ columns there are $\bar{r}$ different column vectors $e_k + e_l$ of length δ, $1 \le k < l \le \delta$, and in the remaining columns there is the all-zero column vector. For each one of the $\bar{r}$ column vectors the rank increases by 1. In fact, if the column vector $e_k + e_l$ is included in S_r, then the quaternary vector $2v_k * v_l$ has only a two in the same coordinate where the column vector $e_k + e_l$ is and $\phi(2v_k * v_l)$ is independent to the vectors $\{\phi(u_i)\}_{i=1}^{\gamma}$,$\{\phi(v_j)\}_{j=1}^{\delta}$, $\{\phi(2v_j)\}_{j=1}^{\delta}$ and $\{\phi(2v_s * v_t)\}$, $\{s, t\} \ne \{k, l\}$. Since the maximum number of columns of S_r is $n - \gamma - \delta$ and the maximum number of different such columns is $\binom{\delta}{2}$, the result follows. □

Let S_r be a matrix over $\mathbb{Z}_4$ of size $\delta \times (n - \gamma - \delta)$ where in $\bar{r} = r - (\gamma + 2\delta)$ columns there are $\bar{r}$ different column vectors $e_k + e_l$ of length δ, $1 \le k < l \le \delta$, and in the remaining columns there are the all-zero column vector. Note that by the proof of Theorem 1, any quaternary linear code $\mathcal{C}$ of length n and type $2^\gamma 4^\delta$ with generator matrix

$$\mathcal{G} = \begin{pmatrix} 2T & 2I_\gamma & \mathbf{0} \\ S_r & \mathbf{0} & I_\delta \end{pmatrix},$$

where T any matrix over $\mathbb{Z}_2$ of size $\gamma \times (n - \gamma - \delta)$, has $rank(\phi(\mathcal{C})) = r = \gamma + 2\delta + \bar{r}$.

Example 2. *By Proposition 1, we know that the possible ranks for $\mathbb{Z}_4$-linear codes, C, of length 18 and type $2^2 4^5$ are $rank(C) = r \in \{12, 13, 14, 15\}$. For each possible r, we can construct a $\mathbb{Z}_4$-linear code C with $rank(C) = r$, taking the following generator matrix of $\mathcal{C} = \phi^{-1}(C)$:*

$$\mathcal{G}_S = \begin{pmatrix} 2T & 2 & \mathbf{0} \\ S_r & \mathbf{0} & I_5 \end{pmatrix},$$

where $S_{12} = (\mathbf{0})$ and S_{13}, S_{14}, and S_{15} are constructed as follows:

$$S_{13} = \begin{pmatrix} 1&0&0 \\ 1&0&0 \\ 0&0&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}, \quad S_{14} = \begin{pmatrix} 1&0&0 \\ 1&1&0 \\ 0&1&0 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}, \quad S_{15} = \begin{pmatrix} 1&0&1 \\ 1&1&0 \\ 0&1&1 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}.$$

4 Kernel Dimension of $\mathbb{Z}_4$-Linear Codes

In this section, we will study the dimension of the kernel of $\mathbb{Z}_4$-linear codes $C = \phi(\mathcal{C})$. We will also show that there exists a $\mathbb{Z}_4$-linear code C with $k = ker(C)$ for any possible value of k.

Lemma 5. *Let $\mathcal{C}$ be a quaternary linear code and let $C = \phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code. Then,*

$$K(C) = \{\phi(u) \mid u \in \mathcal{C} \text{ and } 2u * v \in \mathcal{C}, \forall v \in \mathcal{C}\}.$$

Proof. By Lemma 2, $\phi(u) + \phi(v) \in C$ if and only if $2u * v \in \mathcal{C}$ for all $u, v \in \mathcal{C}$. Thus, the result follows. □

Note that if $\mathcal{G}$ is a generator matrix of a quaternary linear code $\mathcal{C}$ and $C = \phi(\mathcal{C})$, $\phi(u) \in K(C)$ if and only if $u \in \mathcal{C}$ and $2u * v \in \mathcal{C}$ for all $v \in \mathcal{G}$. Moreover, all codewords of order two in $\mathcal{C}$ belong to $K(C)$.

Lemma 6. *Let $\mathcal{C}$ be a quaternary linear code and let $C = \phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code. Given $x, y \in \mathcal{C}$, $\phi(x) + \phi(y) \in K(C)$ if and only if $\phi(x + y) \in K(C)$.*

Proof. By Lemma 1, $\phi(x + y + 2x * y) = \phi(x) + \phi(y)$. Now, by Lemma 5, $\phi(x + y + 2x * y) \in K(C)$ if and only if for all $v \in \mathcal{C}$, $2(x + y + 2x * y) * v = 2(x + y) * v \in \mathcal{C}$; that is, if and only if $\phi(x + y) \in K(C)$. □

Lemma 7. *Let $\mathcal{C}$ be a quaternary linear code of type $2^\gamma 4^\delta$ and let $C = \phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code. Then, $ker(C) \in \{\gamma + \delta, \gamma + \delta + 1, \ldots, \gamma + 2\delta - 2, \gamma + 2\delta\}$.*

Proof. The upper bound $\gamma + 2\delta$ comes from the linear case. The lower bound $\gamma + \delta$ is straightforward, since there are $2^{\gamma+\delta}$ codewords of order two in $\mathcal{C}$ and, by Lemma 5, the binary images by ϕ of all these codewords are in $K(C)$. Also note that if the $\mathbb{Z}_4$-linear code C is not linear, then the dimension of the kernel is equal to or less than $\gamma + 2\delta - 2$ (see [12]). Therefore, $ker(C) \in \{\gamma + \delta, \ldots, \gamma + 2\delta - 2, \gamma + 2\delta\}$. □

Given an integer $m > 0$, a set of vectors $\{v_1, v_2, \ldots, v_m\}$ in $\mathbb{Z}_4^n$ and a subset $I = \{i_1, \ldots, i_l\} \subseteq \{1, \ldots, m\}$, we denote by v_I the vector $v_{i_1} + \cdots + v_{i_l}$. If $I = \emptyset$, then $v_I = \mathbf{0}$.

Proposition 2. *Let $\mathcal{C}$ be a quaternary linear code of type $2^\gamma 4^\delta$, with generator matrix $\mathcal{G}$, and let $C = \phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code with $ker(C) = \gamma + 2\delta - \bar{k}$, where $\bar{k} \in \{2, \ldots, \delta\}$. Then, there exist a set $\{v_1, v_2, \ldots, v_{\bar{k}}\}$ of row vectors of order four in $\mathcal{G}$, such that*

$$C = \bigcup_{I \subseteq \{1,\ldots,\bar{k}\}} (K(C) + \phi(v_I))$$

It is important to note that if C is a $\mathbb{Z}_4$-linear code, then $K(C)$ is a $\mathbb{Z}_4$-linear subcode of C, by Lemma 6. The *kernel* of a quaternary linear code $\mathcal{C}$ of type $2^\gamma 4^\delta$, denoted by $\mathcal{K}(\mathcal{C})$, can be defined as $\mathcal{K}(\mathcal{C}) = \phi^{-1}(K(C))$, where $C = \phi(\mathcal{C})$ is the corresponding $\mathbb{Z}_4$-linear code. By Lemma 5, $\mathcal{K}(\mathcal{C}) = \{u \in \mathcal{C} \mid 2u * v \in \mathcal{C}, \forall v \in \mathcal{C}\}$ and it is easy to see that $\mathcal{K}(\mathcal{C})$ is a quaternary linear subcode of $\mathcal{C}$ of type $2^{\gamma+\bar{k}} 4^{\delta-\bar{k}}$. Moreover, by Proposition 2, given a quaternary linear code $\mathcal{C}$ with generator matrix $\mathcal{G}$, there exist a set $\{v_1, v_2, \ldots, v_{\bar{k}}\}$ of row vectors of order four in $\mathcal{G}$, such that

$$\mathcal{C} = \bigcup_{I \subseteq \{1,\ldots,\bar{k}\}} (\mathcal{K}(\mathcal{C}) + v_I).$$

Proposition 3. *Let $\mathcal{C}$ be a quaternary linear code of length n and type $2^\gamma 4^\delta$ and let $C = \phi(\mathcal{C})$ be the corresponding $\mathbb{Z}_4$-linear code of length $N = 2n$. Let $s = n - \gamma - \delta$. Then,*

$$\begin{cases} \text{if } s = 0, & ker(C) = \gamma + 2\delta, \\ \text{if } s = 1, & ker(C) \in \{\gamma + 2(\delta - \lceil \frac{\delta-1}{2} \rceil), \ldots, \gamma + 2(\delta - 1), \gamma + 2\delta\}, \\ \text{if } s \geq 2, & ker(C) \in \{\gamma + \delta, \gamma + \delta + 1, \ldots, \gamma + 2\delta - 2, \gamma + 2\delta\}. \end{cases}$$

Example 3. *Continuing with Example 1, the dimension of the kernel for a Hadamard $\mathbb{Z}_4$-linear code H was computed in [14] and [10] and the dimension of the kernel for an extended 1-perfect $\mathbb{Z}_4$-linear code C in [5]. Specifically,*

$$ker(H) = \begin{cases} \gamma + \delta + 1 & \text{if } \delta \geq 3 \\ \gamma + 2\delta & \text{if } \delta = 1, 2 \end{cases}$$

and

$$ker(C) = \begin{cases} \bar{\gamma} + \bar{\delta} + 1 & \text{if } \delta \geq 3 \\ \bar{\gamma} + \bar{\delta} + 2 & \text{if } \delta = 2 \\ \bar{\gamma} + \bar{\delta} + t & \text{if } \delta = 1. \end{cases}$$

As in Section 3 for the rank, the next point to be solved here is how to construct $\mathbb{Z}_4$-linear codes with any dimension of the kernel in the range of possibilities given by Proposition 3.

Theorem 2. *Let n, γ, δ be integer numbers satisfying (2). Then, there exists a $\mathbb{Z}_4$-linear code C of length $N = 2n$ and type $2^\gamma 4^\delta$ with $ker(C) = k$ for any*

$$k \in \begin{cases} \{\gamma+\delta, \ldots, \gamma+2\delta-2, \gamma+2\delta\} & \textit{if } s \geq 2 \\ \{\gamma+2(\delta-\lceil\frac{\delta-1}{2}\rceil), \ldots, \gamma+2(\delta-1), \gamma+2\delta\} & \textit{if } s = 1 \\ \{\gamma+2\delta\} & \textit{if } s = 0, \end{cases}$$

where $s = n - \gamma - \delta$.

Proof. Let $\mathcal{C}$ be a quaternary linear code of type $2^\gamma 4^\delta$ with generator matrix

$$\mathcal{G} = \begin{pmatrix} \mathbf{0} & 2I_\gamma & \mathbf{0} \\ S_k & \mathbf{0} & I_\delta \end{pmatrix},$$

where S_k is a matrix over $\mathbb{Z}_4$ of size $\delta \times s$, and let $C = \phi(\mathcal{C})$ be its corresponding $\mathbb{Z}_4$-linear code. Taking S_k as the all-zero matrix over $\mathbb{Z}_4$, the code C is a binary linear code, so $ker(C) = k = \gamma + 2\delta$.

When $s = 1$, for each $\bar{k} \in \{2, 4, \ldots, 2\lceil\frac{\delta-1}{2}\rceil\}$ and $k = \gamma + 2\delta - \bar{k}$, we can construct a matrix S_k over $\mathbb{Z}_4$ of size $\delta \times 1$ with an even number of ones, $\bar{k}$, and zeroes elsewhere. In this case, $ker(C) = k = \gamma + 2\delta - \bar{k}$, by the proof of Proposition 3.

Finally, when $s \geq 2$, for each $\bar{k} \in \{2, 3, \ldots, \delta\}$ and $k = \gamma + 2\delta - \bar{k}$, we can construct a matrix S_k over $\mathbb{Z}_4$ of size $\delta \times s$, such that only in the last $\delta - \bar{k}$ row vectors all components are zero and, moreover, in the first $\bar{k}$ coordinates of each column vector there are an even number of ones and zeros elsewhere. In this case, it is easy to prove that $ker(C) = k = \gamma + 2\delta - \bar{k}$. □

Example 4. *By Proposition 3, we know that the possible dimensions of the kernel for $\mathbb{Z}_4$-linear codes, C, of length 18 and type $2^2 4^5$ are $ker(C) = k \in \{12, 10, 9, 8, 7\}$. For each possible k, we can construct a $\mathbb{Z}_4$-linear code C with $ker(C) = k$, taking the following generator matrix of $\mathcal{C} = \phi^{-1}(C)$:*

$$\mathcal{G}_S = \begin{pmatrix} \mathbf{0} & 2 & \mathbf{0} \\ S_k & \mathbf{0} & I_5 \end{pmatrix},$$

where $S_{12} = (\mathbf{0})$ and S_{10}, S_9, S_8 and S_7 are constructed as follows:

$$S_{10} = \begin{pmatrix} 1\,0\,0 \\ 1\,0\,0 \\ 0\,0\,0 \\ 0\,0\,0 \\ 0\,0\,0 \end{pmatrix}, S_9 = \begin{pmatrix} 1\,0\,0 \\ 1\,1\,0 \\ 0\,1\,0 \\ 0\,0\,0 \\ 0\,0\,0 \end{pmatrix}, S_8 = \begin{pmatrix} 1\,0\,0 \\ 1\,1\,0 \\ 1\,1\,0 \\ 1\,0\,0 \\ 0\,0\,0 \end{pmatrix}, S_7 = \begin{pmatrix} 1\,0\,0 \\ 1\,1\,0 \\ 1\,1\,0 \\ 1\,1\,0 \\ 0\,1\,0 \end{pmatrix}.$$

5 Conclusion

In this paper we studied two structural properties of $\mathbb{Z}_4$-linear codes, the rank and dimension of the kernel. Using combinatorial enumeration techniques, we established lower and upper bounds for the possible values of these parameters. We also gave the construction of a $\mathbb{Z}_4$-linear code with rank r (resp. kernel dimension k) for each feasible value r (resp. k).

The rank, kernel and dimension of the kernel are defined for binary codes and they are specially useful for binary non-linear codes. We showed that for binary codes which are $\mathbb{Z}_4$-linear codes, we can also define the kernel using the corresponding quaternary linear codes, which are subgroups of $\mathbb{Z}_4^n$. In this case, in order to compute the kernel $K(C)$ of a $\mathbb{Z}_4$-linear code C is much easier if we consider the corresponding quaternary linear code $\mathcal{C} = \phi^{-1}(C)$ and we compute $\mathcal{K}(\mathcal{C}) = \phi^{-1}(K(C))$ using a generator matrix of $\mathcal{C}$. Moreover, we also proved that if C is a $\mathbb{Z}_4$-linear code, then $K(C)$ and $\langle C \rangle$ are also $\mathbb{Z}_4$-linear codes. Finally, since $K(C) \subseteq C \subseteq \langle C \rangle$ and C can be written as the union of cosets of $K(C)$, we also have that, equivalently, $\mathcal{K}(\mathcal{C}) \subseteq \mathcal{C} \subseteq \mathcal{S}_{\mathcal{C}}$, where $\mathcal{S}_{\mathcal{C}} = \phi^{-1}(\langle C \rangle)$, and $\mathcal{C}$ can be written as cosets of $\mathcal{K}(\mathcal{C})$.

As a future research in this issue, it would be interesting to establish the bounds of the rank, once the dimension of the kernel is fixed, and give the construction of a $\mathbb{Z}_4$-linear code with rank r and kernel dimension k for each possible pair (r, k).

According to the definition given by Delsarte in 1973 (see [7]), additive codes are subgroups of the underlying abelian group in a translation association scheme. In the special case of a binary Hamming scheme, that is, when the underlying abelian group is of order 2^n, the only structures for the abelian group are those of the form $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, with $\alpha + 2\beta = n$. Therefore, the subgroups $\mathcal{C}$ of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are the only additive codes in a binary Hamming scheme. This kind of codes have been studied in [2], [6], [13], [15]. Hence, as a future research it would also be interesting to generalize these results to the $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, that is, subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$.

References

1. Bauer, H., Ganter, B., Hergert, F.: Algebraic techniques for nonlinear codes. Combinatorica 3, 21–33 (1983)
2. Borges, J., Rifà, J.: A characterization of 1-perfect additive codes. IEEE Trans. Inform. Theory 45(5), 1688–1697 (1999)
3. Borges, J., Fernández, C., Phelps, K.T.: Quaternary Reed-Muller codes. IEEE Trans. Inform. Theory 51(7), 2686–2691 (2005)
4. Borges, J., Phelps, K.T., Rifà, J., Zinoviev, V.A.: On $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like codes. IEEE Trans. Inform. Theory 49(11), 2834–2843 (2003)
5. Borges, J., Phelps, K.T., Rifà, J.: The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear and additive non-$\mathbb{Z}_4$-linear codes. IEEE Trans. Inform. Theory 49(8), 2028–2034 (2003)
6. Borges, J., Fernández, C., Pujol, J., Rifà, J., Villanueva, M.: $\mathbb{Z}_4$-linear codes: generator matrices and duality. IEEE Trans. on Inform. Theory (submitted, 2007) arXiv:0710.1149
7. Delsarte, P.: An algebraic approach to the association schemes of coding theory. Philips Res. Rep. Suppl. 10 (1973)
8. Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals and related codes. IEEE Trans. Inform. Theory 40, 301–319 (1994)

9. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
10. Krotov, D.S.: $\mathbb{Z}_4$-linear Hadamard and extended perfect codes. In: International Workshop on Coding and Cryptography, Paris, France, January 8-12, 2001, pp. 329–334 (2001)
11. MacWillams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes. North-Holland, Amsterdam (1977)
12. Phelps, K.T., LeVan, M.: Kernels of nonlinear Hamming codes. Designs, Codes and Cryptography 6(3), 247–257 (1995)
13. Phelps, K.T., Rifà, J.: On binary 1-perfect additive codes: some structural properties. IEEE Trans. Inform. Theory 48(9), 2587–2592 (2002)
14. Phelps, K.T., Rifà, J., Villanueva, M.: On the additive $\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear Hadamard codes. Rank and Kernel. IEEE Trans. Inform. Theory 52(1), 316–319 (2005)
15. Pujol, J., Rifà, J.: Translation invariant propelinear codes. IEEE Trans. Inform. Theory 43, 590–598 (1997)
16. Wan, Z.-X.: Quaternary Codes. World Scientific, Singapore (1997)

Classic and Quantum Error Correcting Codes

S. González[1], C. Martínez[1], and A.P. Nicolás[2]

[1] Universidad de Oviedo, Spain
c.martinez@uniovi.es
[2] Universidad de Cantabria, Spain

Abstract. Algebraic methods play an important role in coding theory. For instance, there are many connections between codes and groups. In this paper we will present two results that show different applications of algebraic methods in coding theory. One of them refers to the classical context and another one to the quantum error correcting theory. These results can be found in [5] and [13] respectively, where proofs and more details can be found.

1 Some Constructions of Linearly Optimal Group Codes

Algebraic structures, not necessarily associative or commutative, have been used in the construction of codes. For instance in [6] and [7] different classes of recursive MDS codes based on properties of quasigroups are given.

In [8] authors study codes constructed from left ideals of a loop ring $A = RL$ for a finite ring R and a finite loop L.

(Quasi-)group codes are linear codes over a finite ring R obtained from left ideals of a (quasi-)group ring $A = RG$ of a finite (quasi-)group G. Let $G = \{g_1, ..., g_n\}$ and $I \leq {}_A A$ be a left ideal of A. Then the set $\mathcal{K} = \mathcal{K}(I)$ of all words $(r_1, ..., r_n) \in R^n$ such that $\sum r_i g_i \in I$ is a linear n-code over the ring R, i.e. a submodule of the module ${}_R R^n$. Such codes, contained in the group ring, will be also called *G-codes over R.* The left ideal $I \leq {}_A A$ will be identified with the code $\mathcal{K}(I)$ and, with some abuse of notation, we will say that I is an $[n, k, d]_q$-code. Here n is the length of the code, q^k its cardinality and d its distance . Through the previous identification we can define for every $x = \sum r_i g_i \in A$ its *Hamming weight* $||x||$ by $||x|| = ||(r_1, ..., r_n)||$.

Several results about such codes are known in the case $R = \mathbb{F}$ a finite field and G an cyclic group, see e.g. [23,14]. In the case of non-abelian groups there are some results in [24,25,26].

In [8] a computation of parameters, for codes $\mathcal{K} = \mathcal{K}(I)$ and left ideals I of loop-algebras $\mathbb{F}G$ of small orders, was carried out.

A (generally nonlinear) $[n, k, d]$-code $C \subseteq \mathbb{F}_q^n$ is said to be *optimal* if $|C| = q^k$ is the maximum of all possible cardinalities of n-codes with a given distance d (see [14]). Every code C satisfies the inequality $k \leq n - d + 1$ (Singleton bound) and the code C is called MDS-code if $k = n - d + 1$. Clearly, any MDS-code is optimal.

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 56–68, 2008.

Any quasi-group ring $A = RG$ contains two important examples of quasigroup MDS-code: its *fundamental ideal* that is an $[n, n-1, 2]$-code:

$$\Delta(A) = \{\sum_{g\in G} r(g)g : \quad \sum_{g\in G} r(g) = 0\}, \tag{1}$$

and

$$I_0 = A(\sum_{g\in G} g) = F(\sum_{g\in G} g), \tag{2}$$

that is an $[n, 1, n]$-code.

Note that $\Delta(A)$ can be described also as the R-submodule of A spanned by all differences $e - g, \quad g \in G$.

According to the definition of optimal code we will say that a linear $[n, k, d]_q$-code over a field $\mathbb{F}_q$ is *linearly optimal* if k is the maximum of the dimensions of all $\mathbb{F}_q$-linear n-codes with a fixed distance d.

Let $n(k, q)$ (resp. $m(k, q)$) be the maximal length of all MDS-codes C with combinatorial dimension $k = \log_q |C|$ over an alphabet of q elements (resp., for a primary q, the maximal length of all linear MDS codes over the field $\mathbb{F}_q$). Clearly $m(k, q) \leq n(k, q)$.

It is known (see [14] and [23]) that

$$n(k, q) = k + 1 \textit{ if } q \leq k + 1,$$

$$n(k, q) \leq q + k - 1 \textit{ if } k \leq q \textit{ and } q \textit{ is even},$$

$$n(k, q) \leq q + k - 2 \textit{ if } 3 \leq k \leq q \textit{ and } q \textit{ is odd}.$$

The following simple result helps to prove that some codes are linearly optimal.

Proposition 1 ([8]). *Let n, k be natural numbers, q is primary, such that*

$$n > m(k + 1, q).$$

Then any $\mathbb{F}_q$-linear $[n, k, n-k]_q$-code is linearly optimal.

So there are linearly optimal $[8, 4, 4]_q$-codes (for $q = 2, 3, 4, 5$) contained in the group algebras over the dihedral group D_4 or the quaternion group Q_8 of order 8.

In [8] some known codes, for instance the $[7, 4, 3]_2$-Hamming code or the $[8, 4, 4]_2$-Brauer code, are obtained as ideals of a group algebra. But in general, the lattice of left ideals of nonassociative loop algebras $A = FL$, with $|F| \leq 5$, $|L| \leq 7$, have only four ideal $0, I_0, \Delta, A$, so they do not contain interesting loop codes. However, there are linearly optimal codes in the group algebras of non-commutative groups that can not be obtained using abelian groups. This is the case for the $[8, 3, 5]$-code in $\mathbb{F}_4 Q_8$, the $[10, 4, 6]$-codes in $\mathbb{F}_4 D_5$ and in $\mathbb{F}_5 D_5$, the $[12, 8, 4]$- and $[12, 6, 6]$-codes in $\mathbb{F}_4 A_4$ and the $[12, 6, 6]$-code in $\mathbb{F}_4 D_6$. It is remarkable that many of the best codes obtained are linked to algebras that are neither commutative nor semisimple.

1.1 The Main Results

Below we will give constructions of $[n, n-3, 3]_q$ group codes over $F = \mathbb{F}_q$ for $n = 2q$ and $n = 3q$.

Let us note that linear $[n, n-3, 3]_q$-codes over $\mathbb{F}_q$ can be easily constructed from a Hamming $[N, N-3, 3]$-code for $N = q^2 + q + 1$ [3,12]. But here we construct such codes as group codes over $\mathbb{F}_q$.

In what follows 1 will denote the identity element of the field F while the identity element of a group G (that is also identity element of the group ring $F(G)$ will be denoted by e.

It can be proved that Reed-Solomon codes can be represented as group codes.

Theorem 1. *Let $(H, \cdot)$ be a p-elementary abelian group of order $q = p^l$. For a given isomorphism of abelian groups $\varphi : (H, \cdot) \to (F, +)$ we consider the following elements*

$$u_s = \sum_{h \in H} \varphi(h)^s h \in FH, \quad s = 0, \ldots, q-2. \tag{3}$$

Then for every i, $1 \leq i \leq q-1$ the subspace

$$\mathcal{R}_i = Fu_0 + \ldots + Fu_{i-1} \leq {}_F FH \tag{4}$$

is a Reed-Solomon $[q,\ i,\ q+1-i]_q$-MDS code and an ideal in FH. In particular

$$\mathcal{R}_{q-1} = \Delta(FH). \tag{5}$$

If $s = p^c$ for some $1 \leq c \leq l-1$, then

$$\mathcal{R}_s = FHu_{s-1} \tag{6}$$

is a principal ideal.

Theorem 2. *Let G be a group of order $2q$, containing a p-elementary abelian subgroup H of order q. Then there exists a $[2q, 2q-3, 3]_q$ linearly optimal G-code over $\mathbb{F}_q$.*

Proof. Following the previous notation, let $\varphi : (H, \cdot) \to (F, +)$ be an isomorphism of abelian groups and, as in Theorem 1

$$\mathcal{R} = \mathcal{R}_{q-2}, \ \ \beta \in G \setminus H \ \ v \in \Delta(FH) \setminus \mathcal{R}, \ \ \sigma = ev + \beta v. \tag{7}$$

Then the desired code is

$$\mathcal{L} = e\mathcal{R} + \beta\mathcal{R} + F\sigma. \tag{8}$$

In a similar way, $[3q, 3q-3, 3]_q$ linearly optimal codes can be constructed. The construction is a bit more complicated and some extra assumption over the group G has to be made. We will assume that our group G of order $3q$ contains a normal subgroup H that is p-elementary abelian of order q and that $3|q-1$.

Given an arbitrary element $\beta \in G \setminus H$, let us denote $\hat{\beta} : H \to H$ the automorphism of H induced by the conjugation by the element β.

It is well known that H has a "natural" structure of F-vector space and $\hat{\beta}$ is a linear automorphism of H. We will use additive notation to refer to this linear structure.

Note that since $3||G|$ there is an element $\beta \in G$ of order 3, and since $3|q-1$ we have $\beta \notin H$ and

$$G = H \cup \beta H \cup \beta^2 H. \tag{9}$$

For such element β that satisfies $\beta^3 = 1$ the minimal polynomial of the linear map $\hat{\beta}$ divides to $x^3 - 1$. So an arbitrary eigenvalue λ of $\hat{\beta}$ satisfies $\lambda^3 = 1$.

We will assume that $\hat{\beta}$ has at most one eigenvalue $\lambda \in \mathbb{F}_p$, $\lambda \neq 1$, that is,

$$\left| \operatorname{Spec} \hat{\beta} \setminus \{1\} \right| \leq 1. \tag{10}$$

So, always using the above notation and assuming the condition (10), we have the following result.

Lemma 1. *There exist an isomorphism*

$$\varphi : H \to (F, +)$$

and an element $\theta \in F$ of order 3 such that

$$\varphi(a) + \theta\varphi(\hat{\beta}(a)) + \theta^2\varphi(\hat{\beta}^2(a)) = 0 \tag{11}$$

for any $a \in H$.

From now on we assume that θ and φ satisfy (11) and G, H, F satisfy the conditions of Lemma 1. Take $\mathcal{R} = \mathcal{R}_{q-2}$ from Theorem 1 and define

$$f = e + \beta + \beta^2, \;\; g = e + \theta\beta + \theta^2\beta^2, f_1 = f, \; f_2 = fv, \; f_3 = gv, \tag{12}$$

where $v = -u_{q-2}$ from Theorem 1.

Consider, as above, an element $\beta \in G \setminus H$ of order 3. Since

$$G = H \cup \beta H \cup \beta^2 H, \tag{13}$$

it is not difficult to see that the subspace

$$\mathcal{J} = \mathcal{R} + \beta\mathcal{R} + \beta^2\mathcal{R} \tag{14}$$

is a left ideal of the ring FG and also a $[3q, 3(q-2), 3]_q$-code. It can be proved that the subspace

$$\mathcal{L} = \mathcal{J} + Ff_1 + Ff_2 + Ff_3 \tag{15}$$

is a left ideal of the ring FG with the distance 3. So $\mathcal{L}$ is a linearly optimal code. Notice that condition 10 is satisfied if β acts on H by conjugation as a fixed scalar multiplication (in particular, if G is commutative) or if $3 \nmid p-1$.

So we get the following

Theorem 3. *Let $q = p^l > 2$ be a primary number such that $3|q-1$, G be a group of order $3q$, containing an elementary abelian normal p-subgroup H of order q. Let $\beta \in G$ be an element of order 3. Consider H as an l-dimensional vector space over $\mathbb{F}_p$ and denote by $\hat{\beta} : H \to H$ the linear operator on this space defined as the conjugation by β. Suppose the set $\operatorname{Spec} \hat{\beta}$ of all eigenvalues of $\hat{\beta}$ in $\mathbb{F}_p$ satisfies the condition:*

$$\left|\operatorname{Spec} \hat{\beta} \setminus \{1\}\right| \leq 1. \tag{16}$$

Then there exists a $[3q, 3q-3, 3]_q$ linearly optimal G-code.

2 Clifford Codes

Quantum errors can be written in terms of an error operator basis $\mathcal{E}$. Several approaches are possible, but one of the most useful is do it through the *nice error bases* [17]. This type of bases can be obtained by a projective representation of a group E, called *error group*, or, equivalently, by a faithful irreducible ordinary representation of a central extension of E called the *abstract error group G*.

One of the most common construction of quantum error correcting codes is based on binary stabilizer codes [18]. If ρ is a faithful unitary ordinary representation of the abstract error group G, then an stabilizer code is defined as the joint eigenspace Q of the representing matrices $\rho(n)$ for all $n \in N$, where N is a normal subgroup of G.

Clifford codes [18,19] are a further generalization of this type of codes. Their definition involves a normal subgroup N of G that is not necessarily abelian.

So a first problem related to Clifford codes is to decide whether a Clifford code is an stabilizer code. Notice that even if the normal subgroup N used in the construction of a given Clifford code is nonabelian, it is still possible to construct the same Clifford code through another abelian subgroup and so the code would be an stabilizer code. A characterization of Clifford codes which are also stabilizer codes is given in [19].

The result of [19] was extended in [13] by using properties of the characters of the *abstract error groups G*. Those groups are known as *groups of central type* and their characters have been studied in several papers [10,15]. The existence of *fully ramified characters* over certain subgroups of G characterizes *abstract error groups* and makes possible a new formulation of those results.

In [13] Clifford codes over the direct product of abstract error groups were constructed, following the same lines used in the classical case, and their correction properties were studied and compared with the corresponding properties of stabilizer codes.

2.1 Preliminaries

We will remember some notions of representation theory that will be used.

Let $\mathcal{U}(n)$ be the unitary group of degree n, that is, the multiplicative group of all $n \times n$ unitary matrices.

Definition 1. *Let E be a group of order n^2 and $\rho : E \to \mathcal{U}(n)$ a map satisfying:*

1. $\rho(1) = I_n$,
2. $tr(\rho(g)) = n\delta_{g,1}$ *for all* $g \in E$,
3. $\rho(g)\rho(h) = \omega(g,h)\rho(gh)$ *for all* $g, h \in E$,

where ω is a scalar function $\omega : E \times E \to C^*$. A nice error basis on $\mathcal{H} = \mathbb{C}^n$ is a set $\mathcal{E} = \{\rho(g) \in \mathcal{U}(n)\}\, g \in E$.

Notice that Conditions 1 and 3 in the above definition imply that ρ is a $\mathbb{C}$-projective representation of the group E (see [16]) and Condition 2 implies the orthogonality of the matrices $\rho(g)$ with respect the inner product $\langle A, B\rangle = tr(A^\dagger B)/n$. So ρ is an irreducible projective representation.

Let E be a group, $|E| = n^2$, with a nice error basis $\mathcal{E}$. Such a group is called the *index group* of $\mathcal{E}$. The following characterization is known (see [17]).

Theorem 4. *Let $\mathcal{E} = \{\rho(g)\}\, g \in E$ be a set of unitary matrices parametrized by the elements of a finite group E. The set $\mathcal{E}$ is a nice error basis with index group E if and only if $\rho : E \to \mathcal{U}(n)$, $g \to \rho(g)$, is a unitary irreducible faithful projective representation of E of degree $|E|^{1/2}$.*

Usually, instead of E, some central extension G, which is isomorphic to the group generated by the matrices $\{\rho(g) : g \in E\}$, will be used. The projective representation of E becomes an ordinary representation of G. This group is called *abstract error group.*

It can be proved that G is an abstract error group if and only if it satisfies the following two conditions:

- There exists an ordinary irreducible character $\phi \in Irr(G)$ such that $\phi(1) = |G : Z(G)|^{1/2}$,
- the center $Z(G)$ is a cyclic group.

A group with the first property is said to be of *central type*, so G is an abstract error group if and only if G is of central type and its center is cyclic.

We will remind some results of Clifford theory (see chapter 5 of [16] and [9]) which will be used in the study of stabilizer and Clifford codes.

Let N be a normal subgroup of G, and $\chi \in Irr(N)$ an irreducible character of N. Let g be any element of G. Then the conjugate character $\chi^g : N \to \mathbb{C}$ is defined by $\chi^g(n) = \chi(gng^{-1})$, for all $n \in N$. If $\phi \in Irr(G)$, Clifford's Theorem (see Theorem 6.2 in [16]) ensures that all irreducible components of the restriction ϕ_N are conjugate. That is:

Theorem 5 (Clifford's Theorem). *Let $N \trianglelefteq G$ and $\phi \in Irr(G)$. Let χ be an irreducible constituent of ϕ_N (i.e $\langle \phi, \chi\rangle_N \neq 0$) and suppose that $\chi = \chi_1, \chi_2, \ldots, \chi_t$ are the distinct conjugates of χ in G. If $e = \langle \phi, \chi\rangle_N$, we have*

$$\phi_N = e \sum_{i=1}^{t} \chi_i.$$

Clifford theorem can be reformulated in terms of modules. Let us suppose that T is a $\mathbb{C}$-representation of N and g is an element of G. We define the conjugate representation T^g by $T^g(n) = T(gng^{-1})$, for all $n \in N$. It is clear that the character of the conjugate representation is the conjugate character. We say that two $\mathbb{C}N$-modules W_1 and W_2 are conjugated if the $\mathbb{C}$-representations afforded by these two modules are conjugated.

Theorem 6 (Clifford's Theorem for modules). *Let N be a normal subgroup of G and let V be an irreducible $\mathbb{C}G$-module. Let W be any irreducible $\mathbb{C}N$-module of V. Then*

1. *$V = \sum W_i$ where the W_i are irreducible $\mathbb{C}N$-submodules of V.*
2. *Each W_i is of the form Wg_i for some $g_i \in G$ and so is conjugate to W.*

2.2 Clifford and Stabilizer Codes

One of the most quantum codes are *quantum stabilizer codes* (see [18] and [1]).

Definition 2. *Let G be an abstract error group and let ρ be a faithful irreducible unitary representation of G. If $N \trianglelefteq G$, then the joint eigenspace Q of the representing matrices $\rho(n)$ for all $n \in N$ is said to be an stabilizer code.*

If Q is nontrivial, then N is necessarily abelian.

Clifford codes are a generalization of stabilizer codes. They can be constructed from a normal subgroups $N \trianglelefteq G$ which is not necessarily abelian.

Let G be an abstract error group and let $N \trianglelefteq G$. As in Definition 2, let ρ be a faithful irreducible unitary representation of G of degree $|G : Z(G)|^{1/2}$. Let us suppose that the representation ρ affords an irreducible $\mathbb{C}G$-module V. Then, the restriction of ρ_N affords the $\mathbb{C}N$-module V_N which can be decomposed, see Theorem 6, as a sum of irreducible conjugate $\mathbb{C}N$-modules as follows:

$$V_N = \sum W_i = \sum_{i=1}^{s} Wg_i.$$

Let $\{Wg_1, \ldots, Wg_t\}$ be a maximal set of non-isomorphic $\mathbb{C}N$-modules among the $\{Wg_i\}$ $1 \leq i \leq s$. For each $1 \leq i \leq t$, let us denote V_i the sum of all conjugates Wg_j, which are isomorphic to Wg_i as $\mathbb{C}N$-modules. Then $V_N = \sum_{i=1}^{t} V_i$, and the $\mathbb{C}N$-modules V_i are called homogeneous components of V_N (see Definition 49.5 in [9]).

A quantum *Clifford code* Q is a homogeneous component $Q = W \oplus \cdots \oplus W$ of V_N. Note that if N is abelian, then $dim(W) = 1$, so N acts as an scalar over Q, and Q is an stabilizer code. The correcting properties of the code depend on the inertia subgroup $T(W) = \{g \in G : Wg \simeq W\}$ and on the set $Z(W) = \{g \in T(W) : \exists \lambda \in \mathbb{C},\, vg = \lambda v,\, \forall v \in Q\}$ of elements that act on Q as scalars. It can be proved (see [18]) that Q can to correct a set of errors $\varSigma \subseteq G$ always that $e_1^{-1}e_2 \notin T(W) - Z(W)$ for all $e_1,\ e_2$ in $\varSigma$.

Let ϕ be the irreducible character afforded by the $\mathbb{C}G$-module V, and let χ be the afforded one by the $\mathbb{C}N$-module W. It is clear that $\chi \in Irr(N)$ and that the inner product $\langle \phi, \chi \rangle_N \neq 0$. Moreover, the conjugate modules Wg, with $g \in G$, afford the conjugate characters χ^g.

In general, G acts on $Irr(N)$ by conjugation and for each $\chi \in Irr(N)$ its stabilizer is the inertia subgroup

$$T(\chi) = \{g \in G : \chi^g = \chi\} = \{g \in G : \chi(gng^{-1}) = \chi(n),\ \forall n \in N\},$$

which can be identified with the set $T(W)$.

If θ is the character afforded by the $\mathbb{C}T(\chi)$-module Q, then it can be proved that θ is the unique character $\theta \in Irr(T(\chi))$ such that $\langle \theta, \chi \rangle_N \neq 0$ and $\langle \phi, \theta \rangle_{T(\chi)} \neq 0$. The quasi-kernel $Z(\theta) = \{g \in T(\chi) : |\theta(g)| = \theta(1)\}$ consists of those elements of G that act on the code Q as scalars and so can be identified with $Z(W)$. Thus, an error $\rho(g)$ is detectable by the code Q (see [19]) if and only if $g \notin T(\chi) - Z(\theta)$.

Alternatively, Clifford codes can be defined as the image of an orthogonal projector (see [19]). This definition shows more clearly that Clifford codes extend Stabilizer codes.

Definition 3. *Let G be an abstract error group and ϕ an irreducible, faithful character of degree $|G : Z(G)|^{\frac{1}{2}}$. Let ρ be a unitary representation of G affording ϕ, $N \trianglelefteq G$, and $\chi \in Irr(N)$ such that $\langle \phi, \chi \rangle_N \neq 0$. A Clifford Code, denoted by (G, ρ, N, χ), is the image of the orthogonal projector*

$$P = \frac{\chi(1)}{|N|} \sum_{n \in N} \chi(n^{-1})\rho(n).$$

In case that N is abelian, the Clifford code is called an stabilizer code (indeed, this definition coincides with Definition 2).

Since we are interested in Clifford codes that are not stabilizer codes, in what follows, we will consider only Clifford codes (G, ρ, N, χ) where N is nonabelian.

In Theorem 3 in [19] a characterization of those Clifford codes (G, ρ, N, χ) that are stabilizer codes was given. It was assumed that $Z(G) \leq N$, but this condition is not very restrictive because it was proved in Lemma 4 in [19]) that every Clifford code (G, ρ, N, χ) can be also defined over the normal subgroup $N_Z = NZ(G)$.

Theorem 7. *Suppose that $Z(G) \leq N$. A Clifford code (G, ρ, N, χ) is an stabilizer code if and only if $\chi^2(1) = |N|/|A|$ for some $A \in \mathcal{A}$, where $\mathcal{A}$ is defined by:*

$$\mathcal{A} = \{A \leq Z(\theta) : A \trianglelefteq G,\ Z(G) \leq A,\ A \textit{ abelian}\}.$$

Since abstract error groups are groups of central type, some properties of groups of central type can be related to properties of Clifford codes defined over them. Groups of central type can be described by means of fully ramified characters. Some useful properties of this type of characters are summarized in Proposition 4.2 of [15].

Definition 4. *Let $N \lhd G$ and suppose $\chi \in \ Irr(N)$. Then χ is fully ramified in G if $\chi^G = e\theta$ for some $\theta \in \ Irr(G)$ with $e = |G : N|^{1/2}$. Dually, $\theta \in \ Irr(G)$ is fully ramified over N if $\theta_N = e\chi$ for some $\chi \in \ Irr(N)$ with $e = |G : N|^{1/2}$.*

Proposition 2. *Let $N \lhd G$, $\chi \in Irr(N)$ and $\phi \in Irr(G)$ such that $\langle \phi, \chi \rangle_N \neq 0$. Then the following are equivalent:*

1. *χ is fully ramified in G.*
2. *ϕ is fully ramified over N.*
3. *ϕ vanishes off N and ϕ_N is a multiple of χ.*
4. *ϕ vanishes off N and $\phi(1) = |G : N|^{1/2}\chi(1)$.*

In particular, a finite group G with a faithful, irreducible character ϕ is an abstract error group if and only if ϕ is fully ramified over $Z(G)$, and $Z(G)$ is cyclic.

Proposition 3. *Let Q be a Clifford code with data (G, ρ, N, χ). The character χ is fully ramified in $T(\chi)$.*

Corollary 1. *Let Q be a Clifford code with data (G, ρ, N, χ), then $Z(\theta) = Z(\chi)$ and $ker(\theta) = ker(\chi)$, where $\theta \in Irr(T(\chi))$ with $\langle \theta, \chi \rangle_N \neq 0$ and $\langle \phi, \theta \rangle_{T(\chi)} \neq 0$.*

Corollary 1 establishes that $Z(\theta) = Z(\chi) \leq N$ and if $\mathcal{A} = \{A \leq Z(\theta) : A \unlhd G, Z(G) \leq A, \ A \ abelian\}$, then $A \in \mathcal{A}$ implies that $A \leq N$.

Theorem 8. *Let $\chi \in Irr(N)$ and $A \in \mathcal{A}$, χ is fully ramified over A if and only if $\chi^2(1) = |N : A|$.*

The following characterization of Clifford codes which are stabilizer codes, and that improves Theorem 7, can be proved.

Corollary 2. *A Clifford code (G, ρ, N, χ) is an stabilizer code if and only if χ is fully ramified over $Z(\chi)$ and $Z(\chi)$ is a normal abelian subgroup of G.*

Notice that if the Clifford code (G, ρ, N, χ) is an stabilizer code, then the group $N/ker\chi$ is of central type. In fact, the character $\hat{\chi}$ defined by $\hat{\chi}(g\, ker\chi) = \chi(g)$ for all $g \in G$ is a faithful irreducible character of $N/ker\chi$ (see Lemma 2.22 in [16]). By Lemma 2.17 of [16], we know that $Z(N/ker\chi) = Z(\chi)/ker\chi$ is a cyclic group. Since χ is fully ramified over $Z(\chi)$, it follows that

$$\chi(1) = \hat{\chi}(1) = |N : Z(\chi)| = |N/ker\chi : Z(N/ker\chi)|,$$

that is, $\hat{\chi}$ is fully ramified over $Z(N/ker\chi)$. We have proved the following result:

Corollary 3. *Let Q be a Clifford code with data (G, ρ, N, χ). If Q is an stabilizer code, then the group $N/ker\chi$ is of central type.*

3 Codes over Direct Products

Definition 5. *A block code C of length n over a group G is a group code if C is a subgroup of the direct product G^n. If C is a normal subgroup of G^n, the group code is called normal.*

Given a group code C of length n and any $1 \leq k \leq n$, the *output group* G_k is defined as the set of all $g \in G$ that actually occur as k-component c_k of some code sequence $c \in C$, that is $G_k = \pi_k(C)$, where $\pi_k : G^n \to G$ is the canonical projection. Usually $G_k = G$, but it is possible to obtain proper output subgroups, i. e. $G_k < G$. The group code C can be seen as a subgroup of the direct product $W = \prod_{k=1}^{n} G_k$, which is called *output space.*

It can be proved (see Theorem 4 of [11] for details) that if C is a normal code such that the output space $W = \prod G_k$ is nonabelian, then its minimum Hamming distance is $d_H(C) = 1$. This is due to the fact that the commutator subgroup $W' = \prod G'_k$ is nontrivial and thus it can be found a sequence with Hamming weight 1. That is, the best correcting properties are obtained when the output space is an abelian group. This seems also to be the case in the quantum context.

If we want to construct Clifford codes over the direct product of several copies of an abstract error group H, the first problem that we find is that the direct product H^n is not an abstract error group. However it is possible to obtain an abstract error group as a quotient of H^n.

Theorem 9. *Let H be an abstract error group and $\phi \in Irr(H)$ a faithful, fully ramified character over $Z(H)$, then $G = H^n/ker(\phi \times \cdots \times \phi)$ is an abstract error group.*

Let G be the abstract error group of the previous theorem. Let Q be a Clifford code with data (G, ρ, N, χ). We note that if $\pi : G \to G/Z(G)$ is the canonical projection and $S \subseteq G$, then the image $\pi(S) \subseteq \bar{H}^n$ can be seen as a block code of length n over $\bar{H} = H/Z(H)$. Given an element $g \in G$, its Hamming weight $\omega_H(g)$ can be defined by $\omega_H(g) = \omega_{\bar{H}}(\pi(g))$. It is easy to verify that this concept is well defined.

An error $\rho(g)$, $g \in G$ is detectable if and only if $g \notin T(\chi) - Z(\chi)$. It is clear that if the minimum Hamming weight of $T(\chi) - Z(\chi)$ is d, then every error with Hamming weight less than d can be detected. This minimum Hamming weight depends on the properties of the output space.

Theorem 10. *Let (G, ρ, N, χ) be a Clifford code and $\pi : G \to G/Z(G)$ the canonical projection. Let $W_{\pi(N)}$ be the output space of the group code $\pi(N)$, which is supposed to be nonabelian, and let $W'_{\pi(N)}$ be its commutator group. If $\pi^{-1}(W'_{\pi(N)}) \bigcap T(\chi) - Z(\chi) \neq \emptyset$, then minimum the Hamming weight of $T(\chi) - Z(\chi)$ is one.*

A necessary condition for a Clifford code (G, ρ, N, χ) to detect all the errors with Hamming weight one is that $N' \leq Z(\chi)$, since if $N' \nleq Z(\chi)$ then $\pi^{-1}(W'_{\pi(N)}) \bigcap (T(\chi) - Z(\chi)) \neq \emptyset$.

Good candidates of abstract error groups able to detect more than one error are nilpotent groups of class 2.

Proposition 4. *If G is an abstract error group that is nilpotent of class 2, then all Clifford codes (G, ρ, N, χ) satisfy $N' \leq Z(\chi)$.*

Notice that if G is an abstract error group nilpotent of class 2, then the error group $G/Z(G)$ is abelian, and any Clifford code with data (G, ρ, N, χ) is also a Clifford code with respect to $Z(N)$ (see Theorem 6 in [18]). Hence, such a code is an stabilizer code.

If a Clifford code is able to detect all errors with Hamming weight one then a sufficient and needed condition to be stabilizer is found. Some previous results are used.

Theorem 11. *Let Q be a Clifford code with data (G, ρ, N, χ). If Q detects all errors with Hamming weight one, the group $N/ker\chi$ is nilpotent of class 2.*

Lemma 2. *Let (G, ρ, N, χ) be a Clifford code which detects all errors with Hamming weight one. If χ is faithful, then (G, ρ, N, χ) is an stabilizer code.*

Lemma 3. *Let (G, ρ, N, χ) be a Clifford code which detects all errors with Hamming weight one. Then χ is fully ramified over $Z(\chi)$.*

Finally, using Corollary 2 we get the wanted characterization.

Theorem 12. *Let (G, ρ, N, χ) be a Clifford code which detects all errors with Hamming weight one. Then (G, ρ, N, χ) is an stabilizer code if and only if $Z(\chi)$ is normal abelian in G.*

Unfortunately, we do not known any characterization of non-stabilizer Clifford codes that can detect errors with Hamming weight at least one. In order to deal with this problem we tried to find abstract error groups G with a normal subgroup $N \lhd G$ such that $N' \leq Z(\chi)$, where $\chi \in Irr(N)$ is an irreducible component of the restriction ρ_N (remember that ρ is an irreducible character of G such that $\rho(1) = 1G : Z(G)|^{1/2}$). Such groups can produce examples of non-stabilizer Clifford codes.

Only 2-groups and direct products of 2-groups with cyclic groups of prime order different from 2 satisfy this property.

In all cases, the inertia subgroup $T(\chi) = N$ and the quasi-kernel $Z(\chi)$ is an abelian subgroup of N, which is not normal in G. The subgroup N is nilpotent of class 2, the index $|N : Z(\chi)| = 4$ and the dimension of the Clifford code Q is 2.

So, we can reduce our study to abstract error 2-groups. Let us suppose that G is an abstract error 2-group as in the previous section, that is, its error group $G/Z(G)$ is a direct product of several copies of another error group H. In all cases, the quotient group $G/Z(G)$ is isomorphic to the group $D_8 \times D_8$. However, for these codes, minimum Hamming weight is one.

It seems that we can not get better correcting properties by using Clifford codes instead of stabilizer codes.

Notes and Comments. As it was mentioned in the abstract results in the first chapter of this survey were obtained by E. Couselo et al. in [5], while results in the second chapter were obtained by M. Grassl et al. in [13]. Our aim here was to give an insight of algebraic methods, mainly in ring and group theory, to both, classic and quantum error correcting codes.

References

1. Ashikhmin, A., Knill, E.: Nonbinary quantum stabilizer codes. IEEE Trans. Inform. Theory 47, 3065–3072 (2001)
2. Bosma, W., Cannon, J.J., Playoust, C.: The Magma algebra system I: The user language. J. Symb. Comp. 24, 235–266 (1997)
3. Brouwer, A.E.: Bounds on linear codes. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, pp. 295–461. Elsevier, Amsterdam (1998)
4. Interlando, J.C., Palazzo, R., Elia, M.: Group Block Codes over Non Abelian Groups are Asymptotically Bad. IEEE Transactions on Information Theory 48(4), 1277–1280 (1996)
5. Couselo, E., González, S., Martínez, C., Markov, V., Nechaev, A.: Some constructions of linearly optimal group codes (submitted)
6. Couselo, E., Gonzalez, S., Markov, V., Nechaev, A.: Recursive MDS-codes and recursively differentiable k-quasigroups. In: Proceedings of the Sixth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-VI), pp. 78–84 (1998)
7. Couselo, E., Gonzalez, S., Markov, V., Nechaev, A.: Linear Recursive MDS-Codes and Asturian codes. In: International workshop on coding and cryptography, paris, pp. 142–149 (2001)
8. Couselo, E., Gonzalez, S., Markov, V., Nechaev, A.: “Loop codes”. Discr. Math. and Appl. 14(2), 163–172 (2004)
9. Curtis, C.W., Reiner, I.: Representation of finite groups and associative algebras. Wiley (Interscience), New York (1962)
10. DeMeyer, F.R., Janusz, G.J.: Finite Groups with an Irreducible Representation of Large Degree. Math. Z. 108, 145–153 (1969)
11. David Forney Jr., G.: On Hamming Distance Properties of Group Codes. IEEE Transactions on Information Theory 38(6), 1797–1801 (1992)
12. Grassl, M.: Searching for linear codes with large minimum distance. In: Bosma, W., Cannon, J. (eds.) Discovering Mathematics with Magma. Springer, Heidelberg (2006)
13. Grassl, M., Martínez, C., Nicolás, A.P.: Clifford codes and fully ramified characters (submitted)
14. Heise, W., Quattrocci, P.: Informations- und codierungstheorie. Springer, Heidelberg (1995)
15. Howlett, R.B., Martin Isaacs, I.: On Groups of Central Type. Math. Z. 179, 555–569 (1982)
16. Martin Isaacs, I.: Character Theory of Finite Groups. Academic Press, London (1976)
17. Klappenecker, A., Rötteler, M.: Beyond Stabilizer Codes I: Nice Error Basis. IEEE Transactions on Information Theory 48(8), 2392–2395 (2002)
18. Klappenecker, A., Rötteler, M.: Beyond Stabilizer Codes II: Clifford codes. IEEE Transactions on Information Theory 48(8), 2396–2399 (2002)

19. Klappenecker, A., Rötteler, M.: On the structure of nonstabilizer Clifford codes. Quantum Inf. Comput. 4(2), 152–160 (2004)
20. Lambek, J.: Lectures on Rings and Modules. McGill Univ., Blaisdell Publ. Co. (1966)
21. Lang, S.: "Algebra". Colambia Univ., Addisson–Wesley, Reading (1965)
22. Lidl, R., Niederreiter, H.: "Finite fields". Addison –Wesley, Reading (1983)
23. MacWilliams, F.J., Sloane, N.J.A.: The theory of Error-Correcting Codes, vol. 16. Elsevier Science Publishers, B.V., North Holland Mathematical Library (1988)
24. Sabin, R.E., Lomonaco, S.J.: Metacyclic error-correcting codes. Appl. Algebra Eng. Commun. Comput. 6(3), 191–210 (1995)
25. Sabin, R.E.: On determining all codes in semi-simple group rings. In: Cohen, G., et al. (eds.) AAECC 1993. LNCS, vol. 673, pp. 279–290. Springer, Heidelberg (1993)
26. Sabin, R.E.: An ideal structure for some quasi-cyclic error-correcting codes. In: Mullen, G.L., et al. (eds.) Finite fields, coding theory, and advances in communications and computing. Proceedings of the international conference on finite fields, coding theory, and advances in communications and computing, University of Nevada, Las Vegas, USA, August 7-10, 1991. Lect. Notes Pure Appl. Math., vol. 141, pp. 183–194. Marcel Dekker, Inc., New York (1993)
27. Shahriari, S.: On Central type factor groups. Pacific Journal of Mathematics 1, 151–178 (1991)

Evaluating the Impact of Information Distortion on Normalized Compression Distance

Ana Granados, Manuel Cebrián, David Camacho, and Francisco B. Rodríguez

Departamento de Ingeniería Informática, Universidad Autonóma de Madrid, Spain
{Ana.GranadosF,Manuel.Cebrian,David.Camacho,F.Rodriguez}@uam.es

Abstract. In this paper we apply different techniques of information distortion on a set of classical books written in English. We study the impact that these distortions have upon the Kolmogorov complexity and the clustering by compression technique (the latter based on Normalized Compression Distance, NCD). We show how to decrease the complexity of the considered books introducing several modifications in them. We measure how the information contained in each book is maintained using a clustering error measure. We find experimentally that the best way to keep the clustering error is by means of modifications in the most frequent words. We explain the details of these information distortions and we compare with other kinds of modifications like random word distortions and unfrequent word distortions. Finally, some phenomenological explanations from the different empirical results that have been carried out are presented.

1 Introduction

A natural measure of similarity assumes that two objects x and y are similar if the basic blocks of x are in y and vice versa. If this happens we can describe object x by making reference to the blocks belonging to y, thus the description of x will be very simple using the description of y.

This is what a compressor does to code the concatenated xy sequence: a search for information shared by both sequences in order to reduce the redundancy of the whole sequence. If the result is small, it means that a lot of information contained in x can be used to code y, following the similarity conditions described in the previous paragraph. This was formalized by Cilibrasi and Vitányi [1], giving rise to the concept of *Normalized Compression Distance* (NCD), which is based on the use of compressors to provide a measure of the similarity between the objects. This distance may then be used to cluster those objects.

The mathematical formulation is as follows

$$NCD(x,y) = \frac{\max\{C(xy) - C(x), C(yx) - C(y)\}}{\max\{C(x), C(y)\}}, \tag{1}$$

where C is a compression algorithm, $C(x)$ is the size of the C-compressed version of x, and $C(xy)$ is the compressed size of the concatenation of x and y. NCD

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 69–79, 2008.

generates a non-negative number $0 \leq NCD(x, y) \leq 1$. Distances near 0 indicate similarity between objects, while distances near 1 reveal dissimilarity.

The theoretical foundations for this measure can be traced back to the notion of Kolmogorov Complexity $K(X)$ of a string X, which is the size of the shortest program able to output X in a universal Turing machine [2,3,4]. As this function is incomputable due to the Halting problem [5], the most usual estimation is based on data compression: $C(X)$ is considered a good upper estimate of $K(X)$, assuming that C is a reasonably good compressor for X [1].

In our work we apply this distance to text clustering [1,6], with the aim to study the way in which the method is influenced by different types of information distortion. A percentage of words of the books is distorted by using two different word-replacing techniques, which eventually change the amount of information remaining in the books, their (estimated) Kolmogorov Complexity, and the clustering error obtained using the NCD.

Other authors [7] have given a theoretical and experimental basis for explaining the NCD-clustering behavior of elements which have been transmitted through a *symmetric-channel*, i.e. which have been perturbed by a certain amount of uniform random noise. We go a step further by considering a wider spectrum of information distortions, within the framework of a complete experimental setup on a selected text corpus for which an ideal clustering is already known.

The main contributions of this paper are

- New insights for the evaluation and explanation of the behavior of the NCD-driven clustering method,
- a technique to reduce the Kolmogorov complexity of the books while preserving most of the relevant information,
- experimental evidence of how to fine-tune the NCD so that better clustering results are obtained.

This paper is structured as follows. Section 2 describes the distortion/word-replacement method, the clustering assessment and the Kolmogorov Complexity estimation. Section 3 explains the experimental setup and gathers the results of the experiments. Section 4 summarizes the conclusions and describes ongoing research.

2 The Distortion Methods

We want to study the effect of information distortion on NCD-driven text clustering by replacing words from the documents in different manners. After the distortion has been performed, we execute the NCD clustering method on each distorted test set and we quantitatively measure the error of the clustering results obtained. Finally, the Kolmogorov complexity of the distorted documents is estimated, based on the concept that data compression is an upper bound of the Kolmogorov complexity.

2.1 Replacement Methods

We use six different replacement methods, which are pairwise combinations of two factors: *word selection* and *substitution method*.

- Word selection: we incrementally select a percentage p, and we eliminate the p-*most/least/randomly* frequent words in English from the books. We estimate the frequencies of words in English using the British National Corpus [8].
- Substitution method: each character of the word that is distorted according to the word-frequency, is substituted by either a *random character* or an *asterisk*.

Note that all six combinations maintain the length of the document. This is enforced to ease the comparison of the Kolmogorov Complexity among several methods.

2.2 Assessing the Clustering

The CompLearn Toolkit [6] implements the clustering method described in [1]. The clustering method comprises two phases. First, the NCD matrix is calculated using the LZMAX compressor, a Lempel-Ziv-Markov chain Algorithm [9]. Second, the NCD matrix is used as input to the clustering phase and the so-called dendrogram is generated as an output. A dendrogram is an undirected binary tree diagram, frequently used for hierarchical clustering, that illustrates the arrangement of the clusters produced by a clustering algorithm.

In Fig 1 we can observe one of the dendrograms that we have obtained. Each leaf of the dendrogram corresponds to a document, and has a label that starts with the acronym of the author, and ends with the acronym of the title. For example, the node with label $AP.AEoM$ corresponds to the document *An Essay on Man* by Alexander Pope.

Once the CompLearn Toolkit is used to cluster the documents, we need to quantitatively evaluate the error of the dendrograms obtained. We define the distance between two nodes as the minimum number of internal nodes needed to go from one to the other. For example, in Fig 1 the distance between the nodes with label $WS.H$ and $WS.AaC$ would be one, since both nodes are connected to the same internal node. We use this concept to measure the error of a dendrogram.

We add all the pairwise distances between nodes starting with the same string, i.e. we add all the pairwise distances between the documents by the same author. For example, in Fig 1 there are three nodes which label starts with AP, thus we add the distance between $AP.AEoC$ and $AP.AEoM$, between $AP.AEoC$ and $AP.TRotLaOP$, and between $AP.AEoM$ and $AP.TRotLaOP$. We repeat this procedure with the nodes of each author, obtaining a certain total quantity. The bigger the measure, the worse the clustering.

The ideal dendrogram would be a clustering where all the documents by the same author are grouped together. The clustering error corresponding to the ideal dendrogram is 14 for these documents. Note that in Fig 1 the node with

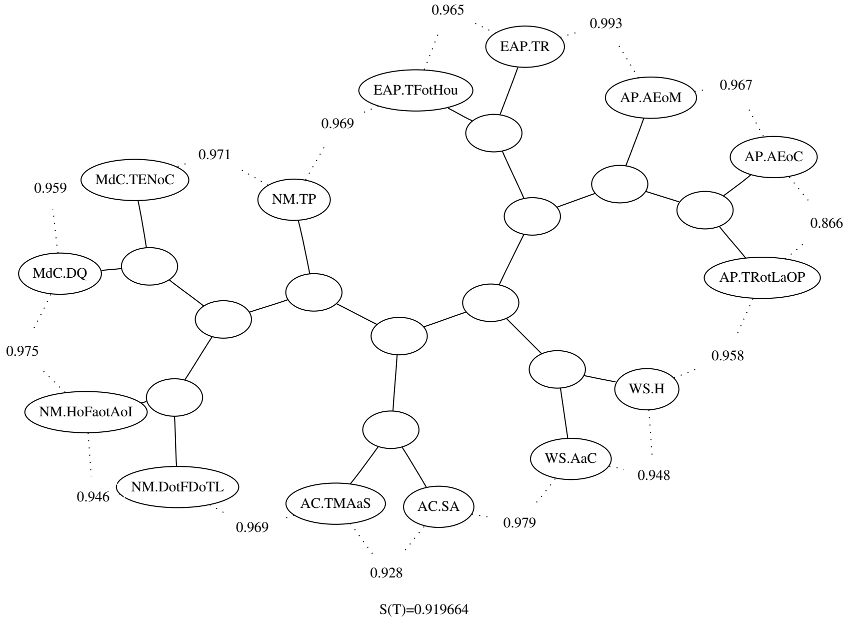


Fig. 1. Example of dendrogram

label *NM.TP* is clustered incorrectly. Thus, the clustering error corresponding to this dendrogram is 16 instead of 14.

The fact that this measure does not explicitly take into account pairwise distances between documents that should not be clustered together is implicitly taken into account due to the finite neighborhood of each node (three nodes in case of a dendrogram). In other words, the erroneous placement of a document near a document to which it is not related, reduces the number of nearby locations in which related nodes can be placed. This increases the distance between related nodes and has a negative effect upon the quality of the cluster.

3 Experiments and Results

The experiments have been designed to evaluate the impact of information distortion on NCD-driven text clustering by incrementally replacing words from the documents in different manners. We measure the error of the clustering in presence of distortion and compare it with two baselines: the ideal clustering, and the non-distorted NCD-driven clustering.

We have applied the NCD clustering method over a set of fourteen classical books written in English. We have two books by Agatha Christie: *The Secret Adversary*, and *The Mysterious Affair at Styles*. Three books by Alexander Pope: *An Essay on Criticism*, *An Essay on Man*, and *The Rape of the Lock, an heroic-comical Poem*. Two books by Edgar Allan Poe: *The Fall of the House of Usher*, and *The Raven*. Two books by Miguel de Cervantes: *Don Quixote*, and *The*

Exemplary Novels. Three books by Niccolò Machiavelli: *Discourses on the First Decade of Titus Livius*, *History of Florence and of the Affairs of Italy*, and *The Prince*. Two books by William Shakespeare: *The tragedy of Antony and Cleopatra*, and *Hamlet*.

We show the results of clustering the classical books when the six different replacement methods are used to preprocess them. Every figure plots the clustering error or the complexity of the books vs. a certain percentage of replaced words. The curve with asterisk markers represents the results obtained when the characters of the words are replaced with asterisks. The curve with square markers corresponds to the results obtained when random characters are used to replace the characters of the distorted words. Furthermore, two constant lines may appear in each figure. One corresponds to the measure in the ideal clustering and the other corresponds to the non-distorted NCD-driven clustering. The former is 14, the latter is 18.

In every graph, the value on the horizontal axis corresponds to the fraction of the total BNC frequency that is associated to the words being distorted. Note that even when all the words included in the BNC are replaced from the texts, the words that are not included in the BNC remain in the documents. For example, in the book *Don Quixote* by Miguel de Cervantes, words like *Dulcinea* or *Micomicona*, the names of two characters, remain in the documents when all the words of the BNC are distorted from the documents.

The clustering error vs. the percentage of replaced words is presented in Figs 2, 4 and 6, which show the results for the $X\%$-*most*/*randomly*/*least* frequent words respectively. Figs 3, 5 and 7 show the evolution of the complexity of the documents as a function of the same percentages.

In Fig 2 we observe that when the characters of the words are replaced with random characters the clustering error increases. When the characters are replaced with asterisks the clustering error remains stable. If we observe the curve with asterisk markers at 80% and 90%, we can see that the results are better than those obtained for the non-distorted documents, although they are not as good as those that would correspond to the ideal clustering.

Looking at Fig 3, we realize that the complexity of the documents rises when the substitution method is based on random characters. However, when it is based on asterisks the complexity of the documents decreases, because a great amount of characters from the documents are replaced with the same character, which increases the redundancy of the document and thus makes it more compressible.

Fig 4 shows the mean and the standard deviation of the results obtained in ten different experiments. The clustering error increases when random character substitution is applied. However, when asterisk substitution is applied the error keeps stable until 60%. From 60% to 100% the error increases. Comparing Figs 2 and 4 we observe that better results are obtained when we start disturbing the most frequent words. This makes us think that the frequency of the replaced words could affect the clustering.

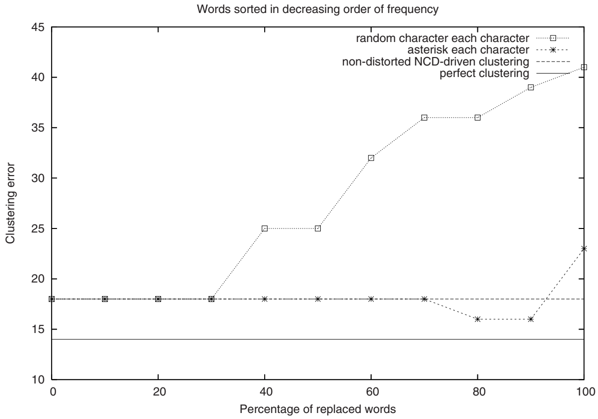


Fig. 2. Clustering error. Words sorted in decreasing order of frequency.

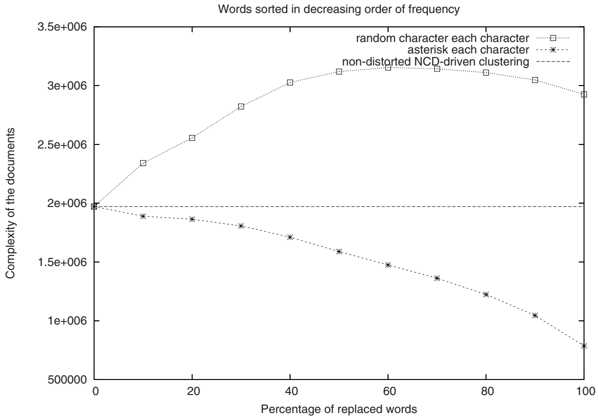


Fig. 3. Complexity of the documents. Words sorted in decreasing order of frequency.

The mean and the standard deviation of the complexity are presented in Fig 5, although the standard deviation is difficult to visualize due to the fact that its absolute value is very small as compared to the mean. Note that this graph decreases faster than the graph which represents the complexity when we start replacing the most frequent words, see Fig 3.

When the characters of the words are replaced with random characters, as shown in Fig 6, the clustering error increases faster than before, see Figs 2 and 4. When the words are replaced with asterisks the clustering error increases rapidly and then remains stable. This phenomenon could be due to the fact that when we start replacing the least frequent words, we replace precisely those words which carry the most information in terms of clustering compression.

When the substitution method is based on random characters, as shown in Fig 7, the complexity of the documents grows sharply compared to the evolution

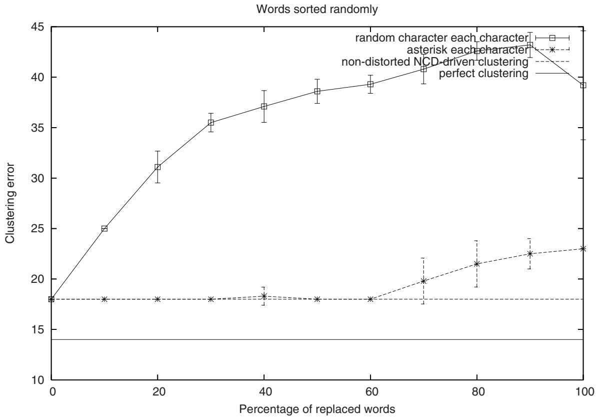


Fig. 4. Clustering error. Words sorted randomly (mean and standard deviation).

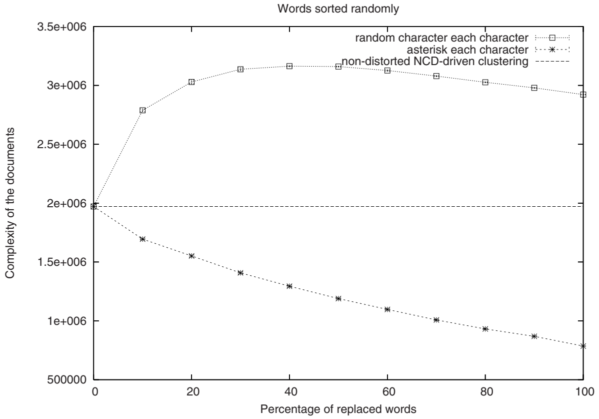


Fig. 5. Complexity of the documents. Words sorted randomly (mean and standard deviation).

observed in Figs 3 and 5. When the substitution method is based on asterisks the complexity of the documents decreases sharply as compared to the same figures. This is due to the fact that when we start disturbing the X%-least frequent words, lots of words are required to achieve the 10% of the BNC frequencies.

In order to give a better comparison we illustrate in Fig 8 the clustering error obtained when the words are replaced with asterisks for the three different word selections: *p-most*/*least*/*randomly* frequent words in English. We observe that the better results are obtained when we start distorting the *p-most* frequent ones, and the worst results are obtained then we start distorting the *p-least* frequent ones. When we select randomly the words the results remain between the others. These facts empirically demonstrate that the frequency of the words affects the clustering results when we cluster these books using the CompLearn Tool with the LZMAX compressor.

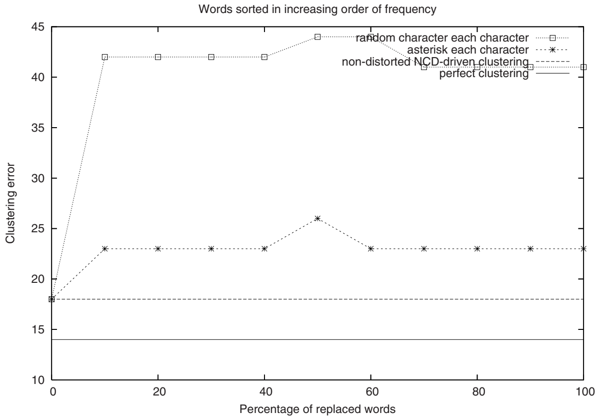


Fig. 6. Clustering error. Words sorted in increasing order of frequency.

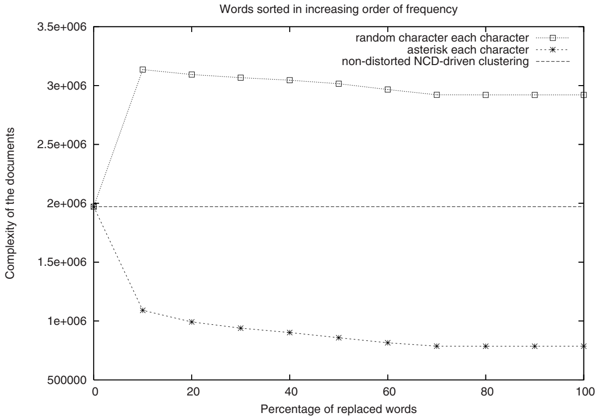


Fig. 7. Complexity of the documents. Words sorted in increasing order of frequency.

In an analogous way, the complexity of the documents for the three word selection techniques is depicted in Fig 9. Comparing Figs 8 and 9 we observe that document complexity and clustering error are negatively correlated. Thus, the best clustering results are obtained using the word selection that reduces the least the complexity of the documents.

To summarize, when random characters are used to replace the words in the text preprocessing phase, the error of the clustering method increases with the percentage of words removed, independently of the word selection used. When the words are replaced using asterisks the clustering error is always smaller than the one obtained when using random characters. Furthermore, the best clustering results are obtained when we select the most frequent words, and the substitution method is based on asterisks. In this case, for 80% and 90%, the results obtained from the original texts are improved. Moreover, comparing all

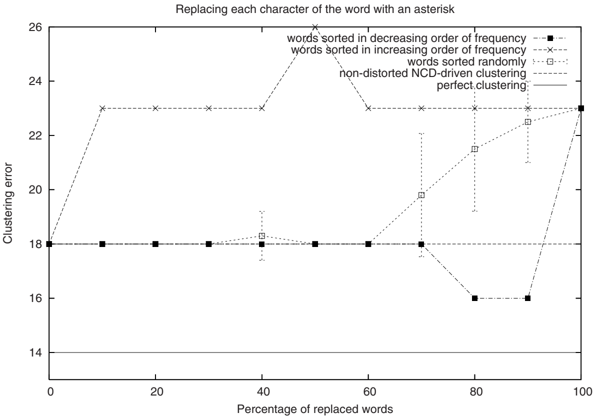


Fig. 8. Clustering Results. Asterisk each character of the replaced word.

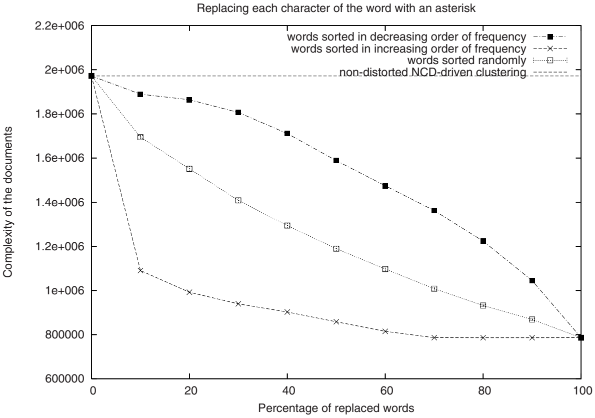


Fig. 9. Complexity of the documents. Asterisk each character of the replaced word.

the figures, it can be observed that the frequency of the removed words has an influence over the clustering error.

4 Conclusions and Discussion

We have applied the clustering method detailed in [1] to cluster several English classical books. We have studied how the clustering method is affected by different types of information distortion. In order to do that, we have measured the clustering error vs. the percentage of words distorted. The Kolmogorov complexity of the books has been estimated as well, to study the impact of the information distortion on the complexity of the documents.

Although several distortion methods have been designed, in this paper we have only considered those which maintain the initial length of the books to ease the comparison of the Kolmogorov complexity among them.

Three main contributions have been presented in this paper. First, we have made an empirical evaluation of the behavior of the NCD-driven clustering method, and the way in which an incremental modification of the books affects the clustering error. Second, we have presented a technique which reduces the Kolmogorov complexity of the books while preserving the relevant information therein. Third, we have observed experimental evidence of how to improve the NCD-clustering method by preprocessing the books in a certain manner.

The experimental results show how the clustering error is maintained even when the information contained in the documents is reduced progressively by replacing the words using a special character. We have found that replacing the most frequent words gives us the better clustering results. This method maintains the clustering error with very high values of distortion, and even improves the non-distorted NCD-driven clustering when the 80%-90% of the words are replaced from the documents, see Fig 2. This means that we are replacing exactly non-relevant parts of the books. This makes it easier for the compressor to estimate the complexity of the documents in an accurate manner. Therefore, the compressor obtains more reliable similarities.

Other techniques, such as randomly selecting the words to replace, or replacing the least frequent ones have been studied and analyzed. Despite the complexity of the documents being reduced too (see Figs 5, and 7), the clustering error increases faster (see Figs 4, and 6). Thus, the information that has been replaced is relevant in the clustering process, and consequently we are losing important information. Therefore, the similarities among the documents are not being correctly measured.

In the future, we plan to work in several ways to study the observed behavior in other textual repositories, like scientific documentation, or genome-based repositories. However, the NCD-based clustering is a general technique so it is possible to use other kinds of sources, such as, music or video. In these domains it would be necessary to analyze how the distortion method could be designed. Other well-known compression algorithms, like PPMZ, BZIP2 or GZIP, will be analyzed to evaluate if the complexity estimation affects the clustering behavior as much as it does in other NCD-driven experiments [10]. Finally, we will apply these techniques in other areas like Information Retrieval.

Acknowledgment

This work was supported by TIN 2004-04363-CO03-03, TIN 2007-65989, CAM S-SEM-0255-2006, TIN2007-64718 and TSI 2005-08255-C07-06. We would also like to thank Francisco Sánchez for his useful comments on this draft.

References

1. Cilibrasi, R., Vitanyi, P.: Clustering by compression. IEEE Transactions on Information Theory 51(4), 1523–1545 (2005)
2. Turing, A.: On computable numbers, with an application to the entscheidungsproblem. Proceedings of the London Mathematical Society 2(42), 230–265 (1936)
3. Kolmogorov, A.: Three approaches to the quantitative definition of information. Problems Information Transmission 1(1), 1–7 (1965)
4. Li, M., Vitányi, P.: An introduction to Kolmogorov complexity and its applications. Graduate Texts In Computer Science, p. 637. Springer, Heidelberg (1997)
5. Sipser, M.: Introduction to the Theory of Computation, 2nd edn. PWS Publishing (2006)
6. Cilibrasi, R., Cruz, A.L., de Rooij, S., Keijzer, M.: CompLearn Toolkit, http://www.complearn.org/
7. Cebrián, M., Alfonseca, M., Ortega, A.: The normalized compression distance is resistant to noise. IEEE Transactions on Information Theory 53(5), 1895–1900 (2007)
8. Consortium, B.N.C.: British National Corpus. Oxford University Computing Services, http://www.natcorp.ox.ac.uk/
9. Pavlov, I.: LZMA, http://www.7-zip.org/sdk.html
10. Cebrián, M., Alfonseca, M., Ortega, A.: Common pitfalls using normalized compression distance: what to watch out for in a compressor. Communications in Information and Systems 5(4), 367–384 (2005)

Codes from Expander Graphs

Tom Høholdt

Department of Mathematics
Technical University of Denmark
T.Hoeholdt@mat.dtu.dk

Abstract. We survey some recent work on codes based on bipartite expander graphs. The code symbols are associated with the branches and the symbols connected to a given node are restricted to be codewords in certain constituent codes (e.g. Reed–Solomon codes). This class turn out to contain some exellent codes. We give results on the parameters of the codes and methods for their encoding. We also analyze the performance under iterative decoding, partly based on a result on cores in random graphs.

References

1. Zèmor, G.: On expander codes. IEEE Trans. Inform. Theory (Special Issue on Codes on Graphs and iterative Algorithms) 47, 835–837 (2001)
2. Barg, A., Zèmor, G.: Error exponents of expander codes. IEEE Trans. Inform. Theory 48, 1725–1729 (2002)
3. Tanner, M.: A Recursive Approach to Low Complexity Codes. IEEE Trans. Inform. Theory 27, 533–547 (1981)
4. Tanner, M.: Explicit Concentrators from Generalized N–Gons. SIAM J. Alg. Disc. Meth. 5(3), 287–293 (1984)
5. Tanner, M.: Minimum-Distance Bounds by Graph Analysis. IEEE Trans. Inform. Theory 47, 808–821 (2001)
6. Sipser, M., Spielman, D.A.: Expander Codes. IEEE Trans. Inform. Theory 42(6), 1710–1722 (1996)
7. Roth, R.M.: Introduction to Coding Theory. Cambridge University Press, Cambridge (2006)
8. Janwa, H., Lal, A.K.: On Tanner Codes: Minimum Distance and Decoding. In: AAECC, vol. 13, pp. 335–347 (2003)
9. Roth, R.M., Skachek, V.: Improved Nearly-MDS Expander Codes. IEEE Trans. Inform. Theory 52(8), 3650–3661 (2006)
10. Feit, W., Higman, G.: The nonexistence of certain generalized polygons. J. Algebra 1, 114–131 (1964)
11. van Maldeghem, H.: Generalized Polygons. Birkhäuser, Basel (1998)
12. McEliece, R., Swanson, L.: On the error probability for Reed-Solomon codes. IEEE Trans. Inform. Theory 32, 701–703 (1986)
13. Pittel, B., Spencer, J., Wormald, N.: Sudden emergence of a giant k-core in a random graph. J. Comb. Theory, Series B 67, 11–151 (1996)
14. Janson, S., Luczak, M.J.: A simple solution to the k-core problem. Random Structures Algorithms 30(1-2), 50–62 (2007)

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 80–81, 2008.

15. Høholdt, T., Justesen, J.: Graph codes with Reed-Solomon component codes. In: Proceedings ISIT 2006, Seattle, Washington, July 2006, pp. 2022–2026 (2006)
16. Høholdt, T., Justesen, J.: Iterative decoding of product codes and graph codes with Reed-Solomon component codes. In: Proceedings ITW 2007 (September 2007)
17. Høholdt, T., Justesen, J.: Graph Codes with Reed-Solomon Component Codes. In: IEEE Trans. Inform. Theory (March 2008) (submitted)

Adaptive Soft-Decision Iterative Decoding Using Edge Local Complementation

Joakim Grahl Knudsen, Constanza Riera, Matthew G. Parker, and Eirik Rosnes

Dept. of Informatics, University of Bergen, Thormøhlensgt. 55, 5008 Bergen, Norway
{joakimk,riera,matthew,eirik}@ii.uib.no

Abstract. We describe an operation to dynamically adapt the structure of the Tanner graph used during iterative decoding. Codes on graphs–most importantly, low-density parity-check (LDPC) codes–exploit randomness in the structure of the code. Our approach is to introduce a similar degree of controlled randomness into the operation of the message-passing decoder, to improve the performance of iterative decoding of classical structured (i.e., non-random) codes for which strong code properties are known. We use ideas similar to Halford and Chugg (IEEE Trans. on Commun., April 2008), where permutations on the columns of the parity-check matrix are drawn from the automorphism group of the code, Aut($\mathcal{C}$). The main contributions of our work are: 1) We maintain a graph-local perspective, which not only gives a low-complexity, distributed implementation, but also suggests novel applications of our work, and 2) we present an operation to draw from Aut($\mathcal{C}$) such that graph isomorphism is preserved, which maintains desirable properties while the graph is being updated. We present simulation results for the additive white Gaussian noise (AWGN) channel, which show an improvement over standard sum-product algorithm (SPA) decoding.

1 Introduction

Inspired by the success of iterative decoding of LDPC codes, originally introduced by Gallager [1] and later rediscovered in the mid 1990's by MacKay and Neal [2], on a wide variety of communication channels, the idea of iterative, soft-decision decoding has recently been applied to classical algebraically constructed codes in order to achieve low-complexity Belief Propagation decoding [3,4,5]. Both Reed-Solomon and Bose-Chaudhuri-Hocquenghem (BCH) codes have been considered in the context of iterative decoding. Certain algebraically constructed bipartite graphs are known to exhibit good code properties, such as large minimum distance and a non-trivial automorphism group. However, these typical 'classical properties' do not necessarily lend themselves well to modern graph-based coding theory. Factors which influence the performance of iterative, soft-decision decoders are pseudo-codewords [6], stopping and trapping sets [7,8], sparsity, girth, and degree distributions [9]. Structural weaknesses of graphical codes are inherent to the particular parity-check matrix, H, which can be said to implement the code in the decoder. This matrix is a non-unique

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 82–94, 2008.

$(n-k)$-dimensional basis for the null space of the code, $\mathcal{C}$, which, in turn, is a k-dimensional subspace of $\{0,1\}^n$. Although any basis (for the dual code, $\mathcal{C}^\perp$) is a parity-check matrix for $\mathcal{C}$, their performance in decoders is not uniform. In this work, we assume that H is of full rank and in 'standard' $[\,I\,|\,P\,]$-form, where I is the identity matrix.

We propose a class of adaptive decoders which facilitate message-passing on classical linear codes, by taking advantage of (non-trivial) graph structure. It is well known that H can be mapped into a bipartite (Tanner) graph, $\mathbf{TG}(H)$, which is described by its adjacency matrix, $\begin{pmatrix} 0 & H \\ H^T & 0 \end{pmatrix}$. With H being in standard form, a specific information set (on the codeword positions) is implied. We will refer to bit nodes (i.e., columns of H) corresponding to I and P as 'parity' and 'information' nodes, respectively,[1] and rows of H correspond to 'constraint' (check) nodes. Using a localized, low-complexity graph edge-operation, we update the parity-check matrix, but still stay within the automorphism group of the code, $\mathrm{Aut}(\mathcal{C})$. Thus, the graph update rule can be viewed as a particular relabelling (isomorphism) of the bit nodes. Furthermore, by selectively or randomly shifting sensitive substructures (e.g., short cycles, or weight-1 nodes) within the graph, we aim to influence the flow of extrinsic information through $\mathbf{TG}(H)$ in a way helpful to the decoding process.

In a recent paper by Halford and Chugg, "random redundant iterative decoding" is achieved by applying permutations drawn at random from $\mathrm{Aut}(\mathcal{C})$ [5]. Rather than applying these permutations to H, the same effect is achieved by permuting the soft input vector. While their strategy is perceived to be a series of global updates, our approach achieves a similar effect by using only local updates on $\mathbf{TG}(H)$. In our characterization of locality, we assume that an edge can not 'see' beyond a radius of a constant number of edges. Similarly to [5], permutations can be drawn from a precomputed list input to the decoder. However, our distributed approach also allows us to dispense with precomputation, to realize a completely distributed and local graph update rule, which, nevertheless, keeps the series of graphs generated within $\mathrm{Aut}(\mathcal{C})$.

2 Edge Local Complementation

The operation of edge local complementation (ELC) [10,11,12], also known as Pivot, is a local operation on a simple graph. Fig. 1(a) shows $G_{\mathcal{N}_u \cup \mathcal{N}_v}$, the local subgraph of a bipartite graph induced by nodes u, v, and their disjoint neighborhoods which we denote $\mathcal{N}_u^v \triangleq \mathcal{N}_u \setminus \{v\}$ and $\mathcal{N}_v^u \triangleq \mathcal{N}_v \setminus \{u\}$, respectively.

Pivot on a bipartite graph is described as the complementation of edges between these two sets; $\forall\ v' \in \mathcal{N}_u^v,\ u' \in \mathcal{N}_v^u$, check whether edge $(u', v') \in G$, in which case it is deleted (otherwise, it is created). Finally, the edges adjacent to u and v are swapped. As such, Pivot updates the set of constraints (rows of H) by changing the edges of $\mathbf{TG}(H)$, whereas nodes are invariant. The complexity of the graph-based algorithm is $\mathcal{O}(\deg(u)\deg(v))$. The fact that Pivot amounts to row

[1] Note that these terms refer to the generator matrix of the code, $G_{\mathcal{C}} \triangleq \left[\, P^T \,|\, I_k \,\right]$.

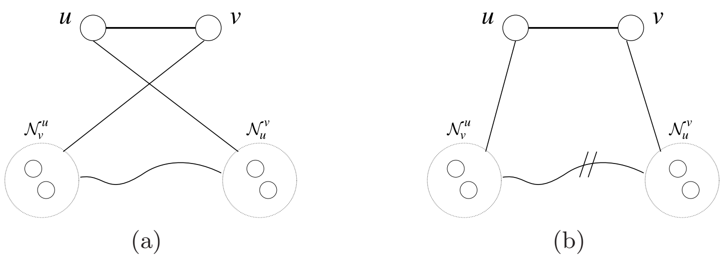


Fig. 1. Pivot (ELC) on edge (u, v) of a bipartite graph. Doubly slashed links mean the edges connecting two sets have been complemented.

additions assures that the code is preserved. In the following, we use the notation G^i to denote a graph G that has been subject to i Pivots (similarly for H^i).

Consider the simple, n-node bipartite graph described by $G = \begin{pmatrix} 0 & P \\ P^T & 0 \end{pmatrix}$. This graph is related to $\mathbf{TG}(H)$ by the abstraction of degree-1 parity nodes, as shown in Figs. 2(a) - 2(b). Keeping track of the bipartition of G (which changes due to the swap), means we can obtain an associated parity-check matrix, H^1, for $\mathcal{C}$ by mapping grey nodes onto rows (constraint nodes), and white nodes to columns (bit nodes), with non-zero entries according to edges. While the mapping of bit nodes must follow the prescription of the labelling of G (i.e., the code), the ordering of rows is arbitrary.

The local application of Pivot has the global effect of row additions on the associated H, thus preserving the bipartiteness and vector space (i.e., $\mathcal{C}$) [12]. Consider again Fig. 1, where we choose u to be a constraint node, and v a bit node. With this setup, Pivoting on edge (u, v) is equivalent to adding 'row u' to rows $u' \in \mathcal{N}_v^u$ (as dictated by the non-zero entries of 'column v'). Since H is in standard form, an immediate effect of Pivoting on some edge (c, p) is that the edges adjacent to information node, p, are swapped with that of the degree-1 parity node adjacent to the constraint node, c, as seen in Fig. 2 (b,e). As opposed to [5], we are permuting H, whereas the soft input vector remains invariantly connected to (the bit nodes of) $\mathbf{TG}(H)$. The indices of Fig. 2 show how the order of the soft input vector is preserved. Extrinsic information is lost on edges deleted in the local complementation. However, SPA update rules are such that these messages remain stored in adjacent bit nodes as *a posteriori probabilities* (APPs) [13].

As can be readily verified, although Pivot preserves the code, it can have a negative impact on parameters of its implementation, H, as a decoder. Edges complemented are at distance 2 from (u, v), so for a typical sparse, girth-6 graph, many 4-cycles result, and density increases [14]. Pivot does not generally preserve graph isomorphism (structure), so the operation will often given us a different structure in the (Pivot) *orbit* of G [15]. The matrices H^i in this orbit are the set of structurally different parity-check matrices for the same code, as discussed in the Introduction. We briefly mention that all information sets of $\mathcal{C}$ may be enumerated by traversing this orbit of G [11].

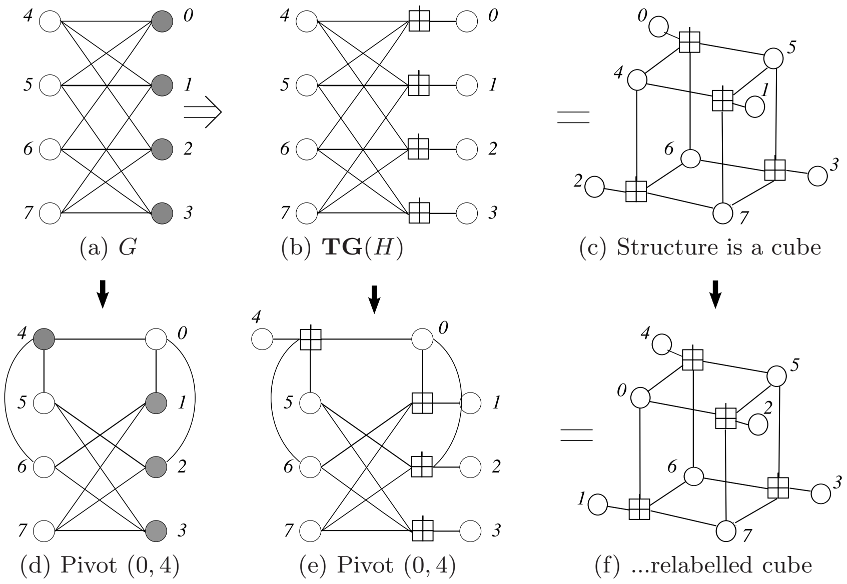


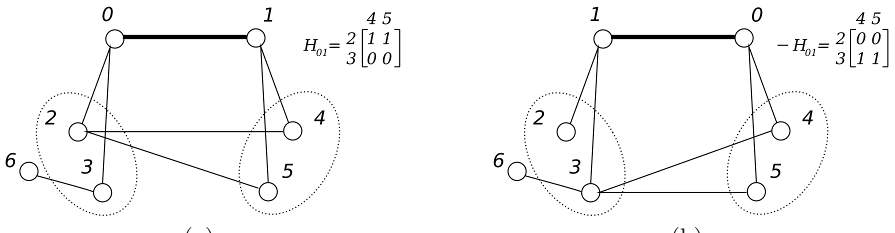
Fig. 2. (a) through (c) are three equivalent representations of the $(8, 4)$ extended Hamming code. (d) through (e) show the corresponding representation after Pivot is applied to edge $(0, 4)$. Fig. 5 shows the parity-check matrices of (b) and (e), respectively.

2.1 Iso-Pivot

In this section we describe an application of Pivot to preserve key features of the graph, to remedy the drawbacks enumerated in the previous section. We define Iso-Pivot as a sequence of Pivot operations over which (global) graph isomorphism is preserved. Such an operation will be in $\mathrm{Aut}(\mathcal{C})$, in that its action has the appearance of a relabelling on the nodes of a graph, or–equivalently–a permutation on the columns of a matrix (H). If there exist sequences of Pivots which preserve the structure of G, then $\mathrm{Aut}(\mathcal{C})$ must be non-trivial. Isomorphism is a certificate on the properties of the resulting graphs (matrices) used during decoding; that these remain the same as for the initial G (H), which can be assumed to have been carefully selected. The relabelling, however, alters the flow of messages in $\mathbf{TG}(H)$, i.e., which nodes are exchanging information. Note in particular how, after the Iso-Pivot in Fig. 2(f), node 4 is no longer part of a 4-cycle (whereas node 0 now is).

In the following, we derive three requirements for Pivot being an isomorphism.

A. Most generally, to have an isomorphism, the number of edges in G must remain invariant under Pivot. Pivot is a local operation, so we only have to consider the subgraph $G_{\mathcal{N}_u \cup \mathcal{N}_v}$. Edge complementation can then be achieved by complementing the corresponding $\deg(u) \times \deg(v)$ submatrix, H_{uv}. Define $\mathrm{wt}(H)$ as the weight (number of non-zero entries) of H. In order for


0
1
$H_{01} = \begin{array}{c|cc} & 4 & 5 \\ \hline 2 & 1 & 1 \\ 3 & 0 & 0 \end{array}$
2
3
4
5
6
1
0
$-H_{01} = \begin{array}{c|cc} & 4 & 5 \\ \hline 2 & 0 & 0 \\ 3 & 1 & 1 \end{array}$
2
3
4
5
6

(a) (b)

Fig. 3. Pivot on $(0, 1)$ is (A) edge-count preserving and (B) a local isomorphism, but not (C) a global isomorphism due to node 6. This node is not local to the Pivot edge.

$\text{wt}(H_{uv}) = \text{wt}(\overline{H_{uv}})$, at least one of the dimensions must be an even number, and $\text{wt}(H_{uv})$ must equal $uv/2$. If these conditions are met, we define the Pivot operation as *edge-count preserving.*

B. More specifically, we define a *local isomorphism* as an operation which preserves the structure of subgraph $G_{\mathcal{N}_u \cup \mathcal{N}_v}$, without making any assumptions on the overall (global) structure of G. We then define the Pivot operation to be *local Iso-Pivot iff* H_{uv} can be recovered from $\overline{H_{uv}}$ by row/column permutations only. Fig. 3 shows a small example.

C. Finally, most specifically, we say that Pivot is a (global) *Iso-Pivot iff* H can be restored from H^1, using only row/column permutations, considering the entire matrix.

These requirements lead to the following observation,

$$C \Rightarrow B \Rightarrow A.$$

In the following, we will consider global isomorphisms only, and we will refer to such sequences as as simply being Iso-Pivot operations, or sequences.

2.2 Iso-Orbit

The definitions of Iso-Pivot are naturally extended to the case where a single Pivot can not by itself be an isomorphism. Consider, for instance, a girth-6 graph. Here, the local neighborhood (of any edge) must be empty, and, after a single Pivot, this neighborhood becomes a complete (bipartite) (sub)graph at distance 2 from the Pivot edge (all 4-cycles). This violates requirement A, and the resultant graph can not be isomorphic to the initial one–neither locally, nor globally.[2]

In the general case, Iso-Pivot is described as an ordered set of d edges on which Pivot must be applied to achieve an isomorphism. This is referred to as a d-iso sequence (or, a length-d iso sequence). The set of all isomorphisms of G (reachable via Iso-Pivot, for $d \geq 1$) is called the *Iso-Orbit* of G, which

[2] This is also evident simply from the change in girth.

corresponds to a subset of $\mathrm{Aut}(\mathcal{C})$. Pivot can be used, in a preprocessing stage, to recursively search for Iso-Pivot sequences. For each such relabelling of G, we keep the corresponding iso sequence leading to it. Since Pivot is reversible, identical isomorphisms may be found via sequences of different length, and involving different edges, where certain operations cancel each other out. As such, for each unique labelling, we keep only the minimum length sequence in the Iso-Orbit.

From a decoding perspective, row permutations of H give the same $\mathbf{TG}(H)$. By canonising the rows of H (in our case, sorting according to decimal value of the binary rows), we ensure that the Iso-Orbit contains only non-trivial isomorphisms of G. The complexity of this search is $\mathcal{O}(n|\mathrm{Aut}(\mathcal{C})|)$, where G has n nodes, so for strongly structured (and large) graphs it may be necessary to bound the recursion with a maximum depth, d_{max}. This possibly partial Iso-Orbit is then simply referred to as the d-Iso-Orbit of G.

2.3 Local Iso Criterions

Although the message-passing decoder can be provided with $\mathbf{TG}(H)$ and a list of iso-sequences, to facilitate adaptive decoding, our stated graph local approach lends itself to *ad hoc* determination of iso-sequences during decoding. In this subsection, we describe some 1-iso conditions which ensure that Pivoting on the single edge (u, v) of G gives an isomorphism of G.

From a local perspective, an edge (u, v) can sometimes determine whether or not (global) structure will be preserved if it applies a Pivot. This edge may only examine its local subgraph, $G_{\mathcal{N}_u \cup \mathcal{N}_v}$. In this manner, we alleviate both the potentially expensive preprocessing stage, as well as the overhead of storing and permuting a list of sequences. Where a local criterion is satisfied, (u, v) may remain unaware of the implicit (iso) permutations that occur–except from the fact that (u, v) remains invariant–hence the term, Pivot.

We define $\ominus$ as the symmetric difference, i.e., for sets A and B, $A \ominus B \triangleq (A \setminus B) \cup (B \setminus A)$.

Lemma 1. *Pivoting on the edge (u, v) of a simple bipartite graph, G, preserves G up to local graph isomorphism if and only if at least one of the sets $\mathcal{N}_u^v$ and $\mathcal{N}_v^u$ satisfy one of the following conditions, with $\{\alpha, \alpha'\} = \{u, v\}$,*

- *$\exists\ \alpha$, α' such that $\mathcal{N}_\alpha^{\alpha'} = \emptyset$, or*
- *$\exists\ \alpha, \alpha'$ such that $\mathcal{N}_\alpha^{\alpha'}$ can be partitioned in pairs $\{w_i, w_i'\}$, where $\mathcal{N}_{w_i} \ominus \mathcal{N}_{w_i'} = \mathcal{N}_{\alpha'}^{\alpha}$ $\forall i, \{w_i, w_i'\} \cap \{w_j, w_j'\} = \emptyset, i \neq j$.*

Global isomorphism can be ensured by the condition that the subgraphs induced by $\mathcal{N}_\alpha^{\alpha'}$ and their neighbors, and $\mathcal{N}_{\alpha'}^{\alpha}$ and their neighbors, are both bipartite complete graphs. Less restrictive conditions will also ensure global isomorphism, depending on the permutation of the vertices of the graph.

Proof. – Either $\mathcal{N}_u^v = \emptyset$, or $\mathcal{N}_v^u = \emptyset$. Let $\mathcal{N}_u^v = \emptyset$. Then Pivot on (u, v) has the effect of disconnecting v from $\mathcal{N}_v^u$, while connecting u to $\mathcal{N}_v^u$. The permutation that gives us the isomorphism is $\sigma = (u\ v)$. The same permutation applies when $\mathcal{N}_v^u = \emptyset$.

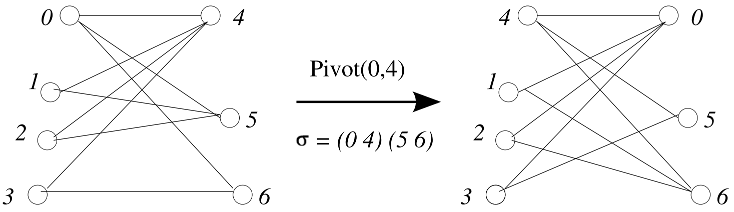


Fig. 4. Example of Lemma 1, where $\alpha = 0,\ \alpha' = 4,\ w_0 = 5,$ and $w_0' = 6$. These graphs are isomorphic.

- For every $w_i \in \mathcal{N}_{\alpha}^{\alpha'}, \exists\ w_i' \in \mathcal{N}_{\alpha}^{\alpha'}$ such that $\mathcal{N}_{w_i} \ominus \mathcal{N}_{w_i'} = \mathcal{N}_{\alpha'}^{\alpha}$: The permutation that gives us the isomorphism is $\sigma = (u\ v) \prod (w_i\ w_i')$. □

An example of Lemma 1 is found in Fig. 4.

As any individual Pivot operation complements edges local to u and v (i.e., 4-cycles), we say that 1-iso 'sequences' can only exist for graphs of girth 4, or locally acyclic (tree) graphs for which the first part of Lemma 1 applies. Similar criteria have been identified for $d = 2$, but these were not applied in this initial work.

3 Structure of the (8, 4) Extended Hamming Code

The $(8, 4)$ extended Hamming code is a well-suited test case for adaptive decoding; it has strong classical properties (large automorphism group and minimum distance), yet for any implementation H it is ill-suited for message-passing (dense, and many 4-cycles). We acknowledge that this is a toy code, which presents obvious difficulties in arguing any sense of 'locality' of such a small graph. However, the positive nature of our results show that this code does suffice as motivation for the proposed class of adaptive decoders, and we direct the reader to the Future Work section of this article.

The associated graph has one structure in its (non-iso) orbit; the cube of Fig. 2(c), meaning that its structure is so strong that any edge of any G^i satisfies Lemma 1 (is an Iso-Pivot). Starting from G as in Fig. 2(b), with parity-check matrix in Fig. 5(a), we find the Iso-Orbit of the graph. Grouped by length, $d = 1$ to 4, this orbit consists of 12, 30, 12, and 1 isomorphisms, respectively, all

$$H = \begin{bmatrix} 1\,0\,0\,0\,1\,1\,1\,0 \\ 0\,1\,0\,0\,1\,1\,0\,1 \\ 0\,0\,1\,0\,1\,0\,1\,1 \\ 0\,0\,0\,1\,0\,1\,1\,1 \end{bmatrix}$$

(a) Standard form

$$H' = \begin{bmatrix} 1\,0\,0\,0\,1\,1\,1\,0 \\ 1\,1\,0\,0\,0\,0\,1\,1 \\ 1\,0\,1\,0\,0\,1\,0\,1 \\ 0\,0\,0\,1\,0\,1\,1\,1 \end{bmatrix}$$

(b) Pivot $(0, 4)$

Fig. 5. The $(8, 4)$ extended Hamming code, implemented by its standard form parity-check matrix (a), and an isomorphism (b)

resembling a cube. Including the initial labelling, this sums up to 56 structurally distinct, non-trivial parity-check matrices for the code.[3] Necessarily, the 12 1-iso sequences correspond to the 12 edges of G (P-part of H).

4 Simulation Results

The adaptive decoder has been tested in two instances, and compared against a SPA decoder using standard flooding scheduling on output $\mathbf{y}$ from the AWGN channel.[4] During implementation we made sure that all decoders were allocated an equal maximum number of iterations ($T = 100$). In the following description, we assume an initial syndrome check has failed, so we have a vector to input to the decoder.[5]

Due to the symmetry of the $(8, 4)$ code in standard form, we know any Pivot will preserve isomorphism. Thus, when considering the adaptive decoders presented and analyzed in the following, the reader is encouraged to think of these as truly localized (i.e., independent of preprocessing and input lists), as if these were determined *ad hoc*. In comparison, Halford and Chugg [5] are applying (non-local) permutations drawn at random from the full automorphism group of the code. They also restrict to a cyclic subgroup of $\mathrm{Aut}(\mathcal{C})$–we do not do this. As discussed, our use of Iso-Pivot naturally gives a subgroup of $\mathrm{Aut}(\mathcal{C})$.

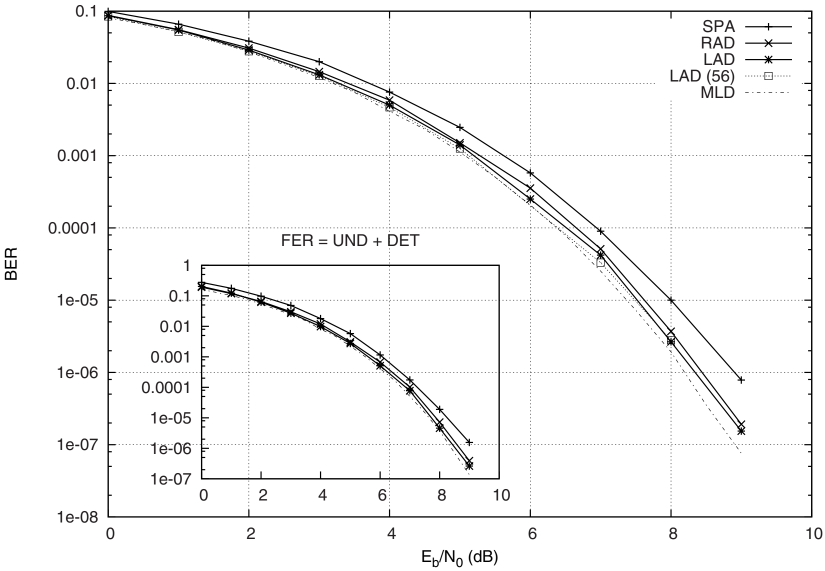
The *random adaptive decoder* (RAD) is a (flooding) SPA decoder, but which is designed to adapt (via random Iso-Pivot) to another G^i, with regular iteration interval, t. The decoder stops as soon as the syndrome check is satisfied (valid codeword, though not necessarily the one sent), or when T iterations are exhausted (detected frame error). In a localized manner, this decoder performs a random walk (with repetitions) in the Iso-Orbit of G, taking advantage of the discussed symmetry. As such, the 'range'–number of matrices available to this decoder–includes all 56 non-trivial isomorphisms.

The *list adaptive decoder* (LAD) is an extension of this idea, but where we apply Iso-Pivot operations from a precomputed list, $L \subseteq \text{Iso-Orbit}(G)$. In addition to the initial labelling, the range of this decoder is $D = |L| + 1$. A pool of T flooding iterations is allocated. Graph G^i, $0 \leq i < D$, is allocated $h_i = \lceil (T - I)/(D - i) \rceil$ iterations to come to a decoder decision, where I is the total number of iterations used by previous decoders G^j, $j < i$. Depending on T and L, h_i may go to 0, so an overall minimum, h_{min}, should be set. This means that, although the list L may not be employed in its entirety, we ensure that the graphs used are doing useful work (more than 1 iteration). This

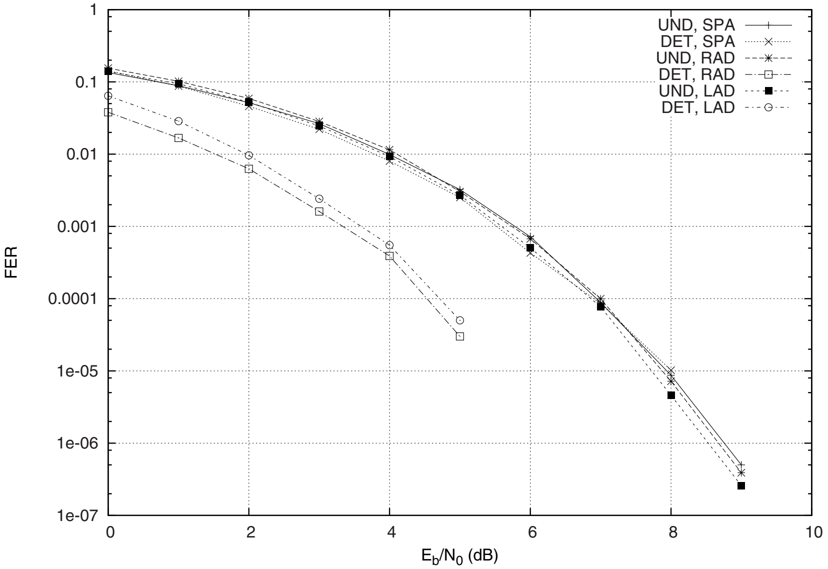
[3] Note that the full automorphism group of this code may be found by row permutations on these generators; $56 \cdot 4! = 1344 = |\mathrm{Aut}(\mathcal{C})|$.

[4] One flooding iteration consists of the SPA update of all bit (information and parity) nodes, followed by the update of all constraint nodes.

[5] For locality, we emphasize that constraint nodes of $\mathbf{TG}(H)$ can be viewed as $[n, n-1, 2]$ component parity-check codes, which can be computed (checked) concurrently and distributively. However, a stopping criterion for the whole code is inherently a global decision.



(a) Our class of decoders (both RAD and LAD) outperform SPA, both in BER and FER. Only a small improvement was seen when using the entire Iso-Orbit, LAD(56).



(b) DETected (timeouts) and UNDetected frame errors compared separately. A significant gain is found in the class of detected word errors.

Fig. 6. Simulations results on an AWGN channel. Maximum $T = 100$ iterations used. $t = 10$ for RAD, and $|L| = 12$ for LAD. At least 100 detected and 100 undetected frame errors were sampled for each E_b/N_0 point.

minium should reflect parameters of the graph and code. Before applying the next Iso-Pivot from L, G^i compares its local decision to a running optimum kept in the decoder, and overwrites if a better decoder output is found (in squared Euclidean distance from $\mathbf{y}$). This comparison is devised to favor valid decoder states, in that distance measures of detected failures are only considered as long as no valid state has been found. The LAD does not stop on reaching a valid decoder state, but continues until "timeout" (T iterations). The final graph, G^δ, $\lfloor T/h_{\text{min}} \rfloor \leq \delta \leq D-1$, outputs the optimum decision as the decoder result. In case no graph found a valid syndrome, the error state nearest to $\mathbf{y}$ (of the δ timeout states) was output. This is in an effort to reduce the bit-error contribution.

Fig. 6 benchmarks the performance of RAD/LAD against standard SPA and the optimal maximum likelihood decoder (MLD), in terms of bit-error rate (BER) and frame-error rate (FER), where an improvement is seen. The LAD plot is slightly nearer to the optimal MLD plot than the RAD, but the gain is not significant compared to the complexity tradeoff (Fig. 7). A detailed look at the (detected and undetected) frame errors, Fig. 6(b), reveals that adaptive decoders outperform SPA in terms of detected errors (timeout), where RAD shows the best gain. The RAD performs a random walk around the 56 sequences in the Iso-Orbit of G, while, for the LAD, we chose the subset of 12 1-iso sequences (defined by the 12 edges of the initial G) such that $h_{\text{min}} = \lceil 100/13 \rceil = 7$.

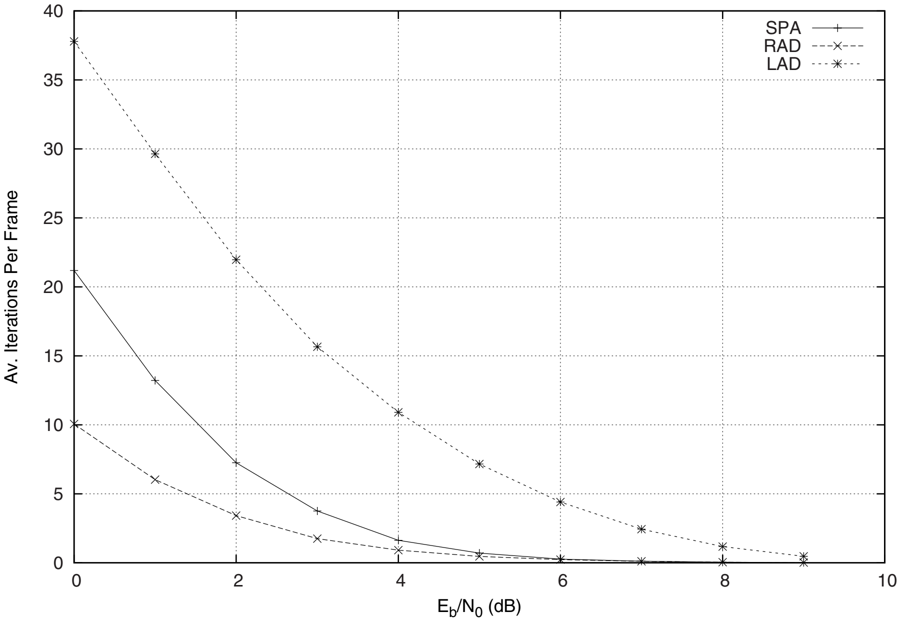


Fig. 7. The total number of iterations used (where timeout states contribute T iterations, and error-free frames contribute 0) averaged over total number of simulated frames

Only a small additional gain was achieved by using the full Iso-Orbit. In this case, we used the same minimum as for the LAD; $h_{\text{min}} = 7$ iterations. This means that not all 56 sequences were guaranteed to be used, so we permuted the order of sequences in L before every decoding instance. As such, in the cases where the graphs did non-negligible work (i.e., there were channel errors), on average each graph ran all its h_{min} iterations. Hence, we may say that 13 random Iso-Pivot operations (sequences) were applied at random from the Iso-Orbit of G. The simulation 'LAD(56)' in Fig. 6(a) demonstrates the benefit of using the entire Iso-Orbit, albeit slim for this small code.

Fig. 7 shows the complexity (average number of flooding iterations used) of the decoders, where we observe another improvement of RAD over SPA and LAD decoding. At high E_b/N_0, complexity averages go to 0, which is due to the majority of received frames satisfying the initial syndrome check (which we do not count as an iteration). While LAD expectedly uses a higher average number of iterations, since it does not stop at the first valid syndrome, an interesting observation is the complexity gain of RAD, which is linked to the reduction in number of timeouts (detected frame errors–see Fig. 6(b)).

5 Conclusion and Future Work

We have described and tested a class of adaptive iterative decoders, which dynamically update the edge-space of the code implementation, $\mathbf{TG}(H)$, using local decisions and operations. Concrete 'iso-criterions' are described and mathematically proven, and simulations on the AWGN channel show a gain when using our ideas. Two related instances of our class of adaptive decoders are described, where we conclude that, although LAD is slightly better than RAD in terms of BER, that gain comes at a cost of increased complexity (average number of iterations used) and loss of locality. Furthermore, RAD outperforms LAD in terms of FER, which gives an interesting latency reduction.

As Iso-Pivot rotates sensitive substructures in $\mathbf{TG}(H)$, we expect a gain in selectively applying Iso-Pivot based on local convergence assessments (e.g., using entropy or reliability measures). We mention shifting short cycles away from unreliable bit nodes–as seen in the cube of Fig. 2. Pivoting adjacent to unreliable positions also causes these to become temporarily 'isolated' in terms of message-passing (weight-1 node), such that these are set in a 'listening state,' rather than confusing the adjacent nodes with its (presumed) unreliable APP [16,17,3]. In our scheme, we achieve this effect without the overhead of Gaussian elimination.

Local iso-criterions for $d = 2$ have been identified, and we are also working on further generalizations. This is interesting, as, due to the link between Pivot and 4-cycles, girth-6 graph isomorphisms can not be preserved with less than 2 Pivots. Our results on global isomorphisms indicate that it is not trivial to find graphs which exhibit a non-empty Iso-Orbit, which simultaneously are good codes (i.e., sparse and girth greater than 4). A reasonable next step is a more methodical search through all codes up to some length, yet we are also looking towards the use of local isomorphisms during decoding. For instance, when girth is not preserved (see Section 2.1), cycle-splitting or cycle-reduction comes to mind–as in the way two 4-cycles can sometimes be split into one 6-cycle.

We are working on a generalized Pivot operation, which does not depend on the matrix (graph) being in standard form. With this tool, we expect to be able to compare our results with the realistically sized BCH code of [5]. We anticipate more significant results where larger Tanner graphs allow more true localization. Euclidean geometry LDPC codes [18] are also potential, sufficiently structured candidates for adaptive decoding.

Enforcing a strictly local perspective does present some practical difficulties, most notably, decoder stopping criterion and optimum decoder state comparison used in LAD. However, in the context of decoding–as in this work–this does not present a problem, yet rather suggests potential implementations of the iterated decoder where the graph nodes are distributed in space and/or time.

Acknowledgments

Thanks to Øyvind Ytrehus and Lars Eirik Danielsen, at the University of Bergen, for helpful discussions.

References

1. Gallager, R.G.: Low-density parity-check codes. IRE Trans. Inform. Theory 8(1), 21–28 (1962)
2. MacKay, D.J.C., Neal, R.M.: Good codes based on very sparse matrices. In: Cryptography and Coding 5th IMA Conf., December 1995, pp. 100–111 (1995)
3. Jiang, J., Narayanan, K.R.: Iterative soft-input soft-output decoding of Reed-Solomon codes by adapting the parity-check matrix. IEEE Trans. Inform. Theory 52(8), 3746–3756 (2006)
4. Jiang, J., Narayanan, K.R.: Iterative soft decision decoding of Reed-Solomon codes. IEEE Commun. Lett. 8(4), 244–246 (2004)
5. Halford, T.R., Chugg, K.M.: Random redundant iterative soft-in soft-out decoding. IEEE Trans. on Commun. 56(4), 513–517 (2008)
6. Vontobel, P.O., Koetter, R.: Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes. IEEE Trans.Inform.Theory (2005) (submitted for publication)
7. Di, C., Proietti, D., Telatar, I.E., Richardson, T.J., Urbanke, R.L.: Finite-length analysis of low-density parity-check codes on the binary erasure channel. IEEE Trans. Inform. Theory 48(6), 1570–1579 (2002)
8. Richardson, T.: Error floors of LDPC codes. In: Proc.41st Annual Allerton Conf.on Commun., Control, and Computing, Monticello, IL, October 2003, pp. 1426–1435 (2003)
9. Richardson, T.J., Urbanke, R.: The capacity of low-density parity-check codes under message-passing decoding. IEEE Trans. Inform. Theory 47(2), 599–618 (2001)
10. Bouchet, A.: Isotropic systems. European Journal of Combinatorics 8, 231–244 (1987)
11. Danielsen, L.E., Parker, M.G.: Edge local complementation and equivalence of binary linear codes. Des. Codes Cryptogr. (to appear, 2008)

12. Riera, C., Parker, M.G.: On Pivot orbits of Boolean functions, optimal codes and related topics. In: Fourth International Workshop on Optimal Codes and Related Topics, Sofia, Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, June 2005, pp. 248–253 (2005)
13. Kschischang, F.R., Frey, B.J., Loeliger, H.A.: Factor graphs and the sum-product algorithm. IEEE. Trans. on Inform. Theory 47(2), 498–519 (2001)
14. Knudsen, J.G.: Randomised construction and dynamic decoding of LDPC codes. Master's thesis, University of Bergen (2006)
15. Danielsen, L.E., Parker, M.G.: On the classification of all self-dual additive codes over GF(4) of length up to 12. Journ. of Comb. Theory, Series A 113(7), 1351–1367 (2006)
16. Catherine, C.: Enhancing the error-correction performance of low-density parity-check codes. PhD thesis, University of Mauritius (2008)
17. Kothiyal, A., Takeshita, O.: A comparison of adaptive belief propagation and the best graph algorithm for the decoding of linear block codes. In: International Symposium on Information Theory, September 2005, pp. 724–728 (2005)
18. Kou, Y., Lin, S., Fossorier, M.P.C.: Low-density parity-check codes based on finite geometries: A rediscovery and new results. IEEE Trans. Inform. Theory 47(7), 2711–2736 (2001)

Minimal Trellis Construction for Finite Support Convolutional Ring Codes

Margreta Kuijper and Raquel Pinto[⋆]

[1] Department of EE Engineering, University of Melbourne, VIC 3010, Australia
m.kuijper@unimelb.edu.au,
[2] Department of Mathematics, University of Aveiro, 3810-193 Aveiro, Portugal
raquel@ua.pt

Abstract. We address the concept of "minimal polynomial encoder" for finite support linear convolutional codes over $\mathbb{Z}_{p^r}$. These codes can be interpreted as polynomial modules which enables us to apply results from the 2007-paper [8] to introduce the notions of "p-encoder" and "minimal p-encoder". Here the latter notion is the ring analogon of a row reduced polynomial encoder from the field case. We show how to construct a minimal trellis representation of a delay-free finite support convolutional code from a minimal p-encoder. We express its number of trellis states in terms of a degree invariant of the code. The latter expression generalizes the wellknown expression in terms of the degree of a delay-free finite support convolutional code over a field to the ring case. The results are also applicable to block trellis realization of polynomial block codes over $\mathbb{Z}_{p^r}$, such as CRC codes over $\mathbb{Z}_{p^r}$.

Keywords: polynomial module, finite ring, row reduced, p-generator sequence, convolutional code, minimal trellis.

1 Introduction

In this paper we consider finite support linear convolutional codes over a finite ring of the type $\mathbb{Z}_{p^r}$, where r is a positive integer and p is a prime integer. Let $\mathbb{Z}_{p^r}[z]$ denote, as usual, the ring of polynomials in the indeterminate z with coefficients in $\mathbb{Z}_{p^r}$. Conform [15,16,5,17] we define a *finite support convolutional code* of length n over $\mathbb{Z}_{p^r}$ as a submodule of $\mathbb{Z}_{p^r}^n[z]$. In case $\mathcal{C}$ admits a basis, that is, can be written as $\mathcal{C} = \text{ im } G(z)$, then $G(z) \in \mathbb{Z}_{p^r}^{k \times n}[z]$ is called an *encoder* for $\mathcal{C}$ and $\mathcal{C}$ is said to have *dimension* k. Note that, for the ring case $r > 1$, there exist finite support convolutional codes that do not have an encoder. A simple example over $\mathbb{Z}_4$ with $n = 1$ is the code $\mathcal{C} = \text{ span } \{2, 1+z\}$.

In this paper we are interested in minimal trellis representations for finite support convolutional codes over $\mathbb{Z}_{p^r}$, i.e., trellis representations with a minimal

[⋆] The research is partially supported by the *Unidade de Investigação Matemática e Aplicações (UIMA)*, University of Aveiro, Portugal, through the *Programa Operacional Ciência e Tecnologia e Inova ção"(POCTI)* of the *Funda ção para a Ciência e Tecnologia (FCT)*, co-financed by the European Union fund FEDER.

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 95–106, 2008.

number of trellis states. Since decoders, such as the Viterbi decoder, are based on trellis representations, minimality is a desirable property that leads to low complexity decoding. Convolutional codes over $\mathbb{Z}_{p^r}$ have obtained a considerable amount of attention in the literature because of their relevance to nonbinary modulation schemes. For $n = 1$ the class of finite support convolutional codes coincides with the so-called *polynomial block codes*, a terminology from [2]. This class contains all cyclic codes and shortened cyclic codes, i.e., CRC codes, see also [12]. The relevance of polynomial block codes over $\mathbb{Z}_{p^r}$ was established by the landmark paper [6] which shows that important families of nonlinear binary codes are images under a Gray map of linear codes over the ring $\mathbb{Z}_4$, see also [1,14].

In the field case, any delay-free finite support convolutional code (that is, a convolutional code which has an encoder $G(z)$ with $G(0)$ full row rank) admits a minimal encoder that gives rise to a minimal trellis representation. Here minimality is defined as "row-reducedness" and a minimal trellis is simply constructed as the controller canonical realization of a row reduced encoder. The number of states in a minimal trellis can then be expressed in terms of the degree of the code which is the sum of the row degrees of a minimal encoder. In this paper we are interested in determining a similar procedure for the ring case.

Although methods to construct a minimal trellis from code sequences carry through from the field case, as in [4], the literature does not provide a practical trellis realization method that starts from a minimal polynomial encoder and parallels the field case. In particular, it is an open problem, as observed in the 2007 paper [17], to express the minimum number of trellis states in terms of the row degrees of a particular polynomial encoder of the code. The reason for this seems to be that an appropriate minimality concept involving "row reducedness" was, until recently, not available for polynomial matrices over $\mathbb{Z}_{p^r}$. The recent paper [8] develops the concept of "row reducedness" for polynomial matrices over $\mathbb{Z}_{p^r}$. Using this concept we define a particular type of polynomial encoder, called *p-encoder*. We also define the concept of a *delay-free p-encoder*. We show that any delay-free finite support convolutional code over $\mathbb{Z}_{p^r}$ ("delay-free" meaning that it admits a delay-free p-encoder) admits a *minimal p-encoder* whose controller canonical realization is a minimal trellis representation for the code. We find that this minimal trellis exhibits nonlinear features. We give a simple expression for the minimum number of trellis states in terms of the sum of the row degrees of a minimal p-encoder. To prove that our practical construction is minimal, we use the minimal trellis of [4] that is constructed from code sequences.

The algorithm of [20,21] also gives a practical trellis construction method but differs from ours in that it considers associated block codes of the type $\mathcal{C}|_{[0,\ell)}$ and then uses the block trellis algorithm of [18] to build a minimal trellis for $\mathcal{C}$. In contrast, our method makes use of the polynomial structure of the convolutional code and gives rise to a simple expression for the minimum number of trellis states in terms of a degree invariant of the code.

In most of the literature on convolutional ring codes, code sequences are Laurent series, so do not necessarily have finite support. In this classical setting it is natural to assume $n > k$ and to interpret code sequences as trajectories on the time-axis $\mathbb{Z}$, rather than $\mathbb{Z}_+$. Also, catastrophicity issues arise that play no role in the finite support case. The reader is referred to our paper [9] for an account on minimal polynomial encoders and minimal trellis construction of convolutional codes over $\mathbb{Z}_{p^r}$ in this classical setting.

2 Preliminaries

A set that plays a fundamental role throughout the paper is the set of "digits", denoted by $\mathcal{A}_p = \{0, 1, \dots, p-1\} \subset \mathbb{Z}_{p^r}$. Recall that any element $a \in \mathbb{Z}_{p^r}$ can be written uniquely as $a = \theta_0 + \theta_1 p + \cdots + \theta_{r-1} p^{r-1}$, where $\theta_\ell \in \mathcal{A}_p$ for $\ell = 0, \dots, r-1$ (*p-adic expansion*). This fundamental property of the ring $\mathbb{Z}_{p^r}$ expresses a type of linear independence among the elements 1, p, ..., p^{r-1}. It leads to the notions of "p-linear independence" and "p-generator sequence" for modules in $\mathbb{Z}_{p^r}^n$, as developed in the 1996 paper [18]. For example, for the simplest case $n = 1$, the elements 1, p, p^2, ..., p^{r-1} are called "p-linearly independent" in [18] and the module $\mathbb{Z}_{p^r} = \text{ span } \{1\}$ is written as $\mathbb{Z}_{p^r} = p\text{−span } \{1, p, p^2, \dots, p^{r-1}\}$. The module $\mathbb{Z}_{p^r}$ is said to have "p-dimension" r.

In this section we recall the main concepts from [8] on modules in $\mathbb{Z}_{p^r}^n[z]$, that are needed in the sequel. We present the notions of p-basis and p-dimension of a submodule of $\mathbb{Z}_{p^r}^n[z]$, which are extensions from [18]'s notions for submodules of $\mathbb{Z}_{p^r}^n$. From [8] we also recall the concept of a reduced p-basis in $\mathbb{Z}_{p^r}^n[z]$ that plays a crucial role in this paper.

Definition 1. *[8] Let $\{v_1(z), \dots, v_m(z)\} \subset \mathbb{Z}_{p^r}^n[z]$. A* ***p*-linear combination** *of $v_1(z), \dots, v_m(z)$ is a vector $\sum_{j=1}^{m} a_j(z) v_j(z)$, where $a_j(z) \in \mathbb{Z}_{p^r}[z]$ is a polynomial with coefficients in $\mathcal{A}_p$ for $j = 1, \dots, m$. Furthermore, the set of all p-linear combinations of $v_1(z), \dots, v_m(z)$ is denoted by* ***p*-span**$(v_1(z), \dots, v_m(z))$*, whereas the set of all linear combinations of $v_1(z), \dots, v_m(z)$ with coefficients in $\mathbb{Z}_{p^r}[z]$ is denoted by* span $(v_1(z), \dots, v_m(z))$.

Definition 2. *[8] An ordered sequence $(v_1(z), \dots, v_m(z))$ of vectors in $\mathbb{Z}_{p^r}^n[z]$ is said to be a* ***p*-generator sequence** *if $p\, v_m(z) = 0$ and $p\, v_i(z)$ is a p-linear combination of $v_{i+1}(z), \dots, v_m(z)$ for $i = 1, \dots, m-1$.*

Lemma 1. *Let $(v_1(z), \dots, v_m(z))$ be a p-generator sequence in $\mathbb{Z}_{p^r}^n[z]$. Then $(v_1(0), \dots, v_m(0))$ is a p-generator sequence in $\mathbb{Z}_{p^r}^n$.*

Theorem 1. *[8] Let $v_1(z), \dots, v_m(z) \in \mathbb{Z}_{p^r}^n[z]$. If $(v_1(z), \dots, v_m(z))$ is a p-generator sequence then p−*span *$(v_1(z), \dots, v_m(z)) =$* span *$(v_1(z), \dots, v_m(z))$. In particular, p−*span *$(v_1(z), \dots, v_m(z))$ is a submodule of $\mathbb{Z}_{p^r}^n[z]$.*

All submodules of $\mathbb{Z}_{p^r}^n[z]$ can be written as the p-span of a p-generator sequence. In fact, if $M = \text{ span } (g_1(z), \dots, g_k(z))$ then M is the p-span of the p-generator sequence $(g_1(z), p g_1(z), \dots, p^{r-1} g_1(z), \dots, g_k(z), p g_k(z), \dots, p^{r-1} g_k(z))$.

Definition 3. *[8] The vectors $v_1(z), \ldots, v_m(z) \in \mathbb{Z}_{p^r}^n[z]$ are said to be* **p-linearly independent** *if the only p-linear combination of $v_1(z), \ldots, v_m(z)$ that equals zero is the trivial one.*

Definition 4. *Let M be a submodule of $\mathbb{Z}_{p^r}^n[z]$, written as a p-span of a p-generator sequence $(v_1(z), \cdots, v_m(z))$. Then $(v_1(z), \cdots, v_m(z))$ is called a* **p-basis** *for M if the vectors $v_1(z), \ldots, v_m(z)$ are p-linearly independent in $\mathbb{Z}_{p^r}^n[z]$.*

Lemma 2. *[8] Let M be a submodule of $\mathbb{Z}_{p^r}^n[z]$ and let $(v_1(z), v_2(z), \cdots, v_m(z))$ be a p-basis for M. Then each vector of M is written in a unique way as a p-linear combination of $v_1(z), \ldots, v_m(z)$.*

Lemma 3. *Let M be a submodule of $\mathbb{Z}_{p^r}^n[z]$ and let $(v_1(z), v_2(z), \cdots, v_m(z))$ be a p-basis for M, such that $v_1(0), \cdots, v_m(0)$ are p-linearly independent in $\mathbb{Z}_{p^r}^n$. Let $(w_1(z), w_2(z), \cdots, w_m(z))$ be another p-basis for M. Then $w_1(0), \cdots, w_m(0)$ are also p-linearly independent in $\mathbb{Z}_{p^r}^n$.*

Proof. It follows from Lemma 1 that $(v_1(0), \cdots, v_m(0))$ and $(w_1(0), \cdots, w_m(0))$ are p-generator sequences in $\mathbb{Z}_{p^r}^n$. Define modules V and W in $\mathbb{Z}_{p^r}^n$ by $V :=$ $p-$span $(v_1(0), \cdots, v_m(0))$ and $W :=$ $p-$span $(w_1(0), \cdots, w_m(0))$. Since the p-generator sequence $(v_1(z), v_2(z), \cdots, v_m(z))$ is a p-basis for M, the vector $w_i(z)$ (with $i \in \{1, \ldots, m\}$) can be written as a p-linear combination of $v_1(z), \ldots, v_m(z)$. Substituting $z = 0$, it now follows that $w_i(0)$ is a p-linear combination of $v_1(0), \cdots, v_m(0)$ and therefore W is a submodule of V. Vice versa, by the same reasoning, V is a submodule of W. Consequently $W = V$ has p-dimension m because of the p-linear independence of $v_1(0), \cdots, v_m(0)$. It now follows from Lemma 2.10 of [8] that $w_1(0), \cdots, w_m(0)$ are p-linearly independent and this proves the lemma.

Next, we recall a particular p-basis for a submodule of $\mathbb{Z}_{p^r}^n[z]$, called "reduced p-basis". We first recall the concept of "degree" of a vector in $\mathbb{Z}_{p^r}^n[z]$, which is the same as in the field case.

Definition 5. *Let $v(z)$ be a nonzero vector in $\mathbb{Z}_{p^r}^n[z]$, written as $v(z) = v_0 + v_1 z + \cdots + v_d z^d$, with $v_i \in \mathbb{Z}_{p^r}^n$, $i = 0, \ldots, d$, and $v_d \neq 0$. Then $v(z)$ is said to have* **degree** *d, denoted by $\deg v(z) = d$. Furthermore, v_d is called the* **leading coefficient vector** *of $v(z)$, denoted by v^{lc}.*

Lemma 4. *[8] Let M be a submodule of $\mathbb{Z}_{p^r}^n[z]$, written as a p-span of a p-generator sequence $(v_1(z), \ldots, v_m(z))$ with $v_1^{lc}, \ldots, v_m^{lc}$ p-linearly independent in $\mathbb{Z}_{p^r}^n$. Then $(v_1(z), \ldots, v_m(z))$ is a p-basis for M.*

Definition 6. *[8] Let M be a submodule of $\mathbb{Z}_{p^r}^n[z]$, written as a p-span of a p-generator sequence $(v_1(z), \ldots, v_m(z))$. Then $(v_1(z), \ldots, v_m(z))$ is called a* **reduced p-basis** *for M if the vectors $v_1^{lc}, \ldots, v_m^{lc}$ are p-linearly independent in $\mathbb{Z}_{p^r}^n$.*

A reduced p-basis in $\mathbb{Z}_{p^r}^n[z]$ generalizes the concept of row reduced basis from the field case. Moreover, it also leads to the predictable degree property and gives rise to several invariants of M, see [8]. In particular, the number of vectors in a reduced p-basis as well as the degrees of these vectors (called **p-degrees**), are invariants of M. Consequently, their sum is also an invariant of M.

Every submodule M of $\mathbb{Z}_{p^r}^n[z]$ has a reduced p-basis. A constructive proof is given by Algorithm 3.11 in [8] that takes as its input a set of spanning vectors and produces a reduced p-basis of M. Moreover, it is easy to see that if the input is already a p-basis of M, consisting of m vectors, then the algorithm produces a reduced p-basis consisting of m vectors. Since m is an invariant of the module, it follows that all p-bases of M have the same number of elements. As a result, the next definition is well-defined and not in conflict with the slightly different definition of [8].

Definition 7. *The number of elements of a p-basis of a submodule M of $\mathbb{Z}_{p^r}^n[z]$ is called the* **p-dimension** *of M, denoted as $p\text{−}\dim(M)$.*

The following lemma will be used in the next section.

Lemma 5. *Let $M = \operatorname{span}(g_1(z), \dots, g_k(z))$ be a submodule of $\mathbb{Z}_{p^r}^n[z]$, where $g_1(z), \dots, g_k(z) \in \mathbb{Z}_{p^r}^n[z]$ are linearly independent. Then $p\text{−}\dim M = rk$.*

Proof. The result follows immediately from the obvious fact that

$$(g_1(z), pg_1(z), \dots, p^{r-1}g_1(z), \dots, g_k(z), pg_k(z), \dots, p^{r-1}g_k(z))$$

is a p-basis for M.

3 p-Encoders and Trellises

It follows from the preceding section that any finite support convolutional code $\mathcal{C}$ of length n admits a p-basis. In the sequel we denote the p-dimension (see Definition 7) of $\mathcal{C}$ by κ. Recall that $\mathcal{A}_p = \{0, 1, \dots, p-1\} \subset \mathbb{Z}_{p^r}$.

Definition 8. *Let $\mathcal{C}$ be a finite support convolutional code over $\mathbb{Z}_{p^r}$ of length n and p-dimension κ. Then $E(z) \in \mathbb{Z}_{p^r}^{\kappa\times n}[z]$ is said to be a* **p-encoder** *of $\mathcal{C}$ if the rows of $E(z)$ are a p-basis for $\mathcal{C}$.*

Definition 9. *Let $E(z)$ be a p-encoder of a finite support convolutional code over $\mathbb{Z}_{p^r}$ of length n, such that the rows of $E(0)$ are a p-basis in $\mathbb{Z}_{p^r}^n$. Then $E(z)$ is said to be a* **delay-free p-encoder**.

The next lemma follows immediately from Lemma 3.

Lemma 6. *Let $\mathcal{C}$ be a finite support convolutional code over $\mathbb{Z}_{p^r}$ of length n that admits a delay-free p-encoder. Then all p-encoders of $\mathcal{C}$ are delay-free.*

Definition 10. *A finite support convolutional code over $\mathbb{Z}_{p^r}$ of length n is said to be a* **delay-free code** *if all its p-encoders are delay-free.*

Not all finite support convolutional codes are delay-free. A simple example over $\mathbb{Z}_2$ with $n = 1$ is the code $\mathcal{C} =$ span $\{z + z^2\}$. In fact, convolutional codes that are not delay-free seem to be of limited interest, as they employ an artificially high lag. From now on we focus on delay-free codes.

Definition 11. *Let $\mathcal{C}$ be a delay-free finite support convolutional code over $\mathbb{Z}_{p^r}$ of length n. Then $E(z)$ is said to be a* **minimal p-encoder** *of $\mathcal{C}$ if the rows of $E(z)$ are a reduced p-basis for $\mathcal{C}$.*

A minimal p-encoder for a delay-free finite support convolutional code $\mathcal{C}$ is obtained by applying Algorithm 3.11 in [8] to any p-encoder of $\mathcal{C}$.

In the sequel, we denote the *leading row coefficient matrix* of a polynomial matrix $V(z)$ by V^{lrc}. If a delay-free finite support convolutional code $\mathcal{C}$ admits an encoder $G(z)$ such that G^{lrc} has full row rank, then a minimal p-encoder is trivially constructed as

$$E(z) = \text{col } (G(z), pG(z), \ldots, p^{r-1}G(z)). \tag{1}$$

An important observation is that all delay-free finite support convolutional codes admit a minimal p-encoder but they do not all admit an encoder $G(z)$ such that G^{lrc} has full row rank.

Note that, because of Lemma 5, the p-dimension κ of a finite support convolutional code of dimension k equals $\kappa = rk$. Also, if such a code is delay-free, it can be easily verified that all its encoders $G(z)$ have the property that $G(0)$ has full row rank.

A convolutional code can be represented by a trellis. Formally, we define a *trellis section* as a four-tuple $X = (\mathbb{Z}_{p^r}^n, S, S', K)$, where S and S' are the *left state set* and *right state set*, respectively, and K is the *set of branches* which is a subset of $S \times \mathbb{Z}_{p^r}^n \times S'$, such that every state is part of at least one branch, see also [4,11,10]. A *trellis* is a sequence $\mathcal{X} = \{X_t\}_{t\in\mathbb{Z}_+}$ of trellis sections $X_t = (\mathbb{Z}_{p^r}^n, S_t, S_t', K_t)$, such that for all $t \in \mathbb{Z}_+$, $S_t' = S_{t+1}$ and $S_0 = \{0\}$. A *path* through the trellis is a sequence $(b_0, \cdots, b_{t-1}, b_t, b_{t+1}, \cdots)$ of branches $b_t = (s_t, c_t, s_{t+1}) \in K_t$ such that b_{t+1} starts in the trellis state where b_t ends, for $t \in \mathbb{Z}_+$. The set of all trellis paths that end at the zero state is denoted by $\pi(\mathcal{X})$. The mapping $\lambda : \pi(\mathcal{X}) \mapsto (\mathbb{Z}_{p^r}^n)^{\mathbb{Z}_+}$ assigns to every path $(b_0, \cdots, b_{t-1}, b_t, b_{t+1}, \cdots)$ its label sequence $(c_0, \cdots, c_{t-1}, c_t, c_{t+1}, \cdots)$. We say that a sequence $\{c_t\}_{t\in\mathbb{Z}_+}$ *passes through state s at time t* if there exists a corresponding path of branches $\{b_t\}_{t\in\mathbb{Z}_+}$, where $b_t = (s_t, c_t, s_{t+1})$, such that $s_t = s$. A trellis $\mathcal{X}$ is called a *trellis representation* for a finite support convolutional code $\mathcal{C}$ if $\mathcal{C} = \lambda(\pi(\mathcal{X}))$ [1].

A trellis representation of a finite support convolutional code can be constructed from a p-encoder of the code. Let us first recall the wellknown controller canonical form. A $\kappa \times n$ matrix $E(z)$ is realized in controller canonical form [7] (see also [3, Sect. 5]) as

$$E(z) = B(z^{-1}I - A)^{-1}C + D. \tag{2}$$

[1] We identify a polynomial $\boldsymbol{c} = c_0 + c_1 z + \cdots + c_m z^m$ in $\mathbb{Z}_{p^r}[z]$ with the finite support sequence $(c_0, c_1, \ldots, c_m) \in \mathbb{Z}_{p^r}^{m+1}$.

Denoting the i'th row of $E(z)$ by $e_i(z) = \sum_{\ell=0}^{\delta_i} e_{i,\ell} z^\ell$, where $e_{i,\ell} \in \mathbb{Z}_{p^r}^{1\times n}$, the matrices A, B, C and D in (2) are given by

$$A = \begin{bmatrix} A_1 & & \\ & \ddots & \\ & & A_\kappa \end{bmatrix}, \quad B = \begin{bmatrix} B_1 & & \\ & \ddots & \\ & & B_\kappa \end{bmatrix}, \quad C = \begin{bmatrix} C_1 \\ \vdots \\ C_\kappa \end{bmatrix}, \quad D = \begin{bmatrix} e_{1,0} \\ \vdots \\ e_{\kappa,0} \end{bmatrix},$$

with

$$A_i = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix}, \quad B_i = \begin{bmatrix} 1\ 0 \cdots 0 \end{bmatrix}, \quad C_i = \begin{bmatrix} e_{i,1} \\ \vdots \\ e_{i,\delta_i} \end{bmatrix} \quad \text{for } i = 1, \ldots, \kappa. \tag{3}$$

Whenever $\delta_i = 0$, the ith block in A as well as C is absent and a zero row occurs in B. Denoting the sum of the δ_i's by δ, it is clear that A is a $\delta \times \delta$ nilpotent matrix. The above controller canonical realization can be visualized as a shift-register with δ registers or, equivalently, as a trellis representation with p^δ trellis states, as expressed in the next definition.

Definition 12. *Let $\mathcal{C}$ be a finite support convolutional code over $\mathbb{Z}_{p^r}$ of length n and p-dimension κ, and let $E(z) \in \mathbb{Z}_{p^r}^{\kappa\times n}[z]$ be a p-encoder of $\mathcal{C}$. Let $\delta = \sum_{i=1}^{\kappa} \operatorname{rowdeg} e_i(z)$, where $e_i(z)$ denotes the i-th row of $E(z)$, and let*

$$(A, B, C, D) \in \mathbb{Z}_{p^r}^{\delta\times\delta} \times \mathbb{Z}_{p^r}^{\kappa\times\delta} \times \mathbb{Z}_{p^r}^{\delta\times n} \times \mathbb{Z}_{p^r}^{\kappa\times n}$$

be a controller canonical realization of $E(z)$ as defined above. Then the **controller canonical trellis** *corresponding to $E(z)$ is defined as $\mathcal{X}_{E(z)} = \{X_t\}_{t\in\mathbb{Z}_+}$, where $X_t = (\mathbb{Z}_{p^r}^n, S_t, S_t', K_t)$ with*

$$S_0 = \{0\} \text{ and } S_t' = \{sA + uB : s \in S_t \text{ and } u \in \mathcal{A}_p^\kappa\},\ t \in \mathbb{Z}_+ \quad \text{and}$$

$$K_t = \{(s(t), s(t)C + u(t)D, s(t)A + u(t)B \mid s(t) \in S_t \text{ and } u(t) \in \mathcal{A}_p^\kappa\}.$$

Note that both inputs and states take their values in a set that is not closed with respect to addition or scalar multiplication (namely $\mathcal{A}_p^\kappa$ and $\mathcal{A}_p^\delta$, respectively).

4 Minimal Trellis Construction from a p-Encoder

A trellis representation $\mathcal{X}$ for a finite support convolutional code $\mathcal{C}$ is called *minimal* if for all $t \in \mathbb{Z}_+$ the size of its trellis state set S_t is minimal among all trellis representations of $\mathcal{C}$. It is wellknown how to construct a minimal trellis representation in terms of the code sequences of $\mathcal{C}$. In fact, the theory of canonical trellis representations from the field case carries through to the ring case, see [19,4,13,10,11,20]. We recall the construction of such a representation (called *two-sided realization* in [19]), adapting it for our case of finite support codes.

Consider two code sequences $\boldsymbol{c} \in \mathcal{C}$ and $\tilde{\boldsymbol{c}} \in \mathcal{C}$. Conform [19], the *concatenation* at time $t \in \mathbb{Z}_+$ of $\boldsymbol{c}$ and $\tilde{\boldsymbol{c}}$, denoted by $\boldsymbol{c} \wedge_t \tilde{\boldsymbol{c}}$, is defined as

$$\boldsymbol{c} \wedge_t \tilde{\boldsymbol{c}}(t') := \begin{cases} c(t') & \text{for } 0 \leq t' < t \\ \tilde{c}(t') & \text{for } t' \geq t \end{cases} .$$

We define a relation in $\mathcal{C}$, for each $t \in \mathbb{Z}_+$, as follows

$$\boldsymbol{c} \simeq_t \tilde{\boldsymbol{c}} \Leftrightarrow \boldsymbol{c} \wedge_t \tilde{\boldsymbol{c}} \in \mathcal{C}, \tag{4}$$

for $\boldsymbol{c}, \tilde{\boldsymbol{c}} \in \mathcal{C}$. The linearity of $\mathcal{C}$ immediately implies that $\simeq_t$ is an equivalence relation on $\mathcal{C}$.

Definition 13. *Let $\mathcal{C}$ be a finite support convolutional code over $\mathbb{Z}_{p^r}$ of length n. The* **canonical trellis** *of $\mathcal{C}$ is defined as $\mathcal{X}_c = \{X_t\}_{t \in \mathbb{Z}_+}$, where $X_t = (\mathbb{Z}_{p^r}^n, S_t, S_t', K_t)$ with*

$$S_t := \mathcal{C} \ mod \simeq_t, \ S_t' := \mathcal{C} \ mod \simeq_{t+1} \ \ and \ K_t := \{([c]_t, c(t), [c]_{t+1})\}.$$

It can be shown as in [19,10] that the above trellis is minimal. Intuitively this is explained from the fact that, by construction, states cannot be merged.

In the field case, a minimal trellis representation for a delay-free finite support convolutional code is obtained as the controller canonical trellis realization of a row reduced encoder. The next theorem presents our main result for delay-free finite support convolutional codes over $\mathbb{Z}_{p^r}$. It obtains a minimal trellis representation as the controller canonical trellis realization of a minimal p-encoder $E(z)$.

Theorem 2. *Let $\mathcal{C}$ be a delay-free finite support convolutional code over $\mathbb{Z}_{p^r}$ of length n and p-dimension κ. Let $E(z)$ be a minimal p-encoder for $\mathcal{C}$. Denote the p-degrees of $\mathcal{C}$ by γ_i for $i = 1, \ldots, \kappa$, and denote $\gamma_{max} := \max \{\gamma_i : i = 1, \ldots, \kappa\}$ and $\gamma := \sum_{i=1}^{\kappa} \gamma_i$. Then the controller canonical trellis $\mathcal{X}_{E(z)}$, defined in Definition 12, is a minimal trellis representation for $\mathcal{C}$. In particular, the number of trellis states of $\mathcal{X}_{E(z)}$ at each instant t equals p^γ, for $t \geq \gamma_{max}$.*

Proof. Consider the mapping $\Theta_t : S_t \mapsto \mathcal{C} \bmod \simeq_t$, given by $\Theta_t(s) := [\boldsymbol{c}]_{\simeq_t}$, where $\boldsymbol{c} \in \mathcal{C}$ passes through state s at time t. For every $t \in \mathbb{Z}_+$, the mapping Θ_t is well-defined since for any s there exists such a code sequence and any two code sequences that pass through state s at time t are obviously equivalent.

Since the canonical trellis $\mathcal{X}_c$ of Definition 13 is minimal, it suffices to prove that Θ_t is a bijection for every $t \in \mathbb{Z}_+$. Surjectivity follows immediately from the fact that all code sequences pass through some state at time t. To prove that Θ_t is injective, let s and $\tilde{s} \in S_t$ be such that $\Theta_t(s) = \Theta_t(\tilde{s})$. Let $\boldsymbol{c}$ and $\tilde{\boldsymbol{c}}$ be code sequences that pass through s and $\tilde{s}$ at time t, respectively. Then $\boldsymbol{c} = \boldsymbol{u}E(z)$ and $\tilde{\boldsymbol{c}} = \tilde{\boldsymbol{u}}E(z)$, for some $\boldsymbol{u}, \tilde{\boldsymbol{u}} \in \mathcal{A}_p^\kappa[z]$. From $\Theta_t(s) = \Theta_t(\tilde{s})$ it follows that the sequence $\boldsymbol{c} \wedge_t \tilde{\boldsymbol{c}} \in \mathcal{C}$. Denote its state at time t by s' and let $\boldsymbol{u}' \in \mathcal{A}_p^\kappa[z]$ be such that $\boldsymbol{c} \wedge_t \tilde{\boldsymbol{c}} = \boldsymbol{u}'E(z)$. We now prove that $s = s'$, as follows. Firstly, it is clear that

$$\begin{bmatrix} c(0)\; c(1) \cdots c(t-1) \end{bmatrix} = \begin{bmatrix} u(0)\; u(1) \cdots u(t-1) \end{bmatrix} \begin{bmatrix} D & BC & BAC & \cdots \\ 0 & D & BC & \cdots \\ 0 & 0 & D & \cdots \\ & & & \ddots \end{bmatrix} \tag{5}$$

$$= \begin{bmatrix} u'(0)\; u'(1) \cdots u'(t-1) \end{bmatrix} \begin{bmatrix} D & BC & BAC & \cdots \\ 0 & D & BC & \cdots \\ 0 & 0 & D & \cdots \\ & & & \ddots \end{bmatrix} . \tag{6}$$

From the fact that the rows of $D = E(0)$ are p-linearly independent it then follows that $u(\ell) = u'(\ell)$ for $0 \le \ell \le t-1$. As a result $s = s'$.

We now prove that $s = \tilde{s}$. By the above, $\boldsymbol{c} \wedge_t \tilde{\boldsymbol{c}}$ is a code sequence that passes through s at time t. Denote by M' the degree of $\boldsymbol{u}'$ and by M'' the degree of $\tilde{\boldsymbol{u}}$. Let $M = \max\{M', M''\}$. By construction the states of $\tilde{\boldsymbol{c}}$ and $\boldsymbol{c} \wedge_t \tilde{\boldsymbol{c}}$ are both zero at time $M + \gamma_{max} + 1$. Denote by $s(j)$ the state at time j of the code sequence $\boldsymbol{c} \wedge_t \tilde{\boldsymbol{c}}$ and by $\tilde{s}(j)$ the state at time j of the code sequence $\tilde{\boldsymbol{c}}$. Now recall the formula (3) for the controller canonical form. Since $s(j) = 0$ for $j \ge M + \gamma_{max} + 1$, we have that $0 = s(M + \gamma_{max})A = \tilde{s}(M + \gamma_{max})A$, and thus the nonzero components of $s(M + \gamma_{max})$ and $\tilde{s}(M + \gamma_{max})$ must be last components in a $1 \times \gamma_i$-block. Also, $\tilde{c}(M + \gamma_{max}) = s(M + \gamma_{max})C = \tilde{s}(M + \gamma_{max})C$, which means that the last components of the $1 \times \gamma_i$-blocks of $s(M + \gamma_{max})$ and $\tilde{s}(M + \gamma_{max})$ are equal. This follows from the fact that states only take values in $\mathcal{A}_p$ and that, by construction, the last rows of the $\gamma_i \times n$-blocks of C are rows from E^{lrc} and are therefore p-linearly independent. Thus $s(M + \gamma_{max}) = \tilde{s}(M + \gamma_{max})$. Repeating this argument again and again, we conclude that $s(j) = \tilde{s}(j)$, for $j \ge M$. As a result, $u(j) = u'(j)$ for $j = M - \gamma_{max} - 1, \ldots, M - 1$.

If $t \ge M$ the theorem is proved. Suppose now that $t < M$. From the fact that $s(M) = \tilde{s}(M)$ and that $u(M-1) = u'(M-1)$, it follows that $s(M-1)A = \tilde{s}(M-1)A$ which means that the first $\gamma_i - 1$ components of the $1 \times \gamma_i$-blocks of $s(M-1)$ and $\tilde{s}(M-1)$ are equal. On the other hand, since $s(M-1)C = \tilde{s}(M-1)C = \tilde{c}(M-1) - u(M-1)D$ we conclude, by the same reasoning as before, that also the last components in the $1 \times \gamma_i$-blocks of $s(M-1)$ and $\tilde{s}(M-1)$ are equal, which means that $s(M-1) = \tilde{s}(M-1)$. Repeating this argument again and again, we conclude that $s = \tilde{s}$, which proves the theorem. Obviously, the number of trellis states at each instant t equals p^{γ}, for $t \ge \gamma_{max}$.

Example 1. Over $\mathbb{Z}_4$: consider the finite support convolutional code $\mathcal{C}$ of length $n = 3$, with encoder

$$G(z) = \begin{bmatrix} g_1(z) \\ g_2(z) \end{bmatrix} = \begin{bmatrix} z^2 + 1 & 1 & 0 \\ 2z & 1 & 2 \end{bmatrix} .$$

The controller canonical trellis associated with $G(z)$ has $4^3 = 64$ trellis states.

Note that $G(0)$ has full row rank but that G^{lrc} does not have full row rank, that is, $G(z)$ is not row reduced. In fact, this code does not admit a row reduced encoder. As a result, it is not possible to construct a minimal trellis as a controller canonical realization of an encoder of $\mathcal{C}$. We now compute a minimal p-encoder for $\mathcal{C}$ from which we construct a minimal trellis.

Firstly, a nonminimal p-encoder of $\mathcal{C}$ is given by

$$E(z) = \begin{bmatrix} g_1(z) \\ 2g_1(z) \\ g_2(z) \\ 2g_2(z) \end{bmatrix} = \begin{bmatrix} z^2+1 & 1 & 0 \\ 2z^2+2 & 2 & 0 \\ 2z & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix}, \quad \text{with} \quad E^{lrc} = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}.$$

Note that the rows of $E(0)$ constitute a p-basis in $\mathbb{Z}_{p^r}^n$. The row reduction algorithm of [8, Algorithm 3.11] is particularly simple in this case: by adding z times the third row to the second row, we obtain the following minimal p-encoder $\bar{E}(z)$ given by:

$$\bar{E}(z) = \begin{bmatrix} z^2+1 & 1 & 0 \\ 2 & z+2 & 2z \\ 2z & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} \quad \text{with} \quad \bar{E}^{lrc} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}.$$

Indeed, the rows of $\bar{E}^{lrc}$ are p-linearly independent. The p-degrees of $\mathcal{C}$ are 2, 1, 1, 0, so that their sum γ equals 4. The controller canonical trellis corresponding to $\bar{E}(z)$ is given by

$$A = \begin{bmatrix} 0\,1\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,0 \end{bmatrix}; \quad B = \begin{bmatrix} 1\,0\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \\ 0\,0\,0\,0 \end{bmatrix}; \quad C = \begin{bmatrix} 0\,0\,0 \\ 1\,0\,0 \\ 0\,1\,2 \\ 2\,0\,0 \end{bmatrix}; \quad D = \begin{bmatrix} 1\,1\,0 \\ 2\,2\,0 \\ 0\,1\,2 \\ 0\,2\,0 \end{bmatrix}.$$

By Theorem 2, this trellis is minimal with $2^4 = 16$ trellis states for $t \geq \gamma_{max} = 2$.

5 Conclusions

In this paper we focus on polynomial encoders for delay-free finite support convolutional codes over $\mathbb{Z}_{p^r}$. We introduce the notion of p-encoder and show that any delay-free finite support convolutional code $\mathcal{C}$ over $\mathbb{Z}_{p^r}$ admits a minimal p-encoder. We present a simple and efficient method to construct a minimal trellis representation for $\mathcal{C}$ from such a minimal p-encoder. The method extends the well-known procedure for constructing minimal trellises for delay-free finite support convolutional codes over a field from a controller canonical realization of a row reduced encoder. In addition, similar to the field case, we obtain an expression for the minimal number of trellis states in terms of the sum of row degrees of a minimal p-encoder. A major difference with the field case is that our minimal trellis employs a nonlinear state space as well as a nonlinear input space.

Finite support convolutional codes of length $n = 1$ are also known as polynomial block codes, which includes all cyclic and CRC codes. It follows from our account that minimal block trellises (not allowing code component permutations) of polynomial block codes over $\mathbb{Z}_{p^r}$ are obtained as minimal trellises of finite support convolutional codes of length $n = 1$. It is a topic of future research to investigate the connections of the results of this paper with the literature on cyclic block codes over $\mathbb{Z}_{p^r}$, see for example [1,14].

References

1. Calderbank, A.R., Sloane, N.J.A.: Modular and p-adic cyclic codes. Designs, Codes and Cryptography 6, 21–35 (1995)
2. Clark, G.C., Cain, J.B.: Error-Correction Coding for Digital Communications. Plenum Press, New York (1981)
3. Fornasini, E., Pinto, R.: Matrix fraction descriptions in convolutional coding. Linear Algebra and its Applications 392, 119–158 (2004)
4. Forney, G.D., Trott, M.D.: The dynamics of group codes: state spaces, trellis diagrams, and canonical encoders. IEEE Trans. Inf. Th. 39, 1491–1513 (1993)
5. Gluesing-Luersen, H., Schneider, G.: State space realizations and monomial equivalence for convolutional codes. Linear Algebra and its Applications 425, 518–533 (2007)
6. Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inf. Th. 40, 301–319 (1994)
7. Kailath, T.: Linear Systems. Prentice Hall, Englewood Cliffs (1980)
8. Kuijper, M., Pinto, R., Polderman, J.W.: The predictable degree property and row reducedness for systems over a finite ring. Linear Algebra and its Applications 425, 776–796 (2007)
9. Kuijper, M., Pinto, R.: On minimality of convolutional ring encoders (submitted; av), http://arxiv.org/abs/0801.3703
10. Loeliger, H.-A., Forney Jr., G.D., Mittelholzer, T., Trott, M.D.: Minimality and observability of group systems. Linear Algebra and its Applications 205-206, 937–963 (1994)
11. Loeliger, H.-A., Mittelholzer, T.: Convolutional codes over groups. IEEE Trans. Inf. Th. IT-42, 1660–1686 (1996)
12. Manganiello, F.: Computation of the weight distribution of CRC codes (2006), http://archiv.org/abs/cs/0607068
13. Mittelholzer, T.: Minimal encoders for convolutional codes over rings. In: Honory, B., Darnell, M., Farell, P.G. (eds.) Communications Theory and Applications, pp. 30–36. HW Comm. Ltd (1993)
14. Pless, V.S., Qian, Z.: Cyclic codes and quadratic residue codes over Z_4. IEEE Trans. Inf. Th. 42, 1594–1600 (1996)
15. Rosenthal, J., Schumacher, J.M., York, E.V.: On behaviors and convolutional codes. IEEE Trans. Inf. Th. 42, 1881–1891 (1996)
16. Rosenthal, J., Smarandache, R.: Maximum distance separable convolutional codes. Appl. Algebra Engrg. Comm. Comput. 10(1), 15–32 (1999)
17. Solé, P., Sison, V.: Quaternary convolutional codes from linear block codes over galois rings. IEEE Trans. Inf. Th. 53, 2267–2270 (2007)

18. Vazirani, V.V., Saran, H., Rajan, B.S.: An efficient algorithm for constructing minimal trellises for codes over finite abelian groups. IEEE Trans. Inf. Th. 42, 1839–1854 (1996)
19. Willems, J.C.: Models for dynamics. Dynamics Rep. 2, 171–282 (1988)
20. Wittenmark, E.: An Encounter with Convolutional Codes over Rings. PhD dissertation, Lund University, Lund, Sweden (1998)
21. Wittenmark, E.: Minimal trellises for convolutional codes over rings. In: Proceedings 1998 IEEE International Symposium in Information Theory (ISIT 1998), Cambridge, USA, p. 15 (1998)

On the Quasi-cyclicity of the Gray Map Image of a Class of Codes over Galois Rings

C.A. López-Andrade[1,2] and H. Tapia-Recillas[2]

[1] Facultad de Ciencias de la Computación, BUAP, 72570, Puebla, México
calopez@cs.buap.mx
[2] Dpto. Matemáticas, UAM-I, 9340, D.F., México
htr@xanum.uam.mx

Abstract. Results on the quasi-cyclicity of the Gray map image of a class of codes defined over the Galois ring $\mathrm{GR}(p^2, m)$ are given. These results generalize some appearing in [8] for codes over the ring $\mathbb{Z}/p^2\mathbb{Z}$ of integers modulo p^2 (p a prime). The ring of (truncated) Witt vectors is a useful tool in proving the main results.

Keywords: Quasi-cyclicity, Galois rings, Gray map, Witt ring.

1 Introduction

After the seminal works [13] and [5] where codes including the non-linear binary Kerdock and Preparata are described as the Gray map image of linear codes over the ring of integers modulo 4, $\mathbb{Z}/4\mathbb{Z}$, the study of codes defined over the ring $\mathbb{Z}/p^m\mathbb{Z}$ of integers modulo p^m (p a prime and m a positive integer), and more generally, codes defined over finite chain rings including Galois rings has increased ([15], [7], [3], [14]). The Gray map has been extended to finite chain rings ([4]) and, specifically, the image under the Gray map of codes defined over the ring $\mathbb{Z}/p^m\mathbb{Z}$ has been studied by several authors ([2], [22], [8], [19]). The ring $\mathbb{Z}/p^m\mathbb{Z}$ is a particular case of a Galois ring (see section 2) and a natural question to ask is to what extent are the known results for codes defined on the former ring and its Gray image valid for codes defined on the latter ring and its Gray image. The Galois ring $\mathrm{GR}(p^2, m)$ has been the subject of study by several authors in areas such as sequences with good correlation properties ([10]), exponential sums ([9]) and repeated root-cyclic codes ([18]). The results presented in this note are also related to codes defined over this ring.

The ring of (truncated) Witt vectors is a useful tool for proving the main results of this note. This ring has been used in several areas including Number Theory, Algebraic Geometry, Coding Theory and Cryptography. In section 2 the definition and basic properties of Galois rings as well as the ring of (truncated) Witt vectors are considered. In particular, it is seen that the Galois ring $\mathrm{GR}(p^2, m)$ and the Witt ring $\mathcal{W}_2(\mathbb{F})$, where $\mathbb{F}$ is the residue field of the Galois ring, are isomorphic. The Gray map on the Witt ring $\mathcal{W}_2(\mathbb{F})$ is recalled and some of its properties are given in section 3. The main results of this note appear in section 4 where a necessary and sufficient condition for a code over the

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 107–116, 2008.

ring $\mathcal{W}_2(\mathbb{F})$ to be $\hat{\alpha}$-cyclic is given in terms of its Gray image (Theorem 2), and a necessary and sufficient condition for the code to be $\hat{\gamma}$-cyclic is also given in terms of its Gray image (Theorem 3). These results generalize some of those appearing in [8] for codes defined over the ring $\mathrm{GR}(p^2, 1) = \mathbb{Z}/p^2\mathbb{Z}$.

2 The Galois and Witt Rings

The definition and basic properties of the Galois ring and the ring of (truncated) Witt vectors are recalled in this section. For further details on Galois rings we refer the reader to [11], Chapter XVI (see also [5]) and for the Witt ring see [17].

2.1 Galois Ring

Let $\mathbb{Z}/p^n\mathbb{Z}$ be the ring of integers modulo p^n, where p is a prime and n a positive integer. An irreducible polynomial $f(x) \in (\mathbb{Z}/p^n\mathbb{Z})[x]$ is said to be *basic* if its reduction modulo p is irreducible. The Galois ring $\mathrm{GR}(p^n, m)$ is defined as:

$$\mathrm{GR}(p^n, m) = (\mathbb{Z}/p^n\mathbb{Z})[x]/\langle f(x)\rangle$$

where $f(x) \in (\mathbb{Z}/p^n\mathbb{Z})[x]$ is a monic, basic, primitive irreducible polynomial of degree m dividing $x^{p^{m-1}} - 1$ and $\langle f(x)\rangle$ is the ideal of $(\mathbb{Z}/p^n\mathbb{Z})[x]$ generated by $f(x)$.

The ring $\mathcal{R} = \mathrm{GR}(p^n, m)$ is local with maximal ideal $\mathcal{M} = \langle p\rangle$ generated by p and its residue field $\mathbb{F} = \mathcal{R}/\mathcal{M}$ is isomorphic to $\mathbb{F}_{p^m}$, the Galois field with p^m elements. The cardinality of $\mathcal{R}$ is $|\mathcal{R}| = p^{nm}$ and the elements of the maximal ideal $\mathcal{M}$ are the zero-divisors of $\mathcal{R}$. Any ideal of the Galois ring is of the form $\langle p^i\rangle$ for $1 \leq i \leq n$ and there is a chain of ideals:

$$\mathcal{R} = \langle 1\rangle \supset \langle p\rangle \supset \cdots \supset \langle p^n\rangle = \{0\}.$$

Let $\mu : \mathcal{R} \longrightarrow \mathbb{F}$, $\mu(\theta) = \overline{\theta}$ be the canonical map from the Galois ring onto its residue field. Let $\mathcal{T} \subset \mathcal{R}$ be a Teichmüller set of representatives of the Galois ring. Then any element $\beta \in \mathcal{R}$ has a unique p-adic (multiplicative) representation:

$$\beta = r_0(\beta) + r_1(\beta)p + \cdots + r_{n-1}(\beta)p^{n-1}$$

where $r_i(\beta) \in \mathcal{T}$.

If $\mathcal{R}^*$ denotes the group of units of $\mathcal{R}$ then $\mathcal{R} = \mathcal{M} \cup \mathcal{R}^*$ and $\mathcal{R}^* = \mathcal{C} \times \mathcal{G}$ where $\mathcal{C}$ is a cyclic group of order $p^m - 1$ and $\mathcal{G}$ is a group of order $p^{(n-1)m}$ (see [11], Theorem XVI.9; [21], Theorem 14.11, pag.319). If $\omega \in \mathcal{R}$ is a root of $f(x)$ then the subgroup $\mathcal{C}$ is generated by ω, its image $\bar{\omega} = \mu(\omega) \in \mathbb{F}_{p^m}$ is a root of the irreducible polynomial $\overline{f(x)} = \mu(f(x))$ and $\mathbb{F}^*_{p^m} = \mathbb{F}_{p^m} \setminus \{0\} = \langle\bar{\omega}\rangle$. If $q = p^m$, the Teichmüller set of representatives of the Galois ring $\mathcal{R}$ can be taken as $\mathcal{T} = \{0, 1, \omega, \omega^2, ..., \omega^{q-2}\}$.

It is easy to see that the Galois ring $\mathcal{R}$ has the structure of a $(\mathbb{Z}/p^n\mathbb{Z})$-module:

$$\mathcal{R} = (\mathbb{Z}/p^n\mathbb{Z})[\omega] = (\mathbb{Z}/p^n\mathbb{Z}) + (\mathbb{Z}/p^n\mathbb{Z})\,\omega + \cdots + (\mathbb{Z}/p^n\mathbb{Z})\,\omega^{m-1}.$$

Examples of Galois rings include:

1. $\mathrm{GR}(p,m) = \mathrm{GF}(p,m) = \mathbb{F}_{p^m}$, $\mathrm{GR}(p^n,1) = \mathbb{Z}/p^n\mathbb{Z}$.
2. Let $f(x) = x^3+x+1 \in (\mathbb{Z}/4\mathbb{Z})[x]$ which is a monic, basic, irreducible polynomial over $\mathbb{Z}/4\mathbb{Z}$. Then $\mathrm{GR}(2^2,3) = (\mathbb{Z}/4\mathbb{Z})[x]/\langle f(x)\rangle$, ([11], pag.297).
3. Let $g(x) = x^3 + 2x^2 + x - 1 \in (\mathbb{Z}/4\mathbb{Z})[x]$ which is also a monic, basic, irreducible polynomial over $\mathbb{Z}/4\mathbb{Z}$. Then $\mathrm{GR}(2^2,3) = (\mathbb{Z}/4\mathbb{Z})[x]/\langle g(x)\rangle$, ([5], Section III).
4. Let $h(x) = x^2 + 4x + 8 \in (\mathbb{Z}/9\mathbb{Z})[x]$ which is a monic, basic, irreducible polynomial over $\mathbb{Z}/9\mathbb{Z}$. Then $\mathrm{GR}(3^2,2) = (\mathbb{Z}/9\mathbb{Z})[x]/\langle h(x)\rangle$, ([21]).

2.2 The Witt Ring $\mathcal{W}_2(\mathbb{F})$

Now we will consider the Galois ring $\mathcal{R} = \mathrm{GR}(p^2,m)$, where $m \geq 1$ is an integer. In this subsection the definition of the ring of (truncated) Witt vectors, $\mathcal{W}_2(\mathbb{F})$, over the finite field $\mathbb{F} = \mathbb{F}_{p^m}$ is recalled and an isomorphism between the Galois ring $\mathcal{R}$ and $\mathcal{W}_2(\mathbb{F})$ is given. This ring is used in later sections to give results on the Gray image of codes defined over the Galois ring $\mathcal{R}$ or equivalently on the Witt ring $\mathcal{W}_2(\mathbb{F})$. For further details on the Witt ring we refer the reader to [17].

Let $(\mathbb{F},+,*) = (\mathbb{F}_{p^m},+,*)$ be the finite field with p^m elements. The underlying set of the Witt ring $\mathcal{W}_2(\mathbb{F})$ is just the cartesian product $\mathbb{F}\times\mathbb{F}$ and the operations "$+_w$", "$*_w$" are defined as follows:

$$(x_0,x_1) +_w (y_0,y_1) = (S_0(x_0,x_1,y_0,y_1), S_1(x_0,x_1,y_0,x_1))$$

where

$$\begin{aligned} S_0(x_0,x_1,y_0,y_1) &= x_0 + y_0 \\ S_1(x_0,x_1,y_0,y_1) &= \left((x_1+y_1) - \tfrac{1}{p}((x_0+y_0)^p - x_0^p - y_0^p)\right) \end{aligned}$$

and

$$(x_0,x_1) *_w (y_0,y_1) = (x_0y_0, x_0^p y_1 + y_0^p x_1)$$

(for elements $a,b \in \mathbb{F}$ we write $a*b = ab$).

If $\mathbb{F} = \mathcal{R}/\mathcal{M}$ is the residue field of the Galois ring $\mathcal{R}$ it is easy to see that the mapping

$$\psi : \mathcal{R} \longrightarrow \mathcal{W}_2(\mathbb{F}),\ \hat{a} = \psi(a) = (\overline{a}_0, \overline{a}_1^p) \tag{1}$$

where $a = a_0 + a_1 p \in \mathcal{R}$, $a_0,a_1 \in \mathcal{T}$, is a ring isomorphism. The inverse mapping is:

$$\psi^{-1} : \mathcal{W}_2(\mathbb{F}) \longrightarrow \mathcal{R},\ \psi^{-1}\left(\overline{b}_0, \overline{b}_1\right) = B_0 + pB_1^{1/p} \tag{2}$$

where $B_0, B_1 \in \mathcal{T}$ are such that $\overline{B}_i = b_i$ (the bar means the image under the canonical mapping μ). If $\hat{a}, \hat{b}$ are any elements of the Witt ring $\mathcal{W}_2(\mathbb{F})$ and no confusion arises, the elements $\hat{a} +_w \hat{b}$ and $\hat{a} *_w \hat{b}$ will just be denoted by $\hat{a}+\hat{b}$ and $\hat{a}\hat{b}$ respectively.

3 The Gray Map

In this section, taking into consideration that the Galois ring $\mathcal{R} = \mathrm{GR}(p^2, m)$ and the Witt ring $\mathcal{W}_2(\mathbb{F})$ are isomorphic, the definition of the Gray map on this last ring is recalled.

Let $\mathbf{c}_0 \in \mathbb{F}^q$ be the vector that lists all the elements of $\mathbb{F}$, let $\mathbf{1} = (1, 1, ..., 1) \in \mathbb{F}^q$ be the all-1 vector of length $q = p^m$ and let M be the $2 \times q$ matrix whose first row is $\mathbf{c}_0$ and the second row is $\mathbf{1}$. Then the Gray map on $\mathcal{W}_2(\mathbb{F})$ is defined as:

$$\widehat{\phi} : \mathcal{W}_2(\mathbb{F}) \longrightarrow \mathbb{F}^q,\ \widehat{\phi}(a_0, a_1) = (a_0, a_1)\mathbf{M}. \tag{3}$$

The relation of the Gray map just defined and the Gray map ϕ as introduced in [4] is that

$$Im(\phi) = Im(\widehat{\phi} \circ \psi)$$

where ψ is the isomorphism between the Galois ring $\mathrm{GR}(p^2, m)$ and the Witt ring $\mathcal{W}_2(\mathbb{F})$ mentioned above.

In the sequel the Galois ring $\mathcal{R} = \mathrm{GR}(p^2, m)$ and the ring of (truncated) Witt vectors $\mathcal{W}_2(\mathbb{F})$ as well as the maps ϕ and $\widehat{\phi}$ will be used freely.

For a positive integer n, the Gray map is extended coordinate-wise to $\mathcal{R}^n$ or equivalently to $\mathcal{W}_2(\mathbb{F})^n$ as:

if $\mathbf{A} = (A_0, ..., A_{n-1}) \in \mathcal{R}^n$ then $\Phi(\mathbf{A}) = (\phi(A_0), ..., \phi(A_{n-1})) \in \mathbb{F}^{nq}$.

In the case $\mathrm{GR}(p^2, 1) = \mathbb{Z}/p^2\mathbb{Z}$ the Gray map just defined and the one given in [8] are the same up to a permutation.

We now recall the definition of the *homogeneous* weight on the Galois ring $\mathcal{R} = GR(p^n, m)$ (cf. [4], [6]):

$$wt_h(\gamma) = \begin{cases} (q-1)q^{n-2}, & \text{if } \gamma \in \mathcal{R} \setminus \langle p^{n-1} \rangle \\ q^{n-1}, & \text{if} \gamma \in \langle p^{n-1} \rangle \setminus \{0\} \\ 0, & \text{otherwise} \end{cases}$$

where as above $q = p^m$. Observe that in our case $n = 2$.

Also, the homogeneous weight is extended to $\mathcal{R}^n$ as:

$$wt_h(\mathbf{A}) = wt_h(A_0) + \cdots + wt_h(A_{n-1}).$$

It is easy to see that the homogeneous weight on $\mathcal{R}^n$ as defined above induces a metric, d_h, on $\mathcal{R}^n$. Let d_H be the Hamming metric on $\mathbb{F}^{nq}$. One of the main properties of the Gray map is the following (cf. [4]):

Theorem 1. *With the notation as introduced above, the Gray map is an injective isometry from $(\mathcal{R}^n, d_h)$ into $(\mathbb{F}^{nq}, d_H)$.*

The Gray map has other properties including the following,

Proposition 1. *With the notation as introduced above, let $\widehat{A} = (a_0, a_1)$ be any element of the Witt ring $\mathcal{W}_2(\mathbb{F})$ and let c_0, b_1 be any elements of $\mathbb{F}$. Then:*

$$\widehat{\phi}(0, c_0) = (c_0, ..., c_0)$$
$$\widehat{\phi}(\widehat{A} +_w (0, b_1)) = \widehat{\phi}(\widehat{A}) + \widehat{\phi}(0, b_1).$$

Proof. The first claim follows at once from the definition of the Gray map $\widehat{\phi}$. For the second part just observe that $\widehat{A} +_w (0, b_1)) = (a_0, a_1 + b_1)$ and the claim also follows from the definition of the Gray map.

In the case $\mathrm{GR}(p^2, 1) = \mathbb{Z}/p^2\mathbb{Z}$, Proposition 1 gives Proposition 2.1 of [8] for $k = 1$.

4 Gray Images of Codes

For the main results of this section a particular way of expressing and enumerating the elements of the residue field $\mathbb{F} = \mathbb{F}_{p^m}$ of the Galois ring $\mathcal{R} = \mathrm{GR}(p^2, m)$ (or the Witt ring $\mathcal{W}_2(\mathbb{F})$) is given.

For $i \in \mathbb{N}$ such that $0 \leq i \leq p^{m-1}$ let $i = d_{i0} + d_{i1}p + \cdots + d_{i(m-2)}p^{m-2}$ where $d_{is} \in \{0, \ldots, p-1\}$ for each $s \in \{0, \ldots, m-2\}$, be the representation for i in base p and let $(i)_p = (d_{i0}, d_{i1}, \ldots, d_{i(m-2)})$.

Since the field $\mathbb{F}$ is an extension of degree m of the base field $\mathbb{F}_p$ let $\Omega = \{1, \bar{\omega}, ..., \bar{\omega}^{m-1}\}$ be a basis of $\mathbb{F}$ over $\mathbb{F}_p$. For any $j \in \mathbb{N}$ such that $0 \leq j \leq p-1$ let

$$(j + (i)_p)\Omega = j + d_{i0}\bar{\omega} + d_{i1}\bar{\omega}^2 + \cdots + d_{i(m-2)}\bar{\omega}^{m-1}$$

and let

$$\mathbf{B}_j : (j + (0)_p)\Omega, (j + (1)_p)\Omega, \ldots, (j + (i)_p)\Omega, \ldots, (j + (p^{m-1} - 1)_p)\Omega, (j + (p^{m-1})_p)\Omega.$$

Then the elements of the field $\mathbb{F}_{p^m}$ can be taken as

$$\{B_0, B_1, ..., B_{p-1}\}.$$

Let M be the $2 \times p^m$ matrix whose first row consists of the elements of the residue field $\mathbb{F}$, taken in the order described above, and whose second row is the all one vector $\mathbf{1}$ of length $q = p^m$. Then the image of $(a_0, a_1) \in \mathcal{W}_2(\mathbb{F})$ under the Gray map, $\hat{\phi}(a_0, a_1) = (a_0, a_1)M$, (see (3)), is the vector of length q:

$$(a_0\mathbf{B}_0 + a_1\mathbf{1}, ..., a_0\mathbf{B}_j + a_1\mathbf{1}, ..., a_0\mathbf{B}_{p-1} + a_1\mathbf{1})$$

where

$$a_0\mathbf{B}_j + a_1\mathbf{1} : (j + (0)_p\Omega)a_0 + a_1, \ldots, (j + (i)_p\Omega)a_0 + a_1, \ldots, (j + (p^{m-1} - 1)_p\Omega)a_0 + a_1$$

for $0 \leq j \leq p - 1$.

Let $\alpha = 1 + Tp$ be a (principal) unit of the Galois ring $\mathcal{R} = GR(p^2, m)$ where $T \in \mathcal{T}$ is such that its image in the residue field $\mathbb{F}$ under the canonical mapping is equal to -1 and let $\hat{\alpha} = (1, p-1)$ be the corresponding element in the Witt ring $\mathcal{W}_2(\mathbb{F})$. Let σ be the usual cyclic shift, i.e., if $\mathbf{X} = (X_1, X_2, ..., X_q)$ then $\sigma(\mathbf{X}) = (X_q, X_1, ..., X_{q-1})$, and for any positive integer k, $0 \leq k \leq q$, σ^k shift k places.

With the notation as above we have the following,

Lemma 1. *Let $\hat{\phi}$ be the Gray map on $\mathcal{W}_2(\mathbb{F})$ and let $\hat{\alpha}$ be as introduced above. Then for any element $\hat{A} = (a_0, a_1) \in \mathcal{W}_2(\mathbb{F})$ such that $a_0 \in \mathbb{F}_p$ we have*

$$\hat{\phi}\left(\hat{\alpha}\hat{A}\right) = \sigma^{p^{m-1}}\left(\hat{\phi}(\hat{A})\right).$$

Proof. From the product on the Witt ring and the definiton of the Gray map it follows that

$$\hat{\phi}\left(\hat{\alpha}\hat{A}\right) = (..., a_0\mathbf{B}_j + ((p-1)a_0 + a_1)\mathbf{1}, ...) = (..., (j + (p-1) + (i)_p\Omega)a_0 + a_1, ...,)$$
$$= (a_0\mathbf{B}_{p-1} + a_1\mathbf{1}, ..., a_0\mathbf{B}_{j+(p-1)} + a_1\mathbf{1}, ..., a_0\mathbf{B}_{p-2} + a_1\mathbf{1})$$

(for $j \in \{0, 1, ..., p-1\}$, $j + (p-1)$ is taken modulo p and the product $\hat{\alpha}\hat{A}$ is taken in the Witt ring).

On the other hand,

$$\sigma^{p^{m-1}}\left(\hat{\phi}(\hat{A})\right) = \sigma^{p^{m-1}}(a_0\mathbf{B}_0 + a_1\mathbf{1}, ..., a_0\mathbf{B}_j + a_1\mathbf{1}, ..., a_0\mathbf{B}_{p-1} + a_1\mathbf{1})$$
$$= (a_0\mathbf{B}_{p-1} + a_1\mathbf{1}, ..., a_0\mathbf{B}_{j-1} + a_1\mathbf{1}, ..., a_0\mathbf{B}_{p-2} + a_1\mathbf{1})$$

and the claim is proved.

Define the following mappings:

1. Let $\hat{\alpha} = (1, p-1) \in \mathcal{W}_2(\mathbb{F})$ be as introduced above. Then,

$$\nu_{\hat{\alpha}} : \mathcal{W}_2(\mathbb{F})^n \longrightarrow \mathcal{W}_2(\mathbb{F})^n,\ \nu_{\hat{\alpha}}(\hat{A}_0, ..., \hat{A}_{n-1}) = (\hat{\alpha}\hat{A}_{n-1}, ..., \hat{A}_{n-2}).$$

2. Let $\mathbb{F} = \mathbb{F}_q$, $(q = p^m)$, be the residue field of the Galois ring $\mathcal{R}$ (or the Witt ring $\mathcal{W}_2(\mathbb{F})$) and σ be the usual cyclic shift. For any positive integer n let,

$$\tilde{\sigma} : \mathbb{F}^{nq} \longrightarrow \mathbb{F}^{nq},\ \tilde{\sigma}(\mathbf{X}) = (\sigma^{p^{m-1}}(\mathbf{X_{n-1}}), \mathbf{X_0}, ..., \mathbf{X_{n-2}})$$

i.e., the action of $\tilde{\sigma}$ on $\mathbf{X} = (\mathbf{X}_0, ..., \mathbf{X}_{n-1})$, where each $\mathbf{X}_i \in \mathbb{F}^q$, is to first apply the usual cyclic shift to $\mathbf{X}$ obtaining $(\mathbf{X}_{n-1}, \mathbf{X}_0, ..., \mathbf{X}_{n-2})$ and then apply the mapping $\sigma^{p^{m-1}}$ to $\mathbf{X}_{n-1}$ and the identity to the other entries $\mathbf{X}_i$.

Definition 1. *With the notation as introduced above, a code $\hat{\mathcal{C}} \subseteq \mathcal{W}_2(\mathbb{F})^n$ is called $\hat{\alpha}$-cyclic if $\nu_{\hat{\alpha}}(\hat{\mathcal{C}}) = \hat{\mathcal{C}}$.*

Proposition 2. *For any positive integer n let $\hat{\mathbf{A}} = (\hat{A}_0, ..., \hat{A}_{n-1}) \in \mathcal{W}_2(\mathbb{F})^n$ and assume that $\hat{A}_{n-1} = (a_0^{(n-1)}, a_1^{(n-1)})$ is such that $a_0^{(n-1)} \in \mathbb{F}_p$. Then*

$$\hat{\Phi} \circ \nu_\alpha = \tilde{\sigma} \circ \hat{\Phi}.$$

Proof. From the definition of the product on the Witt ring and the hypothesis on $a_0^{(n-1)}$, it follows that $\hat{\alpha}\hat{A}_{n-1} = (a_0^{(n-1)}, (p-1)a_0^{(n-1)} + a_1^{(n-1)})$. Then

$$\tilde{\sigma}(\hat{\Phi}(\hat{\mathbf{A}})) = (\sigma^{p^{m-1}}(\hat{\phi}(\hat{A}_{n-1}), \hat{\phi}(\hat{A}_0), ..., \hat{\phi}(\hat{A}_{n-2}))).$$

On the other hand,

$$\hat{\Phi}(\nu_\alpha(\hat{\mathbf{A}})) = (\hat{\phi}(\hat{\alpha}\hat{A}_{n-1}), \hat{\phi}(A_0), ..., \hat{\phi}(A_{n-2})).$$

Thus, in order to prove the claim of the proposition it is enough to show that

$$\sigma^{p^{m-1}}(\hat{\phi}(\hat{A}_{n-1})) = \hat{\phi}(\hat{\alpha}\hat{A}_{n-1})$$

but this relation follows from Lemma 1.

Definition 2. *With the notation as introduced above, a code $\tilde{\mathcal{D}} \subseteq \mathbb{F}^{nq}$ is called first-block quasi-cyclic of index p^{m-1} if $\tilde{\sigma}(\tilde{\mathcal{D}}) = \tilde{\mathcal{D}}$.*

As an immediate consequence of Proposition 2 we have the following:

Theorem 2. *Let $\hat{\mathcal{C}} \subseteq \mathcal{W}_2(\mathbb{F})^n$ be a code such that for each $\hat{\mathbf{A}} = (\hat{A}_0, ..., \hat{A}_{n-1}) \in \hat{\mathcal{C}}$, $\hat{A}_{n-1} = (a_0^{(n-1)}, a_1^{(n-1)}) \in \mathbb{F}_p \times \mathbb{F} \subseteq \mathcal{W}_2(\mathbb{F})$. Then $\hat{\mathcal{C}}$ is $\hat{\alpha}$-cyclic if and only if its Gray image $\hat{\Phi}(\hat{\mathcal{C}})$ is first-block quasi-cyclic of index p^{m-1}.*

Proof. If $\hat{\mathcal{C}} \subseteq \mathcal{W}_2(\mathbb{F})^n$ is a code such that $\hat{\Phi}(\hat{\mathcal{C}})$ is a first-block quasi-cyclic of index p^{m-1}, then from Proposition 2,

$$\hat{\Phi}(\hat{\mathcal{C}}) = \tilde{\sigma}\left(\hat{\Phi}(\hat{\mathcal{C}})\right) = \hat{\Phi}\left(\nu_\alpha(\hat{\mathcal{C}})\right)$$

and the claim follows from the injectivity of the Gray map. The other direction is also immediate from Proposition 2.

Observe that since $\mathbb{Z}/p^2\mathbb{Z} = GR(p^2, 1)$, Theorem 2 gives Theorem 2.4 for the case $k = 1$, i.e. Corollary 2.5 of [8], up to a permutation.

Let $\mathcal{R} = GR(p^2, m)$ be the Galois ring as before, $\mathcal{M}$ its maximal ideal, $\mathbb{F} = \mathbb{F}_q$, $(q = p^m)$ the residue field and $\mathcal{T}$ the Teichmüller set of $\mathcal{R}$. Let $n \in \mathbb{N}$ be such that $(n, p) = 1$ and $n' \in \{1, ..., p-1\}$ such that $nn' \equiv 1 \bmod p$. Let $N' \in \mathcal{T}$ be such that its image under the canonical map is n', $\gamma = 1 + N'p \in 1 + \mathcal{M}$ and $\hat{\gamma} = (1, n') \in \mathcal{W}_2(\mathbb{F})$ be its image in the Witt ring. Observe that for any positive integer k, $\hat{\gamma}^k = (1, (kn')_p)$, where $(*)_p$ means reduction modulo p. In particular $\hat{\gamma}^n = (1, 1)$.

Now define the following mappings:

1. With the notation as above,

$$\chi_{\hat{\gamma}} : \mathcal{W}_2(\mathbb{F})^n \longrightarrow \mathcal{W}_2(\mathbb{F})^n,\ \chi_{\hat{\gamma}}(\hat{\mathbf{A}}) = (\hat{A}_0, ..., \hat{\gamma}^i \hat{A}_i, ..., \hat{\gamma}^{n-1}\hat{A}_{n-1})$$

where $\hat{\mathbf{A}} = (\hat{A}_0, ..., \hat{A}_{n-1})$.

2. Let σ be the usual cyclic shift and let $\tau = \sigma^{p^{m-1}}$. Let

$$\tilde{\tau} : \mathbb{F}^{nq} \longrightarrow \mathbb{F}^{nq},\ \tilde{\tau}(\mathbf{X}) = (\tau^{(-0n')_p}(\mathbf{X}_0), ..., \tau^{(-in')_p}(\mathbf{X}_i), ..., \tau^{(-(n-1)n')_p}(\mathbf{X}_{n-1}))$$

where $\mathbf{X} = (\mathbf{X}_0, ..., \mathbf{X}_{n-1})$.

Definition 3. *With the notation as above, a code $\hat{\mathcal{C}} \subseteq \mathcal{W}_2(\mathbb{F})^n$ is said to be $\hat{\gamma}$-cyclic if $\chi_{\hat{\gamma}}(\hat{\mathcal{C}}) = \hat{\mathcal{C}}$.*

Definition 4. *If $\mathbb{F}$ is the residue field of the Galois ring $\mathcal{R}$, a code $\mathcal{D} \subseteq \mathbb{F}^{nq}$ is said to be $\tilde{\tau}$-quasi-cyclic if $\tilde{\tau}(\mathcal{D}) = \mathcal{D}$.*

Proposition 3. *With the notation as above, for any $\hat{\mathbf{A}} = (\hat{A}_0, ..., \hat{A}_{n-1}) \in \mathcal{W}_2(\mathbb{F})^n$ with $\hat{A}_i = (a_0^{(i)}, a_1^{(i)})$, $a_0^{(i)} \in \mathbb{F}_p$ for $i = 0, 1, ..., n-1$, the following relation holds:*

$$\hat{\Phi}\left(\chi_{\hat{\gamma}}(\hat{\mathbf{A}})\right) = \tilde{\tau}\left(\hat{\Phi}(\hat{\mathbf{A}})\right)$$

where $\hat{\Phi}$ is the Gray map on $\mathcal{W}_2(\mathbb{F})^n$.

Proof. From the definition of the mapping $\chi_{\hat{\gamma}}$ and the Gray map on $\mathcal{W}_2(\mathbb{F})^n$ it follows that,

$$\hat{\Phi}\left(\chi_{\hat{\gamma}}(\hat{\mathbf{A}})\right) = (\hat{\phi}(\hat{A}_0), ..., \hat{\phi}(\hat{\gamma}^i \hat{A}_i), ..., \hat{\phi}(\hat{\gamma}^{n-1}\hat{A}_{n-1})).$$

On the other hand, from the definition of the mapping $\tilde{\tau}$,

$$\tilde{\tau}(\Phi(\hat{\mathbf{A}})) = (\tau^{(-0n')_p}(\hat{\phi}(\hat{A}_0)), ..., \tau^{(-in')_p}(\hat{\phi}(\hat{A}_i)), ..., \tau^{(-(n-1)n')_p}(\hat{\phi}(\hat{A}_{n-1})).$$

From the product on the Witt ring and the hypothesis on $\hat{A}_i$ it follows that,

$$\hat{\phi}(\hat{\gamma}^i\hat{A}_i) = \left(a_0^{(i)}\mathbf{B}_{(\mathbf{in'})_\mathbf{p}} + a_1^{(i)}\mathbf{1}, ..., a_0^{(i)}\mathbf{B}_{(\mathbf{j+in'})_\mathbf{p}} + a_1^{(i)}\mathbf{1}, ..., a_0^{(i)}\mathbf{B}_{(\mathbf{p-1+in'})_\mathbf{p}} + a_1^{(i)}\mathbf{1}\right)$$

and

$$\tau^{(-in')_p}(\hat{\phi}(\hat{A}_i)) = \left((\tau^{-1})^{(in')_p}(a_0^{(i)}\mathbf{B_0} + a_1^{(i)}\mathbf{1}, ..., a_0^{(i)}\mathbf{B_j} + a_1^{(i)}\mathbf{1}, ..., a_0^{(i)}\mathbf{B_{p-1}} + a_1^{(i)}\mathbf{1})\right).$$

Observe that if $\mathbf{\Lambda} = (\Lambda_0, \Lambda_1, ..., \Lambda_{p-1})$ where $\Lambda_j = a_0^{(i)}\mathbf{B_j} + a_1^{(i)}\mathbf{1}$, it is easy to see that $\tau = \sigma^{p^{m-1}}$ acts on $\mathbf{\Lambda}$ as the usual cyclic shift, i.e., $\tau(\mathbf{\Lambda}) = (\Lambda_{p-1}, \Lambda_0, ..., \Lambda_{p-2})$ and for any positive integer k, $\tau^{-k}(\mathbf{\Lambda}) = (\Lambda_k, \Lambda_{k+1}, ..., \Lambda_{j+k}, ..., \Lambda_{p-2+k})$, (where $j+k$ is taken modulo p).

From this observation we conclude that $\hat{\phi}(\hat{\gamma}^i\hat{A}_i) = \tau^{(-in')_p}(\hat{\phi}(\hat{A}_i))$ for $i = 0, 1, ..., n-1$, proving the claim.

Now we have the following,

Theorem 3. *Let $\hat{\mathcal{C}} \subseteq \mathcal{W}_2(\mathbb{F})^n$ be a code of length n relatively prime to p such that for any $\hat{\mathbf{A}} = (\hat{A}_0, ..., \hat{A}_{n-1}) \in \hat{\mathcal{C}}$, $\hat{A}_i = (a_0^{(i)}, a_1^{(i)}) \in \mathbb{F}_p \times \mathbb{F}$, $0 \leq i \leq n-1$. Then the code $\hat{\mathcal{C}}$ is $\hat{\gamma}$-cyclic if and only if $\hat{\Phi}(\hat{\mathcal{C}})$ is a $\tilde{\tau}$-quasi-cyclic code of length nq over $\mathbb{F}$.*

Proof. If $\hat{\mathcal{C}} \subseteq \mathcal{W}_2(\mathbb{F})^n$ is a code such that $\hat{\Phi}(\hat{\mathcal{C}})$ is a $\tilde{\tau}$-quasi-cyclic code, from Proposition 3,

$$\hat{\Phi}(\hat{\mathcal{C}}) = \tilde{\tau}\left(\hat{\Phi}(\hat{\mathcal{C}})\right) = \hat{\Phi}\left(\chi_{\hat{\gamma}}(\hat{\mathcal{C}})\right)$$

and the claim follows from the injectivity of the Gray map. The other direction is also immediate from Proposition 3.

Notes and Comments. Let $n \in \mathbb{N}$ be such that $(n,p) = 1$, $\hat{\gamma} = (1, n')$ be as defined above and let $\hat{\beta}$ be its inverse. Let $\mathcal{A}_n = \mathcal{W}_2(\mathbb{F})[x]/\langle x^n - 1\rangle$, $\mathcal{B}_n = \mathcal{W}_2(\mathbb{F})[x]/\langle x^n - \hat{\beta}\rangle$ and $P : \mathcal{W}_2(\mathbb{F})^n \longrightarrow \mathcal{A}_n,\ P(\hat{a}_0, ..., \hat{a}_{n-1}) = \hat{a}_0 + \hat{a}_1 x + \cdots + \hat{a}_{n-1}x^{n-1}$, $P' : \mathcal{W}_2(\mathbb{F})^n \longrightarrow \mathcal{B}_n,\ P'(\hat{b}_0, ..., \hat{b}_{n-1}) = \hat{b}_0 + \hat{b}_1 x + \cdots + \hat{b}_{n-1}x^{n-1}$ be the polynomial representation mappings of $\mathcal{W}_2(\mathbb{F})^n$ into the rings $\mathcal{A}_n$ and $\mathcal{B}_n$, respectively. The following claims are easy to see (cf. [8], Section III):

1. $\mu_{\hat{\gamma}} : \mathcal{A}_n \longrightarrow \mathcal{B}_n,\ \mu_{\hat{\gamma}}(a(x)) = a(\hat{\gamma}x)$ is a ring isomorphism and in particular I is and ideal of $\mathcal{A}_n$ if and only if $\mu_{\hat{\gamma}}(I)$ is an ideal of $\mathcal{B}_n$.
2. A code $\hat{\mathcal{C}} \subset \mathcal{W}_2(\mathbb{F})^n$ is cyclic if and only if $P(\hat{\mathcal{C}})$ is an ideal of $\mathcal{A}_n$.
3. A code $\hat{\mathcal{C}} \subset \mathcal{W}_2(\mathbb{F})^n$ is $\hat{\beta}$-cyclic if and only if $P'(\hat{\mathcal{C}})$ is an ideal of $\mathcal{B}_n$.
4. $\mu_{\hat{\gamma}} \circ P = P' \circ \chi_{\hat{\gamma}}$.

Based on the claims just mentioned, Theorem 3 can be related to the concept of cyclicity and $\hat{\beta}$-cyclicity of a $\mathcal{W}_2(\mathbb{F})$-code of length n relatively prime to p but due to space limitations we are not able to provide further details.

References

1. Calderbank, A.R., Sloane, N.J.A.: Modular and p-adic Cyclic Codes. Des., Codes and Cryptogr. 6(1), 21–35 (1995)
2. Carlet, C.: Z_{2^k}-linear Codes. IEEE Trans. Inform. Theory 44, 1543–1547 (1998)
3. Dinh, H.Q., López-Permouth, S.R.: Cyclic and Negacyclic Codes Over Finite Chain Rings. IEEE Trans. Inform. Theory 50(8), 1728–1744 (2004)
4. Greferath, M., Schmidt, S.E., Gray, S.E.: isometries for Finite Chain rings and a Nonlinear Ternary $(36, 3^{12}, 15)$ Code. IEEE Trans. Inform. Theory 45, 2522–2524 (1999)
5. Hammons Jr., A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inform. Theory 40, 301–319 (1994)
6. Heise, W., Honold, T., Nechaev, A.A.: Weighted modules and representations of codes. In: Proc. ACCT, Pskov, Russia, vol. 6, pp. 123–129 (1998)
7. Kanwar, K., Lopez-Permouth, S.R.: Cyclic Codes over the Integers Modulo p^m. Finite Fields and Their Applications 3(4), 334–352 (1997)
8. Ling, S., Blackford, T.: $\mathbb{Z}_{p^{k+1}}$-linear Codes. IEEE Trans. Inform. Theory 48(9), 2592–2605 (2002)
9. Ling, S., Özbudak, F.: An Improvement of the Bound of Exponential Sums Over Galois Rings With Some Applications. IEEE Trans. Inform. Theory 50(10), 2529–2539 (2004)
10. Ling, S., Solé, P.: Non-linear p-ary sequences. J. Applied Algebra in Engineering Communication and Computing (AAECC) 14, 117–125 (2003)
11. McDonald, B.R.: Finite rings with identity. Pure and Applied Mathematics 28 (1974)
12. Nechaev, A.A.: The Kerdock code in a cyclic form. Math. Appl. 1, 365–384 (1991); (English translation of Diskret. Mat., 1989)
13. Nechaev, A.A., Kuzmin, A.S.: Kerdock codes in a cyclic form. Discr. Math. Appl. 1, 365–384 (1991)

14. Norton, G., Salagean-Mandache, A.: On the structure of linear cyclic codes over finite chain rings. Appl. Algebra Eng. Commun. Comput (AAECC) 10(6), 489–506 (2000)
15. Pless, V., Qian, Z.: Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. IEEE Trans. Inform. Theory 42, 1594–1600 (1996)
16. Pless, V., Solé, P., Qian, Z.: Cyclic self-dual $\mathbb{Z}_4$ codes. Finite Fields and their Applications 3, 48–69 (1997)
17. Serre, J.P.: Corps locaux. Publications de L'Institute de Mathématique de L'Université de Nancago VIII, Herman, Paris (1962)
18. Tapia-Recillas, H., The Gray, H.: map on GR(p^2, n) and Repeated-Root Cyclic Codes. In: Mullen, G.L., Poli, A., Stichtenoth, H. (eds.) Fq7 2003. LNCS, vol. 2948, pp. 181–196. Springer, Heidelberg (2004)
19. Tapia-Recillas, H., Vega, G.: On the $\mathbb{Z}_{2^k}$-Linear and Quaternary Codes. SIAM Journal on Discrete Mathematics 17(1), 103–113 (2003)
20. van Ash, B., van Tilborg, H.C.A.: Two "Dual" families of Nearly-Linear Codes over $\mathbb{Z}_p$, p odd. J. Applied Algebra in Engineering Communication and Computing (AAECC) 11, 313–329 (2001)
21. Wan, Z.X.: Lectures on Finite Fields and Galois Rings. World Scientific Publish. Co., Singapure (2003)
22. Wolfmann, J., Binary, W.: images of cyclic codes over $\mathbb{Z}_4$. IEEE, Trans. Inform. Theroy 47, 1773–1779 (2001)

Algebraic Geometry Codes from Castle Curves

C. Munuera[1], A. Sepúlveda[2], and F. Torres[2]

[1] Dept. of Applied Mathematics, University of Valladolid
Avda Salamanca SN, 47012 Valladolid, Castilla, Spain
[2] IMECC-UNICAMP, Cx.P. 6065, 13083-970, Campinas-SP, Brasil

Abstract. The quality of an algebraic geometry code depends on the curve from which the code has been defined. In this paper we consider codes obtained from *Castle curves*, namely those whose number of rational points attains the Lewittes' bound for some rational point Q and the Weierstrass semigroup at Q is symmetric.

1 Introduction

Goppa constructed error correcting linear codes by using tools from Algebraic Geometry: a nonsingular, projective, geometrically irreducible, algebraic curve $\mathcal{X}$ of genus g defined over $\mathbf{F}_q$, the finite field with q elements, and two rational divisors D and G on $\mathcal{X}$; see [12,13,30]. These divisors are chosen in such a way that they have disjoint supports and D equals to a sum of pairwise distinct rational points, $D = P_1 + \ldots + P_n$. The *algebraic geometry* (or simply AG) code defined by the triple $(\mathcal{X}, D, G)$ is the q-ary linear space

$$C(\mathcal{X}, D, G) := \{ev(f) := (f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\},$$

where $\mathcal{L}(G) = \{f \in \mathbf{F}_q(\mathcal{X})^* : G + \mathrm{div}(f) \succeq 0\} \cup \{0\}$ is the Riemann-Roch space associated to G. Soon after its introduction, AG codes become an important instrument in Coding Theory; for example, Tsfasman, Vlăduţ and Zink showed that the Gilbert-Varshamov bound can be improved by using them, [32]. Later, Pellikaan, Shen and van Wee [28] noticed that any arbitrary linear code is in fact an AG-code.

The study of AG codes, which is based on resources from algebraic geometry, is usually difficult. For example, it is well known that the parameters k and d (the dimension and the minimum distance) of $C(\mathcal{X}, D, G)$ verify

1. $k = \ell(G) - \ell(G - D)$, where $\ell(\cdot)$ denotes the dimension of $\mathcal{L}(\cdot)$; and
2. $d \geq d(\mathcal{X}, D, G) := n - \deg(G)$ (the *Goppa bound*).

However the exact determination of k and d is often not possible. If $2g - 2 < \deg(G) < n$ then the code $C(\mathcal{X}, D, G)$ is called *strongly* AG; in this case, the Riemann-Roch theorem gives $k = \deg(G) - 1 + g$. In other cases $\ell(G)$ and/or $\ell(G - D)$ are rather difficult to compute. On the other hand, if $\deg(G) \geq n$, the above bound on d does not give any information; nevertheless, Munuera [24]

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 117–127, 2008.

improved (2) by using another geometric invariant of the curve, see (1) below. For an integer $r \geq 1$, set

$$\gamma_r = \gamma_r(\mathcal{X}, q) := \min\{\deg(A) : A \text{ is a } \mathbf{F}_q\text{-rational divisor on } \mathcal{X} \text{ with } \ell(A) \geq r\}\,.$$

The number $\gamma(\mathcal{X}, q) := \gamma_2$ and the sequence $(\gamma_r)_{r\geq 1}$ are called respectively the *gonality* (resp. *gonality sequence*) of $\mathcal{X}$ over $\mathbf{F}_q$; cf. [34]. We have

$$d \geq n - \deg(G) + \gamma_{a+1}\,, \tag{1}$$

where a is the *abundance* of the code, namely $a := \ell(G-D)$; unfortunately both the genus and the gonality sequence of curves are usually very hard to compute.

Other lower bounds on the minimum distance on AG-codes have been developed by several authors; it seems that the more interesting of them is the *order* (or *Feng-Rao*) bound cf. [19], but it can be applied only to the duals of *one-point* AG codes; i.e., those AG codes for which G is a multiple of a rational point (although there is an analogous for “two-point” AG codes, see [5,27]). We stress that, in general, the minimum distance of the dual $C^{\perp}$ of C does not give information on the minimum distance of C.

Let $C(\mathcal{X}, D, mQ)$ be a one-point AG code. The space $\mathcal{L}(G)$ is closely related to the Weierstrass semigroup at Q

$$S(Q) = \{0 = \rho_1(Q) < \rho_2(Q) < \ldots\} = \{-v_Q(f) : f \in \cup_{r=0}^{\infty}\mathcal{L}(rQ)\}$$

where v_Q is the valuation at Q. The element $\rho_2(Q)$ is usually called the *multiplicity* at (resp. of) Q (resp. $S(Q)$). As we mentioned above, $k = m - 1 + g$ for $2g - 2 < m < n$. In any case, if $\rho_i(Q) \leq m < \rho_{i+1}(Q)$ then $k = i$, so $S(Q)$ gives the dimension of $C(\mathcal{X}, D, mQ)$. Analogously, the computation of the order bound of the code $C(\mathcal{X}, D, mQ)^{\perp}$ depends also on the semigroup $S(Q)$, see [19]. Therefore, the problems of computing the dimension and the minimum distance of (the duals of) one-point AG codes go through the problem of computing Weierstrass semigroups, which is not an easy problem at all.

Fortunately, we know some curves that combine the good properties of having a reasonable handling and giving one-point codes with excellent parameters (some times records in the tables [18]); such curves include the Deligne-Lusztig varieties of dimension one [6] (namely the projective line, the Hermitian curve, the Suzuki curve and the Ree curve), the generalized Hermitian curves [9], the Norm-Trace curves [10], etc. It is natural to ask if these curves share some common characteristic that motives all these good properties. At the first look, all the aforementioned curves have 'many' rational points; as a matter of fact, the Deligne-Lusztig curves are *optimal* in the sense that they have the maximum number of rational points that curves of its genus defined over the same ground field can have, see [15]. Several bounds on the number of rational points of curves are available in the literature, see e.g. [30]. For our purposes it is relevant the one given by Lewittes in [21]: if Q is a rational point of $\mathcal{X}$, then

$$\#\mathcal{X}(\mathbf{F}_q) \leq q\rho_2(Q) + 1\,. \tag{2}$$

This bound was proved by using the theory of Algebraic Function Fields of one variable (or see Theorem 1 below). It was recently improved by Geil and Matsumoto in [11].

In this paper we are interested in curves reaching equality in (2) and for which the semigroup $S(Q)$ is symmetric (in the sense that $\rho \in S(Q)$ if and only if $2g - 1 - \rho \notin S(Q)$). We shall refer to these curves as *Castle curves* (here the word 'castle' is used to honoring the place where this meeting is realized!). The aforementioned Norm-Trace curve, the generalized Hermitian curve and Deligne-Lusztig curves are all of them Castle curves. Also we shall show some common properties of one-point Goppa codes arising from Castle curves.

2 Castle Curves

Let $\mathcal{X}$ be a curve over $\mathbf{F}_q$ with $(n+1)$ $\mathbf{F}_q$-rational points. Write $\mathcal{X}(\mathbf{F}_q) = \{Q, P_1, \ldots, P_n\}$. The following Theorem, due to Geil and Matsumoto [11, Thm. 1], gives an upper bound on $\#\mathcal{X}(\mathbf{F}_q)$. It generalizes a previous result of Lewittes [21, Thm. 1]. For the convenience of the reader we shall include a short proof of the Lewittes bound.

Theorem 1. *Let $S(Q)$ be the Weierstrass semigroup at Q. Set $s + S(Q) := \{s + \rho : \rho \in S(Q)\}$ and $S^*(Q) := S(Q) \setminus \{0\}$. Then*

$$\#\mathcal{X}(\mathbf{F}_q) \leq \#(S(Q) \setminus (qS^*(Q) + S(Q))) + 1\,.$$

In particular $\#\mathcal{X}(\mathbf{F}_q) \leq q\rho_2(Q) + 1$.

Proof. Set $\rho_2 = \rho_2(Q)$ and let $f \in \mathcal{L}(\rho_2 Q)$ be a rational function such that $\rho_2 = -v_Q(f)$. Then $f^q \in \mathcal{L}(q\rho_2 Q)$ and $ev(f^q) = ev(f)$. Since ev is injective for $m = q\rho_2 < n = \#\mathcal{X}(\mathbf{F}_q) - 1$ and $f^q \neq f$, we have $q\rho_2 \geq n$, which is the Lewittes' bound. A similar reasoning leads to the Geil-Matsumoto bound.

Example 1. A rational curve is clearly a Castle curve. A hyperelliptic curve is a Castle curve if and only if it has just one hyperelliptic rational point and attains equality in the hyperelliptic bound $\#\{$rational nonhyperelliptic points$\} + 2\#\{$rational hyperelliptic points$\} \leq 2q + 2$.

Example 2. (The Norm-Trace curve). Let us consider the curve defined over $\mathbf{F}_{q^r}$ by the affine equation

$$x^{(q^r-1)/(q-1)} = y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y$$

or equivalently by $N_{\mathbf{F}_{q^r}|\mathbf{F}_q}(x) = T_{\mathbf{F}_{q^r}|\mathbf{F}_q}(y)$, where the maps N and T are respectively the norm and trace from $\mathbf{F}_{q^r}$ to $\mathbf{F}_q$. This curve has $2^{2r-1} + 1$ rational points and the Weierstrass semigroup at the unique pole Q of x is given by

$$S(Q) = \langle q^{r-1}, (q^r - 1)/(q-1) \rangle\,.$$

Since every semigroup generated by two elements is symmetric, this is a Castle curve. Codes on these curves have been studied by Geil, [10].

Example 3. (Generalized Hermitian curves) For $r \geq 2$ let us consider the curve $\mathcal{X}_r$ over $\mathbf{F}_{q^r}$ defined by the affine equation

$$y^{q^{r-1}} + \ldots + y^q + y = x^{1+q} + \ldots + x^{q^{r-2}+q^{r-1}}$$

or equivalently by $s_{r,1}(y, y^q, \ldots, y^{q^{r-1}}) = s_{r,2}(x, x^q, \ldots, x^{q^{r-1}})$, where $s_{r,1}$ and $s_{r,2}$ are respectively the first and second symmetric polynomials in r variables. Note that $\mathcal{X}_2$ is the Hermitian curve. These curves were introduced by Garcia and Stichtenoth in [9] and they have $q^{2r-1}+1$ rational points. Let Q be the only pole of x. Then $S(Q) = \langle q^{r-1}, q^{r-1}+q^{r-2}, q^r+1\rangle$. This semigroup is telescopic (loc. cit.) and hence symmetric (see e.g. [22]). Therefore, $\mathcal{X}_r$ is a Castle curve. AG-codes based on these curves were studied by Bulygin [4] in the binary case and by Sepúlveda [29] in the general case.

To show that the Deligne-Lusztig curves are Castle curves, we shall point out an interesting interplay between Castle curves and Jacobian Varieties of curves (cf. [8]). Let $L(t)$ be the numerator of the Zeta function of $\mathcal{X}$ over $\mathbf{F}_q$. Set

$$h(t) := t^{2g} L(t^{-1}) \,.$$

Then $h(t)$ is monic of degree $2g$ and its independent term is nonzero. Moreover it is the characteristic polynomial of the Frobenius morphism $\mathbf{\Phi}_{\mathcal{J}}$ on the Jacobian $\mathcal{J}$ of $\mathcal{X}$ (here we see $\mathbf{\Phi}_{\mathcal{J}}$ as an endomorphism acting on the Tate module). Let

$$h(t) = \prod_j h_j^{r_j}(t)$$

be the factorization of $h(t)$ in $\mathbf{Z}[t]$. Since $\mathbf{\Phi}_{\mathcal{J}}$ is semisimple and the representation of endomorphisms of $\mathcal{J}$ on the Tate module is faithfully (see [33, Thm. 2], [20, VI§3]), it follows that

$$\prod_j h_j(\mathbf{\Phi}_{\mathcal{J}}) = 0 \,. \tag{3}$$

Let $\mathbf{\Phi} : \mathcal{X} \to \mathcal{X}$ denote the Frobenius morphism on $\mathcal{X}$. Let $\pi : \mathcal{X} \to \mathcal{J}$ be the natural morphism given by $P \mapsto [P-Q]$, $Q \in \mathcal{X}(\mathbf{F}_q)$. Since $\pi \circ \mathbf{\Phi} = \mathbf{\Phi}_{\mathcal{J}} \circ \pi$, (3) implies the following equivalence of divisors on $\mathcal{X}$

$$\prod_j h_j(\mathbf{\Phi})(P) \sim mQ \,, \quad \text{with} \quad P \in \mathcal{X} \text{ and } m = \textstyle\prod_j h_j(1) \,. \tag{4}$$

This suggests to study the linear series $\mathcal{C} := |mQ|$. Remark that $\mathcal{C}$ is independent of the rational point Q, and $|m|$ belongs to the Weierstrass semigroup at any rational point. Let us write

$$\prod_j h_j(t) = t^U + \alpha_1 t^{U-1} + \ldots + \alpha_{U-1} t + \alpha_U \,.$$

Proposition 1. *Notation as above. Suppose that* (i) $\alpha_1 \geq 1$, (ii) $\alpha_{j+1} \geq \alpha_j$ *for* $j = 1, \ldots, U-1$, *and* (iii) $\#\mathcal{X}(\mathbf{F}_q) \geq q\alpha_U + 1$. *Then, for any* $P \in \mathcal{X}(\mathbf{F}_q)$ *we have*

1. $\#\mathcal{X}(\mathbf{F}_q) = q\rho_2(P) + 1$;
2. $\rho_2(P) = \alpha_U$;
3. $\gamma(\mathcal{X}, q) = \alpha_U$.

Proof. We first show that α_U is a generic non-gap (that is, a non-gap at a point which is not a Weierstrass point). In fact, by applying $\mathbf{\Phi}_*$ to (4) we get

$$\alpha_U R \sim \mathbf{\Phi}^{U+1}(R) + (\alpha_1 - 1)\mathbf{\Phi}^{U}(R) + (\alpha_2 - \alpha_1)\mathbf{\Phi}^{U-1}(R) + \ldots + (\alpha_U - \alpha_{U-1})\mathbf{\Phi}(R).$$

By (i) and (ii), α_U is a non-gap at any point R such that $\phi^{U+1}(R) \neq R$, i.e., at any point which is not a fixed point of ϕ^{U+1}. Since the number of fixed points of this morphism is finite, the claim follows. By standard Weierstrass point theory, it holds that $\rho_2(P) \leq \alpha_U$. Thus from (iii) and the Lewittes' bound (2), we have

$$q\alpha_U + 1 \leq \#\mathcal{X}(\mathbf{F}_q) \leq q\rho_2(P) + 1 \leq q\alpha_U + 1$$

and (1), (2) follow. Now set $\gamma = \gamma(\mathcal{X}, q)$. Then, as $\gamma \leq \alpha_U$ by definition of γ and $\#\mathcal{X}(\mathbf{F}_q) \leq (q+1)\gamma$, (iii) holds as $\alpha_U \leq q$.

For the definition of the for the Hermitian curve $\mathcal{H}$, the Suzuki curve $\mathcal{S}$, and the Ree curve $\mathcal{R}$, as well as for their main properties, we refer to the bibliography [15,16,19,23]. In particular, the polynomials $h(t)$ for these curves are as follows, see e.g. [15]:

(I) $h_{\mathcal{H}}(t) = (t + \ell)^{2g}$, where $q = \ell^2$ and $g = \ell(\ell - 1)/2$;
(II) $h_{\mathcal{S}}(t) = (t^2 + 2q_0 t + q)^g$, where $q = 2q_0^2 > 2$ and $g = q_0(q - 1)$;
(III) $h_{\mathcal{R}}(t) = (t^2 + q)^A(t^2 + 3q_0 t + q)^B$, where $q = 3q_0^2 > 3$, $A = q_0(q - 1)(q + 3q_0 + 1)/2$, $B = q_0(q^2 - 1)$ and $g = 2A + 2B$.

By using these polynomials, and after some computations, we obtain the following data for any rational point P.

Curve $\mathcal{X}$	Hermitian	Suzuki	Ree
$\rho_2(P) = \gamma(\mathcal{X}, q)$	ℓ	q	q^2
$\#\mathcal{X}(\mathbf{F}_q)$	$\ell^3 + 1$	$q^2 + 1$	$q^3 + 1$
m	$1 + \ell$	$1 + 2q_0 + q$	$(1 + q)(1 + 3q_0 + q))$
$\mathcal{C}$	$\|(1 + \ell)P\|$	$\|(1 + 2q_0 + q)P\|$	$\|(1 + q)(1 + 3q_0 + q)P\|$

.

In order to study the symmetry of the Weierstrass semigroups associated to these curves, let us first recall some facts from the Stöhr-Voloch theory, concerning to a geometric bound on the number of rational points of curves over finite fields [31]. Let x, y be rational functions such that

$$\mathrm{div}_\infty(x) = \rho_2(P)P \quad \text{and} \quad \mathrm{div}_\infty(y) = mP.$$

Consider the morphism $\phi = (1 : x : y) : \mathcal{X} \to \mathbf{P}^2(\overline{\mathbf{F}}_q)$. The linear series $\mathcal{E}$ associated to ϕ is given by the divisors $\{\mathrm{div}(\ell) + mP : \ell = a + bx + cy\,, (a : b : c) \in \mathbf{P}^2(\overline{\mathbf{F}}_q)\}$. Let $v = v_Q$ denote the valuation at $Q \in \mathcal{X}$. For all but finitely many points Q, there exist lines $\ell_0 = \ell_0(Q), \ell_1 = \ell_1(Q)$ and $\ell_2 = \ell_2(Q)$, such that $v(\ell_0) = 0$, $v(\ell_1) = 1$ and $v(\ell_2) = \epsilon_2 > 1$, this number being independent of Q [31, Thm. 1.5]. To deal with rational points, we consider the sequence $0 = \nu_0 < \nu_1$ where $\nu_1 = 1$ or $\nu_1 = \epsilon_2 > 1$. According to [31, Sect. 2], the last case occurs if and only if $\mathbf{\Phi}(Q) \in \mathrm{div}(\ell_2) + mP$ for all but finitely many points Q. In our case, the last condition holds true by (4). Thus it holds that

$$y^q - y = \frac{dy}{dx}(x^q - x)\,. \tag{5}$$

Proposition 2. *Let P be a rational point of the Hermitian, Suzuki or Ree curve. Then the Weierstrass semigroup at P is symmetric.*

Proof. For Hermitian and Suzuki curves the Weierstrass semigroups are known and the symmetry follows after some arithmetical computations (although alternative conceptual proofs can be done by using the above reasoning). We shall omit them. For the Ree curve it seems that the structure of $S(P)$ $(P \in \mathcal{X}(\mathbf{F}_q))$ is no available; nevertheless, we can still prove the symmetry property via the linear series $\mathcal{E}$. Here we have $\rho_2(P) = q^2 \quad$ and $\quad m = (1+q)(1+3q_0+q)$. Let t be a local parameter at P. We will show that $v(\frac{dx}{dt}) = 2g-2$. Remark that $\#\mathcal{X}(\mathbf{F}_q) = q^3+1 = (q-3q_0+1)m$ and $2g-2 = (3q_0-2)m$. By applying the chain rule to (5), and since $\gcd(m,q) = 1$, we have

$$v(\frac{dx}{dt}) - qm = -m - 1 - q\rho_2(P) = -m - \#\mathcal{X}(\mathbf{F}_q)$$

or equivalently

$$v(\frac{dx}{dt}) = (q-1)m - m - (q-3q_0+1)m = (3q_0-2)m.$$

Example 4. (Castle maximal curves) Let $\mathcal{X}$ be a maximal curve of genus g over $\mathbf{F}_q$, $q = \ell^2$. Then $\mathcal{X}$ is a Castle curve if and only if there exists $Q \in \mathcal{X}(\mathbf{F}_q)$ such that $1 + \ell^2 + 2g\ell = 1 + \ell^2\rho_2(Q)$. Thus $\mathcal{X}$ must be a curve of genus $g = \ell(\rho_2(Q) - 1)/2$. Apart from the Hermitian curve, such curves do exist. For example:

- The curve defined by $y^{\ell/2} + y^{\ell/2^2} + \ldots + y^2 + y = x^{\ell+1}$ with ℓ even; here the genus is $\ell(\ell-2)/4$ and $\rho_2(Q) = \ell/2$ where Q is the unique pole of x (see [2]);
- The curve defined by $y^{\ell/3} + y^{\ell/9} + \ldots + y^3 + y = ax^{\ell+1}$, where ℓ is a power of three, $a \in \mathbf{F}_q$ with $a^{\ell-1} = -1$; here the genus is $\ell(\ell-3)/6$ and $\rho_2(Q) = \ell/3$ at P the unique pole of x (see [3]).

Further examples can be find in [1].

The next Proposition collects some properties of Castle curves. Let us remember that by $\gamma_r = \gamma_r(\mathcal{X}, q)$ we denote the r-th gonality of $\mathcal{X}$ over $\mathbf{F}_q$.

Proposition 3. *Let $\mathcal{X}$ be a Castle curve with respect to a point $Q \in \mathcal{X}(\mathbf{F}_q)$, where the multiplicity at Q satisfy $\rho_2(Q) \leq q+1$. Then*

1. *$\gamma_2 = \rho_2(Q)$;*
2. *$\gamma_i = \rho_i(Q)$ for $i \geq g - \gamma + 2$; that is,*

$$\gamma_i = \rho_i(Q) = \begin{cases} i + g - 2 & \textit{if } g - \gamma + 2 \leq i \leq g; \\ i + g - 1 & \textit{if } i > g; \end{cases}$$

3. *We have the equivalence of divisors on $\mathcal{X}$*

$$\sum_{P \in \mathcal{X}(\mathbf{F}_q)} P \sim (q\rho_2(Q) + 1)Q\,.$$

Proof. Set $\rho_i := \rho_i(Q)$. (1) We have $\rho_2 - (\rho_2 - 1)/(q + 1) \leq \gamma \leq \rho_2$ and the hypothesis on ρ_2 implies the result. (2) The statement about the gonalities of high order follows from the fact that both, the semigroup $S(Q)$ and the set of gonalities $GS(\mathcal{X}) = (\gamma_r)_{r \geq 1}$ verify the same symmetry property: for every integer a, it holds that $a \in S(Q)$ (resp. $a \in GS(\mathcal{X})$) if and only if $2g-1-a \notin S(Q)$ (resp. $2g - 1 - a \notin GS(\mathcal{X})$), cf. [26]. (3) As we have seen in the proof of Theorem 1, the code $C(\mathcal{X}, P_1 + \ldots + P_n, nQ)$ is abundant, hence $\ell(nQ - D) = 1$.

3 Codes on Castle Curves

Let $\mathcal{X}$ be a curve of genus g over $\mathbf{F}_q$ with $(n + 1)$ $\mathbf{F}_q$-rational points, $\mathcal{X}(\mathbf{F}_q) = \{Q, P_1 \ldots, P_n\}$. Consider the sequence of codes $(C_m)_{m \geq 1}$, where $C_m = C(\mathcal{X}, P_1 + \ldots + P_n, mQ)$, and let k_m, d_m be the dimension and the minimum distance of C_m, respectively. Let $S(Q) = \{0 = \rho_1 < \rho_2 < \ldots\}$ be the Weierstrass semigroup at Q. Define the function $\iota = \iota_Q : \mathbf{N}_0 \to \mathbf{N}$ by $\iota(m) = \max\{i : \rho_i \leq m\}$. Note that $\iota(m) = \ell(mQ)$. Let us remember that two $\mathbf{F}_q$-codes C_1 and C_2 of the same length n, are *isometric* if there is an n-uple $\mathbf{x}$ of nonzero elements in $\mathbf{F}_q$ such that $C_1 = \mathbf{x} * C_2 := \{\mathbf{x} * \mathbf{c} : \mathbf{c} \in C_2\}$, where $*$ stands for the coordinate wise product, see [25].

Proposition 4. *If $\mathcal{X}$ is a Castle curve with respect to Q, then*

1. *For $m < n$, the dimension of C_m is $k_m = \iota(m)$;*
2. *For $m \geq n$, C_m is an abundant code of abundance $\iota(m - n)$ and dimension $k_m = \iota(m) - \iota(m - n)$;*
3. *The dual of C_m is isometric to $C_{n+2g-2-m}$;*
4. *For $1 \leq m < n$, d_m reaches Goppa bound if and only if d_{n-m} does;*
5. *The minimum distance of C_n verifies $d_n \geq \rho_2(Q)$.*

Proof. (1) Since ev is injective over $\mathcal{L}(mQ)$ for $m < n$, the result follows from the fact that $\iota(m) = \ell(mQ)$. (2) We have already seen that C_n is abundant. Thus, in view of Proposition 3, if $m \geq n$ the abundance of C_m for $m \geq n$ is $\ell(mQ-D) = \ell(mQ-nQ) = \iota(m-n)$. The statement about the dimension follows trivially. (3) The dual of C_m is $C(D, D + W - mQ)$, where W is a differential form with simple poles and residue 1 at each P_i (see [25]). Now, in view of Proposition 3, $P_1 + \ldots + P_n \sim nQ$ and $(2g - 2)Q \sim W$ (as the semigroup S is symmetric). Thus $P_1 + \ldots + P_n + W - mQ \sim (n + 2g - 2 - m)Q$ and codes C_m, $C_{n+2g-2-m}$ are isometric, see [25]. (4) For $m < n$, C_m reaches equality in the Goppa bound if and only if then there exists $D', 0 \leq D' \leq D$ such that $mQ \sim D'$. Let $D'' = D - D'$. Thus $mQ \sim D - D'' \sim nQ - D''$, hence $(n - m)Q \sim D''$ and the code C_{n-m} also reaches equality in the Goppa bound. (5) Since $\gamma_2 = \rho_2$, this is just the improved Goppa bound on the minimum distance.

Remark 1. Since isometric codes have the same parameters, property 3 of the above Proposition allows us to use the order bound to estimate the minimum distance of these codes.

Example 5. Let us consider codes on the Suzuki curve $\mathcal{S}$ over $\mathbf{F}_8$. Here $g = 2(8-1) = 14$ and $\#\mathcal{S}(\mathbf{F}_8) = 8^2 + 1 = 65$.

Let $m = 50$. We have $k_{50} = 50 + 1 - 14 = 37$. The Goppa bound gives $d_{50} \geq 14$ and by applying the order bound we in fact obtain a $[64, 37, \geq 16]$ code over $\mathbf{F}_8$. Note that according to the Grassl tables [14], it is not known a $[64, 37]$ code over $\mathbf{F}_8$ having minimum distance $d > 16$.

Analogously, for $m = 73$ we obtain a $[64, 58, \geq 4]$ which has the best known parameters.

Finally, by applying now the bound stated in item 5 of the above proposition for $m = 63$, we get a $[64, 50, \geq 8]$ code, again a record. All these facts were unknown up the the moment, even if the codes are known longtime ago. By the way, note that the order bound on the minimum distance of this last code gives $d([64, 50]) \geq 6$. This shows that the order bound is not always better that the improved Goppa bound.

4 A Worked Example

In [7], Deolalikar constructed a subcover of the Garcia-Stichtenoth curve (see Example 3) in the particular case $r = 3$. In this section, we generalize his construction obtaining Castle curves.

Proposition 5. *Let $\mathcal{X}_r$ be a Garcia-Stichtenoth curve over $\mathbf{F}_{q^r}$ and let $b \in \mathbf{F}_{q^r}^*$ such that $T_{\mathbf{F}_{q^r}|\mathbf{F}_q}(b) = 0$, being T the trace function. Then for $j = 1, \ldots, r-2$, the curve $\mathcal{X}_r^j$ defined over $\mathbf{F}_{q^r}$ by the affine equation*

$$s_{r,2}(x, x^q, \ldots, x^{q^{r-1}}) =$$

$$y_j^{q^j} - \left(\frac{1}{b^{q^j - q^{j-1}}} + \cdots + \frac{1}{b^{q^j - 1}}\right) y_j^{q^{j-1}} - \cdots - \left(\frac{1}{b^{q^2 - q}} + \frac{1}{b^{q^2 - 1}}\right) y_j^q - \frac{1}{b^{q-1}} y_j,$$

where $s_{r,2}$ is the second symmetric polynomial, is covered by $\mathcal{X}_r$.

Proof. A covering map $c : \mathcal{X}_r \rightarrow \mathcal{X}_r^j$ is given by $c(x, y) =$

$$(x, y^{q^{r-j-1}} + (b^{q^{r-1}-1} + \cdots + b^{q^{r-j}-1} + 1) y^{q^{r-j-2}} + \cdots + (b^{q^{r-1}-1} + \cdots + b^{q^2-1} + 1) y)$$

Let $Q^j \in \mathcal{X}_r^j$ be the only pole of x.

Proposition 6. *The curve $\mathcal{X}_r^j$, $j = 1, \ldots, r-2$, verifies the following properties.*

1. *Q^j is totally ramified.*
2. *The genus of $\mathcal{X}_r^j$ is $g = (q^j - 1)q^{r-1}/2$.*
3. *The number of rational points of $\mathcal{X}_r^j$ is $q^{r+j} + 1$.*
4. *The Weierstrass semigroup at $Q^j \in \mathcal{X}_r^j$ is $S(Q^j) = \langle q^j, q^{r-1} + 1 \rangle$.*

Proof. (1) $Q \in \mathcal{X}_r$ is totally ramified. (2) and (3) follow from [7, Thm. 3.5]. (4) It is clear that $-v_Q(x) = q^j$. Let us consider the rational function $z := x^{1+q} + x^{1+q^2} + \cdots + x^{q^{r-3}+q^{r-2}} - y_j^{q^{j-1}}$. Then $z^q = x^{q+q^2} + x^{q+q^3} + \cdots + x^{q^{r-2}+q^{r-1}} - y_j^{q^j}$ and, by using the defining equation of $\mathcal{X}_r^j$, we obtain $-v_Q(z) = q^{r-1} + 1$. Now, since the genus of $\langle q^j, q^{r-1} + 1 \rangle$ is g, we get the equality.

In particular, $\mathcal{X}_r^j$ is a Castle curve. Other consequence of the above Proposition is the following.

Proposition 7. *Let $z = x^{1+q} + x^{1+q^2} + \cdots + x^{q^{r-3}+q^{r-2}} - y_j^{q^{j-1}}$. Then $\mathcal{L}(mQ^j) = \langle \{x^i z^k : i \cdot q^j + k \cdot (q^{r-1} + 1) \leq m, 0 \leq i$ and $0 \leq k < q^j\} \rangle$, for all $m \geq 0$.*

For $m = 0, 1, 2, \ldots$, we can consider the codes $\mathcal{C}_{r,m}^j := C(\mathcal{X}_r^j, D, mQ_\infty^j)$, where D is the sum of all rational points of $\mathcal{X}_r^j$ except Q^j. The length of these codes is $n = q^{r+j}$. The dimension and minimum distance can be estimated as shown in Proposition 4.

Example 6. For $q = 2$ and $r = 3$, the curve $\mathcal{X}_3^1$ is hiperelliptic of genus 2 over $\mathbf{F}_8$. It has 17 rational points. By using the order bound, we show that for $m = 13$ we get a $[16, 12, 4]$ code over $\mathbf{F}_8$. Note that, according to the main conjecture on MDS codes, there is no $[16, 12, > 4]$ code over $\mathbf{F}_8$.

When $q = 2$ and $j = 1$, then $\mathcal{X}_r^j$ is a hyperelliptic curve and Q_∞^j a hyperelliptic point. Let us consider the code $\mathcal{C}_{r,m}^1 = C(\mathcal{X}_r^1, D, mQ_\infty^1)$. Assume $m < n$. If m is even then there exists a divisor $D' \leq D$ such that $D' \sim sQ$ (simply write D' as a sum of $s/2$ pairs of conjugated points). Then the minimum distance of $\mathcal{C}_{r,m}^1$ is $d = n - m$. Thus, for m odd we have $n - s \leq d(\mathcal{C}_{r,m}^1) \leq n - m + 1$. In particular, for $m \leq 2^{r-1}$, if m even then $\mathcal{C}_{r,m}^1$ has dimension $(m/2) + 1$ and if m is odd then $\mathcal{C}_{r,m}^1 = \mathcal{C}_{r,m-1}^1$. Since this code does not meet the Goppa bound, according to Proposition 4, item (4), the same happens for $m' = n - m$. We conclude that for m odd, $n - 2^{r-1} \leq m < n$, the code $\mathcal{C}_{r,m}^1$ has dimension $m + 1 - 2^{r-2}$ and minimum distance $n - m + 1$.

References

1. Abdón, M., Garcia, A.: On a characterization of certain maximal curves. Finite Fields Appl. 10, 133–158 (2004)
2. Abdón, M., Torres, F.: On maximal curves in characteristic two. Manuscripta Math. 99, 39–53 (1999)
3. Abdón, M., Torres, F.: On $\mathbf{F}_{q^2}$-maximal curves of genus $q(q-3)/6$. Beitr. Algebra Geom. 46, 241–260 (2005)

4. Bulygin, S.V.: Generalized Hermitian codes over $GF(2^r)$. IEEE Trans. Inform. Theory 52, 4664–4669 (2006)
5. Carvalho, C., Munuera, C., Silva, E., Torres, F.: Near orders and codes. IEEE Trans. Inform. Theory 53, 1919–1924 (2009)
6. Deligne, P., Lusztig, G.: Representations of reductive groups over finite fields. Ann. of Math. 103, 103–161 (1976)
7. Deolalikar, V.: Determining irreducibility and ramification groups for an additive extension of the rational function fields. J. Number. Theory 97, 269–286 (2002)
8. Fuhrmann, R., Torres, F.: On Weierstrass points and optimal curves. Supplemento ai Rendiconti del Circolo Matematico di Palermo 51, 25–46 (1998)
9. Garcia, A., Stichtenoth, H.: A class of polynomials over finite fields. Finite Fields Their Applic. 5, 424–435 (1999)
10. Geil, O.: On codes from norm-trace curves. Finite fields and their Applications 9, 351–371 (2003)
11. Geil, O., Matsumoto, H.: Bounding the number of rational places using Weierstrass semigroups (preprint, 2007)
12. Goppa, V.D.: Geometry and Codes. Mathematics and its applications, vol. 24. Kluwer, Dordrecht (1991)
13. Goppa, V.D.: Codes associated with divisors. Problems Inform. Transmission 13, 22–26 (1977)
14. Grassl, M.: Bounds on the minimum distance of linear codes, http://www.codetables.de
15. Hansen, J.P.: Deligne-Lusztig varieties and group codes. Lect. Notes Math. 1518, 63–81 (1992)
16. Hansen, J.P., Pedersen, J.P.: Automorphism group of Ree type, Deligne-Lusztig curves and function fields. J. Reine Angew. Math. 440, 99–109 (1993)
17. Hansen, J.P., Stichtenoth, H.: Group codes on certain algebraic curves with many rational points. Applicable Algebra Eng. Comm. Comput. 1, 67–77 (1990)
18. Henn, H.W.: Funktionenkörper mit grosser Automorphismgruppen. J. Reine Angew Math. 302, 96–115 (1978)
19. Høholdt, T., van Lint, J.H., Pellikaan, R.: Algebraic-Geometry codes. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, vol. 1. Elsevier, Amsterdam (1998)
20. Lang, S.: Abelian Varieties. Interscience Pub., New York (1959)
21. Lewittes, J.: Places of degree one in function fields over finite fields. J. Pure Appl. Algebra 69, 177–183 (1990)
22. Kirfel, C., Pellikaan, R.: The minimum distance of codes in an array coming from telescopic semigroups. IEEE Trans. Inform. Theory 41, 1720–1732 (1995)
23. Matthews, G.: Codes from the Suzuki function field. IEEE Trans. Inform. Theory 50, 3298–3302 (2004)
24. Munuera, C.: On the generalized Hamming weights of geometric Goppa codes. IEEE Trans. Inform. Theory 40(6), 2092–2099 (1994)
25. Munuera, C., Pellikaan, R.: Equality of geometric Goppa codes and equivalence of divisors. J. Pure Appl. Algebra 90, 229–252 (1993)
26. Munuera, C., Torres, F.: Bounding the trellis state complexity of algebraic geometric codes. Applicable Algebra Eng. Comm. Computing 15, 81–100 (2004)
27. Munuera, C., Torres, F.: The structure of algebras admitting well agreeing near weights. J. Pure Appl. Algebra 212, 910–918 (2007)
28. Pellikaan, R., Shen, B.Z., van Wee, G.J.M.: Which Linear Codes are Algebraic-Geometric. IEEE Trans. Inform. Theory 37, 583–602 (1991)

29. Sepúlveda, A.: Generalized Hermitian codes over $\mathrm{GF}(\mathrm{q}^{\mathrm{r}})$ (preprint, 2007)
30. Stichtenoth, H.: Algebraic Function Fields and Codes. Springer, New York (1993)
31. Stöhr, K.O., Voloch, J.F.: Weierstrass points and curves over finite fields. Proc. London Math. Soc., 1–19 (1986)
32. Tsfasman, M.A., Vlăduţ, S., Zink, T.: Modular curves, Shimura curves and Goppa codes better that Varshamov-Gilbert bound. Math. Nachr. 109, 21–28 (1982)
33. Tate, J.: Endomorphisms of abelian varieties over finite fields. Inventiones Math. 2, 134–144 (1966)
34. Yang, K., Kumar, P.V., Stichtenoth, H.: On the weight hierarchy of geometric Goppa codes. IEEE Trans. Inform. Theory 40, 913–920 (1994)

Two-Point Codes on Norm-Trace Curves

C. Munuera[1], G.C. Tizziotti[2], and F. Torres[2]

[1] Dept. of Applied Mathematics, University of Valladolid
Avda Salamanca SN, 47012 Valladolid,
Castilla, Spain
[2] IMECC-UNICAMP, Cx.P. 6065, 13083-970, Campinas-SP, Brasil

Abstract. We determine the Weierstrass semigroup of a pair of rational points on Norm-Trace curves. We use this semigroup to improve the lower bound on the minimum distance of two-point algebraic geometry codes arising from these curves.

1 Introduction

The theory of Weierstrass semigroups is an important part in the study of Algebraic Geometry (AG) codes. Its use comes from the theory of *one-point* codes; given a curve $\mathcal{X}$ and a (one point, AG) code $C(D, mQ)$ arising from $\mathcal{X}$, there exist close conections between the parameters of $C(D, mQ)$ and its dual $C(D, mQ)^{\perp}$ with the Weierstrass semigroup $H(Q)$ of $\mathcal{X}$ at Q, see for example [5]. Later these results were extended to codes and semigroups over two points. Matthews [10] proved that the Weierstrass gap set of a pair of points may be exploited to define a code with minimum distance greater than the Goppa bound. By using results obtained by Homma and Kim [6,8], she determined the Weierstrass semigroup of a pair of any two points on a Hermitian curve and, as a consequence, she improved the lower bound on the minimum distance of codes defined by a linear combination of two points.

Despite the great interest of these codes, its utility is limited by the difficulty of computing the Weierstrass semigroup of two points. In this paper, we focus our attention on Norm-Trace curves, which are a natural generalization of Hermitian curves. We determine the Weierstrass semigroup of a pair of points and use it to improve the Goppa bound on the minimum distance of the corresponding codes.

The article is organized as follows. In section 2 we introduce some basic facts and definitions. In section 3 we determine the Weierstrass semigroup of a pair of points on Norm-Trace curves. By using this semigroup, in section 4 we are able to improve the lower bound on the minimum distance of two-point codes and show that these two-point codes can have better parameters than one-point codes over these curves.

2 Preliminaries

2.1 Curves and Codes

The construction of algebraic geometry codes is well known. Let $\mathcal{X}$ be a non-singular, projective, geometrically irreducible, algebraic curve of genus g over a

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 128–136, 2008.

finite field $\mathbf{F}_q$. For a rational divisor E on $\mathcal{X}$, we consider the vector spaces $L(E) := \{\text{rational functions } f : (f) + G \geq 0\} \cup \{0\}$ and $\Omega(E) := \{\text{rational differential forms } \omega : (\omega) + G \geq 0\} \cup \{0\}$. Let G and $D = P_1 + \ldots + P_n$ be two divisors on $\mathcal{X}$ such that $P_i \neq P_j$ for $i \neq j$ and $\text{supp}(G) \cap \text{supp}(D) = \emptyset$. The algebraic geometry codes $C_L(D, G)$ (or simply $C(D, G)$) and $C_\Omega(D, G)$ are defined by (see [11])

$$C(D, G) := \{(f(P_1), \ldots, f(P_n)) \; ; \; f \in L(G)\}$$

$$C_\Omega(D, G) := \{(res_{P_1}(\omega), \ldots, res_{P_n}(\omega)) \; ; \; \omega \in \Omega(G - D)\}.$$

$C(D, G)$ and $C_\Omega(D, G)$ are dual to each other. Their minimum distances verify $d_L \geq n - \deg(G)$ and $d_\Omega \geq \deg(G) - 2g + 2$ (the Goppa bound). If $G = aQ \geq 0$ for some rational point Q on $\mathcal{X}$ and D it is the sum of all the other rational points, then they are called *one-point*. Analogously, if $G = aQ_1 + bQ_2$ for two distinct rational points, then $C(D, G)$ and $C_\Omega(D, G)$ are called *two-point codes*.

2.2 Weierstrass Semigroups

Let Q be a rational point on $\mathcal{X}$. It is well known that the set

$$H(Q) := \{n \in \mathbf{N}_0 : \text{ there exists a rational function } f \text{ with } (f)_\infty = nQ\}$$

is a semigroup, called the *Weiertrass semigroup* of $\mathcal{X}$ at Q. Its complement, $G(Q) := \mathbf{N}_0 \setminus H(Q)$ is the *Weierstrass gap set* of Q. It has precisely g elements. These definitions can be translated to the two-point case. For given two distinct rational points Q_1 and Q_2 on $\mathcal{X}$ the semigroup of $\mathbf{N}_0^2$

$$H(Q_1, Q_2) = \{(n, m) \in \mathbf{N}_0^2 : \text{ there exists a rational function } f \text{ with } (f)_\infty = nP_1 + mP_2\}$$

is the *Weierstrass semigroup* of $\mathcal{X}$ at Q_1 and Q_2. The set $G(Q_1, Q_2) := \mathbf{N}_0^2 \setminus H(Q_1, Q_2)$ is called the *Weierstrass gap set* of the pair (Q_1, Q_2). It is always finite, and its cardinality depends on Q_1 and Q_2.

2.3 The Norm-Trace Curve

Let q be a prime power and let $r \geq 2$ an integer. The curve $\mathcal{X}_{q,r}$ defined over $\mathbf{F}_{q^r}$ by the affine equation

$$x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y$$

is called the *Norm-Trace* curve. If $r = 2$ then it is a Hermitian curve. Note that the zeros of $x^{\frac{q^r-1}{q-1}} - (y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y) = 0$ in $\mathbf{F}_{q^r}^2$ are the pairs $(\alpha, \beta) \in \mathbf{F}_{q^r}^2$ such that $\mathcal{N}_{\mathbf{F}_{q^r}/\mathbf{F}_q}(\alpha) = \mathcal{T}_{\mathbf{F}_{q^r}/\mathbf{F}_q}(\beta)$, where $\mathcal{N}$ stands for the norm and $\mathcal{T}$ for the trace.

The Norm-Trace curve has been studied in detail by Geil, [3]. $\mathcal{X}_{q,r}$ has a single rational point at infinity, $P_\infty = (0 : 1 : 0)$, plus q^{2r-1} affine rational points. Its genus is $g = (q^{r-1} - 1)(\dfrac{q^r - 1}{q - 1} - 1)/2$.

3 The Weierstrass Semigroup $H(P_{0,0}, P_\infty)$ for Norm-Trace Curves

The Weierstrass semigroup of $\mathcal{X}_{q,r}$ at P_∞ is well known. Let $P_{a,b}$ denote the common zero of $x-a$ and $y-b$, where $a,b \in \mathbf{F}_{q^r}$. The divisors of x and y are given by

$$(x) = P_{0,0} + \sum_{\alpha} P_{0,\alpha} - q^{r-1} P_\infty \ , \ (y) = \frac{(q^r-1)}{q-1} P_{0,0} - \frac{(q^r-1)}{q-1} P_\infty \qquad (1)$$

where α runs over the roots of $t^{q^{r-2}} + \ldots + t + 1 = 0$. Using these functions and the fact that $|G(P_\infty)| = g$, we can prove that $H(P_\infty) = \langle q^{r-1}, (q^r-1)/(q-1) \rangle$, [3]. Let us study now the semigroup over two points.

3.1 The Weierstrass Semigroup $H(P_{0,0}, P_\infty)$ for $q = 2$

In this section we restrict to the binary case, $q = 2$. Furthermore we shall assume $r \geq 3$ (if $r = 2$ we get the Hermitian curve). Then the curve has genus $g = (2^{r-1}-1)^2$ and $H(P_\infty) = \langle 2^{r-1}, 2^r - 1 \rangle$.

Proposition 1. *Let $\gamma = 2^r - 2$. The Weierstrass semigroup of $\mathcal{X}_{2,r}$ at $P_{0,0}$ is given by*

$$H(P_{0,0}) = \langle \gamma, \gamma+1, 2\gamma-1, 3\gamma-2, \ldots, \frac{\gamma}{2}\gamma - (\frac{\gamma}{2} - 1) \rangle.$$

Proof. From 1 we have

$$\left(\frac{x}{y}\right)_\infty = (2^r-2)P_{0,0} \ \text{ and } \ \left(\frac{1}{y}\right)_\infty = (2^r-2)P_{0,0}.$$

Furthermore, given an integer m, $0 \leq m < 2^{r-2} + 2^{r-3} + \ldots + 2$,

$$\left(\frac{x^{2m+2+1}}{y^{m+2}}\right)_\infty = ((2(m+1)-m)(2^r-1) - (m+1))P_{0,0}.$$

Thus $\gamma, \gamma+1, 2\gamma-1, 3\gamma-2, \ldots, \frac{\gamma}{2}\gamma - (\frac{\gamma}{2}-1) \in H(P_{0,0})$. To see the equality it is enough to prove that the semigroup $\langle \gamma, \gamma+1, 2\gamma-1, 3\gamma-2, \ldots, \frac{\gamma}{2}\gamma - (\frac{\gamma}{2}-1) \rangle$ has $g = (2^{r-1}-1)^2$ gaps. A simple computation shows that $|G(P_{0,0})| = (\gamma - 1) + (\gamma-3) + (\gamma-5) + \ldots + 3 + 1 = (2^{r-1}-1)^2 = g$.

Once the semigroups $H(P_{0,0}), H(P_\infty)$ are known, let us study the semigroups over two points. Given $Q_1, Q_2 \in \mathcal{X}_{2,r}(\mathbf{F}_{2^r})$, for $\alpha \in G(Q_1)$ we define $\beta_\alpha := \min\{\beta \in \mathbf{N}_0 \ ; \ (\alpha, \beta) \in H(Q_1, Q_2)\}$. It is known, [8], that $\{\beta_\alpha \ ; \ \alpha \in G(Q_1)\} = G(Q_2)$. Let $\alpha_1 < \alpha_2 < \ldots < \alpha_g$ be the gap sequence at Q_1 and $\beta_1 < \beta_2 < \ldots < \beta_g$ be the gap sequence at Q_2. The above equality implies that there exist a one-to-one correspondence between $G(Q_1)$ and $G(Q_2)$ so that $\beta_{\alpha_i} = \beta_{\sigma(i)}$, where σ is a permutation of the set $\{1, 2, \ldots, g\}$. We will often denote this permutation by $\sigma(Q_1, Q_2)$ and the graph of the bijective map between $G(Q_1)$ and $G(Q_2)$ by $\Gamma(Q_1, Q_2)$, that is

$$\Gamma(Q_1, Q_2) := \{(\alpha_i, \beta_{\sigma(i)}) : i = 1, 2, \ldots, g\} = \{(\alpha_i, \beta_{\alpha_i}) : i = 1, 2, \ldots, g\}.$$

Lemma 1. *Let Γ' be a subset of $(G(Q_1)\times G(Q_2))\cap H(Q_1,Q_2)$. If there exists a permutation τ of $\{1,\dots,g\}$ such that $\Gamma'=\{(\alpha_i,\beta_{\tau(i)}):i=1,\dots,g\}$, then $\Gamma'=\Gamma(Q_1,Q_2)$.*

Proof. From the definition of $\sigma=\sigma(Q_1,Q_2)$ we have $\beta_{\tau(i)}\geq\beta_{\sigma(i)}$ for all $i=1,\dots,g$. Thus $\tau=\sigma$.

Theorem 1. *Let us consider the two-point semigroup $H(P_\infty,P_{0,0})$. It holds that*

$$\beta_{2(i-j)a+j}=(2a-1)j-2i\ ,\ 1\leq j\leq i\leq a-1,\ \textit{and}$$

$$\beta_{(2(i-j)+1)a+j}=(2a-1)-(2i+1)\ ,\ 1\leq j\leq i\leq a-2,$$

where $a=2^{r-1}$.

Proof. Let us prove the first statement. By the structure of $G(P_\infty)$ and $G(P_{0,0})$, for every pair (i,j) such that $1\leq j\leq i\leq a-1$, it holds that $2(i-j)a+j\in G(P_\infty)$ and $j(2a-1)-2i=2(j-1)(a-1)+(2(a-1)-2i+j)\in G(P_{0,0})$. Let us first show that $2(i-j)a+j\neq 2(i'-j')a+j'$ if $i\neq i'$ or $j\neq j'$ (*). If this assertion is false, there exist two pairs $(i,j)\neq(i',j')$ such that $2(i-j)a+j=2(i'-j')a+j'$. If $i-j=i'-j'$, then $2(i-j)a+j=2(i'-j')a+j'$ hence $(i,j)=(i',j')$. Therefore $i-j\neq i'-j'$. Assume $i-j>i'-j'$. Then $i-j=i'-j'+k$, for some $0<k\in\mathbf{N}$ and hence $2(i'-j'+k)a+j=2(i'-j')a+j'$ so $j'=2ak+j$,which is a contradiction because $1\leq j,j'\leq a-1$. Then (*) is proved. Let us prove now that $j(2a-1)-2i\neq j'(2a-1)-2i'$ if $(i,j)\neq(i',j')$ (**). Suppose again that this assertion is false. Thus there exist $(i,j)\neq(i',j')$ such that $j(2a-1)-2i=j'(2a-1)-2i'$. Since $j(2a-1)-2i=j'(2a-1)-2i'$, we have $i\neq i'$ and $j\neq j'$. Write $i=i'+k$, with $k\in\mathbf{N}$, $1\leq k<a-1$. Thus $j(2a-1)=j'(2a-1)+2k$ hence $(j-j')(2a-1)=2k<2a-1$, which contradicts $j\neq j'$. This proves (**). Now, for $1\leq j\leq i\leq a-1$, we have

$$\left(\frac{x^{2i}}{y^j}\right)_\infty=(2(i-j)a+j)P_\infty+(j(2a-1)-2i)P_{0,0}$$

and hence $(2(i-j)a+j,j(2a-1)-2i)\in H(P_\infty,P_{0,0})$. Thus, if $\alpha_l=2(i-j)a+j$ and $\beta_{l'}=j(2a-1)-2i$, for $l,l'=1,\dots,g$, we have $(\alpha_l,\beta_{l'})\in(G(P_\infty)\times G(P_{0,0}))\cap H(P_\infty,P_{0,0})$. Let τ be a permutation of $\{1,\dots,g\}$ such that $\tau(l)=l'$. By Lemma 1, $\Gamma'=\{(\alpha_l,\beta_{\tau(l)}:l=1,\dots,g\}=\Gamma(P_\infty,P_{0,0})$ so $\beta_{2(i-j)a+j}=(2a-1)j-2i$ for $1\leq j\leq i\leq a-1$. This proves the first statement. The second one is proved in the same way, by using that $\beta_{(2(i-j)+1)a+j}=(2a-1)-(2i+1)$ for $1\leq j\leq i\leq a-2$.

This Theorem allows us to compute $\Gamma(P_{0,0},P_\infty)$, and hence $H(P_{0,0},P_\infty)$ as follows. Given $\mathbf{x}=(\alpha_1,\beta_1),\mathbf{y}=(\alpha_2,\beta_2)\in\mathbf{N}_0^2$, the *least upper bound* (or lub) of $\mathbf{x}$ and $\mathbf{y}$ is defined as

$$\mathrm{lub}(\mathbf{x},\mathbf{y}):=(\max\{\alpha_1,\alpha_2\},\max\{\beta_1,\beta_2\}).$$

It is well known that for $\mathbf{x},\mathbf{y}\in H(Q_1,Q_2)$, we have $\mathrm{lub}(\mathbf{x},\mathbf{y})\in H(Q_1,Q_2)$ (see [8]).

Lemma 2. *Let Q_1 and Q_2 be two distinct rational points. Then $H(Q_1,Q_2)=\{\mathrm{lub}(\mathbf{x},\mathbf{y}):\mathbf{x},\mathbf{y}\in\Gamma(Q_1,Q_2)\cup(H(Q_1)\times\{0\})\cup(\{0\}\times H(Q_2))\}$.*

Proof. See [8] Lemma 2.2.

3.2 The Weierstrass Semigroup $H(P_{0,0}, P_\infty)$ for Any q

Let us study now the general case. Set $a = ((q^r - 1)/(q-1)) - 1$. We have the pole divisors

$$\left(\frac{x}{y}\right)_\infty = aP_{0,0}\ ,\ \left(\frac{1}{y}\right)_\infty = (a+1)P_{0,0},$$

and for $0 \leq m \leq q^{r-2} + q^{r-3} + \ldots + q - 1$,

$$\left(\frac{x^{mq+q+1}}{y^{m(q-1)+q}}\right)_\infty = (((m+1)q - m)a - (m+1))P_{0,0}.$$

Proposition 2. *The Weierstrass semigroup $H(P_{0,0})$ is given by*

$$H(P_{0,0}) = \langle a, a+1, qa-1, (2q-1)a-2, (3q-2)a-3, \ldots, ((\lambda+1)q-\lambda)a-(\lambda+1)\rangle$$

where $\lambda = q^{r-2} + q^{r-3} + \ldots + q - 1$.

Proof. Since all integers $a, a+1, qa-1, (2q-1)a-2, (3q-2)a-3, \ldots, ((\lambda+1)q-\lambda)a-(\lambda+1)$ are elements of $H(P_{0,0})$, it is enough to show that this semigroup has g gaps. The proof of this fact is analogous to the case $q = 2$.

Theorem 2. *Let q be a prime power, $r \geq 3$ and $a = q^{r-1} + q^{r-2} + \ldots + q^2 + q$. Let us consider the semigroup $H(P_{0,0}, P_\infty)$. Then for every s such that $1 \leq s \leq q^{r-2} + \ldots + q + 1$ and every pair (i,j) with $1 \leq j \leq i \leq a - s$ and $(s-1)q - (s-1) \leq i - j \leq sq - (s+1)$, we have*

$$\beta_{(i-j)(a+1)+j} = (q^{r-1} - (i-j+1))(a+1) - jq^{r-1}.$$

Proof. Let us first prove that when $(i,j) \neq (i',j')$ then $(i-j)(a+1)+j \neq (i'-j')(a+1)+j'$. Suppose that this assertion is false. Thus there exist $(i,j) \neq (i',j')$ such that $(i-j)(a+1)+j = (i'-j')(a+1)+j'$. Since $i-j \neq i'-j'$, we can write $i-j = i'-j'+m$, with $1 \leq m \leq q-1$. Thus $m(a+1)+j = j'$, which is not possible, because $1 \leq j' \leq a-1$. Now, let us show that the numbers $(q^{r-1} - (i-j+1))(a+1) - jq^{r-1}$ are distinct for distinct pairs (i,j). Otherwise there exist $(i,j) \neq (i',j')$ such that $(q^{r-1} - (i-j+1))(a+1) - jq^{r-1} = (q^{r-1} - (i'-j'+1))(a+1) - j'q^{r-1}$. As above we have $i-j \neq i'-j'$. Write $i-j = i'-j'+m$, $1 \leq m \leq q-1$. Thus $(j-j')q^{r-1} = m(a+1) = m(q^{r-1} + \ldots + q + 1)$, hence q^{r-1} divides $m(q^{r-1} + \ldots + q + 1)$, a contradiction. Finally, let us see that the numbers $(q^{r-1} - (i-j+1))(a+1) - jq^{r-1}$ are gaps at P_∞. Otherwise, if $(q^{r-1} - (i_0 - j_0 + 1))(a+1) - j_0 q^{r-1} \in \langle q^{r-1}, q^{r-1} + \ldots + q + 1\rangle$ for a pair (i_0, j_0), then there exist positive integers α, β, such that

$$\alpha q^{r-1} + \beta(q^{r-1} + \ldots + q + 1) = (q^{r-1} - (i_0 - j_0 + 1))(a+1) - j_0 q^{r-1}$$

$$= (q^{r-1} - (i_0 - j_0 + 1))(q^{r-1} + \ldots + q + 1) - j_0 q^{r-1}$$

and hence $(\alpha + j_0)q^{r-1} = (q^{r-1} - (i_0 - j_0 + 1 + \beta))(q^{r-1} + \ldots + q + 1)$. We have $\alpha + j_0 > 0$ and $i_0 - j_0 + 1 + \beta > 0$, so q^{r-1} divides $(q^{r-1} - (i_0 - j_0 + 1 +$

$\beta))(q^{r-1}+\ldots+q+1)$, a contradiction because $q^{r-1}-(i_0-j_0+1+\beta)<q^{r-1}$ and q is a prime power.

By Proposition 2, it holds that $(i-j)(a+1)+j \in G(P_{0,0})$. Then, by considering the pole divisor

$$\left(\frac{x^{a+1-j}}{y^{i-j+1}}\right)_\infty = ((i-j)(a+1)+j)P_{0,0} + ((q^{r-1}-(i-j+1))(a+1)-jq^{r-1})P_\infty$$

we conclude that $((i-j)(a+1)+j,(q^{r-1}-(i-j+1))(a+1)-jq^{r-1}) \in (G(P_{0,0}) \times G(P_\infty)) \cap H(P_{0,0},P_\infty)$. Let $\alpha_1<\ldots<\alpha_g$ and $\beta_1<\ldots<\beta_g$ be the gap sequences of $P_{0,0}$ and P_∞. Let τ be the permutation of $\{1,\ldots,g\}$ such that $\beta_{\tau(l)}=(q^{r-1}-(i-j+1))(a+1)-jq^{r-1}$ if $\alpha_l=(i-j)(a+1)+j$, $l=1,\ldots,g$. Then $\Gamma'=\{(\alpha_l,\beta_{\tau(l)}):l=1,\ldots,g\} \subseteq (G(P_{0,0}) \times G(P_\infty)) \cap H(P_{0,0},P_\infty)$, hence $\Gamma'=\Gamma(P_{0,0},P_\infty)$ by Lemma 1. Thus $\beta_{(i-j)(a+1)+j}=(q^{r-1}-(i-j+1))(a+1)-jq^{r-1}$ and the proof is done.

4 Codes on Norm-Trace Curves

In this section we will show how the knowledge of the Weierstrass semigroup $H(P_{0,0},P_\infty)$ on Norm-Trace curves $\mathcal{X}_{q,r}$, can be used to improve the parameters of the corresponding codes. Our starting point is the following result, due to Matthews [10].

Theorem 3. *Assume that* $(\alpha_1,\alpha_2) \in G(Q_1,Q_2)$ *with* $\alpha_1 \geq 1$ *and* $l(\alpha_1 Q_1+\alpha_2 Q_2)=l((\alpha_1-1)Q_1+\alpha_2 Q_2)$. *Suppose* $(\gamma_1,\gamma_2-t-1) \in G(Q_1,Q_2)$, *for all* t, $0 \leq t \leq \min\{\gamma_2-1,2g-1-(\alpha_1+\alpha_2)\}$. *Let* $G=(\alpha_1+\gamma_1-1)Q_1+(\alpha_2+\gamma_2-1)Q_2$ *and* $D=\sum_{j=1}^n P_j$, *where* $Q_1,Q_2,P_1,\ldots,P_n$ *are distinct* $\mathbf{F}_q$*-rational points. If the dimension of* $C_\Omega(D,G)$ *is positive, then its minimum distance is at least* $\deg(G)-2g+3$.

This Theorem can be improved for Norm-Trace curves as follows.

Theorem 4. *Let us consider the code* $C_\Omega(D,G)$ *arising from the curve* $\mathcal{X}_{q,r}$, *with* $G=(\alpha_1+\gamma_1-1)P_{0,0}+(\alpha+\gamma-1)P_\infty$ *and* $D=\sum_{j=1}^n P_j$, *where the points* $P_{0,0},P_\infty,P_1,\ldots,P_n$ *are rational and distinct. Suppose that*

a) $\alpha \geq 1, (\alpha_1,\alpha) \in G(P_{0,0},P_\infty)$ *and* $l(\alpha_1 P_{0,0}+\alpha P_\infty)=l(\alpha_1 P_{0,0}+(\alpha-1)P_\infty)$.

b) $(\gamma_1-t-1,\gamma),(\gamma_1-t-1,\gamma+1),(\gamma_1-t-1,\gamma+\dfrac{q^r-1}{q-1}),(\gamma_1,\gamma) \in G(P_{0,0},P_\infty)$, *for all* t, $0 \leq t \leq \min\{\gamma_1-1,2g-1-(\alpha_1+\alpha)\}$.

Under these conditions, if the dimension of $C_\Omega(D,G)$ *is positive, then its minimum distance at least* $\deg(G)-2g+4$.

Proof. By Theorem 3, the minimum distance of the code $C=C_\Omega(D,G)$ is at least $\deg(G)-2g+3$. Let $d=\deg(G)-2g+3$. If there exists a codeword $\mathbf{c} \in C$ of weight d, then there exists a differential $\omega \in \Omega(G-D)$ with exactly d simple poles in the set $\{P_1,\ldots,P_n\}$. Let $Q_1,\ldots,Q_d$ be such poles. Now $\deg(\omega)=2g-2=$

$\deg(G)-d+1$, that is, $(\omega) \geq G-(Q_1+\ldots+Q_d)$. So $(\omega) = G-(Q_1+\ldots+Q_d)+P$, where P is a $\mathbf{F}_{q^r}$-rational point, with $P \neq Q_i$, for $1 \leq i \leq d$. On the other hand, since $l(\alpha_1 P_{0,0}+\alpha P_\infty) = l(\alpha_1 P_{0,0}+(\alpha-1)P_\infty)$, by the Riemann-Roch Theorem we have that $l(W-(\alpha_1 P_{0,0}+\alpha P_\infty)) = l(W-(\alpha_1 P_{0,0}+(\alpha-1)P_\infty))-1$, that is, $L(W-(\alpha_{0,0}P_1+(\alpha-1)P_\infty)) \neq L(W-(\alpha_1 P_{0,0}+\alpha P_\infty))$, where W is a canonical divisor. Thus, there exists a rational function h such that

$$(h) = (\alpha-1)P_\infty + (\alpha_1+t)P_{0,0} - W + E,$$

where E is a effective divisor whose support does not contain neither $P_{0,0}$ nor P_∞, and $0 \leq t \leq 2g-1-(\alpha_1+\alpha)$ because $\deg(h)=0$. Thus

$$(\omega) = G-(Q_1+\ldots+Q_d)+P = (\omega) \sim W \sim (\alpha-1)P_\infty + (\alpha_1+t)P_{0,0} + E$$

and since $G = (\alpha_1+\gamma_1-1)P_{0,0}+(\alpha+\gamma-1)P_\infty$, there exists a rational function f such that

$$(f) = -\gamma P_\infty - (\gamma_1-t-1)P_{0,0} - P + (Q_1+\ldots+Q_d) + E.$$

Let us show that this is impossible. To that end we shall consider two cases.

Case 1. $t \leq \gamma_1 - 1$. If $P \in \operatorname{supp}(E)$, then $(f)_\infty = \gamma P_\infty + (\gamma_1-t-1)P_{0,0}$, contradicting the fact that $(\gamma_1-t-1,\gamma) \in G(P_{0,0},P_\infty)$. If $P = P_\infty$, then $(f)_\infty = (\gamma+1)P_\infty+(\gamma_1-t-1)P_{0,0}$, contradicting again the fact that $(\gamma_1-t-1,\gamma+1) \in G(P_{0,0},P_\infty)$. The same occurs if $P = P_{0,0}$, because then $(\gamma_1-t,\gamma) \in H(P_{0,0},P_\infty)$. Finally, if $P = P_j$ for some $P_j \notin \{Q_1,\ldots,Q_d\}$, since $(y) = ((q^r-1)/(q-1))P_{0,0} - ((q^r-1)/(q-1))P_\infty$, we have $(f.y)_\infty = (\gamma + \dfrac{q^r-1}{q-1})P_\infty + (\gamma_1-t-1)P_{0,0}$, contradicting $(\gamma_1-t-1,\gamma+(q^r-1)(q-1)) \in G(P_{0,0},P_\infty)$.

Case 2. $\gamma_1 - 1 < t \leq 2g-1-(\alpha_1+\alpha)$. A similar reasoning shows that when $P \in \operatorname{supp}(E)$ or $P = P_{0,0}$ then γ is a gap. If $P = P_\infty$ then $\gamma+1$ is a gap. Finally, if $P = P_j$ for some $P_j \notin \{Q_1,\ldots,Q_d\}$, then $\gamma+(q^r-1)(q-1)$ is a gap. Therefore $d \geq \deg(G)-2g+4$.

Let us remember that given a $[n,k,d]$ code C, we define its *information rate* by $R = k/n$ and its *relative minimum distance* by $\delta = d/n$. These parameters allows us to compare codes of different length. Our final result states that two-point codes from Norm-Trace curves can have better relative parameters than the corresponding one-point codes. More precisely, we have the following.

Theorem 5. *There are two-point codes $C_\Omega(D,G)$ on $\mathcal{X}_{q,r}$ of length $|\mathcal{X}_{q,r}|-2$, having relative parameters better than every one-point code $C_L(\overline{D}, mq^{r-1}P_\infty)$ on $\mathcal{X}_{q,r}$.*

Proof. Let us consider the one-point code $C_L(\overline{D}, mq^{r-1}P_\infty)$, where $\overline{D}$ is the sum of all q^{2r-1} affine rational points. As we know, these points are either of the form $(0,\alpha_s^{(0)})$, being the $\alpha_s^{(0)}$'s the roots in $\mathbf{F}_{q^r}$ of $y^{q^{r-1}}+y^{q^{r-2}}+\ldots+y=0$, or of the form $(\alpha^j, \alpha_s^{(j)})$, $0 \leq j \leq q^r - 2$, where α is a generator of $\mathbf{F}_{q^r}^*$ and the $\alpha_s^{(j)}$'s are the roots in $\mathbf{F}_{q^r}$ of $y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y = \alpha^j$. Let d be the minimum distance of $C_L(\overline{D}, mq^{r-1}P_\infty)$. The function $f = \prod_{i=1}^{m}(x - \alpha^i) \in L(mq^{r-1}P_\infty)$, has mq^{r-1} zeros and hence it gives a codeword of weight $q^{2r-1} - mq^{r-1}$. On the other hand, by the Goppa bound we have that $d \geq n - \deg(G) = q^{2r-1} - mq^{r-1}$. Thus we have equality, $d = q^{2r-1} - mq^{r-1}$. On the other hand, it is easy to compute that the dimension of this code is $k = mq^{r-1} - g + 1$.

Now let us consider the two-point code $C_\Omega(D, G)$, where $D = \sum_{j=1}^{q^{2r-1}-1} P_j$, $P_j \neq P_{0,0}, P_\infty$ and $G = P_{0,0} + (q^{2r-1} + 2g - mq^{r-1} - 4)P_\infty$. Its length is $n = q^{2r-1} - 1$. Its dimension is easy to compute: according to the Goppa's estimates, and since $\deg(G) > 2g - 2, \deg(W - G + D) \geq 2g - 2$, where W is a canonical divisor, we have $\dim(C_\Omega(D, G)) = i(G - D) = l(W - G + D) = mq^{r-1} - g + 1$. Finally its minimum distance can be estimated by using Theorem 3. To see this note that $(\alpha_1, \alpha) = (1, 2g - 2) \in G(P_{0,0}, P_\infty)$ by Theorem 2; furthermore for all m such that $q^r - (q^{r-1} + q^{r-2} + \ldots + q^2 + q) + q \leq m < q^r$, we have $(\gamma_1, \gamma) = (1, q^{2r-1} - mq^{r-1} - 1) \in G(P_{0,0}, P_\infty)$, and these pairs satisfy the condition $(\gamma_1, \gamma - t - 1) \in G(P_{0,0}, P_\infty)$ for all t in the range $0 \leq t \leq \min\{\gamma - 1, 2g - 1 - (\alpha_1 + \alpha)\}$. Therefore the minimum distance of $C_\Omega(D, G)$ at least $\deg(G) - 2g + 3 = q^{2r-1} - mq^{r-1}$.

Then $C_\Omega(D, G)$ has relative parameters R, δ, better than the corresponding of $C_L(\overline{D}, mq^{r-1}P_\infty)$.

Example 1. Take $q = r = 3$ and let us consider the Norm-Trace curve $\mathcal{X}_{3,3}$ of genus $g = 48$ over $\mathbf{F}_{27}$. With the same notation as in Theorem 2, we have $a = 12$ and $1 \leq s \leq 4$. The Weierstrass semigroups are as follows,

- $H(P_\infty) = \langle 9, 13 \rangle$, hence $G(P_\infty) = \{1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 14, 15, 16, 17, 19, 20, 21, 23, 24, 25, 28, 29, 30, 32, 33, 34, 37, 38, 41, 42, 43, 46, 47, 50, 51, 55, 56, 59, 60, 64, 68, 69, 73, 77, 82, 86, 95\}$;
- $H(P_{0,0}) = \langle 12, 13, 35, 58, 81 \rangle$, hence $G(P_{0,0}) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\ 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 27, 28, 29, 30, 31, 32, 33, 34, 40, 41, 42, 43, 44, 45, 46, 53, 54, 55, 56, 57, 66, 67, 68, 69, 79, 80, 92\}$.

Thus, by using Theorem 2, we get $\Gamma(P_{0,0}, P_\infty) = \{(1, 95), (2, 86), (3, 77), (4, 68), (5, 59), (6, 50), (7, 41), (8, 32), (9, 23), (10, 14), (11, 5), (14, 82), (15, 73), (16, 64), (17, 55), (18, 46), (19, 37), (20, 28), (21, 19), (22, 10), (23, 1), (27, 69), (28, 60), (29, 51), (30, 42), (31, 33), (32, 24), (33, 15), (34, 6), (40, 56), (41, 47), (42, 38), (43, 29), (44, 20), (45, 11), (46, 2), (53, 43), (54, 34), (55, 25), (56, 16), (57, 7), (66, 30), (67, 21), (68, 12), (69, 3), (79, 17), (80, 8), (92, 4)\}$,
and by Lemma 2,

- $H(P_{0,0}, P_\infty) = \{\mathrm{lub}(\mathbf{x}, \mathbf{y} : \mathbf{x}, \mathbf{y} \in \Gamma(P_{0,0}, P_\infty) \cup (H(P_{0,0}) \times \{0\}) \cup (\{0\} \times H(P_\infty))\}$.

Now let us consider the codes $C_L(\overline{D}, 180P_\infty)$ and $C_\Omega(D, P_{0,0} + 155P_\infty)$, where $\overline{D}$ is the sum of all 243 affine rational points and $D = \sum P_j$, $P_j \neq P_{0,0}, P_\infty$. The relative parameters of code $C_L(\overline{D}, 180P_\infty)$ are $\delta_1 = 63/243$ and $R_1 = 133/243$. Using Theorems 3 and 5, the relative parameters of the two-point code $C_\Omega(D, P_{0,0} + 155P_\infty)$ are $\delta_2 \geq 63/242$ and $R_2 = 133/242$.

References

1. Carvalho, C., Torres, F.: On Goppa codes and Weierstrass gaps at several points. Designs, Codes and Cryptography 35, 211–225 (2005)
2. Garcia, A., Kim, S.J., Lax, R.F.: Consecutive Weierstrass gaps and minimum distance of Goppa codes. J. Pure Applied Algebra 84, 199–207 (1993)
3. Geil, O.: On codes from norm-trace curves. Finite Fields and Their Applications 9, 351–371 (2003)
4. Hansen, J.P., Stichtenoth, H.: Group codes on certain curves with many rational points. Applicable Algebra Eng. Comm. Computing 1, 67–77 (1990)
5. Høholdt, T., van Lint, J., Pellikaan, R.: Algebraic geometry codes. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, vol. 1. Elsevier, Amsterdam (1998)
6. Homma, M., Kim, S.J.: Goppa codes with Weierstrass pairs. J. Pure Applied Algebra 162, 273–290 (2001)
7. Homma, M.: The Weierstrass semigroup of a pair of points on a curve. Archiv. Math. 67, 337–348 (1996)
8. Kim, S.J.: On index of the Weierstrass semigroup of a pair of points on a curve. Archiv. Math. 62, 73–82 (1994)
9. Matthews, G.L.: Codes from the Suzuki function field. IEEE Transactions on Information Theory 50, 3298–3302 (2004)
10. Matthews, G.L.: Weierstrass pairs and minimum distance of Goppa codes. Designs, Codes and Cryptography 22, 107–121 (2001)
11. Stightenoth, H.: Algebraic function fields and codes. Springer, Berlin (1993)

Close Encounters with Boolean Functions of Three Different Kinds*

Matthew G. Parker

The Selmer Centre
Department of Informatics, University of Bergen
P.O. Box 7800, N-5020 Bergen, Norway
matthew@ii.uib.no
http://www.ii.uib.no/~matthew/

Abstract. Complex arrays with good aperiodic properties are characterised and it is shown how the joining of dimensions can generate sequences which retain the aperiodic properties of the parent array. For the case of $2 \times 2 \times \ldots \times 2$ arrays we define two new notions of aperiodicity by exploiting a unitary matrix represention. In particular, we apply unitary rotations by members of a size-3 cyclic subgroup of the local Clifford group to the aperiodic description. It is shown how the three notions of aperiodicity relate naturally to the autocorrelations described by the action of the Heisenberg-Weyl group. Finally, after providing some cryptographic motivation for two of the three aperiodic descriptions, we devise new constructions for complementary pairs of Boolean functions of three different kinds, and give explicit examples for each.

Keywords: Aperiodic autocorrelation, complementary sequences, local Clifford group, Heisenberg-Weyl group, Boolean functions, Pauli group, quantum codes, graph states.

1 Introduction

Boolean functions with desirable properties are required in many fields, and are used, in particular, as components in both cryptosystems and communications systems [17]. In the former, one typically requires the Boolean function to be robust to linear and differential approximations [8], and in the latter, one requires the one-dimensional sequences derived from Boolean functions, to have an 'evenly-spread' Fourier spectrum and low magnitude out-of-phase autocorrelation sidelobes [21]. Such technical demands are often met by Boolean functions and sequences which are spectrally optimal in a periodic sense, that is they have Fourier spectra which are well-controlled at certain spectral points. However, at least for sequences for communications, one often requires an evenly-spread Fourier spectrum over a continuum of points [10]. This translates into a requirement for low magnitude out-of-phase *aperiodic autocorrelation* sidelobes [12].

* This work was supported by the Norwegian Research Council.

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 137–153, 2008.

Constructions of Boolean functions with good aperiodic properties is not a well-developed area of research in cryptography [12,9].

In this paper we start by considering the problem of designing bipolar sequences with good aperiodic properties. We then extend this problem to the design of bipolar arrays with good aperiodic properties and show how, for 'perfect' arrays, their aperiodic properties can be carried over to related sequences, where the sequences are obtained from the arrays by recursive *joining* of dimensions [22,23,13] We also show how to interpret this relationship in the Fourier domain.

We then focus on the construction of bipolar arrays in $\mathcal{C}_2^n$, which can be described by *generalised Boolean functions*, where these functions have good aperiodic properties [9]. By re-expressing the autocorrelation and Fourier properties of these functions using unitary matrix terminology, we view our problem within a wider context, where the multidimensional continuous discrete Fourier transform is a tensor product of members of an infinite-size set of 2×2 unitary matrices [25,19,28]. We call this set of 2×2 unitaries the *type-I* set. We then identify a size-3 cyclic subgroup, $\mathbb{T}$, of the *local Clifford group*, comprising 2×2 unitaries, where $\mathbb{T} = \{I, \lambda, \lambda^2\}$, and, by right-multiplication (rotation) of each member of the type-I set by λ, the generator of $\mathbb{T}$, and by λ^2, we generate two more infinite-size sets of 2×2 unitary matrices, respectively, namely the *type-II* and *type-III* sets. The problem of constructing arrays in $\mathcal{C}_2^n$ (generalised Boolean functions) with good aperiodic autocorrelation properties is related to the flatness of the spectrum resulting from the multiplicative left-action of any matrix which is a tensor product of type-I unitaries on the array. Further, the type-II and type-III matrix sets highlight new 'aperiodic' questions for the array. Therefore we consider three different kinds of aperiodic property of a Boolean function, where the 'type-I' kind relates to conventional aperiodicity.

Having characterised type-I, type-II, and type-III aperiodicity, we then give some cryptographic meaning to the properties possessed by Boolean functions which are type-I or type-II optimal. We also place the three kinds of array into a more general context by considering arrays which are optimal, in some sense, with respect to the action of the *Heisenberg-Weyl* (or *Pauli*) group [11]. Type-I, II, and III properties relate to the action of the Heisenberg-Weyl group under some restrictions. Moreover, those quadratic Boolean functions which represent one-dimensional *quantum codes* with good distance [9,4] also have good properties with respect to the action of the Heisenberg-Weyl group.

We would particularly like to construct Boolean functions with perfect aperiodic properties (i.e. whose aperiodic autocorrelation sidelobes are of zero magnitude), as applying the joining described above would preserve these perfect properties, but such functions do not exist, so we therefore propose to construct *pairs* of Boolean functions whose out-of-phase aperiodic sidelobes sum to zero. These are, by definition, *Golay complementary array pairs.* A construction exists for complementary sequences, as proposed by Golay [14,15], and Shapiro-Rudin [31], and later generalised by Turyn [30]. Pairs of Boolean functions constructed via an array form of the Golay-Turyn [24,23,13] construction have optimised type-I properties. We call such a pair a *type-I pair*. By rotating a type-I pair by λ and by λ^2, respectively, we obtain a *type-II pair*, and a *type-III pair*, respectively. But a more general result can be obtained by rotating the Golay-Turyn construction itself. By rotating the Golay-Turyn construction by λ and by λ^2 we obtain two 'new' constructions which we call type-II and type-III complementary constructions, respectively. In particular, in addition to the type-I complementary pairs, this allows us to construct, directly, pairs of Boolean functions which are type-II and type-III complementary, respectively.

We finish by presenting some open problems arising from the paper.

2 Aperiodic Autocorrelation and the Continuous Fourier Transform

Let $\tilde{A} \in \mathcal{C}_N = (\tilde{A}_0, \tilde{A}_1, \ldots, \tilde{A}_{N-1})$ be a finite sequence of N complex numbers, where we take the convention that neither of the two end elements, $\tilde{A}_0$ and $\tilde{A}_{N-1}$, are zero. We represent the sequence $\tilde{A}$ by the polynomial $\tilde{A}(y) = \tilde{A}_0 + \tilde{A}_1 y + \ldots + \tilde{A}_{N-1} y^{N-1}$. The aperiodic autocorrelation of $\tilde{A}$ is then given by the coefficients of $K_{\tilde{A}}(y) = K_{\tilde{A}_{1-N}} y^{1-N} + \ldots + K_{\tilde{A}_{-1}} y^{-1} + K_{\tilde{A}_0} y^0 + K_{\tilde{A}_1} y^1 + \ldots + K_{\tilde{A}_{N-1}} y^{N-1}$, where

$$K_{\tilde{A}}(y) = \frac{\tilde{A}(y)\tilde{A}^*(y)}{||\tilde{A}||^2},$$

where $\tilde{A}^*(y) = \overline{\tilde{A}(y^{-1})}$, and $\overline{x}$ means x with complex-conjugated coefficients. We desire all out-of-phase sidelobes of the aperiodic autocorrelation of $\tilde{A}$ to be of low magnitude, which means that we want $K_{\tilde{A}_j}$ to have low magnitude $\forall j \neq 0$. Ideally we would like all $K_{\tilde{A}_j} = 0$ for $j \neq 0$, in which case $K_{\tilde{A}}(y) = 1$ is called a *δ-function*, independent of y, but this is impossible for $N \geq 2$. We later discuss how to obtain an ideal (δ-function) response for the sum of the aperiodic autocorrelations of a pair of sequences.

The continuous Fourier power spectrum of $\tilde{A}$ is the set of evaluations of $K_{\tilde{A}}(y)$ on the unit circle and is summarised by

$$\mathcal{F}(\tilde{A}) = \{K_{\tilde{A}}(\upsilon) \quad | \quad |\upsilon| = 1\}.$$

If $\tilde{A}$ had a perfect response then $\mathcal{F}(\tilde{A}) = \{1\}$, i.e. the Fourier power spectrum would be *flat*. More realistically, if $\tilde{A}$ has a near-perfect aperiodic autocorrelation response then, loosely, its Fourier power spectrum is *near-flat*. We later discuss how to obtain a flat power spectrum for the sum of the Fourier power spectra of a pair of sequences, implying that the power spectrum for each member of the pair is near-flat.

3 Aperiodic Autocorrelation of Arrays and the Multi-dimensional Continuous Fourier Transform

Let $A \in \mathcal{C}_{N_0} \times \mathcal{C}_{N_1} \times \ldots \times \mathcal{C}_{N_{n-1}}$ be an n-dimensional array with $\prod_{j=0}^{n-1} N_j$ complex elements where, to avoid degeneracy, we take the convention that no 'surface' of the array can have elements which are all zero, i.e. for each dimension index, h, the set of elements $\{A_{0,\ldots,0,k,0,\ldots,0} \quad | \quad \forall k\}$ and $\{A_{N_0-1,\ldots,N_{h-1}-1,k,N_{h+1}-1,\ldots,N_{n-1}-1} \quad | \quad \forall k\}$ must each include at least one non-zero entry. The aperiodic autocorrelation, $K_A(z)$, of A is given by

$$K_A(z) = \frac{A(z)A^*(z)}{||A||^2}, \tag{1}$$

where $z = (z_0, z_1, \ldots, z_{n-1})$, $z^{-1} = (z_0^{-1}, z_1^{-1}, \ldots, z_{n-1}^{-1})$, and the coefficients of $A(z)$ are the array elements of A, i.e. $A(z) = \sum_{j \in \mathcal{Z}_{N_0} \times \mathcal{Z}_{N_1} \times \ldots \times \mathcal{Z}_{N_{n-1}}} A_j z_0^{j_0} z_1^{j_1} \ldots z_{n-1}^{j_{n-1}}$. We desire all out-of-phase sidelobes of the aperiodic autocorrelation of A to be of low magnitude, which means that we want K_{A_j} to have low magnitude $\forall j \in \mathcal{Z}_{N_0} \times \mathcal{Z}_{N_1} \times \ldots \times \mathcal{Z}_{N_{n-1}}$, $j \neq 0$. Ideally we would like all $K_{A_j} = 0$ for $j \neq 0$, in which case $K_A(z) = ||A||^2$ is a *δ-function*, independent of z, but, as with the sequence case, this is impossible. We later discuss how to obtain an ideal (δ-function) response for the sum of the aperiodic autocorrelations of a pair of arrays.

The continuous Fourier power spectrum of the array A is given by the set of evaluations of $K_A(z)$ on the multi-unit circle, and is summarised by

$$\mathcal{F}(A) = \{K_A(\upsilon) \quad | \quad |\upsilon_j| = 1, 0 \leq j < n\}, \tag{2}$$

where $\upsilon = (\upsilon_0, \upsilon_1, \ldots, \upsilon_{n-1})$. If A had a perfect response then $\mathcal{F}(A) = \{1\}$, i.e. the Fourier power spectrum would be *flat* everywhere. More realistically, if A has a near-perfect aperiodic autocorrelation then, loosely, its Fourier power spectrum is *near-flat*. We later discuss how to obtain a flat power spectrum for the sum of the Fourier power spectra of a pair of Golay complementary arrays.

4 Sequences Obtained by Joining Array Dimensions

Let A be a $N = N_0 \times N_1 \times \ldots \times N_{n-1}$ complex array of n dimensions, as represented by the polynomial $A(z) = A(z_0, z_1, \ldots, z_{n-1})$. Then, by substituting into $A(z)$ the variables $z_0 = y$, and $z_k = z_{k-1}^{N_{k-1}}$, $\forall k$, $1 \leq k < n$, we obtain the univariate polynomial $\tilde{A}(y)$ whose coefficients represent a sequence of length N. The important point about these substitutions is that they ensure that the elements of both the array, A, and derived sequence, $\tilde{A}$, are taken from the same alphabet[1]. We refer to this series of substitutions as the *joining* of dimensions [13]. By an identical series of substitutions in $K_A(z)$, which is the aperiodic autocorrelation of the array $A(z)$, one obtains the aperiodic autocorrelation, $K_{\tilde{A}}(y)$, of the sequence, $\tilde{A}(y)$. This is not the only possible substitution for $A(z)$ and $K_A(z)$, as, at the array level, the ordering of variables z_0, z_1, ...etc, is arbitrary. Thus, more generally, one can apply the series of substitutions $z_{\pi(0)} = y$, and $z_{\pi(k)} = z_{\pi(k-1)}^{N_{\pi(k-1)}}$, $\forall k$, $1 \leq k < n$, where $\pi \in \mathcal{S}_n$ is any permutation of $\{0, 1, \ldots, n-1\}$. Moreover the ordering of coefficients in one or more

[1] We do not consider, in this paper, the alternative substitution strategy using the Chinese Remainder theorem when the dimensions are relatively prime.

dimensions, j, may be reversed and/or multiplied by a unit phase, α, $|\alpha| = 1$, without changing the aperiodic coefficient magnitudes, and these symmetries can be expressed by replacing z_j by $\alpha_j z_j^{\pm 1}$ for all dimensions to be reversed and/or phase-shifted. Thus, each array, $A(z)$, can generate a family of sequences $\{\tilde{A}\} = \{A(z) \quad | \quad z_{\pi(0)} = y, z_{\pi(k)} = \alpha_k z_{\pi(k-1)}^{\pm N_{\pi(k-1)}}, |\alpha_k| = 1, 1 \leq k < n, \forall \pi \in \mathcal{S}_n\}$, each with the same aperiodic autocorrelation, $K_{\tilde{A}}$, where the number of distinct sequences in the family depends on internal symmetries of the specific array.

All sequences in family $\{\tilde{A}\}$ have an aperiodic autocorrelation, given by $K_{\tilde{A}}$, where the coefficients of $K_{\tilde{A}}$ are a relatively straightforward combination of the coefficients of K_A. In particular, if we had an array, A, with perfect (δ-function) aperiodic autocorrelation, then all sequences in $\{\tilde{A}\}$ would also have a perfect δ-function response. Although such ideal arrays do not exist, there are pairs of Golay complementary arrays whose aperiodic autocorrelations sum to a δ-function and, by joining, one can extract from such array pairs a family of sequence pairs whose aperiodic autocorrelations sum to a δ-function.

The continuous Fourier power spectrum of A is summarised by (2). Likewise, the continuous Fourier power spectrum of $\tilde{A}$ is summarised by,

$$\mathcal{F}(\tilde{A}) = \{K_{\tilde{A}}(\upsilon_0, \upsilon_0^{N_0}, \ldots, \upsilon_{n-1}^{N_0 N_1 \ldots N_{n-2}}) \quad | \quad |\upsilon_0| = 1.\}, \tag{3}$$

By comparing right-hand sides of (2) and (3) one concludes that

$$\mathcal{F}(\tilde{A}) \subseteq \mathcal{F}(A). \tag{4}$$

Let $P(A)$ be the maximum value in $\mathcal{F}(A)$, i.e.

$$P(A) = \max(u \quad | \quad u \in \mathcal{F}(A)). \tag{5}$$

We refer to $P(A)$ as the *peak-to-average power ration* (PAPR) of A. If, for a particular array, A, one has an upper bound, $\mathcal{P}$, on $P(A)$, then, from (4), $\mathcal{P}$ is also an upper bound on $P(\tilde{A})$. If A had a perfect aperiodic autocorrelation then $\mathcal{F}(\tilde{A}) = \mathcal{F}(A) = \{1\}$, i.e. the Fourier power spectrum of the sequence obtained by joining is *flat* everywhere, implying that $P(A) = P(\tilde{A}) = 1$. Although such perfect arrays are impossible, we can obtain a near-flat Fourier power spectrum for $\tilde{A}$ and $\tilde{B}$ by constructing a pair of Golay complementary arrays, (A, B), such that $P(A) = \frac{||A||^2 + ||B||^2}{||A||^2}$ and $P(B) = \frac{||A||^2 + ||B||^2}{||B||^2}$, leading to $P(\tilde{A}) \leq P(A)$ and $P(\tilde{B}) \leq P(B)$ for all possible sequences in families $\{\tilde{A}\}$ and $\{\tilde{B}\}$, respectively.

5 Three Kinds of Aperiodicity for Generalised Boolean Functions

We now focus our discussion on characterisation and construction of aperiodic *Boolean functions*. We here consider an n-variable generalised *Boolean function*, $A : \mathbb{F}_2^n \rightarrow \mathcal{C}$, which is a $2 \times 2 \times \ldots \times 2$ n-dimensional array, where the kth entry in the array, $k \in \mathbb{F}_2^n$, is given by $A(k) \in \mathcal{C}$. In other words $A \in \mathcal{C}_2^n$.

We characterise the aperiodicity of a generalised Boolean function using unitary matrices. Let

$$V_I = \{\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \alpha \\ 1 & -\alpha \end{pmatrix} \quad | \quad \forall \alpha, |\alpha| = 1\}$$

be an infinite-size class of 2×2 unitary matrices. Then, from (2),

$$\mathcal{F}(A) = \mathcal{F}_I(A) = \{\hat{A}_{U,k} \quad | \quad \hat{A}_U = UA, \forall U \in V_I^{\otimes n}, \forall k \in \mathbb{F}_2^n\},$$

where we now refer to $\mathcal{F}(A)$ as $\mathcal{F}_I(A)$ to indicate that all transforms are taken with respect to unitaries from $V_I^{\otimes n}$. In other words, the set of points comprising the continuous Fourier transform of A is equal to the union of the set of array elements of $\hat{A}_U$, taken over all possible $2^n \times 2^n$ matrices U in $V_I^{\otimes n}$, where $\hat{A}_U$ is the unitary transform of A with respect to U. From the previous section we see that aperiodicity of A can be assessed by examining the 'flatness' of $\mathcal{F}_I(A)$ and, from (5), one measure of this flatness is $P(A)$, the PAPR of A, which from now on we refer to as $P_I(A)$.

The complete class of 2×2 unitary matrices can be given by

$$V = \{\Delta \begin{pmatrix} \cos\theta & \sin\theta\alpha \\ \cos\theta & -\sin\theta\alpha \end{pmatrix} \quad | \quad \forall \alpha, |\alpha| = 1, \forall \theta\}, \tag{6}$$

where Δ is any diagonal or anti-diagonal unitary 2×2 matrix. V_I is only a subclass of V. Are there are any other infinite-size unitary matrix subclasses over which another type of aperiodicity of A could be assessed?

We therefore consider aperiodicity of an n-variable generalised Boolean function, A, with respect to $V_I^{\otimes n}$, $V_{II}^{\otimes n}$ and $V_{III}^{\otimes n}$, where

$$V_{II} = \{\begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} \quad | \quad \forall \theta\}$$

and

$$V_{III} = \{\begin{pmatrix} \cos(\theta) & i\sin(\theta) \\ \sin(\theta) & -i\cos(\theta) \end{pmatrix} \quad | \quad \forall \theta\}, \quad \text{where } i = \sqrt{-1}.$$

We refer to these three types of aperiodicity as *type-I, type-II, and type-III aperiodicity*, as characterised by the spectral sets F_I, F_{II}, and F_{III}, where

$$\mathcal{F}_{II}(A) = \{\hat{A}_{U,k} \quad | \quad \hat{A}_U = UA, \forall U \in V_{II}^{\otimes n}, \forall k \in \mathbb{F}_2^n\},$$

and

$$\mathcal{F}_{III}(A) = \{\hat{A}_{U,k} \quad | \quad \hat{A}_U = UA, \forall U \in V_{III}^{\otimes n}, \forall k \in \mathbb{F}_2^n\}.$$

We define the generalised Boolean function, A, to have optimal type-I, type-II, or type-III aperiodic properties if $P_I(A)$, $P_{II}(A)$, or $P_{III}(A)$ is as small as possible, respectively.

The relationship between V_I, V_{II}, and V_{III} is via the multiplicative action on V_I of a cyclic group, $\mathbb{T} = \{I, \lambda, \lambda^2\}$, of order 3, where

$$\lambda = \frac{\omega^5}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$$

is a generator of $\mathbb{T}$ of order 3, ω is a primitive eighth root of one, and I is the 2×2 identity matrix. Specifically,

$$V_I = \Delta V_{III}\lambda = \Delta' V_{II}\lambda^2 = \Delta'' V_I \lambda^3,$$

where Δ, Δ', and Δ'' are diagonal and/or anti-diagonal 2×2 unitaries. The action of λ *rotates* V_I to V_{II}, V_{II} to V_{III}, and V_{III} to V_I, all modulo the group of diagonal/anti-diagonal matrices $\{\Delta\}$. The reason that we choose to rotate by λ is because we consider $\mathbb{T}$ to be important - the *local Clifford group*, $\mathbb{C}$, for 2×2 unitaries, splits as $\mathbb{D} \times \mathbb{T}$, where $\mathbb{D}$ is a subgroup comprising 64 diagonal and anti-diagonal 2×2 unitaries, and the local Clifford group, $\mathbb{C}$, is defined to be the group of 192 matrices that *stabilizes* the *Pauli group*, $\mathbb{P}$, otherwise known as the *discrete Heisenberg-Weyl group.* For 2×2 unitaries, $\mathbb{P}$ comprises $\{I, X, Z, Y\}$, where

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = -iXZ.$$

The term 'stabilizes' means that $UWU^{-1} = W'$, $\forall U \in \mathbb{C}$, $\forall W, W' \in \mathbb{P}$.

We have introduced three types of aperiodicity in spectral ('frequency' or 'residue') terms by means of the rotation action of $\mathbb{T}$ on the infinite-size set of transforms, V_I, over which conventional aperiodicity is defined. We now give the polynomial equations which reflect the 'time' ('non-residue') viewpoint for this aperiodicity. Specifically, given an n-variable generalised Boolean function, A, and associated multivariate polynomial $A(z) = A(z_0, z_1, \ldots, z_{n-1})$,

Lemma 1

Type-I aperiodic properties of A are expressed by $K_A^I(z) = \frac{A(z)A^*(z)}{||A||^2}$,
Type-II aperiodic properties of A are expressed by $K_A^{II}(z) = \frac{2^n A(z)^2}{||A||^2 \prod_{j=0}^{n-1}(1+z_j^2)}$,
Type-III aperiodic properties of A are expressed by $K_A^{III}(z) = \frac{2^n A(z)A(-z)}{||A||^2 \prod_{j=0}^{n-1}(1-z_j^2)}$.

A is a perfect generalised Boolean function of type-I, II, or III if $K_A^I(z) = 1$, $K_A^{II}(z) = 1$, or $K_A^{III}(z) = 1$, respectively.

Proof. Let $\upsilon = (\upsilon_0, \upsilon_1, \ldots, \upsilon_{n-1})$, and let $\mathcal{R}$ and $\mathcal{I}$ be the sets of real and imaginary values, respectively. One can verify that the sets of spectral power values $\mathcal{F}_I(A)$, $\mathcal{F}_{II}(A)$, and $\mathcal{F}_{III}(A)$ can be obtained via the following evaluations of certain equations in $A(z)$ over the unit circle, real axis, and imaginary axis, respectively,

$$\begin{aligned}
\mathcal{F}_I(A) &= \{\tfrac{A(\upsilon)A^*(\upsilon)}{||A||^2} \quad | \quad |\upsilon_j| = 1, 0 \le j < n\}, \\
\mathcal{F}_{II}(A) &= \{\tfrac{2^n A(\upsilon)^2}{||A||^2 \prod_{j=0}^{n-1}(1+\upsilon_j^2)} \quad | \quad \upsilon_j \in \mathcal{R}, 0 \le j < n\}, \\
\mathcal{F}_{III}(A) &= \{\tfrac{2^n A(\upsilon)A(-\upsilon)}{||A||^2 \prod_{j=0}^{n-1}(1-\upsilon_j^2)} \quad | \quad \upsilon_j \in \mathcal{I}, 0 \le j < n\}.
\end{aligned}$$

A is a perfect aperiodic generalised Boolean function of type-I, II, or III, if $P_I(A) = 1$, $P_{II}(A) = 1$, or $P_{III}(A) = 1$, respectively, which occurs when $\mathcal{F}_I(A) = \{1\}$, $\mathcal{F}_{II}(A) = \{1\}$, or $\mathcal{F}_{III}(A) = \{1\}$, respectively, and this is only possible when the conditions of the lemma are satisfied. QED.

We now apply dimension joining to the Boolean array, A, to obtain two new types of aperiodic sequence action. From the array $A(z_0, z_1, \ldots, z_{n-1})$, via the substitution $z_0 = y$, $z_k = z_{k-1}^2$, $\forall k$, $1 \leq k < n$, one obtains the length 2^n sequence $\tilde{A}$, and applying the same substitutions to the multivariate polynomial equations of lemma 1 gives the following univariate polynomial equation in $\tilde{A}(y)$,

Lemma 2

Type-I aperiodic properties of $\tilde{A}$ are expressed by $K^I_{\tilde{A}}(y) = \frac{\tilde{A}(y)\tilde{A}^*(y)}{||\tilde{A}||^2}$,
Type-II aperiodic properties of $\tilde{A}$ are expressed by $K^{II}_{\tilde{A}}(y) = \frac{2^n \tilde{A}(y)^2}{||\tilde{A}||^2 \prod_{j=0}^{n-1}(1+y^{2^{j+1}})}$,
Type-III aperiodic properties of $\tilde{A}$ are expressed by $K^{III}_{\tilde{A}}(y) = \frac{2^n \tilde{A}(y)\tilde{A}(-y)}{||\tilde{A}||^2 \prod_{j=0}^{n-1}(1-y^{2^{j+1}})}$.

$\tilde{A}$ is a perfect complex sequence of length 2^n of type-I, II, or III if $K^I_{\tilde{A}}(y) = 1$, $K^{II}_{\tilde{A}}(y) = 1$, or $K^{III}_{\tilde{A}}(y) = 1$, respectively.

Each array generates a family of type-I sequences, which we shall now call $\{\tilde{A}_I\}$, each member of which generates the same aperiodic autocorrelation, which we shall now call $K^I_{\tilde{A}}(y)$. Likewise, each array, $A(z)$, can also generate a family of type-II and type-III sequences, $\{\tilde{A}\}_{II}$, and $\{\tilde{A}\}_{III}$, respectively, where each member of $\{\tilde{A}\}_{II} = \{A(z) \mid z_{\pi(0)} = y, z_{\pi(k)} = \alpha_k z^{\pm 2}_{\pi(k-1)}, \alpha_k \in \mathcal{R}, 1 \leq k < n, \forall \pi \in \mathcal{S}_n\}$, has the same type-II aperiodic profile, $K^{II}_{\tilde{A}}$, and where each member of $\{\tilde{A}\}_{III} = \{A(z) \mid z_{\pi(0)} = y, z_{\pi(k)} = \alpha_k z^{\pm 2}_{\pi(k-1)}, \alpha_k \in \mathcal{R}, 1 \leq k < n, \forall \pi \in \mathcal{S}_n\}$, has the same type-III aperiodic profile, $K^{III}_{\tilde{A}}$.

6 Some Cryptographic Interpretations and Context for Type-I, II, and III Aperiodicity

Let $a(x)$ be a Boolean function in n variables, where $A_k = (-1)^{a(k)} \in \{-1, 1\}^n$, $k \in \mathbb{F}_2^n$.

6.1 Cryptographic Motivation

Having characterised three types of aperiodicity for a generalised Boolean function we now provide some cryptographic motivation as to the relevance of these characterisations for Boolean functions of types I and II.

– The conventional *differential* properties of a are measured by the closeness of $a(x)$ to $a(x + s)$, $s \in \mathbb{F}_2^n$, i.e. by the maximum magnitude of $\sigma_s = \sum_{x \in \mathbb{F}_2^n} (-1)^{a(x)+a(x+s)}$, $\forall s \neq 0$ [8]. A differentially perfect function will be maximally distant from its differential, for all values of $s \neq 0$, i.e. ideally $\sigma_s = 0, \forall s \neq 0$, in which case the differential $a(x)+a(x+s)$ remains completely unbiased $\forall s \neq 0$, on the assumption that x is not known. But type-I aperiodicity measures the biasedness of $a(x) + a(x + s)$ on the assumption that x_j is known for each $s_j = 1$, and a perfect type-I aperiodic function would remain completely unbiased for all $s \neq 0$ even under this assumption [9].

- The conventional *linear* properties of a are measured by the closeness of $a(x)$ to an affine function, $t \cdot z$, $t \in \mathbb{F}_2^n$, i.e. by the maximum magnitude of $\hat{a}_t = \sum_{x\in\mathbb{F}_2^n}(-1)^{a(x)+t\cdot x}$, $\forall t$ [8]. A linearly perfect function will be maximally distant from all affine functions, i.e. $\hat{a}$ will have magnitude $2^{n/2}$, $\forall t$, in which case $a(x)+t\cdot x$ is minimally biased $\forall t$. There is an implicit assumption that each of the input variables $x_0, x_1, \ldots, x_{n-1}$ is '0' with probability $\frac{1}{2}$. But type-II aperiodicity measures the biasedness of $a(x)+t\cdot x$, $\forall t$, where no assumption is made on the input probability of $x_j = 0$, $\forall j$.

6.2 Wider Context

The autocorrelation action of the Heisenberg-Weyl (HW) group [11] on an n-variable Boolean function, a, can be described by,

$$\mathcal{H}_{s,t}(a) = \sum_{x\in\mathbb{F}_2^n}(-1)^{a(x)+a(x+s)+x\cdot t+s\cdot t} = \quad < A, X^s Z^t A >, \quad s,t \in \mathbb{F}_2^n. \qquad (7)$$

There are 4^n coefficients, $\mathcal{H}_{s,t}(a)$. The Boolean function, a, (array A), can be considered to be a good HW function if all magnitudes $|\mathcal{H}_{s,t}(a)|$ are small $\forall s$ and $t \neq 0$. A perfect HW Boolean function would have $\mathcal{H}_{s,t}(a) = 0$ for all $\forall s$ and $t \neq 0$, but this is impossible. Let $s = (s_0, s_1, \ldots, s_{n-1}) \in \mathbb{F}_2^n$ let $\bar{s} = (s_0+1, s_1+1, \ldots, s_{n-1}+1)$.

- [9] Type-I aperiodicity is measured by the coefficients $\mathcal{H}_{s,t}(a)$ where $t \preceq s$. A perfect type-I function would have $\mathcal{H}_{s,t}(a) = 0$, $\forall s$ and $t \neq 0$, $t \preceq s$.
- Type-II aperiodicity is measured by the coefficients $\mathcal{H}_{s,t}(a)$ where $t \preceq \bar{s}$. A perfect type-II function would have $\mathcal{H}_{s,t}(a) = 0$, $\forall s$ and $t \neq 0$, $t \preceq \bar{s}$.
- Type-III aperiodicity is measured by the coefficients $\mathcal{H}_{s,t}(a)$ where $s \preceq t$. A perfect type-III function would have $\mathcal{H}_{s,t}(a) = 0$, $\forall s$ and $t \neq 0$, $s \preceq t$.

Each of type-I, II, III identifies 3^n of the 4^n HW coefficients. For the 3^n type-I coefficients and the 4^n HW coefficents we know the following identities.

$$\begin{array}{ll} \sum_{s,t,t\preceq s}|\mathcal{H}_{s,t}(a)|^2 = \int_{|v_j|=1,\forall j}|A(v)|^4, & \text{Wiener-Kinchine} \\ \sum_{s,t}|\mathcal{H}_{s,t}(a)|^2 = 2^n, & \text{Moyal's identity [11].} \end{array}$$

The impossibility of perfect type-I, II, or III functions implies the impossiblity of a perfect HW function. But, in the next section, we identify perfect pairs of type-I, II, and III functions which are also constructible, whereas the far stricter HW criteria does not appear to allow such pairs. However, recent activity [18,16] has identified N-element sequences and (one) array which realise the value of $|\mathcal{H}_{s,t}(a)|^2 = \frac{1}{N+1}$ everywhere, which is the theoretical min-max. Such objects are called *equiangular lines* and, in the context of *quantum tomography*, are known as SIC-POVMs. Whilst a number of SIC-POVM sequences have been found over unwieldy alphabets, only one $2 \times 2 \times 2$ SIC-POVM array has been found (the *Hoggar lines*), and this is not over the alphabet $\{1, -1\}$ [16]. Moreover, [16] has shown that SIC-POVM arrays in $\mathcal{C}_2^n$ do not exist for $n > 3$.

When viewing the n-variable Boolean function, a, as a quantum state of n qubits, as described by pure-state vector $|A >= 2^{-n/2}A$, then the action of the HW group on $|A >$ identifies the qubit *bit-flip*, *phase-flip*, and combined phase-flip then bit-flip errors on $|A >$ (the action of unitaries X, Z, and XZ), respectively. Those Boolean functions, a, for which $\mathcal{H}_{s,t}(a) = 0$ when $\mathrm{wt}(s) + \mathrm{wt}(t) - \mathrm{wt}(s + t) < 2d$ ('wt' means Hamming wieght) represent one-dimensional *quantum codes* of distance d [6,4], and include highly-entangled *graph states*, which have been proposed as a resource for *measurement-based quantum computing* [20]. This quantum condition on the $\mathcal{H}_{s,t}(a)$ coefficients is conveniently expressed by the *fixed-aperiodic autocorrelation* of Boolean functions, as proposed and investigated in [9], this comprising the union of coefficients arising from the aperiodic autocorrelation of a, with those from the aperiodic autocorrelation of any function, $a_\downarrow$, obtained by fixing one or more of the input variables of a to '0' or '1' - a total of 5^n coefficients. Related to these 5^n fixed-aperiodic autocorrelation coefficients we have the following conjectured identity.

$$\textstyle\sum_{s,t} \binom{n}{e_{s,t}} 2^{e_{s,t}} |\mathcal{H}_{s,t}(a)|^2 = \int_{U \in V^{\otimes n}} ||U|A > ||^4,$$

where $e_{s,t} = n - \mathrm{wt}(s + t + s \cdot t)$, and V is the set of all 2×2 unitaries, as defined in (6).

7 Complementary and Near-Complementary Pairs and Their Construction

Conventional (type-I) Golay complementary sequence pairs, $(\tilde{A}, \tilde{B})$, satisfy the property,

$$K^I_{\tilde{A}}(y) + K^I_{\tilde{B}}(y) = 2. \tag{8}$$

In other words $(\tilde{A}, \tilde{B})$ are ideal as a pair of type-I sequences. But, as shown recently [13], the Golay property is often, primarily, an array property, and a pair of (type-I) Golay arrays, (A, B), satisfy,

$$K^I_A(z) + K^I_B(z) = 2., \tag{9}$$

where $z = (z_0, z_1, \ldots, z_{n-1})$, in which case (A, B) are ideal as a pair of type-I arrays. Let $\{(\tilde{A}, \tilde{B})\}$ be a family of sequence pairs obtained from (A, B) by joining. It follows from the ideal properties of the array pair that,

$$P_I(A) = \frac{||A||^2 + ||B||^2}{||A||^2}, \qquad P_I(B) = \frac{||A||^2 + ||B||^2}{||B||^2}.$$

In particular, if $||A||^2 = ||B||^2$, which is the case for Boolean arrays $A = (-1)^a$, $B = (-1)^b$, then

$$P_I(A) = P_I(B) = 2.$$

It follows from (4) that,

$$P_I(\tilde{A}) \le P_I(A), \qquad P_I(\tilde{B}) \le P_I(B).$$

So, if (A, B) is type-I complementary, then so is $(\tilde{A}, \tilde{B})$ for all $(\tilde{A}, \tilde{B}) \in \{(\tilde{A}, \tilde{B})\}$. Complementary array properties imply complementary sequence properties, but a complementary pair of sequences is not necessarily derived from a pair of higher-dimensional arrays. For instance, the length-10 (type-I) complementary pair of sequences over the alphabet $\{1, -1\}$ is not derived from a 2×5 two-dimensional (type-I) complementary array pair over the alphabet $\{1, -1\}$ [23].

We further extend our definition of PAPR to array or sequence pairs. Specifically, let,

$$K^I_{AB}(z) = \frac{A(z)A^*(z) + B(z)B^*(z)}{||A||^2 + ||B||^2},$$

and

$$\mathcal{F}_I(A, B) = \{K^I_{AB}(v) \quad | \quad |v_j| = 1, 0 \leq j < n\}.$$

$\mathcal{F}_I(\tilde{A}, \tilde{B})$ is similarly defined, where

$$\mathcal{F}_I(\tilde{A}, \tilde{B}) \subseteq \mathcal{F}_I(A, B).$$

The type-I PAPR of the array pair, (A, B), and sequence pair, $(\tilde{A}, \tilde{B})$, are given by,

$$\begin{aligned} P_I(A, B) &= \max(u \quad | \quad u \in \mathcal{F}_I(A, B)), \\ P_I(\tilde{A}, \tilde{B}) &= \max(u \quad | \quad u \in \mathcal{F}_I(\tilde{A}, \tilde{B}), \end{aligned}$$

and

$$P_I(\tilde{A}, \tilde{B}) \leq P_I(A, B).$$

The (type-I) Golay construction for sequence pairs [14,15] was generalised by Turyn [30], further generalised by Borwein and Ferguson [5], and has recently been generalised to arrays [13]. We here give a further generalisation to *near-complementary pairs* [27,29], building on the notation of [5]. Let $x = (z_0, z_1, \ldots, z_{n-1})$, $y = (z_n, z_{n+1}, \ldots, z_{n+m-1})$, and $z = (z_0, z_1, \ldots, z_{n+m-1})$. Let $(A(x), B(x))$, $(C(y), D(y))$, and $(F(z), G(z))$ be three pairs of polynomials of n, m, and $n+m$ variables, respectively.

Lemma 3. *Let*

$$F(z) = C(y)A(x) + D^*(y)B(x), \qquad G(z) = D(y)A(x) - C^*(y)B(x).$$

Then,

$$P_I(F, G) = P_I(A, B)P_I(C, D).$$

In particular, if (A, B) and (C, D) are both (type-I) Golay complementary pairs then, by definition, $P_I(A, B) = P_I(C, D) = 1$ and, therefore, as $P_I(F, G) = 1$, then (F, G) is a (type-I) Golay complementary pair.

From lemma 3 one can derive a similar construction for sequence pairs. We call the construction of lemma 3 a *type-I construction.* If $P_I(A, B) = 1 + \epsilon$ and $P_I(C, D) = 1 + \epsilon'$, then $P_I(F, G) = 1 + \epsilon''$, where ϵ'' is small if ϵ and ϵ' are small, in which case we have a construction for *near-complementary pairs.*

Previously we showed that, for arrays in $\mathcal{C}_2^n$, one can rotate the concept of aperiodicity by successive multiplications of the transform kernel by λ. This also implies a rotated concept of complementarity and we now define type-II and type-III complementarity for arrays in $\mathcal{C}_2^n$, i.e. for generalised Boolean functions. For $A, B \in \mathcal{C}_2^n$,

Type-II complementary array pairs, (A, B), satisfy the property,

$$K_A^{II}(z) + K_B^{II}(z) = 2. \tag{10}$$

Type-III complementary array pairs, (A, B), satisfy the property,

$$K_A^{III}(z) + K_B^{III}(z) = 2. \tag{11}$$

By means of unitary rotation by λ, as described in section 5, we can not only rotate the set of transforms over which aperiodicity and complementarity is determined, but also rotate the (type-I) Turyn construction itself. We obtain the following type-II and type-III constructions for (near-)complementary pairs, where the meanings of $P_{II}(A, B)$ and $P_{III}(A, B)$, …etc, follow in exactly the same way as for type-I.

Lemma 4. *Let*

$$F(z) = C(y)A(x) + D(y)B(x), \qquad G(z) = D(y)A(x) - C(y)B(x).$$

Then,

$$P_{II}(F, G) = P_{II}(A, B)P_{II}(C, D).$$

In particular, if (A, B) and (C, D) are both type-II complementary pairs then, by definition, $P_{II}(A, B) = P_{II}(C, D) = 1$ and, therefore, as $P_{II}(F, G) = 1$, then (F, G) is a type-II complementary pair.

Lemma 5. *Let*

$$F(z) = C(y)A(x) + D(-y)B(x), \qquad G(z) = D(y)A(x) - C(-y)B(x).$$

Then,

$$P_{III}(F, G) = P_{III}(A, B)P_{III}(C, D).$$

In particular, if (A, B) and (C, D) are both type-III complementary pairs then, by definition, $P_{III}(A, B) = P_{III}(C, D) = 1$ and, therefore, as $P_{III}(F, G) = 1$, then (F, G) is a type-III complementary pair.

The construction of lemma 3 is valid for arrays of all dimensions, and the constructions of lemmas 4 and 5 are at least valid for arrays in $\mathcal{C}_2^n$, i.e. for generalized Boolean functions. For the special case where the elements of the array are in the alphabet $\{1, -1\}$, we can express the type-I, II, and III constructions using Boolean functions. Let (a, b), (c, d), and (f, g) be three pairs of Boolean functions of n, m, and $n + m$ disjoint sets of variables, respectively, where $a, b : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, $c, d : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$, and $f, g : \mathbb{F}_2^{n+m} \rightarrow \mathbb{F}_2$. By $P_I(a, b)$ we mean $P_I(A, B)$. Let $\overleftarrow{a}(x_0, x_1, \ldots, x_{n-1}) = a(x_0 + 1, x_1 + 1, \ldots, x_{n-1} + 1)$.

Lemma 6. *Let*

$$f = (a+b)(c+\overleftarrow{d}) + a + \overleftarrow{d}, \qquad g = (a+b)(\overleftarrow{c} + d) + b + \overleftarrow{c}.$$

Then,

$$P_I(f,g) = P_I(a,b)P_I(c,d).$$

Lemma 7. *Let*

$$f = (a+b)(c+d) + a + d, \qquad g = (a+b)(c+d) + b + c.$$

Then,

$$P_{II}(f,g) = P_{II}(a,b)P_{II}(c,d).$$

Lemma 8. *Let (c,d) be defined over the m binary variables, $(x_0, x_1, \ldots, x_{m-1})$. Let $l_m = \sum_{j=0}^{m-1} x_j$. Let*

$$f = (a+b+l_m)(c+d) + a + d, \qquad g = (a+b+l_m)(c+d) + b + c + l_m.$$

Then,

$$P_{III}(f,g) = P_{III}(a,b)P_{III}(c,d).$$

It is interesting to note that the type-II Boolean construction is identical to a certain construction for bent functions [2,8,7], which states that, if a, b, c, and d are bent, then f is bent. Moreover, if a and b are t resilient, and c and d are u resilient, then f is $t+u+1$ resilient. Finally, if a, b, c, and d are self-dual bent, then f is self-dual bent, and if a and b are bent duals, c is self-dual bent, and d is anti-self-dual bent, then f is self-dual bent [3].

8 Explicit Examples of Type-I, II, and III Complementary Pairs of Boolean Functions

For type-I there is, to within symmetries discussed previously, only one known [10] class of complementary pairs of Boolean functions, (f,g), as given by,

$$f = \sum_{j=0}^{n-2} x_j x_{j+1}, \qquad g = f + x_0, \quad \text{or} \quad g = f + x_{n-1}.$$

By interpreting the quadratic terms of f as edges of a simple graph we see that f represents the *path graph* of n vertices.

For type-II we have found, to within symmetries discussed previously, only one class of complementary pairs of Boolean functions, (f,g), as given by,

$$f = \sum_{j<k} x_j x_k, \qquad g = f + \sum_j x_j.$$

f represents the *complete graph* of n vertices.

Some type-III pairs were identified by Abdelraheem in [1], as follows. For type-III there is an infinite number of classes of complementary pairs of quadratic or affine Boolean functions, (f, g). To begin with, (f, g) are type-III complementary for any affine f and g. By passing these into the input of the type-III construction of lemma 5, an infinite number of classes of type-III complementary pairs of quadratic Boolean functions arise at the output. However, one particularly interesting class is

$$f = \sum_{j=1}^{n-1} x_0 x_j, \qquad g = f + \sum_{j=1}^{n-1} x_j \quad \text{or } g = f + x_0.$$

For this particular class, f represents the *star graph* of n vertices.

Although we have focused on Boolean complementary pairs we observe that type-I, II, and III pairs from the alphabet $\{1, -1\}$ can be rotated round to type-II, III, and I pairs from the alphabet $\{0, 1, i, -1, -i\}$, respectively, by the multiplicative action of λ on each of the pairs, and round to type-III, I, and II pairs from the alphabet $\{0, 1, i, -1, -i\}$, respectively, by the multiplicative action of λ^2. In particular, this allows us to generate new Golay (type-I) complementary pairs which are defined, indirectly, using type-II or type-III Boolean functions.

9 Conclusion and Open Problems

The purpose of this paper was, first, to show how aperiodic arrays can be used to generate aperiodic sequences and, secondly, to present a wider notion of aperiodicity for arrays in $\mathcal{C}_2^n$. Three different notions of aperiodicity were defined by exploiting the action of a size-3 cyclic subgroup of the local Clifford group on the aperiodic description. The three types of aperiodicity related to the autocorrelations generated by the Heisenberg-Weyl group. The three aperiodic types also lead to three types of construction for complementary pairs of arrays. Explicit examples of complementary pairs of Boolean functions were given for each of the three types.

We identify some open problems.

- Does another class of complementary $\{1, -1\}$ sequences exist of length 2^n other than the 'path graph' class described in this paper? One can generalise this question to ask whether (type-I) complementary Boolean functions other than the path graph class exist.
- We only know of one class of type-II complementary Boolean function pair, namely that described by the 'complete graph'. As with type-I, it is an open problem as to whether another class of type-II complementary Boolean function pair exists.
- We know of no complementary pair of Boolean functions of types I, II or III whose component functions have degree greater than 2. Can one prove that higher-degree complementary pairs of Boolean functions do not exist?

- The complementary Boolean functions described in this paper are of algebraic degree ≤ 2. But, for cryptographic purposes, it is usually desirable to construct high-degree Boolean functions. Assuming that complementary pairs of Boolean functions of degree greater than 2 do not exist, how close to complementarity can one get for a pair of Boolean functions of degree d, and how does one construct and/or bound such a pair?
- Is it possible to effectively combine two or more of the type-I, II, or III constructions? Observe that the type-I and type-II constructions differ only in the application of $\overleftarrow{*}$ to c and d for type-I. Thus, if we can find a pair of Boolean functions (c, d) that satisfy the conditions $c = \overleftarrow{c}$ and $d = \overleftarrow{d}$, then we can apply type-I and type-II constructions simultaneously. Unfortunately we do not know of a pair (c, d) which is simultaneously both type-I and type-II complementary (and we do not expect that such a pair exists), but it is possible to find near-complementary pairs that satisfy the conditions.
- It is reasonable to expect that there are no pairs of Boolean functions which are complementary with respect to the Heisenberg-Weyl group. Can this be proved? If we can't find pairs, then what is the smallest size set of Boolean functions which are complementary with respect to the Heisenberg-Weyl group for a non-trivial number of variables, n? Note that it is possible to extract complementary sets from quantum codes, however the size of these sets grows exponentially with the number of binary variables, so they are of little interest.
- Are there any other interesting types of aperiodicity? For instance, the three types of aperiodicity describes herein are for arrays in $\mathcal{C}_2^n$. One expects that more interesting types may turn up as the size of array dimension increases.

Acknowledgments. The author would like to acknowledge that any 'new' ideas in this paper owe a lot to joint research and discussions with Lars Eirik Danielsen, Frank Fiedler, Jonathan Jedwab, Constanza Riera, and Mohamed Abdelraheem. In particular, the results on generalised complementary constructions follow naturally from recent joint work on multidimensional complementary arrays with Fiedler and Jedwab.

References

1. Abdelraheem, M.A.A.M.A.: A database for Boolean functions and constructions for generalized complementary pairs. Master's thesis, University of Bergen (June 2008)
2. Adams, C.M., Tavares, S.E.: Generating and Counting Binary Bent Sequences. IEEE Trans. Inf. Theory 36(5), 1170–1173 (1990)
3. Carlet, C., Danielsen, L.E., Parker, M.G., Solé, P.: Self-dual bent functions. In: Fourth International Workshop on Boolean Functions: Cryptography and Applications (BFCA 2008), Copenhagen, Denmark, May 19–21 (2008)
4. Danielsen, L.E., Parker, M.G.: On the classification of all self-dual additive codes over GF(4) of length up to 12. Journal of Combinatorial Theory, Series A 113(7), 1351–1367 (2006)

5. Borwein, P.B., Ferguson, R.A.: A complete description of Golay pairs for lengths up to 100. Mathematics of Computation 73, 967–985 (2003)
6. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum Error Correction Via Codes Over GF(4). IEEE Trans. Information Theory 44, 1369–1387 (1998)
7. Carlet, C.: On the secondary constructions of resilient and bent functions. In: Feng, K., Niederreiter, H., Xing, C. (eds.) Proceedings of the Workshop on Coding, Cryptography and Combinatorics 2003, pp. 3–28. Birkhauser Verlag, Basel (2004)
8. Carlet, C.: Boolean functions for cryptography and error correcting codes (preprint, 2008)
9. Danielsen, L.E., Gulliver, T.A., Parker, M.G.: Aperiodic Propagation Criteria for Boolean Functions. Inform. Comput. 204(5), 741–770 (2006)
10. Davis, J.A., Jedwab, J.: Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes. IEEE Trans. Information Theory 45, 2397–2417 (1999)
11. Howard, S.D., Calderbank, A.R., Moran, W.: The finite Heisenberg-Weyl groups in radar and communications. EURASIP Journal on Applied Signal Processing 2006(1) (2006)
12. Dmitriev, D., Jedwab, J.: Bounds on the growth rate of the peak sidelobe level of binary sequences. Advances in Mathematics of Communications 1, 461–475 (2007)
13. Fiedler, F., Jedwab, J., Parker, M.G.: A multi-dimensional approach to the construction and enumeration of Golay complementary sequences. Journal of Combinatorial Theory (Series A) (accepted, 2007)
14. Golay, M.J.E.: Static multislit spectrometry and its application to the panoramic display of infrared spectra. J. Opt. Soc. Amer. 41, 468–472 (1951)
15. Golay, M.J.E.: Complementary series. IRE Trans. Inform. Theory IT-7, 82–87 (1961)
16. Godsil, C., Roy, A.: Equiangular lines, mutually unbiased bases, and spin models (2005) (preprint) arXiv:quant-ph/0511004 v2
17. Golomb, S.W., Gong, G.: Signal Design for Good Correlation. Cambridge University Press, Cambridge (2005)
18. Grassl, M.: Tomography of quantum states in small dimensions. Electron. Notes Discrete Math. 20, 151–164 (2005)
19. Gulliver, T.A., Parker, M.G.: The Multivariate Merit Factor of a Boolean Function. In: ITW 2005, IEEE ITSOC Information Theory Workshop 2005 on Coding and Complexity, Rotorua, New Zealand, 29th Aug.–1st (Sept 2005)
20. Hein, M., Dur, W., Eisert, J., Raussendorf, R., Van den Nest, M., Briegel, H.-J.: Entanglement in Graph States and its Applications. In: Zoller, P., Casati, G., Shepelyansky, D., Benenti, G. (eds.) International School of Physics Enrico Fermi, Quantum computers, algorithms and chaos 162, Varenna, Italy, vol. 162 (2006), http://xxx.soton.ac.uk/abs/quant-ph/0602096
21. Helleseth, T., Kumar, P.V.: Sequences with Low Correlations. In: Pless, V., Huffmann, G. (eds.) Handbook in Coding Theory. Kluwer Acad. Publ., Dordrecht (1998)
22. Jedwab, J., Parker, M.G.: There are no Barker arrays having more than two dimensions. Designs, Codes and Cryptography 43(2-3), 79–84 (2007)
23. Jedwab, J., Parker, M.G.: Golay Complementary Array Pairs. Designs, Codes and Cryptography 44, 209–216 (2007)
24. Luke, H.D.: Sets of one and higher dimensional Welti codes and complementary codes. IEEE Trans. Aerospace Electron. Systems. AES-21, 170–179 (1985)

25. Parker, M.G.: Univariate and Multivariate Merit Factors. In: Helleseth, T., Sarwate, D., Song, H.-Y., Yang, K. (eds.) SETA 2004. LNCS, vol. 3486, pp. 72–100. Springer, Heidelberg (2005)
26. Parker, M.G., Paterson, K.G., Tellambura, C.: Golay Complementary Sequences. In: Proakis, J.G. (ed.) Wiley Encyclopedia of Telecommunications. Wiley Interscience, Chichester (2002)
27. Parker, M.G., Tellambura, C.: Generalised Rudin-Shapiro Constructions. In: WCC 2001 International Workshop on Coding and Cryptography, Paris(France). Jan 8–12 (2001), Electronic Notes in Discrete Mathematics, April 6 (2001)
28. Riera, C., Parker, M.G.: Generalised Bent Criteria for Boolean Functions (I). IEEE Trans Inform. Theory 52(9), 4142–4159 (2006)
29. Schmidt, K.-U.: On cosets of the generalized first-order Reed-Muller code with low PMEPR. IEEE Trans. Inform. Theory 52, 3220–3232 (2006)
30. Turyn, R.J.: Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings. J. Combin. Theory (A) 16, 313–333 (1974)
31. Shapiro, H.S.: Extremal Problems for Polynomials. M.S. Thesis, M.I.T (1951)

Wiretapping Based on Node Corruption over Secure Network Coding: Analysis and Optimization

Mohammad Ravanbakhsh, Mehdi M. Hassanzadeh, and Dag Haugland

Department of Informatics, University of Bergen, Bergen N-5020, Norway
{mohammad.ravanbakhsh,mehdi.hassanzadeh,dag.haugland}@ii.uib.no

Abstract. A new type of attack on secure network coding is introduced in this paper. In this model, network nodes, which handle the traffic from the source node to sink nodes are potentially viewed to be corruptible. We study the maximum security capacity for this problem for a single-source single-sink scenario, and we generalize our study for multicast with network coding. Based on our study, two optimization problems are introduced to increase the security against the attacks under study. We have shown by simulation results that our proposed optimization method has increased the security against node corruption considerably, and at the same time, the cost per level of security is lower compared to optimization methods without constraints on node corruption.

1 Introduction

Network coding was introduced by Ahlswede et al. in [1]. With network coding, network nodes are allowed not only to forward exact copies of packets, as routers in a classical store-and-forward network are restricted to, but also to modify and combine incoming packets prior to forwarding them. In [10], Li et al. proved that linear network coding suffices to multicast information from a single source to a fixed set of receivers at a rate equal to the minimum (over all receivers) of the min-cut of the network flow from the source to each receiver.

In [4], Cai and Yeung presented a method for secure multicasting that can be alleviated by network coding. They introduced a model for secure linear network coding that achieves perfect information security against a wiretapper who can eavesdrop on a limited number of network links. Their method is based on using secret sharing ideas combined with constraints on the field size for secure network coding. In [5], Feldman et al. proposed a method based on the model by Cai and Yeung. In a work by Hassanzadeh et al. [6], the ideas in [4] are extended, and a two layer secret sharing approach is proposed for secure network coding. In these three models, the attacker has access to links. In [8], Lima et al. considered a different approach to provide secure network coding. In their model, any node is a potential eavesdropper. Hence, imposing a limit on the input degree of nodes, prevents nodes from extracting the message. Additionally, they showed that the security of the model depends fully on the network topology.

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 154–162, 2008.

In our approach, we have extended the idea from [8] and we have defined a different class of attacking. In our model, the attacker is not limited to a single node. The objective of the attacker is to corrupt as many nodes as possible such that the aggregate flow to all corrupted nodes provides the required information to extract the secret message. In this paper, we analyze these types of attacks and we propose two algorithms for increasing the security against them.

The paper is organized as follows: Section 2 contains an introduction to network coding and to secret sharing. Wiretapping based on node corruption is described in Section 3, which also contains two optimization methods for increasing the security against the newly defined attacks. Simulation results are presented in Section 4, and conclusions are drawn in Section 5.

2 Preliminaries

2.1 The Network Coding Model

We represent a communication network with a directed graph $G = (V, E)$, where V is the set of nodes (routers, a single source, and sinks/receivers) and E is the set of edges or links. Each link (i, j) represents a lossless point-to-point communication link from node i to node j. The sets $\Gamma_I(i)$ and $\Gamma_O(i)$ contain links entering and leaving node i, respectively.

The goal of a multicast session is to convey a sequence of information symbols generated at a set of sources ($S \subset V$) to a set $T \subset V$ of nodes (referred to as the set of sinks). Unless otherwise stated, we assume that S consists of a single source[1]. The maximum amount of transferable directed flow between a source and a sink in a directed graph is known as the max-flow, which, by the well-known max-flow theorem is identical to the min-cut between the source and the sink. In a multicast, where a source node sends information to all sink nodes; it is possible to reach max-flow for each sink by applying network coding [1]. Without network coding, this is not always possible. In network coding, intermediate nodes not only copy and forward their received packets but can also combine them. Establishing a predetermined network code consists of two steps: 1) Finding a subgraph for transferring the max-flow of information, and 2) Given this subgraph, finding a specific method of encoding; that is, a detailed procedure for how each node shall combine its received packets at its outgoing links. In [7], a deterministic method is proposed for encoding and in [3], this algorithm is extended for subgraphs with cycles (flow cycles).

2.2 Secret Sharing

In cryptography, secret sharing refers to any method for distributing a secret (with a dealer) amongst a group of n participants (players), each of which is

[1] The single-source scenario can easily be generalized to one with multiple sources. For simplicity and convenience, we mainly consider the single-source scenario in this paper.

allocated a share of the secret. In an (n, t_{ss})-threshold secret sharing scheme, the secret can only be reconstructed if at least t_{ss} shares are combined together. Secret sharing was invented independently in 1979 by A. Shamir [11] and G. Blakley [2]. The goal of secret sharing is to divide a secret m into n shares $m_1, \ldots, m_n$ in such a way that:

1. Knowledge of any t_{ss} or more shares makes m easily computable.
2. Knowledge of any $t_{ss} - 1$ or fewer shares leaves m completely undetermined.

Consider the trivial (n, n)-threshold scheme, i. e. t_{ss} is equal to n. In this scheme, $n-1$ random numbers $(r_1, \ldots, r_{n-1})$ are generated as $n-1$ shares, and for the last share we have: $r_n = m \oplus r_1 \oplus r_2 \cdots \oplus r_{n-1}$, where $\oplus$ is any discrete formal addition. It is straightforward to see that S could be reconstructed with knowledge of all the shares, while no subset of $n-1$ or fewer shares can reconstruct the secret m.

3 Wiretapping Based on Node Corruption

3.1 Definition and Analysis

Assume the network G is available for communication. A source node $s \in S$ wants to send a secret message m to a sink or terminal node $t \in T$ in a way that is *secure against eavesdropping.* The message m may of course be encrypted, but this may require a key distribution scheme which can be inconvenient; thus we will assume that an attacker who is able to read the whole message is also able to understand its meaning. We will further assume that all the edges are secure from eavesdropping, for example because link encryption is applied to all links. However, an attacker may attempt to take control over intermediate nodes in order to learn the content of m. We will also assume that the source and the sink cannot be corrupted. Our basic problem can be formulated as:

$$\text{How many nodes must the attacker corrupt to learn } m? \tag{1}$$

Clearly, if the message is sent along a single path, the simple answer to this question is that it is sufficient to corrupt any single node along the path. In order to improve this, the secret message m can be represented by an (n, n) secret sharing scheme. Thus, instead of sending m we will send n message parts $m_1, \ldots, m_n$, in such a way that anyone who can collect all n parts will be able to reconstruct the original secret message m, while knowledge to $n-1$ parts will give no information at all about m. Such a secret sharing scheme can easily be designed for any n. The n parts are then sent independently along node-disjoint paths from the source and the sink. Then our basic problem can be reformulated as:

$$\text{What is the maximum number of node disjoint paths from } s \text{ to } t \text{ in } G? \tag{2}$$

In a set of node disjoint paths, every node (except from the source and sink nodes) has exactly one incoming and one outgoing link. Based on the node disjoint property, our problem in (2) can be formulated as a max-flow problem with the following constraints:

1. All links have unit capacity.
2. All the nodes except sink nodes can only receive a single unit of flow.

Conditions on the single-source single-sink case imply the fact that controling the amount of flow entering each node is the key to achieve the maximum secure capacity. We have generalized the problem in ([2]) for more than one sink node. As it has been mentioned in Section 2.1, it is possible to reach max-flow capacity by applying network coding. In the next sections, two algorithms are proposed for providing secure network coding against node corruption attacks. In our setup, we consider that a smart move by the attacker is to concentrate his efforts on the neighbors of s and t. Hence, we try to secure the neighbors and assume that the neighbors of s and t are incorruptible.

3.2 Optimization

In a multicast scenario, the same collection of information is sent to all sink nodes. Each sink receives different information flows over disjoint paths. The union of all the disjoint paths forms a subgraph that carries the traffic from the source node to all sink nodes. By routing, the problem is to find disjoint Steiner trees [12], which is known to be NP-hard; and the resulting solutions are comparatively wasteful with respect to network resources. For even a moderate number of sink nodes, it may be impossible to allocate such trees. The new obvious alternative approach is to use network coding. By applying network coding, not only the required paths can be provided but also optimization methods are available to find the lowest cost subgraph. Based on the work by Lun et al. [9], we investigate a linear program (LP) to minimize the cost and to provide our objectives. The goal here is to search a subgraph that includes the required flow for each sink with minimum cost. A fixed cost and unit capacity is considered for each link.

As we have mentioned in the previous section, control over the amount of flow entering each node is the key to achieve the maximum secure capacity. In other words, for each node the *Node Input Flow* (NIF) should be minimized. Before presenting a linear formulation for NIF, we define some notation. For each link $(i, j) \in E$, we define the constants a_{ij} and c_{ij} as cost and capacity, respectively, and the variable z_{ij} as flow. Further, $x_{ij}^{(t)}$ is the variable representing the amount of flow destined to sink t passing through link (i, j). After solving the LP problem to be given shortly, it is possible to see which links are used in the subgraph by looking at the value of the z_{ij} variables, and it is also possible to see which links are used for a specific sink by checking $x_{ij}^{(t)}$ for all links.

Now we can define NIF:

$$NIF = \max_{j \in V \setminus (T \cup S)} \{ \sum_{(i,j) \in \Gamma_I(j)} z_{ij} \} \tag{3}$$

The less the NIF is, the more nodes need to be corrupted to gather required flow for extracting the secret message. In the context of single-source single-sink, the value of NIF is one, which is its lowest possible value. Our objective is to setup an optimization problem that minimizes the NIF and also provides the cheapest possible subgraph. Two approaches are proposed in this paper: Two Step Optimization (TOPT) and Joint Cost and Security Optimization (JOPT). The following sections introduce these approaches.

TOPT. The TOPT problem is a two step network coding optimization, which is based on the work in [9]. Each step is an LP problem. In the first step, the minimum value of NIF is computed. In (4), the first step is shown.

$$\begin{aligned} &\text{minimize} \quad NIF \\ &\text{subject to:} z_{ij} \leqslant c_{ij} \quad \forall (i,j) \in E \\ &\qquad 0 \leqslant x_{ij}^{(t)} \leqslant z_{ij} \quad \forall (i,j) \in E \ \forall t \in T \\ &\qquad \sum_{(i,j)\in \Gamma_O(i)} x_{ij}^{(t)} - \sum_{(j,i)\in \Gamma_I(i)} x_{ji}^{(t)} = \sigma_i^{(t)} \quad \forall i \in V \ \forall t \in T \\ &\qquad \sum_{(i,j)\in \Gamma_I(j)} z_{ij} \leqslant NIF \quad \forall j \in V \setminus (T \cup S). \end{aligned} \tag{4}$$

In the second step, the computed value of NIF is used to find a low cost subgraph. The second step is shown in (5). In the second step, NIF represents a constant value.

$$\begin{aligned} &\text{minimize} \sum_{(i,j)\in E} a_{ij} z_{ij} \\ &\text{subject to:} z_{ij} \leqslant c_{ij} \quad \forall (i,j) \in E \\ &\qquad 0 \leqslant x_{ij}^{(t)} \leqslant z_{ij} \quad \forall (i,j) \in E \ \forall t \in T \\ &\qquad \sum_{(i,j)\in \Gamma_O(i)} x_{ij}^{(t)} - \sum_{(j,i)\in \Gamma_I(i)} x_{ji}^{(t)} = \sigma_i^{(t)} \quad \forall i \in V \ \forall t \in T \\ &\qquad \sum_{(i,j)\in \Gamma_I(j)} z_{ij} \leqslant NIF \quad \forall j \in V \setminus (T \cup S). \end{aligned} \tag{5}$$

In (5) and (4) we have:

$$\sigma_i^{(t)} = \begin{cases} R, & \text{if } \ i = s \\ -R, & \text{if } \ i = t \\ 0, & \text{otherwise.} \end{cases} \tag{6}$$

where

$$R = \min_{t\in T}\{\text{max-flow}(t)\}, \tag{7}$$

and max-flow(t) is the maximum flow from s to t in G with link capacities c_{ij}.

In other words, the first optimization problem (4) maximizes the security, whereas the problem in (5) searches for a low-cost subgraph.

JOPT. Here, two steps of TOPT are formulated in one LP problem. Therefore the objective function consists of two parts; security and cost. The cost is the same as the second step in TOPT, but security is slightly different from the first step of TOPT. The LP problem for JOPT is shown in (8). The NIF variable is multiplied by a constant coefficient E_r. The reason for this coefficient is twofold. First, since NIF is comparably smaller than the cost objective, and without the constant coefficient the result of the optimization thus has less emphasis on the security. Second, we have to choose the constant coefficient equal to $|V| - |T| - |S|$ (the number of intermediate nodes) to transfer the effect of NIF to all the intermediate nodes. The formulation of JOPT becomes:

$$\begin{aligned}
&\text{minimize} \sum_{(i,j)\in E} a_{ij} z_{ij} + E_r \cdot NIF \\
&\text{subject to:} z_{ij} \leqslant c_{ij} \quad \forall (i,j) \in E \\
&\qquad 0 \leqslant x_{ij}^{(t)} \leqslant z_{ij} \quad \forall (i,j) \in E \ \forall t \in T \\
&\qquad \sum_{(i,j)\in \Gamma_O(i)} x_{ij}^{(t)} - \sum_{(j,i)\in \Gamma_I(i)} x_{ji}^{(t)} = \sigma_i^{(t)} \quad \forall i \in V \ \forall t \in T \\
&\qquad \sum_{(i,j)\in \Gamma_I(j)} z_{ij} \leqslant NIF \quad \forall j \in V \setminus (T \cup S).
\end{aligned} \tag{8}$$

In this setup, cost and security are optimized together. In Section 4, the difference between the results of TOPT and JOPT is compared.

4 Simulation Results

In this section, the performance of TOPT and JOPT are shown, and they are compared with the ordinary optimization (OOPT). The OOPT is the LP problem defined in [9]. Since OOPT has no restrictions on the value of NIF, the optimal subgraph of OOPT has the maximum value of NIF.

4.1 The Level of Security

The level of security, denoted by $\varPhi$, depends on NIF. If R is the rate for secure communication, then R/NIF is the minimum number of nodes that are needed to access the complete R rate flow. The larger NIF is, the fewer intermediate nodes are needed to be corrupted for a successful attack. Based on the properties of R/NIF we define $\varPhi$ in the following form:

$$\varPhi = 1 - \frac{NIF}{R}. \tag{9}$$

In Fig. 1, simulation results for $\varPhi$ are shown for all three approaches. In our approaches (TOPT and JOPT), we achieve a considerable improvement of the level of security. It is also observable that TOPT and JOPT almost provide the same level of security. Since in TOPT, NIF has its minimum value, TOPT has a slightly better level of security.

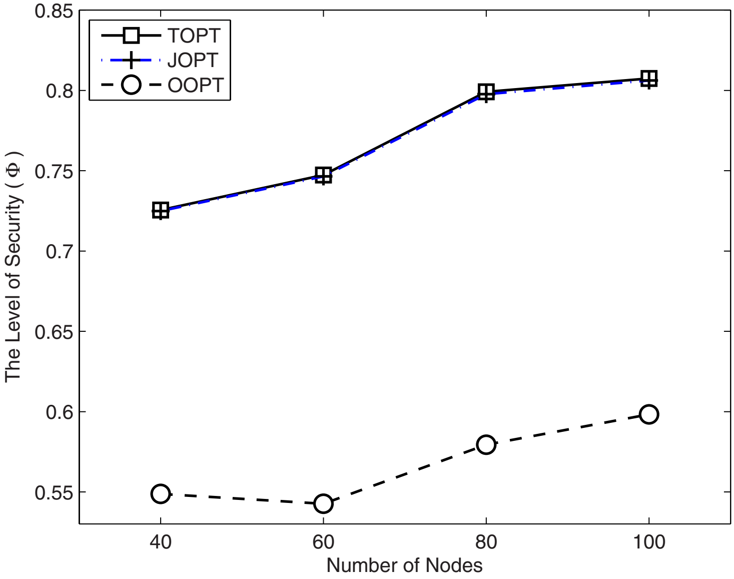


Fig. 1. The level of security

4.2 The Cost Per Level of Security

Since there is always a trade-off between level of security and the total cost (P), we provide a new metric Ω defined as the cost per level of security. Cost is defined in the following form:

$$P = \sum_{(i,j)\in E} a_{ij} z_{ij}. \tag{10}$$

We define Ω in (11) below, and simulation results are shown in Figs. 2 and 3. Fig. 2 shows Ω according to the number of nodes for the fixed number of sinks, and Fig. 3 shows Ω according to the number of sinks for the fixed number of nodes.

$$\Omega = \frac{P}{\Phi \cdot 100}. \tag{11}$$

Based on Figs. 2 and 3, we observe that in our approaches, more security is gained with lower cost. By comparing the cost in our simulations we find that the cost in TOPT and JOPT is slightly different from OOPT, but since TOPT and JOPT have constraints on NIF, the resulting subgraph is not concentrated to a small subgraph. Further, the subgraph is spread to more places in the network and more nodes are handling the max-flow rate. To access the complete flow from the source, the attacker hence needs to corrupt more nodes.

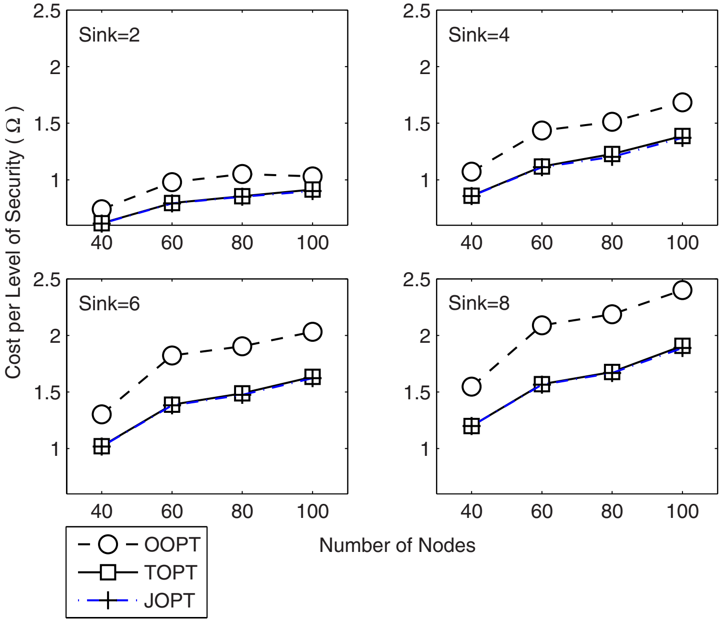


Fig. 2. Cost per level of security for fixed number of sinks

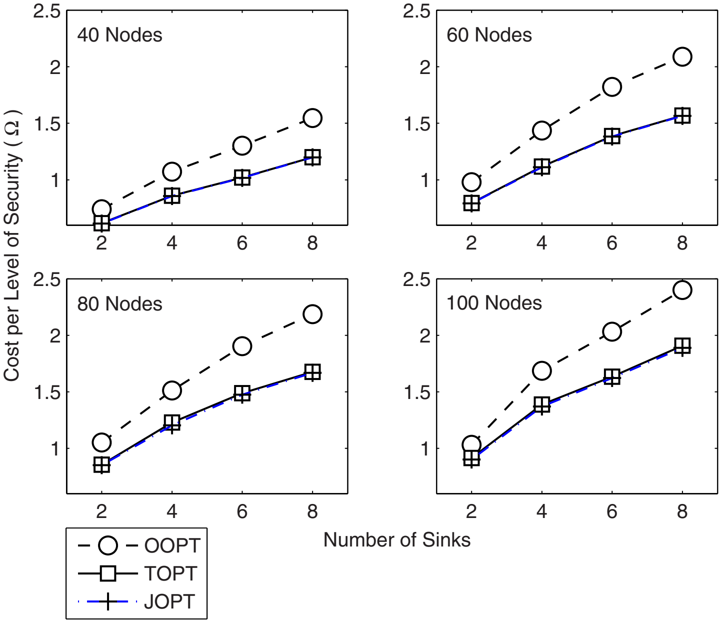


Fig. 3. Cost per level of security for fixed number of nodes

5 Conclusion

In this paper, we have introduced an attack model for secure network coding based on node corruption. We have studied the maximum security capacity for this problem, and two optimization problems are introduced to increase the security against the attacks under study. We have defined two metrics, namely the level of security and the cost per level of security. Our simulations showed considerable improvement in these metrics.

References

1. Ahlswede, R., Cai, N., Li, S.-Y.R., Yeung, R.W.: Network information flow. IEEE Transactions on Information Theory 46(4), 1204–1216 (2000)
2. Blakley, G.R.: Safeguarding cryptographic keys. In: Proc. National Computer Conference, vol. 48, pp. 313–317 (1979)
3. Barbero, Á.I., Ytrehus, Ø.: Cycle-logical treatment for "Cyclopathic" networks. IEEE Transactions on Information Theory 52(6), 2795–2804 (2006)
4. Cai, N., Yeung, R.W.: Secure network coding. In: Proc. IEEE International Symposium on Information Theory, vol. 323 (2002)
5. Feldman, J., Malkin, T., Servedio, R.A., Stein, C.: On the Capacity of Secure Network Coding. In: Proc. 42nd Annual Allerton Conference on Communication, Control and Computing (2004)
6. Hassanzadeh, M.M., Ravanbakhsh, M., Ytrehus, Ø.: Two Layer Secure Network Coding – (2-LSNC). In: 4th Biannual International Symposium on Telecommunications, Tehran, Iran (submitted, 2008)
7. Jaggi, S., Sanders, P., Chou, P.A., Effros, M., Egner, S., Jain, K., Tolhuizen, L.M.G.M.: Polynomial time algorithms for multicast network code construction. IEEE Transactions on Information Theory 51(6), 1973–1982 (2005)
8. Lima, L., Medard, M., Barros, J.: Random linear network coding: a free cipher? In: Proc. IEEE International Symposium on Information Theory, Nice, France (2007)
9. Lun, D.S., Ratnakar, N., Medard, M., Koetter, R., Karger, D.R., Ho, T., Ahmed, E., Zhao, F.: Minimum-cost multicast over coded packet networks. IEEE Transactions on Information Theory 52(6), 2608–2623 (2006)
10. Li, S.-Y.R., Yeung, R.W., Cai, N.: Linear network coding. IEEE Transactions on Information Theory 49(2), 371–381 (2003)
11. Shamir, A.: How to share a secret. Communications of the ACM 22(1), 612–613 (1979)
12. Winter, P.: Steiner problem in networks: A survey. Networks 17, 129–167 (1987)

On the Kronecker Product Construction of Completely Transitive q-Ary Codes*

Josep Rifà[1] and Victor Zinoviev[2]

[1] Dept. of Information and Communications Engineering, Universitat Autònoma de Barcelona, Spain
josep.rifa@uab.cat

[2] Institute for Problems of Information Transmission of the Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 101447, Russia

Abstract. For any integer $\rho \geq 1$ and for any prime power q, the explicit construction of an infinite family of completely transitive (and completely regular) q-ary codes with minimum distance $d = 3$ and with covering radius ρ is given.

Keywords: Completely regular codes, completely transitive codes, covering radius, Kronecker product.

1 Introduction

Let $\mathbb{F}_q$ be a finite field of the order q. Let $\mathrm{wt}(\mathbf{v})$ denote the *Hamming weight* of a vector $\mathbf{v} \in \mathbb{F}_q^n$ and let $d(\mathbf{v}, \mathbf{u}) = \mathrm{wt}(\mathbf{v} - \mathbf{u})$ denote the *Hamming distance* between two vectors $\mathbf{v}, \mathbf{u} \in \mathbb{F}_q^n$. We say that two vectors $\mathbf{v}$ and $\mathbf{u}$ are *neighbors* if $d(\mathbf{v}, \mathbf{u}) = 1$. A q-ary linear $[n, k, d]_q$-code C is a k-dimensional subspace of $\mathbb{F}_q^n$, where n is the *length*, $N = q^k$ is the *cardinality* of C and d is the *minimum distance*,

$$d \;=\; \min\{d(\mathbf{v}, \mathbf{u}) :\; \mathbf{v}, \mathbf{u} \in C,\; \mathbf{v} \neq \mathbf{u}\}.$$

For the binary case, i.e. for the case $q = 2$, we use notation $[n, k, d]$. The error correcting capability of a code C with minimum distance d is given by $e = \lfloor \dfrac{d-1}{2} \rfloor$ and we will refer to C as a e-code.

Given any vector $\mathbf{v} \in \mathbb{F}_q^n$, its *distance to the code* C is $d(\mathbf{v}, C) = \min_{\mathbf{x} \in C}\{d(\mathbf{v}, \mathbf{x})\}$ and the *covering radius* of the code C is

$$\rho = \max_{\mathbf{v} \in \mathbb{F}_q^n}\{d(\mathbf{v}, C)\}.$$

Let $D = C + \mathbf{x}$ be a *coset* of C, where $+$ means the component-wise addition in $\mathbb{F}_q$. The *weight* $\mathrm{wt}(D)$ of D is the minimum weight of the codewords of D. For an arbitrary coset D of C of weight $s = \mathrm{wt}(D)$ denote

* This work has been partially supported by the Spanish MEC and the European FEDER Grants MTM2006-03250 and TSI2006-14005-C02-01 and also by the Russian fund of fundamental researches (the number of project 06 - 01 - 00226).

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 163–170, 2008.

by $\mu(D) = (\mu_0(D), \mu_1(D), ..., \mu_n(D))$ its weight distribution, where $\mu_j(D)$, $j = 0, \ldots, n$ denotes the number of words of D of weight j. Notice that $\mu_j(D) = 0$ for all $j < s$ or $j > \rho$.

Definition 1. *A q-ary linear code C with covering radius ρ is called* completely regular *if the weight distribution of any coset D of C of weight i, $i = 0, 1, ..., \rho$ is uniquely defined by the minimum weight of D, i.e. by the number $i = wt(D)$.*

Solé in [10] used the direct sum of ℓ copies of a fixed perfect binary 1-code of length n for the construction of infinite families of binary completely regular codes of length $n{\cdot}\ell$ with covering radius $\rho = \ell$. Thus, in the construction of [10], the covering radius of the resulting code is growing to infinity, if the length of the code is growing.

The main purpose of the present paper is to describe a method of construction of linear completely regular and completely transitive codes (see Definition 3 in Section 2) with arbitrary covering radius, which is constant when the length of the resulting code is growing to infinity. More exactly, for any prime power q and for any natural number ℓ we give an explicit construction of an infinite family of linear q-ary completely regular and completely transitive codes with lengths $n = (q^m - 1)(q^\ell - 1)/(q - 1)^2$ and with fixed covering radius $\rho = \ell$, where $m \geq \ell$ is any integer.

2 Preliminary Results

For a given q-ary code C with covering radius $\rho = \rho(C)$ define

$$C(i) \; = \; \{\mathbf{x} \in \mathbb{F}_q^n : \; d(\mathbf{x}, C) = i\}, \;\; i = 0, 1, \ldots, \rho.$$

We also use the following alternative standard definition of completely regularity (see, for example, [7]).

Definition 2. *A code C is completely regular, if for all $l \geq 0$ every vector $\mathbf{x} \in C(l)$ has the same number c_l of neighbors in $C(l-1)$ and the same number b_l of neighbors in $C(l+1)$. Also, define $a_l = (q-1){\cdot}n - b_l - c_l$ and note that $c_0 = b_\rho = 0$. Refer to $(b_0, \ldots, b_{\rho-1}; c_1, \ldots, c_\rho)$ as the intersection array of C.*

For a q-ary $[n, k, d]_q$ code C with weight distribution $\mu(C) = (\mu_0, \ldots, \mu_n)$ define the *outer distance* $s = s(C)$ as the number of nonzero coordinates $\mu_i^\perp$, $i = 1, \ldots, n$ of the vector $(\mu_0^\perp, \ldots, \mu_n^\perp)$ obtained by the MacWilliams transform of $\mu(C)$ [4]. Hence, since C is a linear code, $s(C)$ is the number of different nonzero weights of codewords in the dual code $C^\perp$.

Lemma 1 ([4]). *For any code C with covering radius $\rho(C)$ and with outer distance $s(C)$ we have $\rho(C) \leq s(C)$. If C is completely regular then $\rho(C) = s(C)$.*

Let C be a linear code of length n over $\mathbb{F}_q$, a finite field of size a prime power q. Following [6], if $q = 2$, the automorphism group $Aut(C)$ of C is a subgroup of the symmetric group S_n consisting of all $n!$ permutations of the n coordinate positions which send C into itself.

Let M be a monomial matrix, i.e. a matrix with exactly one nonzero entry in each row and column. If q is prime, then $Aut(C)$ consists of all $n \times n$ monomial matrices M over $\mathbb{F}_q$ such that $\mathbf{c}M \in C$ for all $\mathbf{c} \in C$. If q is a power of a prime number, then $Aut(C)$ also contains all the field automorphisms of $\mathbb{F}_q$ which preserve C.

The group $Aut(C)$ induces an action on the set of cosets of C in the following way: for all $\sigma \in Aut(C)$ and for every vector $\mathbf{v} \in \mathbb{F}_q^n$ we have $(\mathbf{v}+C)^\sigma = \mathbf{v}^\sigma + C$.

In [10] it was introduced the concept of completely transitive binary linear code and it can be generalized to the following definition, which also corresponds to the definition of coset-completely transitive code in [5].

Definition 3. *Let C be a linear code over $\mathbb{F}_q$ with covering radius ρ. Then C is completely transitive if $Aut(C)$ has $\rho+1$ orbits when acts on the cosets of C.*

Since two cosets in the same orbit should have the same weight distribution, it is clear that any completely transitive code is completely regular.

3 Kronecker Product Construction

In this section we describe a new construction which provides for any natural number ρ and for any prime power q an infinite family of q-ary linear completely regular codes with covering radius ρ.

Definition 4. *For two matrices $A = [a_{r,s}]$ and $B = [b_{i,j}]$ over $\mathbb{F}_q$ define a new matrix H which is the Kronecker product $H = A \otimes B$, where H is obtained by changing any element $a_{r,s}$ in A by the matrix $a_{r,s}B$.*

Consider the matrix $H = A \otimes B$ and let C, C_A and C_B be the codes over $\mathbb{F}_q$ which have, respectively, H, A and B as a parity check matrices. Assume that A and B have size $m_a \times n_a$ and $m_b \times n_b$, respectively. For $r \in \{1, \cdots, m_a\}$ and $s \in \{1, \cdots, m_b\}$ the rows in H look as

$$(a_{r,1}b_{s,1}, \cdots, a_{r,1}b_{s,n_b}, a_{r,2}b_{s,1}, \cdots, a_{r,2}b_{s,n_b}, \cdots, a_{r,n_a}b_{s,1}, \cdots, a_{r,n_a}b_{s,n_b}).$$

Arrange these rows taking blocks of n_b coordinates as columns such that the vectors $\mathbf{c}$ in code C are presented as matrices of size $n_b \times n_a$:

$$\mathbf{c} = \begin{bmatrix} c_{1,1} & \cdots & c_{1,n_a} \\ c_{2,1} & \cdots & c_{2,n_a} \\ \vdots & \vdots & \vdots \\ c_{n_b,1} & \cdots & c_{n_b,n_a} \end{bmatrix} = \begin{bmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \\ \vdots \\ \mathbf{c}_{n_b} \end{bmatrix}, \qquad (1)$$

where $c_{i,j} = a_{r,j}b_{s,i}$ and $\mathbf{c}_r$ denotes the r-th row vector of this matrix.

We will call matrix representation the above way to present the vectors $\mathbf{c} \in C$.

Let us go to a further view on the codewords of C, the code over $\mathbb{F}_q$ which has $H = A \otimes B$ as a parity check matrix. Consider vector $\mathbf{c} \in C$ by using the representation in (1), hence $\mathbf{c} = (\mathbf{c}_1^t, \mathbf{c}_2^t, \cdots, \mathbf{c}_{n_b}^t)$. By definition of C we have

$$B\big(A\mathbf{c}_1^t, A\mathbf{c}_2^t, \ldots, A\mathbf{c}_{n_b}^t\big)^t = 0$$

(here $(\cdot)^t$ means the transpose vector) and so i

$$B\big(A\mathbf{c}^t\big)^t = B{\cdot}\mathbf{c}{\cdot}A^t = 0. \tag{2}$$

With this last property it is easy to note that any $(n_b \times n_a)$-matrix with codewords of C_A as rows belong to the code C and also any $(n_b \times n_a)$-matrix with codewords of C_B as columns belongs to the code C. Vice versa, all the codewords in C can always be seen as linear combinations of matrices of both types above.

Moreover, it is straightforward to state the following well known fact.

Lemma 2. *The codes defined by the parity check matrices $A \otimes B$ and $B \otimes A$ are permutation equivalent.*

From now on, we assume that matrix A (respectively, B) is a parity check matrix of a Hamming code with parameters $[n_a, k_a, 3]_q$ (respectively, $[n_b, k_b, 3]_q$), where $n_a = (q^{m_a} - 1)/(q-1) \geq 3$ (respectively, $n_b = (q^{m_b} - 1)/(q-1) \geq 3$) and $k_a = n_a - m_a$ (respectively, $k_b = n_b - m_b$).

Denote by H_m the parity check matrix of a perfect Hamming $[n, k, 3]_q$-code C over $\mathbb{F}_q$, where $n = (q^m - 1)/(q-1)$. Let $\{\xi_0 = 0, \xi_1 = 1, \ldots, \xi_{q-1}\}$ denote the elements of $\mathbb{F}_q$. Then the matrix H_m can be expressed, up to equivalence, through the matrix H_{m-1} as follows [11]:

$$H_m = \left[\begin{array}{c|c|c|c|c} 0\cdots 0 & 1\cdots 1 & \cdots & \xi_{q-1}\cdots\xi_{q-1} & 1 \\ \hline H_{m-1} & H_{m-1} & \cdots & H_{m-1} & \mathbf{0} \end{array}\right],$$

where $\mathbf{0}$ is the zero column and where $H_1 = [1]$. Note that, under such construction, the following lemmas are straightforward (see, for example, [11]).

Lemma 3. *Matrix H_m contains as columns, among other, all the m possible binary vectors of length m and of weight* 1*.*

Lemma 4. *For $i = 1, \ldots, m$, let $\mathbf{r}_i$ denote the i-th row of H_m. Let $\mathbf{g} = \sum_{i=1}^{m} \xi_i \mathbf{r}_i$, with $\xi_i \in \mathbb{F}_q$, be any linear combination of the rows of H_m. If $wt(\mathbf{g}) \neq 0$, then $wt(\mathbf{g}) = q^{m-1}$.*

Any codeword $\mathbf{c} \in C$, which has nonzero elements only in one row (or only in one column) will be called a *line*. Since A and B are parity check matrices of Hamming codes (i.e. they have minimum distances 3), there are lines of weight 3. For example, a row line $L_r = (\alpha_1, \alpha_2, \alpha_3)_{(s_1,s_2,s_3)}$ (respectively, a column line $L_s = (\alpha_1, \alpha_2, \alpha_3)_{(r_1,r_2,r_3)}$) means that the codeword $\mathbf{c}$ of weight 3, whose nonzero rth row (respectively, nonzero sth column) has nonzero elements α_1, α_2, α_3 in columns s_1th, s_2th, s_3th (respectively, in rows r_1th, r_2th, r_3th). Recall that this means the following equality for the corresponding columns $\mathbf{a}_{s_1}$, $\mathbf{a}_{s_2}$, and $\mathbf{a}_{s_3}$ of matrix A (respectively, for the columns $\mathbf{b}_{r_1}$, $\mathbf{b}_{r_2}$, and $\mathbf{b}_{r_3}$ of matrix B):

$$\sum_{i=1}^{3} \alpha_i \, \mathbf{a}_{s_i} \; = \; \mathbf{0} \quad (\text{respectively}, \sum_{i=1}^{3} \alpha_j \, \mathbf{b}_{r_j} \; = \; \mathbf{0}).$$

Define the set R of row indices as $R = \{1, \ldots, n_b\}$ (respectively, of column indices as $S = \{1, \ldots, n_a\}$). By definition of perfect codes, for a fixed row index $r \in R$ (respectively, column index $s \in S$), for any two nonzero elements $\alpha_1, \alpha_2 \in \mathbb{F}_q$ and for any two different $s_1, s_2 \in S$ (respectively, $r_1, r_2 \in R$) there is a unique row line $L_r = (\alpha_1, \alpha_2, \alpha_3)_{(s_1,s_2,s_3)}$ (respectively, column line $L_s = (\alpha_1, \alpha_2, \alpha_3)_{(r_1,r_2,r_3)}$) for some nonzero element $\alpha_3 \in \mathbb{F}_q$ and for some $s_3 \in S$ (respectively, $r_3 \in R$).

It is well known that the linear span of the vectors of weight three in a Hamming code gives all the code. Hence, the linear span of the row lines of weight three and the column lines of weight three gives all the codewords of C.

Given a vector $\mathbf{v} \in \mathbb{F}_q^{n_b \cdot n_a}$ let $\mathbf{v} = [v_{ij}]$ be its matrix representation. Suppose that after doing the elementary operations described above we obtain a new vector in the same coset $\mathbf{v} + C$ such that its matrix representation has no more than one nonzero row and no more than one nonzero column. Now let M_r (respectively, M_c) be the set of all the vectors $v_{i,j}\mathbf{b}_i$ for $i \in \{1, \ldots, n_b\}$ (respectively, $v_{i,j}\mathbf{a}_j$ for $j \in \{1, \ldots, n_a\}$), where $\mathbf{b}_i$ (respectively, $\mathbf{a}_j$) are the corresponding column vectors in B (respectively, A). The size of M_r and M_c is the same but it is not necessarily the distance from $\mathbf{v}$ to code C. However, we can compute $d(\mathbf{v}, C)$ as $min(rank(M_r), rank(M_c))$. The following proposition will show this.

Proposition 1. *Let $\mathbf{v} \in \mathbb{F}_q^{n_b \cdot n_a}$ be a vector such that the matrix representation has, at the most, one nonzero coordinate in each row and each column. Let M_r and M_c be the matrices defined above and $s = min(rank(M_r), rank(M_c))$. Then the distance of $\mathbf{v}$ to code C is $d(\mathbf{v}, C) = s$.*

Proof. Let the length of M_r and M_c be greater than s. This means that doing simplification using column or row lines we can obtain a new vector belonging to $\mathbf{v} + C$ and with, at the most, s nonzero positions. This shows that $d(\mathbf{v}, C) \leq s$.

Hence, we are going to prove that $s \leq d(\mathbf{v}, C)$. The proof will be by contradiction. Assume $s > d(\mathbf{v}, C)$ and consider the vector $\mathbf{c} \in C$ with the same coordinates as $\mathbf{v}$ and, moreover the new coordinates (strictly less than s) that we need to add to $\mathbf{v}$ to obtain a vector $\mathbf{c}$ in C.

We can suppose that $\mathbf{c} = [c_{ij}]$ has only one nonzero coordinate in each row, otherwise if there are more than one nonzero coordinate we pass a line through two points and simplify. We follow in this way till we reach a vector in C with only one nonzero coordinate in each row. We will call c_{i,j_i} the value of the nonzero position in ith row and vector $\mathbf{c}$ will be $\mathbf{c} = [c_{i,j_i}]$, where there are at the most $2s$ nonzero values. From ([2]) we know that vectors in $\mathbf{c} \in C$ fulfill $B\mathbf{c}A^t = 0$ and so, all the row vectors in M_r are orthogonal to all the row vectors in M_c, where

$$M_r = \left(c_{1,j_1}\mathbf{a}_{j_1}\ c_{2,j_2}\mathbf{a}_{j_2}\ \dots\ c_{n_b,j_{n_b}}\mathbf{a}_{j_{n_b}} \right)$$

and

$$M_c = \left(\mathbf{b}_1\ \mathbf{b}_2\ \dots\ \mathbf{b}_{n_b} \right).$$

Erase the zero columns in the above matrices and realize that the length of matrices M_r and M_c coincides with the number of nonzero positions in $\mathbf{c}$, so it is strictly lower than $2s$. Hence, the rank in one of the two matrices is necessarily less than s which contradicts to our initial assumption. □

Lemma 5. *Let C be the code over $\mathbb{F}_q$ which has $H = A \otimes B$ as a parity check matrix, where A and B are parity check matrices of Hamming codes $[n_a, k_a, 3]_q$ and $[n_b, k_b, 3]_q$, respectively, where $n_a = (q^{m_a} - 1)/(q - 1) \geq 3$; $n_b = (q^{m_b} - 1)/(q - 1) \geq 3$. Let J_1 and J_2 be two sets of columns of B (respectively, of A) of the same cardinality less or equal to m_b (respectively, m_a). Then there exists a monomial matrix ϕ from $Aut(B)$ (respectively, from $Aut(A)$) which acts as a permutation of coordinate positions (up to a scalar factor) that moves the columns from J_1 into the columns from J_2.*

Proof. It is enough to prove this only for the matrix B. Let T_i, $i = 1, 2$ be the $(m_b \times m_b)$-matrix formed by the m_b columns from J_i where each column is up to a scalar factor. It is straightforward to find an invertible $m_b \times m_b$ matrix K over $\mathbb{F}_q$ such that $K\,T_1 = T_2$. Since B is the parity check matrix of a Hamming code, the matrix KB is again a parity check matrix for a Hamming code and $KB = B\phi$ for some monomial matrix ϕ. Moreover, if G_B is the corresponding generator matrix for this Hamming code, i.e. $BG_B^t = 0$, then $(B\phi)G_B^t = (KB)G_B^t = 0$ and so $\phi \in Aut(B)$. Furthermore, ϕ acts as a permutation of coordinate places (up to a scalar factor) that moves the vectors from J_1 into the vectors from J_2. □

The following theorem shows that the code constructed by the Kronecker product is a completely transitive code and, therefore, is a completely regular code.

Theorem 1. *Let C be the code over $\mathbb{F}_q$ which has $H = A \otimes B$ as a parity check matrix, where A and B are parity check matrices of Hamming codes $[n_a, k_a, 3]_q$ and $[n_b, k_b, 3]_q$, respectively, where $n_a = (q^{m_a} - 1)/(q - 1) \geq 3$; $n_b = (q^{m_b} - 1)/(q - 1) \geq 3$; $k_a = n_a - m_a$ and $k_b = n_b - m_b$. Then:*

(i) The code C has length $n = n_a \cdot n_b$, dimension $k = n - m_a \cdot m_b$ and minimum distance $d = 3$.
(ii) The covering radius of C is $\rho = min\{m_a, m_b\}$.
(iii) C is a completely transitive code and, therefore, a completely regular code.

Proof. It is straightforward to check that the code C has length $n = n_a \cdot n_b$, dimension $k = n - m_a \cdot m_b$ and minimum distance $d = 3$.

Assume that $m_b < m_a$. In respect of the covering radius, take a vector $\mathbf{v} \in \mathbb{F}_q^{n_b \cdot n_a}$ with only one nonzero coordinate in each one of the m_b rows indexed by independent column vectors of B and of the m_b columns indexed by independent column vectors of A. From Proposition 1 this previous vector $\mathbf{v}$ is at distance m_b from code C, so $\rho \geq m_b$.

Vice versa, given any vector $\mathbf{v} \in \mathbb{F}_q^{n_b \cdot n_a}$ we can simplify the rows and columns in its matrix representation to obtain a new vector in the same coset $\mathbf{v} + C$ with at most m_b nonzero coordinates and so $d(\mathbf{v}, C) \leq m_b$.

For the case $m_a \leq m_b$ we reach the analog result by considering the Kronecker product $B \otimes A$ which gives a permutation equivalent code (see Lemma 2). This proves (ii).

To prove that C is a completely transitive code it is enough to show that starting from two vectors $\mathbf{x}, \mathbf{y} \in C(\ell)$, there exists a monomial matrix $\phi \in Aut(C)$ such that $\mathbf{x}\phi \in \mathbf{y} + C$.

Vectors $\mathbf{x}$ and $\mathbf{y}$ can be written as $\mathbf{x} = \mathbf{x}_1 + \mathbf{c}_x$ and $\mathbf{y} = \mathbf{y}_1 + \mathbf{c}_y$, respectively, where $\mathbf{c}_x, \mathbf{c}_y \in C$ and both vectors $\mathbf{x}_1, \mathbf{y}_1$ have weight ℓ.

Write the vectors $\mathbf{x}_1$ and $\mathbf{y}_1$ as $(n_b \times n_a)$-matrices and note that the ℓ nonzero columns (respectively, rows) in both vectors $\mathbf{x}_1$ and $\mathbf{y}_1$ correspond to ℓ linearly independent columns of the matrix A (respectively, of the matrix B), otherwise the weight of $\mathbf{x}$ (respectively, of $\mathbf{y}$) would be strictly less than ℓ.

Let ϕ_1 be any monomial $(n_a \times n_a)$-matrix and ϕ_2 be any monomial $(n_b \times n_b)$-matrix. It is clear that

$$(A\phi_1) \otimes (B\phi_2) = (A \otimes B)(\phi_1 \otimes \phi_2)$$

and $\phi_1 \otimes \phi_2$ is a monomial $(n_a n_b \times n_a n_b)$-matrix.

Now, using Lemma 5 we can find $\phi \in Aut(A)$ and $\phi' \in Aut(B)$ such that $\phi \otimes \phi'$ is a monomial map in $Aut(A \otimes B)$ and $\mathbf{x}_1(\phi \otimes \phi') = \mathbf{y}_1$.

But, $Aut(A \otimes B) = Aut\big((A \otimes B)^{\perp}\big) = Aut(C)$ and $\mathbf{x}(\phi \otimes \phi') = (\mathbf{x}_1 + \mathbf{c}_x)(\phi \otimes \phi') = \mathbf{y}_1 + \mathbf{c}_x(\phi \otimes \phi') \in \mathbf{y} + C$. □

References

1. Borges, J., Rifa, J., Zinoviev, V.A.: On non-antipodal binary completely regular codes. Discrete Mathematics 308(16), 3508–3525 (2008)
2. Brouwer, A.E., Cohen, A.M., Neumaier, A.: Distance-Regular Graphs. Springer, Berlin (1989)
3. Cohen, G., Honkala, I., Litsyn, S., Lobstein, A.: Covering Codes. Elsevier, Amsterdam (1997)
4. Delsarte, P.: An algebraic approach to the association schemes of coding theory. Philips Research Reports Supplements 10 (1973)
5. Giudici, M., Praeger, C.E.: Completely Transitive Codes in Hamming Graphs. Europ. J. Combinatorics 20, 647–662 (1999)
6. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes. North-Holland, New York (1977)
7. Neumaier, A.: Completely regular codes. Discrete Maths. 106/107, 335–360 (1992)
8. Rifa, J., Zinoviev, V.A.: On new completely regular q-ary codes. Problems of Information Transmission 43(2) (2007)

9. Rifa, J., Zinoviev, V.A.: On new completely regular codes from perfect codes. In: Proceedings of the Tenth Intern. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-X), Zvenigorod, Russia, September 03-09 (2006)
10. Solé, P.: Completely Regular Codes and Completely Transitive Codes. Discrete Maths. 81, 193–201 (1990)
11. Semakov, N.V., Zinoviev, V.A., Zaitsev, G.V.: Class of maximal equidistant codes. Problems of Information Transmission 5(2), 84–87 (1969)

Quaternary Unequal Error Protection Codes

Ludo Tolhuizen

Philips Research, High Tech Campus 37, 5656 AE Eindhoven, The Netherlands
ludo.tolhuizen@philips.com

Abstract. We consider codes that offer unequal error protection to different information symbols, as measured by the so-called separation vector (a generalisation of the minimum Hamming distance).

We determine the parameters of all optimal linear quaternary codes of length at most eleven.

1 Introduction

In certain applications of coded transmission or storage, some codeword digits or information digits are more relevant than others. One such application is the transmission of numerical data, where errors in the sign or high order digits can be more significant than errors in the low order digits. [1] Another application is the protection of digits originating from hierarchical source coding: if only part of these digits is correctly recovered, a reasonable signal quality can be obtained. Unequal error protection (UEP) codes offer different degrees of protection to different codeword digits or information digits.

Coding for unequal error protection has received little attention in the coding textbooks, a notable exception being the book of Morelos-Zaragoza [2]. The present paper gives a short introduction to UEP coding, and provides some new results on optimal linear quaternary UEP codes of small length, similar to the results from [3] in the binary case. We restrict ourselves to block codes and take as performance indicator the so-called separation vector [4], a generalization of the minimum (Hamming) distance of a code. The separation vector yields an indication of the information digit error rates after bounded-distance decoding on a q-ary symmetric channel with small cross-over probability. In [5], procedures are described for finding encodings and decodings for a given linear code that simultaneously minimize the error rates for all the message symbols for more general channels. Other techniques for obtaining unequal error protection codes include UEP convolutional codes [6], UEP with the aid of coded modulation [7][8], and UEP with (irregular) LDPC codes [9].

Throughout the paper, we denote with $\mathbb{F}_q$ the finite field with q elements. As usual, a q-ary $[n, k]$ code is a k-dimensional code of length n over $\mathbb{F}_q$, that is, a k-dimensional subspace of $\mathbb{F}_q^n$. If $q = 4$, we speak about quaternary codes

[1] A very simple form of unequal error protection recently has been agreed upon for the transmission of an integer number in the uplink control channel in the upcoming 3G-PP cellular communication standard [1].

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 171–185, 2008.

(instead of 4-ary codes). The weight of a vector $\mathbf{x}$ is its number of non-zero entries. The $m \times m$ identity matrix is denoted by I_m. Finally, we call a vector $\mathbf{s} = (s_1, s_2, \ldots, s_k) \in \mathbb{N}^k$ *non-increasing* if for $i = 1, 2, \ldots, k-1$, we have that $s_i \geq s_{i+1}$; if $\mathbf{s}$ and $\mathbf{t}$ are integer-valued vectors of equal length k, then $\mathbf{s} \geq \mathbf{t}$ means that $s_i \geq t_i$ for all $i = 1, 2, \ldots, k$.

The paper is organized as follows. In Section 2, we provide a short review of UEP codes based on the concept of separation vector. In Section 3, we recall some bounds on the size of UEP codes from literature. In Section 4, we give constructions of linear UEP codes, both for general fields and specifically for $\mathbb{F}_4$. In the final section, we obtain the parameters of all optimal quaternary linear UEP codes of length at most eleven. The appendix contains proofs of the non-existence of quaternary UEP codes for some specific parameters.

2 Unequal Error Protection Codes and the Separation Vector

UEP codes were introduced by Masnick and Wolf [10]. Since then, there have been quite some investigations of codes with unequal error protection of information digits, or of codeword digits. Early work includes [11], [12], [4], [13], [14], and [15]. The references in [14] indicate a considerable interest in UEP coding in the Soviet Union in the 1970s – unfortunately, most of these references appeared in Russian only.

In this paper, UEP properties will be measured by the separation vector, introduced by Dunning and Robbins [4].

Let C be a code of length n over a q-ary alphabet Q with q^k words, and let $E : Q^k \rightarrow C$ be an encoding function. For $1 \leq i \leq k$, $s_i(E)$ is the minimum Hamming distance between the images of two strings in Q^k with different i-th symbol, so

$$s_i(E) = \min\{d(E(\mathbf{m}), E(\mathbf{m}')) \mid \mathbf{m} \in Q^k, \mathbf{m}' \in Q^k, m_i \neq m'_i\}.$$

The vector $\mathbf{s}(E) = (s_1(E), s_2(E), \ldots, s_k(E))$ is called the *separation vector* of E. Note that for each encoding function E, the smallest entry of $\mathbf{s}(E)$ equals the minimum Hamming distance of C.

If $Q = \mathbb{F}_q$, and C is a linear code, any generator matrix G of C induces a linear encoding that maps $\mathbf{m}$ to $\mathbf{m}G$. By abuse of notation, we write $\mathbf{s}(G)$ for the separation vector of the encoding function induced by G. As the Hamming distance between two vectors equals the weight of their difference, we have that

$$s_i(G) = \min\{\mathrm{wt}(\mathbf{m}G) \mid m_i \neq 0\}.$$

As is well known, if a code with minimum Hamming distance d is employed, then the transmitted codeword can be retrieved whenever the number of errors t and the number of erasures e satisfy

$$2t + e \leq d - 1.$$

Similarly, if E is employed for encoding, then the i-th information symbol can be retrieved whenever the number of errors t and the number of erasures e satisfy

$$2t + e \leq s_i(E) - 1, \tag{1}$$

see [4, Thm. 2]. A code that has an encoder E such that not all entries of $\mathbf{s}(E)$ are equal is called an Unequal Error Protection (UEP) code. If the code under consideration is linear, we speak about a linear UEP code, or LUEP code.

Dunning and Robbins [4] prove the following beautiful fundamental result.

Theorem 1. *Let C be an $[n, k]$ code over $\mathbb{F}_q$. There exists a $k \times n$ generator matrix G^* of C such that $\mathbf{s}(G^*)$ is non-increasing, and for every encoder E of C for which $\mathbf{s}(E)$ is non-increasing, we have that $\mathbf{s}(G^*) \geq \mathbf{s}(E)$.*

The matrix G^* is called an optimal *generator matrix for C, and $\mathbf{s}(G^*)$ is called the* separation vector *of C.*

Theorem 1 is proved in [4] by showing that the following greedy construction yields an optimal generator matrix G^*. Choose as k-th row of G^* a non-zero codeword of minimum weight. For $1 \leq i \leq k-1$, choose as the i-th row of G^* a codeword of minimum weight that is not in the linear span of the rows $i+1, \ldots, k$ of G^*. The optimal generator matrix G^* obtained in this manner is a *minimum weight* optimal generator matrix, and for $i = 1, 2, \ldots, k$, the i-th row of G^* has weight $s_i(G^*)$.

Remark. Through Inequality 1, the separation vector yields an indication of the message digit error rates after bounded distance decoding (and ML decoding) for a q-ary symmetric channel with small cross-over probability. In [5], Dunning generalizes Theorem 1 to more general channels by describing procedures for finding encodings and decodings of linear block codes that simultaneously minimize the error rates for all the message symbols, given that the occurrence probability of error vectors is known and independent of the transmitted codeword.

Remark. For non-linear codes, an encoding with a component-wise maximum separation vector need not exist, see [4, Example 2].

The following definitions [3] capture the notion of optimality of LUEP codes.

Definition 1. *For each $\mathbf{s} \in \mathbb{N}^k$, we define*[2]

$$n_q(\mathbf{s}) = \min\{n \mid \text{there is an } [n, k] \text{ code over } \mathbb{F}_q \text{ with separation vector at least } \mathbf{s}\},$$

$$n_q^{\text{ex}}(\mathbf{s}) = \min\{n \mid \text{there is an } [n, k] \text{ code over } \mathbb{F}_q \text{ with separation vector exactly } \mathbf{s}\}.$$

[2] Note that the definitions make sense: for any vector $\mathbf{s} \in \mathbb{N}^k$, there is a code of dimension k with separation vector exactly equal to $\mathbf{s}$, namely the code of length $\sum_{i=1}^k s_i$ for which the j-th row of the generator matrix has ones in the positions indexed by the elements of $\{\sum_{i=1}^{j-1} s_i + t \mid 1 \leq t \leq s_j\}$, and zeroes elsewhere.

A q-ary $[n_q(\mathbf{s}), k, \mathbf{s}]$ code is called length-optimal.
A q-ary $[n_q(\mathbf{s}), k, \mathbf{s}]$ code is called optimal *if an $[n_q(\mathbf{s}), k, \mathbf{t}]$ code with $\mathbf{t}\geq\mathbf{s}$, $\mathbf{t}\neq\mathbf{s}$ does not exist.*

It is clear that $n_q(\mathbf{s}) \leq n_q(\mathbf{t})$ whenever $\mathbf{s} \leq \mathbf{t}$, but this is not true for the n_q^{ex}-function, see [3].

Much of the research on UEP codes focussed on the binary case. In [3], Van Gils constructed nearly all optimal binary LUEP codes of length at most 15; he completed the few remaining cases in [16]. In [17], the results of a computer search for binary cyclic UEP codes of length up to 65 are reported, while [18] describes a class of binary primitive BCH codes.

In [19], a description is provided of a class of q-ary codes, $q = 2^s$, where the separation vector has entries 3 and 5. It is shown that the codes have the smallest possible redundancy among all systematically encoded UEP codes of equal length and separation vector. The construction generalizes a construction for the binary case from [14] and, interestingly enough, is based on a description with parity check matrices. One of the few other papers dealing with non-binary UEP codes is [20], that will shortly be discussed in Section 4.

The present paper focusses on quaternary codes where relatively little is known. We use the knowledge on the minimum distance of small linear quaternary codes, see [21] and the references therein.

3 Bounds on the Length of LUEP Codes

In this section, we present lower bounds on the functions $n_q(\mathbf{s})$ and $n_q^{\mathrm{ex}}(\mathbf{s})$. We start with a generalization of the Griesmer bound for linear equal error protection codes, that was proved by Katsman for the binary case [13] and by Van Gils for the general case [3].

Theorem 2. *Let $\mathbf{s} = (s_1, s_2, \ldots, s_k) \in \mathbb{N}^k$ be non-increasing, then*

$$n_q(\mathbf{s}) \geq s_1 + n_q(\lceil s_2/q\rceil, \ldots, \lceil s_k/q\rceil).$$

By repeatedly applying this inequality, we find that

$$n_q(\mathbf{s}) \geq \sum_{i=1}^{k} \lceil \frac{s_i}{q^{i-1}} \rceil.$$

As each term in the sum in Theorem 2 is at least one, Theorem 2 has the following corollary.

Corollary 1. *For any non-increasing vector $\mathbf{s} = (s_1, \ldots, s_k) \in \mathbb{N}^k$, we have that $n_q(\mathbf{s}) \geq s_1 + k - 1$.*

Corollary 1 can be considered as a generalization of the Singleton bound. It implies that each component of the separation vector of an $[n, k]$ MDS code equals $n - k + 1$. As $[n, k]$ MDS codes over $\mathbb{F}_q$ exist whenever $n \leq q + 1$ [22, Ch. 11], optimal LUEP codes over $\mathbb{F}_q$ of length smaller than $q + 2$ do not exist.

The Singleton bound holds for all codes, linear or not. As a contrast, the following example from [23] shows that Corollary 1 does not hold for non-linear codes.

Example. Let C_0 consist of 512 binary vectors of length 15 and weight at most three (note that there are 576 of such vectors), and let C_1 consist of 512 binary vectors of length 15 and weight at least 12, and let $C = C_0 \cup C_1$. Let E be an encoding of 10-bits information strings to C such that for all $\mathbf{m} = (m_1, \ldots, m_{10}) \in \mathbb{F}_2^{10}$, we have that $E(\mathbf{m}) \in C_{m_1}$. As any two words $\mathbf{c}_0 \in C_0$ and $\mathbf{c}_1 \in C_1$ differ in at least nine positions, $s_1(E) \geq 9$, and obviously $s_i(E) \geq 1$ for $i = 2, \ldots, 10$. According to Corollary 1, the length of a linear 10-dimensional code with a separation vector larger than or equal to (9,1,…,1) is at least $9 + 10 - 1 = 18$.

Theorem 3. *Let* $\mathbf{s} = (s_1, \ldots, s_k) \in \mathbb{N}^k$ *be non-increasing. We have that* $n_q(\mathbf{s}) \geq 1 + n_q(s_1, \ldots, s_{k-1})$.

Proof. See [3, Thm. 8]. □

Lemma 1. *Let G be a $k \times n$ matrix with non-increasing separation vector* $\mathbf{s} = (s_1, \ldots, s_k)$. *Let v be such that $s_{v-1} > s_v$, and assume that G has a column with zeroes in all rows $v, v+1, \ldots, k$. By deleting this column from G, we obtain a $k \times (n-1)$ matrix G' with separation vector at least* $(s_1 - 1, \ldots, s_{v-1} - 1, s_v, \ldots, s_k)$.

Proof. Let $1 \leq i \leq k$, and let $\mathbf{m} \in \mathbb{F}_q^k$ be such that $m_i \neq 0$.

It is clear that $\mathrm{wt}(\mathbf{m}G') \geq \mathrm{wt}(\mathbf{m}G) - 1 \geq s_i - 1$.

Now, suppose that $1 \leq i \leq v - 1$. If $m_1 = \ldots = m_{v-1} = 0$, then $\mathrm{wt}(\mathbf{m}G') = \mathrm{wt}(\mathbf{m}G) \geq s_i$. Otherwise, $\mathrm{wt}(\mathbf{m}G') \geq \mathrm{wt}(\mathbf{m}G) - 1 \geq s_{v-1} - 1 \geq s_i$. □

Theorem 4. *Let* $\mathbf{s} = (s_1, \ldots, s_k) \in \mathbb{N}^k$ *be non-increasing. Let v be such that* $s_{v-1} > s_v$ *and* $\sum_{i=v}^{k} s_i \leq n_q^{ex}(\mathbf{s}) - 1$.

We have that $n_q^{ex}(\mathbf{s}) \geq 1 + n_q(s_1 - 1, \ldots, s_{v-1} - 1, s_v, \ldots, s_k)$.

Proof. This theorem is in fact Theorem 11 from [3]. We give a short proof here. Let G be a minimum weight $k \times n$ matrix with separation vector $\mathbf{s}$ (so the i-th row of G has weight s_i). The rows $v, v+1, \ldots, k$ of G jointly contain $\sum_{i=v}^{k} s_i$ nonzeroes, which, according to the premisses, is less than $n_q^{ex}(\mathbf{s})$, so surely less than n. Hence, G has a column that contains only zeroes in the rows $v, v+1, \ldots, k$, and we can apply Lemma 1. □

We end this subsection by remarking that Bross and Litsyn recently presented an improved asymptotic upper bound on the size of binary LUEP codes with two protection levels, that is, for codes for which the entries of the separation vector attain two distinct values [24].

4 Constructions of LUEP Codes

In this section, we describe the constructions that will be used to generate all quaternary LUEP codes of length eleven or less. We start with constructions for general alphabets, and subsequently give specialized constructions for the quaternary case.

4.1 Constructions for General Fields

Throughout this section, we denote the non-zero elements of $\mathbb{F}_q$ by $\alpha_1, \dots, \alpha_{q-1}$. Our first construction yields all optimal two-dimensional LUEP codes.

Construction A. Let $s_1 \geq s_2$. We define $u := s_1 - s_2 + \lceil s_2/q \rceil, v := \lceil s_2/q \rceil$ and $t := q + s_2 - q\lceil s_2/q \rceil$.

The $2\times$ $(s_1 + \lceil s_2/q \rceil)$ matrix $\begin{bmatrix} \overbrace{1\cdots1}^{u} & \overbrace{0\alpha_1\cdots\alpha_{q-1}\cdots0\alpha_1\cdots\alpha_{q-1}}^{(v-1)times} & 0\alpha_1\cdots\alpha_{t-1} \\ 0\cdots0 & 1\,1\cdots\ 1\cdots\cdots1\,1\cdots\ 1 & 1\,1\cdots\ 1 \end{bmatrix}$ has separation vector (s_1, s_2).

Corollary 2. *Let $s_1 \geq s_2$ and let C be an optimal $[n, 2, (s_1, s_2)]$ code over $\mathbb{F}_q$. Then q divides s_2, and $n = s_1 + s_2/q$.*

Proof. Combination of Construction A and Theorem 2. □

Construction B
Let $q = 2^r$, let $m \geq 2$, and let $1 \leq i_m \leq \cdots \leq i_1 \leq q - 1$.

$$\text{Define} \quad G := \begin{bmatrix} 001\cdots1 & 001\cdots1 & \cdots & 001\cdots1 \\ G_{i_1} & O & \cdots & O \\ O & G_{i_2} & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & G_{i_m} \end{bmatrix}.$$

Here, O denotes an all-zero matrix of appropriate size, and G$_s$ denotes the $2\times(s+2)$ matrix $\begin{bmatrix} 10\alpha_1\cdots\alpha_s \\ 01\alpha_1^2\cdots\alpha_s^2 \end{bmatrix}$.

The matrix G generates a $[\sum_{j=1}^{m}(i_j + 2), 2m + 1]$ code over $\mathbb{F}_q$; moreover, $s_1(G) = \sum_{j=1}^{m} i_j$, and $s_{2j}(G) = s_{2j+1}(G) = 1 + i_j, 1 \leq j \leq m$.

Proof. For $1 \leq j \leq m$, let $V_j = \{t + \sum_{v=1}^{j-1}(i_v + 2) \mid 1 \leq t \leq 2 + i_j\}$. It is easy to check that the matrix $\begin{bmatrix} 001\ldots1 \\ G_s \end{bmatrix}$ generates an $[s + 2, 3, s]$ code (as q is even, $\alpha_i^2 \neq \alpha_j^2$ if $i \neq j$). From this it follows that for $j = 1, 2, \dots, m$, the sum of the top row of G and any linear combination of the bottom $2m$ rows of G has weight at least i_j in the positions from V_j; this implies the bound on $s_1(G)$. As the matrix G_s generates a code with minimum distance $s+1$, the word $\mathbf{m}G$ has weight at least $i_j + 1$ in the positions from V_j whenever $m_1 = 0$ and $m_{2j} \neq 0$ or $m_{2j+1} \neq 0$. □

Corollary 3. *Let q be a power of two. For each $m \geq 2$ there exists an optimal q-ary $[m(q + 1), 2m + 1, (m(q - 1), q, \dots, q)]$ code.*

Proof. In Construction B, take $\mathrm{i}_1 = \cdots = i_m = q-1$. The optimality follows from Theorem 2. □

The following simple constructions [25] are very useful. Let G be a $k \times n$ matrix for which $\mathbf{s}(G) = (s_1(G), \ldots, s_k(G))$ is non-increasing.

Construction C

If $\mathrm{s}_k(G) \geq 2$, then the matrix $G' = \begin{bmatrix} & 0 \\ G & \vdots \\ & 0 \\ 10\cdots0 & 1 \end{bmatrix}$ has separation vector $(s_1(G), \ldots, s_k(G), 2)$.

If $s_k(G) = 2$ and the code generated by G is optimal, then the code generated by G' is optimal as well.

Proof. For any vector $\mathbf{c}$ of length n, we obviously have that $\mathrm{wt}((\mathbf{c}0)+(10\ldots01)) \geq \mathrm{wt}(\mathbf{c})$. This proves the expression for $\mathbf{s}(G')$.

It follows from Theorem 3 that if G generates a length-optimal code, then G' generates a length-optimal code as well. Now suppose that $s_k(G) = 2$. Let $\mathbf{t}' = (t_1, \ldots, t_{k+1}) = (\mathbf{t}, t_{k+1}) \in \mathbb{N}^{k+1}$ be non-increasing and suppose that $\mathbf{t}' \geq \mathbf{s}(G')$ and $\mathbf{t}' \neq \mathbf{s}(G')$. As $s_k(G') = s_{k+1}(G')$, there is an $i \in \{1, \ldots, k\}$ such that $t_i > s_i(G')$, and so $\mathbf{t} \geq \mathbf{s}(G)$ and $\mathbf{t} \neq \mathbf{s}(G)$. If G generates an optimal code, we have that $n_q(\mathbf{t} > n_q(\mathbf{s}(G) = n$. Theorem 3 implies that $n_q(\mathbf{t}') \geq 1 + n_q(\mathbf{t}) > n+1 \geq n_q(\mathbf{s}(G'))$. □

Construction D

Suppose that for each $i \in \{1, \ldots, k\}$, the i-th row of G has weight $s_i(G)$. Let $\mathbf{e}_j$ be the column vector of length k which has a 1 in position j and zeroes elsewhere. The matrix $[G \mid \mathbf{e}_j]$ has separation vector $\mathbf{s}(G) + \mathbf{e}_j^T$. This separation vector need not be nonincreasing.

Construction E

If we delete a column from G, we obtain a matrix G' which satisfies
$s_i(G') \geq s_i(G) - 1,\ i = 1, \ldots, k$.

4.2 Construction of Quaternary LUEP Codes

Throughout this section, the elements of $\mathbb{F}_4$ are denoted by 0,1,α and β, where $\beta = \alpha^2 = 1 + \alpha$.

Construction F

Let k and n be such that $n \geq \max(2k, k+3)$.

The $k \times n$ matrix $G = \begin{bmatrix} 1\cdots1 & 0\cdots0 & 1\cdots1 & \alpha\beta \\ & & 0\cdots0 & 11 \\ I_{k-1} & I_{k-1} & \vdots & \vdots\vdots \\ & & 0\cdots0 & 11 \end{bmatrix}$

generates an optimal $[n, k, (n-k+1, 4, \ldots, 4)]$ code.

Proof. Let $\mathbf{m} = (1, m_2, \ldots, m_k) \in \mathbb{F}_4^k$, and let $\mathbf{c} = \mathbf{m}G$.

For $1 \leq j \leq k-1$, we have that $c_j + c_{j+k-1} = 1$, so $\mathbf{c}$ has weight at least $k-1$ in its $2k-2$ leftmost positions.

If equality holds, $\mathbf{c}$ has only zeroes and ones in its leftmost $2k-2$ positions, which implies that $\mathbf{c}$ ends in (α, β) or (β, α). As $\mathbf{c}$ has only ones in the positions $2k-1, \ldots, n-2$, we conclude that wt($\mathbf{c}$)$\geq (k-1) + (n-2k) + 2 = n-k+1$. So we assume that $\mathbf{c}$ has weight at least k in its leftmost $2k-2$ positions. As the rightmost two entries of $\mathbf{c}$ add to 1, at least one of them is non-zero. As $\mathbf{c}$ has ones in the positions $2k-1, \ldots, n-2$, we conclude that $\mathbf{c}$ has weight at least $k + (n-2k) + 1 = n-k+1$.

So indeed, $s_1(G) = n-k+1$. It is obvious that $s_i(G) = 4$ for $2 \leq i \leq k$. The optimality follows from Theorem 2. □

Construction G

Let G_0 be a generator matrix for a quaternary [6,3,4] code for which the bottom row has weight six (the existence of such a word follows from the explicit formulas for the weight enumerator of an MDS code, see [22, Ch. 11, Sec. 3]). Let $2 \leq d \leq 4$, and let G_1 generate a quaternary $[d+1, 2, d]$ code. Let G be the $3 \times (7+d)$ matrix defined as

$$G = \begin{pmatrix} & G_1 \\ G_0 & \\ & 0 \ldots 0 \end{pmatrix}.$$

Then G generates an optimal quaternary $[(7+d, 3, (d+4, d+4, 6)]$ code.

Proof. Let $\mathbf{m}$ be a non-zero vector in $\mathbb{F}_4^3$, and let $\mathbf{c} = \mathbf{m}G$.

If $m_1 \neq 0$ or $m_2 \neq 0$, then $\mathbf{c}$ has weight at least 4 in its six leftmost positions, and weight at least d in its $d+1$ rightmost positions, so wt($\mathbf{c}$) $\geq 4 + d$.

If $m_1 = m_2 = 0$, then $\mathbf{c}$ is a non-zero multiple of the bottom row of G, and so $\mathbf{c}$ has weight six.

The length-optimality of the codes follows from Theorem 2. For $d = 2$, optimality follows from Theorem 2. For $d = 3$, optimality follows from the non-existence of a quaternary [10,3,7] code [28]. To prove the optimality for the case $d = 4$, we apply Theorem 4 and find that $n_4^{\text{ex}}(8,8,7) \geq 1 + n_4(7,7,7) = 11$. □

Remark. Construction G is a special case of Construction X [22, Ch. 18, Sec. 7] for adding tails to words from nested codes. Özbudak and Stichtenoth applied the same method to construct LUEP codes from codes derived from algebraic curves [20]. Construction X has been applied in [27] in conjunction with LUEP codes as well; however, in [27], the tails are words from LUEP codes, and the aim is to construct codes with a large minimum distance.

5 The Parameters of All Optimal Quaternary LUEP Codes of Length at Most Eleven

We use the bounds and constructions from the previous sections to construct a table of the parameters of all optimal quaternary LUEP codes of length at most eleven. The results for codes of length at most nine appeared before in [26]. The letters in the table indicate the construction used to find a code with the given separation vector. With $d_4(n,k)$, we denote the maximal minimum distance of any quaternary $[n,k]$ code; the values were obtained from [21]. In order to improve readability, we omitted the commas in the separation vector; components of a separation vector consisting of two digits are preceded by a dot.

Theorem 5. *All codes in Table 1 are optimal, and there are no optimal quaternary LUEP codes of length at most eleven with other separation vectors.*

Table 1. The separation vectors of all optimal quaternary LUEP codes of length at most 11

n	k	$d_4(n,k)$	
6	2	4	54^A
	4	2	3332^C
7	2	5	64^A
	3	4	544^F
	4	3	$4442^C, 4333^E$
	5	2	33322^C
8	2	6	74^A
	3	5	644^F
	4	4	5444^F
	5	3	$44422^C, 43333^B$
	6	2	333222^C
9	2	7	84^A
	3	6	744^F
	4	5	6444^F
	5	4	$54442^C, 54433^B$
	6	3	$444222^C, 433332^C$
	7	2	3332222^C
10	2	8	94^A
	3	6	$776^G, 844^D$
	4	6	7444^D
	5	5	64444^B
	6	4	$544422^C, 544332^C$
	7	3	$4442222^C, 4333322^C$
	8	2	33322222^C
11	2	8	$10.4^A, 98^A$
	3	7	$886^G, 944^D$
	4	7	8444^D
	5	6	74444^B
	6	5	$644442^C, 633333^{E(F)}$
	7	4	$5444222^C, 5443322^C$
	8	3	$44422222^C, 43333222^C$
	9	2	333222222^C

Proof. As remarked after Corollary 1, no optimal $[n, k]$ LUEP codes exist if there is an $[n, k, n-k+1]$ code. Hence, our table contains no entries for $n \leq 5$, $k = n$, $k = n-1$, $k = 1$, and $[n, k] = [6, 3]$.

The optimality of the two-dimensional codes and the codes obtained from Construction F has already been proved. The optimality of the $[n, n-2]$ codes can be shown using Theorem 3 and the non-existence of a $[6, 4, 3]$ code. The optimality of the codes with a separation vector ending in at least two 2's obtained with Construction C has already been demonstrated. In the remaining cases, as far as not covered explicitly below, we used Theorem 3.

By Theorem 2, we have that $n_4(4, 3, 3, 3) \geq 7$. By Theorem 4, we have that $n_4^{ex}(4, 4, 4, 3) \geq 1 + n_4(3, 3, 3, 3) = 8$; in the same way it can be shown that $n_4^{ex}(4, 4, 3, 3) \geq 8$. In other words, neither a [7,4,(4,4,4,3)] code, nor a [7,4,(4,4,3,3)] code over $\mathbb{F}_4$ exists. Combination of these observations shows the optimality of the [7,4] codes.

By Theorem 3, we have that $n_4(4, 4, 3, 3, 1) \geq 1 + n_4(4, 4, 3, 3) = 9$, which shows the optimality of the [8,5] codes.

By Theorem 2, we have that $n_4(5, 5, 1, 1, 1) \geq 10$. Hence, to show the optimality of the [9,5] codes it is sufficient to show that neither a [9,5,(5,4,4,4,4)] code, nor a [9,5,(5,4,4,4,3)] code exists. This has been shown in [26]; for completeness, a modified proof is contained the appendix. The optimality of the [9,6,(4,3,3,3,3,2)] code is shown by verifying that a [9,6,(4,3,3,3,3,3)] code does not exist; again, this verification has been performed in [26], and for completeness is contained in the appendix.

By Theorem 2, we have that $n_4(5, 4, 4, 3, 3, 3) \geq 10$. We thus can apply Theorem 4 and find that $n_4^{ex}(5, 4, 4, 3, 3, 3) \geq 1 + n_4(4, 3, 3, 3, 3, 3) > 10$. In the appendix, we prove the non-existence of quaternary $[10, 6, (5, 4, 3, 3, 3, 3)]$ and $[10, 6, (5, 3, 3, 3, 3, 3)]$ codes.

Combination of Construction E and the non-existence of a $[10, 6, (5, 3, 3, 3, 3, 3)]$ code shows the non-existence of an $[11, 6, (6, 4, 4, 4, 4, 4)]$ code. Combination of Theorem 4 and the non-existence of a $[10, 6, (5, 3, 3, 3, 3, 3)]$ code shows the non-existence of an $[11, 6, \mathbf{s}]$ code with $\mathbf{s}$ equal to $(6, 4, 4, 4, 4, 3)$, $(6, 4, 4, 4, 3, 3)$ or $(6, 4, 4, 3, 3, 3)$. The non-existence of an $[11, 6, (6, 4, 3, 3, 3, 3)]$ code is shown in the appendix. □

References

1. Tolhuizen, L., Baker, M.: Error-correcting coding for uplink control information in UTRA Release 7. In: 28-th Symposium on Information Theory in the Benelux, pp. 93–100 (2007)
2. Morelos-Zaragoza, R.H.: The art of error-correcting coding, 2nd edn. Wiley, Chichester (2006)
3. van Gils, W.J.: Two topics on linear unequal error protection codes: bounds on their lengths and cyclic code classes. IEEE Trans. Inform. Theory 29(6), 866–876 (1983)
4. Dunning, L.A., Robbins, W.E.: Optimal encoding of linear block codes for Unequal Error Protection. Information and Control 37, 150–178 (1978)

5. Dunning, L.A.: Encoding and decoding for the minimization of message symbol error rates in linear block codes. IEEE Trans. Inform. Theory 33, 91–104 (1987)
6. Pavlushkov, V., Johannesson, R., Zyablov, V.V.: Unequal error protection for convolutional codes. IEEE Trans. Inform. Theory 52(2), 700–708 (2006)
7. Morelos-Zaragoza, R.H., Fossorier, M.P.C., Lin, S., Imai, H.: Multilevel coded modulation for unequal error protection and multistage decoding – Part I: Symmetric Constellations. IEEE Trans. Communications 48(2), 204–212 (2000)
8. von Deetzen, N., Henkel, W.: Unequal error protection multilevel codes and hierarchical modulation for multimedia transmission. In: Proc. IEEE 2008 Int. Symp. Inform. Theory, ISIT 2008, pp. 2237–2241 (2008)
9. Pishro-Nik, H., Rahnavard, N., Fekri, F.: Nonuniform error correction using low-density parity-check codes. IEEE Trans. Inform. Theory 51(7), 2702–2714 (2005)
10. Masnick, B., Wolf, J.K.: On linear unequal error protection codes. IEEE Trans. Inform. Theory 13(4), 600–607 (1967)
11. Mandelbaum, D.: Unequal-error-protection codes derived from difference sets. IEEE Trans. Inform. Theory 18(5), 686–687 (1972)
12. Kilgus, C.C., Gore, W.C.: A class of cyclic unequal-error-protection codes. IEEE Trans. Inform.Theory 18(5), 687–690 (1972)
13. Katsman, G.L.: Bounds on volume of linear codes with unequal information-symbol protection. Probl. Inform. Transmission 16(2), 99–104 (1980) (Russian original: pages 25-32)
14. Boyarinov, I., Katsman, G.: Linear unequal error protection codes. IEEE Trans. Inform. Theory 27(2), 168–175 (1981)
15. Driessen, L.: On an infinite series of $[4n, 2n]$ codes. IEEE Trans. Inform. Theory 30(2), 392–395 (1984)
16. van Gils, W.J.: Some constructions of optimal binary linear unequal error protection codes. Philips Journal of Research 39(6), 293–304 (1984)
17. Lin, M.C., Lin, C.C., Lin, S.: Computer search for binary cyclic UEP codes of odd length up to 65. IEEE Trans. Inform. Theory 36(4), 924–935 (1990)
18. Morelos-Zaragoza, R.H., Lin, S.: On primitive BCH codes with unequal error correction capabilities. IEEE Trans. Inform. Theory 41(3), 788–790 (1995)
19. Morelos-Zaragoza, R.H., LIn, S.: On a class of optimal nonbinary linear unequal error protection codes for two sets of messages. IEEE Trans. Inform. Theory 40(1), 196–200 (1994)
20. Özbudak, F., Stichtenoth, H.: Constructing linear unequal error protection codes from algebraic curves. IEEE Trans. Inform. Theory 49(6), 1523–1527 (2003)
21. Grassl, M.: Bounds on the minimum distance of linear codes, http://www.codetables.de
22. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
23. Englund, E.K.: Nonlinear unequal error protection codes are sometimes better than linear ones. IEEE Trans. Inform. Theory 37(5), 1418–1420 (1991)
24. Bross, S.I., Litsyn, S.: Improved upper bounds for codes with unequal error protection. In: Proc. IEEE 2005 Int. Symp. Inform. Theory, ISIT 2005, pp. 790–794 (2005)
25. van Gils, W.J.: Unequal Error Protection Codes from shorter ones. IEEE Trans. Inform. Theory 30(3), 544–546 (1984)
26. Tolhuizen, L.M.G.M.: On the optimal use and the construction of linear block codes, M.Sc. Report, Dept. of Mathematics and Computing Science, 368 (1986)

27. Bierbrauer, J., Edel, Y., Tolhuizen, L.M.G.M.: New codes via the lengthening of BCH codes with UEP codes. Finite Fields and their Applications 5(4), 345–353 (1999)
28. Greenough, P.P., Hill, R.: Optimal linear codes over GF(4). Discrete Mathematics 125, 187–199 (1994)

Appendix: Non-existence Proofs

In this appendix, we describe the verifications for the non-existence of certain codes. For the codes of length at most nine, these verifications are a modified version of the proofs in [26]. The verifications for the codes of length ten and eleven are new.

The general pattern of the verifications is as follows. It is shown that if an $[n, k]$ code with separation vector $\mathbf{s}$ exists, then there exists a $k \times n$ matrix with separation vector $\mathbf{s}$ that has a specific form. By a complete search (either by hand, or by computer), it is shown that no matrix with this specific form has separation vector $\mathbf{s}$.

For space reasons, we do not give the details of the verifications from [26], but merely explain to which reduced class of matrices we restricted our search. The first non-existence proof is quite extensive; the other proofs are more sketchy, as many of the proof elements from the first case are repeated.

Theorem 6. *A* $[9, 5, (5, 4, 4, 4, 4)]$ *code does not exist.*

Proof. By contradiction. Suppose a [9,5, $\mathbf{s}$=(5,4,4,4,4)] code does exist.

Let $G = \left(\begin{array}{c|c} 1\ 0000 & \\ * & \\ * \quad \mathrm{I}_4 & \mathrm{P} \\ * & \\ * & \end{array}\right)$ be an optimal, canonical generator matrix ([14]). As $s_1 = 5$, the top row of P has weight four. By multiplying the columns of P with appropriate non-zero constants, we obtain that we can assume that the top row of P consists of four ones. After a column permutation, we obtain a matrix G' with separation vector $\mathbf{s}$ of the form

$$G' = \begin{pmatrix} 11111 & 0000 \\ Q & I_4 \end{pmatrix}.$$

If a row of Q contains the field element x more than once, then the sum of $x(111110000)$ and the corresponding row of G' has weight at most four. As $s_1(G') = 5$, it follows that $x = 0$. In other words, each row of G' contains each non-zero element of $\mathbb{F}_4$ at most once. As $s_i(G') = 4$ for $i \geq 2$, each row of Q has weight at least three. We conclude that each row of Q has weight three, and contains each non-zero element of $\mathbb{F}_4$ exactly once.

We can also assume without loss of generality that the leftmost non-zero entry of each row of Q is a 1: if not, we multiply that row with an appropriate non-zero constant (this does not change the separation vector), and multiply the last four columns of G with appropriate non-zero constants to keep the identity matrix. For each row of Q, there are thus $\binom{5}{3} \times 2 = 20$ choices (the factor two comes from the fact that the second and third non-zero entry of each row are either (α, β) or (β, α)). By an appropriate column permutation, we obtain that we can assume that Q has top row $1\alpha\beta00$.

Finally, any two rows of Q are linearly independent, as $s_i(G') \geq 3$ for $i \geq 2$. As a consequence, it is sufficient to test $\binom{19}{3}$ matrices Q; none of these choices yields a separation vector $(5, 4, 4, 4, 4)$.

We remark that by further reasoning, the number of matrices Q to be tested can be reduced so that checking the non-existence by hand is feasible [26]. □

Theorem 7. *A* $[9, 5, (5, 4, 4, 4, 3)]$ *code does not exist.*

Proof. Suppose a code $[9, 5, \mathbf{s} = (5, 4, 4, 4, 3)]$ code does exist.

Let G be a minimum weight generator matrix. We can assume without loss of generality that $G(5, 9) = 1$. By adding a scalar multiple of the bottom row of G to other rows, we do not change the separation vector. Hence, there exists a generator matrix G' with separation vector $\mathbf{s}$ for which the rightmost column has a one in the bottom row, and zeroes elsewhere. We can replace the rows 2,3, and 4 of G' by three rows that generate the same space as these rows, without changing the separation vector (as $s_2 = s_3 = s_4$). Hence, we can assume without loss of generality that the 3×3 matrix consisting of rows 2,3,4 and columns 6,7,8 of G' equals the identity matrix. As adding scalar multiples of rows 2,3,4 of G' does not change the separation vector, we can assume without loss of generality that G' has the form

$$G' = \begin{pmatrix} \mathbf{x} & 000 & 0 \\ Q & I_3 & \mathbf{0} \\ \mathbf{y} & \mathbf{z} & 1 \end{pmatrix},$$

where the vector $\mathbf{yz}$ has weight two.

Like in the proof of Theorem 6, it can be shown that we can assume without loss of generality that $\mathbf{x}$=11111, Q has top row $1\alpha\beta00$, and that each row of Q has 1 as leftmost non-zero entry and contains each non-zero field element exactly once. There are thus $2 \times \binom{5}{2} = 20$ candidates for each row of Q (one of which has already been used as top row); there are thus $\binom{19}{2}$ choices for the two remaining rows of G'. For the bottom row, there are $\binom{8}{2} \times 9 = 72$ choices. Of the $\binom{19}{2} \times 72$ choices, none yields a separation vector equal to $(5, 4, 4, 4, 4, 3)$.

In [26], a further reasoning is presented that allows to prove Theorem 7 by hand. □

Theorem 8. *A* $[9, 6, (4, 3, 3, 3, 3, 3)]$ *code does not exist.*

Proof. Suppose a $[9, 6, \mathbf{s} = (4, 3, 3, 3, 3, 3)]$ code does exist.

Like in the proof of Theorem 6, it can be shown that there then exists a generator matrix G with separation vector $\mathbf{s}$ of the form

$$\begin{pmatrix} 1111 & 00000 \\ Q & I_5 \end{pmatrix}.$$

Note that each row of Q has weight at least two, and contains each of the elements 1,α, β at most once. Also, we can assume that the leftmost non-zero entry of each row of Q is a 1. This implies there are 20 candidate rows for Q: 8 of weight three, and 12 of weight two. Also, the rows of Q are linearly independent. None of the $\binom{20}{5}$ choices for Q yields a separation vector $\mathbf{s}$.

In [26], a further reasoning is presented that allows to complete the proof by hand. □

Theorem 9. *A* $[10, 6, (5, 3, 3, 3, 3, 3)]$ *code does not exist.*

Proof. Suppose a $[10, 6, \mathbf{s} = (5, 3, 3, 3, 3, 3)]$ code C does exist.

Like in the proof of Theorem 6, we can assume without loss of generality that C has a generator matrix G of the form

$$G = \begin{pmatrix} 11111 & 00000 \\ Q & I_5 \end{pmatrix}.$$

Clearly, each row of Q has weight at least two. Moreover, as $s_1 = 5$, each row of Q contains each non-zero element at most once. We consider two cases.

(a) Each row of Q has weight two. As the non-zero entries of a row are distinct, and we can assume the leftmost non-zero entry equals 1, there are $\binom{5}{2} \times 2 = 20$ choices for any row of Q. As the rows of Q must be distinct, we have to investigate $\binom{20}{5}$ matrices Q.
(b) Q has a row of weight three. We can assume without loss of generality that Q has top row $1\alpha\beta00$. As every row of Q of weight three contains each of the elements 1,α and β once, and we can assume the leftmost non-zero entry equals 1, there are $2 \times \binom{5}{3} = 20$ candidate rows of weight three; one of them has been used already. Like above, there are 20 candidate rows of weight two. We thus have to investigate $\binom{39}{4}$ matrices Q.

In both cases (a) and (b), none of the choices for Q yields a matrix with separation vector (5,3,3,3,3,3). □

Theorem 10. *A* $[10, 6, (5, 4, 3, 3, 3, 3)]$ *code does not exist.*

Proof. Suppose a [10,6,(5,4,3,3,3,3)] code C does exist.

Let G be a minimum weight optimal generator matrix for C (see [4]). The 4×10 matrix X that consists of the bottom four rows of G does not have an all-zero column, as otherwise, according to Lemma 1, there would exist an $[9, 6, \mathbf{s}]$ code with $\mathbf{s} \geq (4, 3, 3, 3, 3, 3)$, contradicting Theorem 8. As each row of X has weight three, X contains twelve non-zeroes. Hence, X contains at most two columns of weight exceeding one, and so each row of X has at least 3-2=1 non-zero entry that is the unique non-zero entry in that column of X. We thus can assume without loss of generality that the four rightmost columns of X form the identity matrix.

We can add linear combinations of the four bottom rows of G to the top row and second row without changing the separation vector. Hence, we can assume that G is of the form

$$G = \begin{pmatrix} A & 0 \\ B & I_4 \end{pmatrix},$$

where each row of B has weight two. The second row of G has a non-zero entry; we assume without loss of generality that $G(2,6) = 1$. We can add a linear multiple of the second row of G to the top row without changing the separation vector; hence, we assume without loss of generality that G has the following form

$$G = \begin{pmatrix} \mathbf{x} & 0 & 0000 \\ \mathbf{y} & 1 & 0000 \\ Q & \mathbf{z}^T & I_4 \end{pmatrix}.$$

As $s_1(G) = 5$, $\mathbf{x}$ has weight five; without loss of generality, we take it to be the all-one vector. Like in the proof of Theorem 6, we can assume that $\mathbf{y}$=$(1\alpha\beta000)$. We can thus assume that G has the following form:

$$G = \begin{pmatrix} 111110 & 0000 \\ 1\alpha\beta001 & 0000 \\ R & I_4 \end{pmatrix}.$$

Every row of R has weight two and can be assumed to have a 1 as leftmost non-zero entry. If a row of R ends in a zero, then its two non-zero entries are different; this thus yields $2 \times \binom{5}{2} = 20$ candidate rows. There are $3\times\binom{5}{1} = 15$ choices for rows of R with a non-zero in position 7. Hence, there are 35 candidate rows, and we need to investigate $\binom{35}{4}$ candidate matrices R. None of them yields a separation vector $(5,4,3,3,3,3)$. □

Theorem 11. *An* $[11,6,(6,4,3,3,3,3)]$ *code does not exist.*

Proof. Suppose a $[11,6,(6,4,3,3,3,3)]$ code does exist.

Let G be an optimal minimum weight generator matrix. There is no column of G that has only zeroes in its four bottom positions (as otherwise, according to Lemma 1, there would exist an [10,6,$\mathbf{s}$] code with $\mathbf{s}\geq (5,3,3,3,3,3)$). As the four bottom rows of G together contain twelve non-zero entries, G has one column that has two non-zeros in its bottom four rows, and ten columns that have one non-zero in its four bottom rows. Hence, like in the proof of Theorem 10, we can assume without loss of generality that G is of the form

$$G = \begin{pmatrix} 1111110 & 00000 \\ 1\alpha\beta0001 & 0000 \\ Q & I_4 \end{pmatrix},$$

where each row of Q has weight two.

A row of Q that ends in a zero has distinct entries; this yields $2 \times \binom{6}{2} = 30$ possible candidates. There are $3 \times \binom{6}{1} = 18$ candidate rows for Q that have weight two and end in a non-zero element. All in all, we need to investigate $\binom{48}{4}$ matrices Q, and none of them yields a separation vector $(6,4,3,3,3,3)$. □

Communication on Inductively Coupled Channels: Overview and Challenges

Øyvind Ytrehus

Dept. of Informatics, University of Bergen,
N-5020 Bergen, Norway
oyvind@ii.uib.no

Abstract. This paper presents an overview of coding methods and cryptographic techniques for inductively coupled channels. The paper discusses the requirements for coding on such channels, review modulation codes in use in practical systems, and propose new modulation coding techniques. Error correcting codes and the ways in which it may aid the communication on these channels are also covered. Cryptography is another crucial ingredient for a complete communication system. Inductively coupled channels pose special challenges for building a secure system. We give a brief overview of these challenges, and of some cryptographic building blocks and protocols that have been proposed to meet them.

Keywords: Inductively coupled channels, RFID, modulation codes, error detection, error correction, cryptographic primitives, cryptographic protocols.

1 Introduction

There is a need to design and deploy electronic devices that can operate without relying on a battery for providing electrical power. For example, once futuristic visions of *pervasive* or *ubiquitous* computing may materialize before long. Such visions comprise an ambience dense with tiny sensors that can measure physical parameters, and operational devices that we may command to perform certain tasks. Exchanging or maintaining the batteries for these devices could be a very complex task. Examples of such applications are networks containing passive sensors, and some RFID[1] systems including governmental and commercial applications like passports, tickets for public transport, and merchandise tags.

An attractive method of operating such tiny battery-free electronic devices is to use *inductive coupling*. In inductive coupling, a component of the battery

[1] The term *RFID* literally means Radio Frequency Identification. The technique origins from World War II, when challenge-response radio signals were used to identify aircraft to determine whether they were friendly or hostile. In current terminology, the term RFID refers to a variation of physical technologies, among which inductive coupling is a prominent one.

A. Barbero (Ed.): ICMCTA, LNCS 5228, pp. 186–195, 2008.

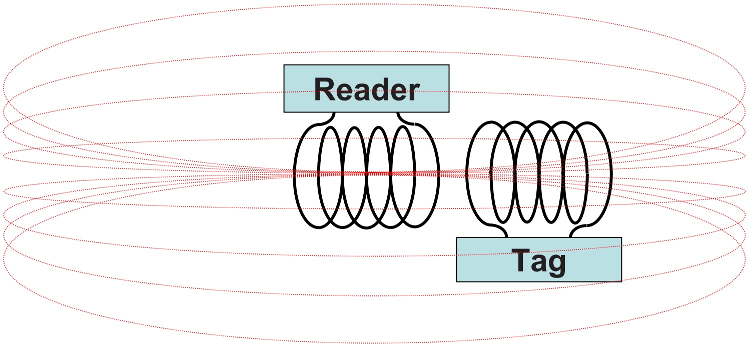


Fig. 1. Inductive coupling. The reader is passing an alternating current through its antenna coil. The resulting magnetic field will induce a corresponding current in the coil antenna of the tag.

free device, called a *tag*, contains an antenna in the shape of a *coil*. Another device, which does contain a power source and which, belying its more general functionality, is commonly called a *reader*, contains another coil-shaped antenna. The reader generates an alternating current (of a relatively low frequency) in the antenna, thereby generating a magnetic field. This magnetic field in turn induces an alternating current of the same frequency in the tag antenna. Figure 1 shows the principle.

Inductive coupling not only provides operation power to the device, but the coupling itself can be modulated and thus provide half duplex communication between the reader and the tag. However, the reader and the tag need to be tuned to the same frequency. This limits the methods by which information can be modulated for transmission on this channel, and in general only amplitude modulation (AM) is used.

The literature contain few papers with an information theoretic or coding theoretic approach to inductively coupled channels, and codes used in practice seem to be selected on an ad hoc basis. This paper, and the corresponding presentation at *2ICMCTA*, will attempt to give an overview of issues related to coding and cryptography for communication on inductively coupled channels. We start in Section 2 by discussing coding, including modulation codes and error controlling codes. Section 3 deals with security related matters.

2 Coding for Inductively Coupled Communication Channels

The reader and the tag face asymmetrical constraints on the processing complexity that they can support. The reader to tag communication channel must employ coding schemes that allow very simple decoding methods. The tag to reader communication, on the other hand, requires a simple encoding method at the expense of a possibly more complex decoding method.

2.1 General Coding Requirements

A code used on an inductively coupled channel must provide solutions to the challenges in a number of areas. Some of these will be discussed in more detail in the context of modulation codes and of error controlling codes, respectively. General coding requirements concern *processing cost* and *code rate*:

Processing Cost: A tag has strictly limited processing capacity, and hence can perform only tasks of limited processing complexity. The term "processing complexity" will not be accurately defined in this paper, because it is difficult to do so: The term can be extended to cover the cost of all signal processing associated with transmission or reception of information, to the extent that this cost depends also on the choice of code. For example, the choice of a simple code may facilitate the processing associated with bit or frame synchronization, at the price of for example a reduced code rate, a reduced power content, or inferior error performance compared to other codes.

Code Rate: As in all coding applications, the number of user bits per sent channel symbol (or per unit of time) is an essential design parameter. Its importance depends on the actual application. In general it is desirable with a high code rate, but this can be traded against other parameters. Many of the applications served by inductively coupled channels do not operate on large amounts of data, and hence the time for data transfer must be related to the time required to set up and manage communications, which may also be affected by the choice of code.

2.2 Modulation Codes for Inductively Coupled Communication Channels

In the inductive coupling channel shown in Figure 1, note that the antennas of the reader and the tag need to be tuned to the same frequency. The information transmission and the power transfer are sensitive to variations in frequency. For this reason it is not customary to use frequency modulation in order to transmit information. Hence, although other modulation schemes are feasible, we will assume *binary* amplitude modulation where the transmitted signal $s(t)$ at time t is represented by

$$s(t) = A_c(1 + u \cdot m(t)) \cdot \cos(W_c \cdot t) \tag{1}$$

where A_c is the carrier amplitude, W_c is the carrier frequency, u is the modulation index ($0 < u \leq 1$), and $m(t)$ is the modulation encoded message.

Bit synchronization and timing and *power content* are important considerations for the selection of modulation codes.

Bit Synchronization and Timing: A crucial limitation of a tag is that it may not possess an internal clock, or even a phase-locked loop. Hence timing information must be extracted from *frequent* signal transitions embedded in the encoded signal. For application specific reasons the tag will not offer the facilities of an on board oscillator of the phase-locked loop. Thus bit synchronization must be facilitated by properties of the code.

Power Content: Since the tag gets its entire power from the signal, the information should be modulated in a way that maximizes the power transferred to the tag. With binary amplitude modulation as in (1) it is desirable if the modulated code sequence $m(t)$ contains as many "1"s as possible.

Existing Modulation Codes. A variety of modulation codes are being used in practical implementations. Popular ones include [3,5] the Manchester code, the 1 out of 4 or 1 out of 256 codes, as well as many proprietary codes.

Existing codes are selected so that they, at least to some degree, observe some of the general coding requirements set forth in Section 2.1 and the special considerations mentioned above for modulation codes. The Manchester code, though not designed for it, still guarantees that on average half of the symbols are ones, and hence guarantee a certain minimum power. The 1 out of 4 or 1 out of 256 codes used in the ISO 15693 [5] standard (for near vicinity cards) represent a variant of permutation modulation and guarantee a high power content but offer poor runlength properties.

Constrained Codes with Increased Power Content. In [3] new modulation codes were introduced that observe restrictions on both the runlengths and the power content. Here follows a brief summary of [3].

A runlength limitation can be represented by a finite state machine (FSM) [7,8]. For binary codes, each edge in the FSM is associated with a label of one bit. A legal runlength limited sequence corresponds to the sequence of edge labels picked up by following a path through the FSM. Each state in the FSM has a label indicating the recent history of paths that are allowed to pass through that state.

The code rate of any constrained code cannot be higher than the *capacity* $C = \log_2 \lambda$ [9], where λ is the largest real eigenvalue of the adjacency matrix or transition matrix corresponding to the FSM.

For the runlength-and-power constrained codes in [3], the FSM will observe these formal requirements, parametrized by the maximum K of consecutive "1"s, and the minimum local power m/n (such a code will be referred to as a (K, m, n) code):

– Each state will be labelled by the number of symbols since the last "0". If this number for some state is equal to K, then edges emanating from that state are not allowed to have an edge label equal to "1".
– Each state will also be labelled by the number of "1"s in the last $m - 1$ symbols. If this number is less than n, edges emanating from that state are not allowed to have an edge label equal to "0".

Table 1 shows the capacities for a selected set of constraints.

Then the state-splitting algorithm [1] is applied, possibly succeeded by state merging. In [3] this procedure gave the results shown Table 2.

Variable Length Modulation Codes. In recording applications like magnetic recording or optical recording, practitioners frown upon proposals of using variable length codes because such codes make it hard to determine the actual

Table 1. Capacities of a selected set of (K, m, n) constraints

K	m	n	Cap.
2	1	3	0.6942
2	3	5	0.2556
3	2	3	0.2878
5	7	10	0.5342
9	8	9	0.1054

Table 2. Examples of codes with comparison of some code properties. K: Maximum runlength, N: Complexity (number of trellis states). P_{min} and P_{avg} are the minimum ratio and the average ratio, of the number of "1"s to the total number of symbols, minimized (resp. averaged) over long code sequences. Manchester refers to the Manchester code, (0,1) to a well known runlength limited code used in magnetic recording, and CodeA, CodeB, CodeC, and CodeD are new constructions derived in [3]. As an example, the encoder state diagram of CodeC is shown in Figure 2.

Code	Rate	K	m	n	P_{min}	P_{avg}	N
Manchester	1/2	2	1	3	1/2	1/2	1
(0,1)	2/3	2	1	3	1/3	1/2	2
CodeA	1/4	2	3	5	3/5	.619	16
CodeB	1/3	2	1	2	5/9	11/18	3
CodeC	1/4	3	2	3	11/16	23/32	4
CodeD	1/10	9	8	9	.89	.895	10

amount of physical space required on a magnetic or optical disk for storing a binary data sequence of a fixed length.

For an application on an inductively coupled channel, use of a variable length code just means that the *time* needed for transferring data is variable. However, the communication time will in any case depend on communication setup time

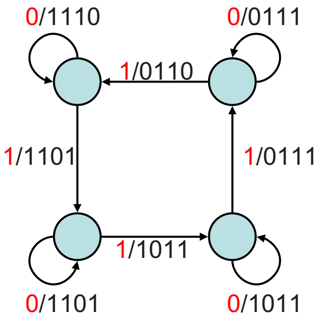


Fig. 2. Encoder state diagram for CodeC of Table 2 [3]. Edges are labelled $u/abcd$, where u is the user information bit which is input to the encoder and $abcd$ are the four encoder output bits that depend on the encoder state.

as well as data transfer time, and will be subject to a wide variation depending on, among other things, the geometric conditions of the communication scenario. Therefore the use of such codes may be more attractive for inductively coupled channels.

Thus, a variable length $(K, K-1, K)$ code can be implemented by the following simple fixed mapping of (user bit ↔ modulation symbols):

$$0 \leftrightarrow 1^{K-1}0, \quad 1 \leftrightarrow 1^{K}0, \tag{2}$$

where 1^x denotes a sequence of x ”1”s.

Provided that input symbols are equally probable, the expected length of these codes is given by $0.5 \cdot (K + K + 1)$, so the average code rate is $2/(2K + 1)$. For numerical examples, the (3,2,3) code has an average rate of 0.2857 and the (9,8,9) code has an average rate of 0.1053. Consulting with Table 1 we see that this is very close to capacity in each case. It is also easy to see that P_{min} and P_{avg}, as defined in the caption of Table 2, are given by

$$P_{\text{min}} = \frac{K-1}{K} \text{ and } P_{\text{avg}} = \frac{2K^2 - 1}{2(K^2 + K)}.$$

2.3 Codes for Error Control for Inductively Coupled Communication Channels

Codes for error control need to observe the general coding requirements in Section 2.1 in addition to the following:

Noise Immunity and Error Correction: The reader to tag channel usually has much more signal power than the tag to reader channel. Since the signal-to-noise ratio (SNR) can be assumed to be high, we will assume that additive noise is a small problem, and that most errors are due to incorrect timing (see Figure 3 below. Thus, if any error correction code is used, it should be designed to combat the effects of timing faults. The tag to reader channel may experience a lower received signal power and hence a lower SNR than the reader to tag channel, and additive noise may be the limiting factor of the communication. Thus it may be beneficial to include an error correcting code in order to combat additive noise. Note that the SNR is likely to be unknown at the receiver as decoding commences, but may be estimated through the progress of the decoding.

Existing Codes: The Electronic Product Code (EPC) format [10], which regulates all devices that use inductively coupled channels, mandates that data be stored on a device using the CCITT-CRC for error detection. This format is then also used for communications purposes and may be used in an Automatic Repeat-Request (ARQ) system. The CCITT-CRC is a cyclic redundancy check, i. e. a shortened cyclic code with generator polynomial $x^{16} + x^{12} + x^5 + 1$.

I *assume* that the choice of error detection scheme here is made out of convenience. However, the choice of code combined with modulation code is not the best one, for these two reasons.

1. It is commonly claimed (as in [5]) that the probability of undetected error of the CRC-CCITT code is, in the worst case, 0.002 % (or 2^{-16}), based on the case of a binary symmetric channel with a BSC transition probability equal to 1/2. However, it is shown in [4] that for shortened codes, the worst case probability of undetected error on a BSC for the CRC-CCITT polynomial will occur for a BSC transition probability *less* than a half. For a user data length of 80 bits the worst BSC transition probability is about 0.03 in which case the probability of undetected error is slightly more than 2^{-16}. In the EPC application, the code will be severely shortened; maybe to a length of few hundred bits or less. There exist other choices of CRC polynomials that perform much better.
2. Consider the model of transmission that is shown in Figure 3. Errors can arise in at least three ways: (i) the additive noise is so high that it affects the sample values, (ii) the threshold based on which the detector determines if a sample value is low or high may be set incorrectly. This can easily happen since the exact relative position between tag and reader must be assumed to be unknown; and hence the nominal "high" signal value is unknown at the start of communication, (iii) there is a mismatch between the bit cell length at the reader and the tag sides. Even though timing is resynchronized at the receiver side upon detection of signal transitions, if the mismatch is large enough, it may cause a *timing error* where sample values are interpreted as belonging to an incorrect bit cell.

The actual channel is in fact, in many applications [6] and especially for the reader to tag communication more sensitive to timing errors than to the classical thermal noise that create the typical additive white Gaussian noise

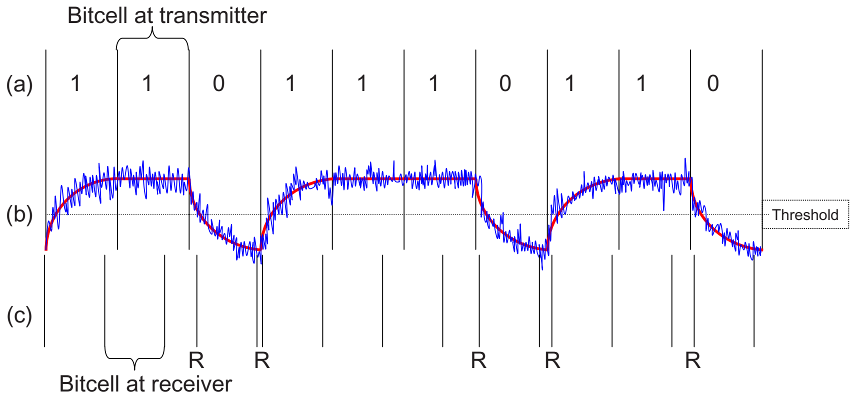


Fig. 3. Signal detection: (a) modulated sequence (sequence $m(t)$ in (1)) (b) Ideal detected signal and detected signal with additive white Gaussian noise added. (c) bit cells at receiver side may not correspond to the bit cells at the transmitter side because the clocking circuitry may be out of tune. However, the receiver side bit cells may be resynchronized each time (marked R in the figure) the receiver, in some way, detects a change in the signal. The resulting signal is sampled once or several times in each bit cell.

channels. With *most modulation codes in common use* today, timing errors may translate into insertion and deletion errors and this may complicate the design of error detection or error correction codes.

Use of Variable Length Modulation Codes: The variable length codes introduced in equation (2) will convert timing errors into simple additive errors, and the channel will be transferred into for example a binary symmetric channel or an AWGN channel, depending on the precise implementation of the signal detection process.

Error Correcting Codes are in general currently not used for commercial products for inductively coupled channels. One reason for this may be that error correction is perceived to be too expensive for the lightweight devices.

Since the tag in particular will have limited computing power, we may anticipate that error detection will be favored for this direction of communication. On the other hand, provided a variable length modulation code is used, an error correcting code designed for the binary symmetric channel or the AWGN channel may be implemented for the tag to reader communication. In order to minimize hardware, it may be of interest to use the same code for these purposes. Since the data lengths may vary, a convolutional code or an LDPC convolutional code may be favored. Observe that the *error detecting* capability for such codes has not been studied much, and this may be an area of future research.

3 Security Issues for Inductively Coupled Communication Channels

There are several highly publicized failure stories in the area of RFID security[2].

Inductively coupled channels have some features that facilitate security. It is in fact difficult (but not impossible) to eavesdrop stealthily on a conversation taking place on such systems. The reason is that an eavesdropper needs to insert his/her own additional antenna into the system of Figure 1, and this may detune the overall system and make it difficult or impossible to carry out the legitimate conversation. An ordinary antenna for these channels need to be very close, typically around 20cm. Specialized eavesdropping antennas may pick up signals at a distance of a few meters, but covert eavesdropping is more difficulty than for ordinary wireless channel. Nevertheless it is appropriate to apply a simple cipher to communications.

Authentication is a real and generally unsolved problem. Depending on the application, this authentication should cover both the reader and the tag. A security problem which is particular to inductively coupled channels is that the tag has severely limited computing power, so that public key cryptography may be difficult to implement.

[2] One example involves Dutch bus cards [12].

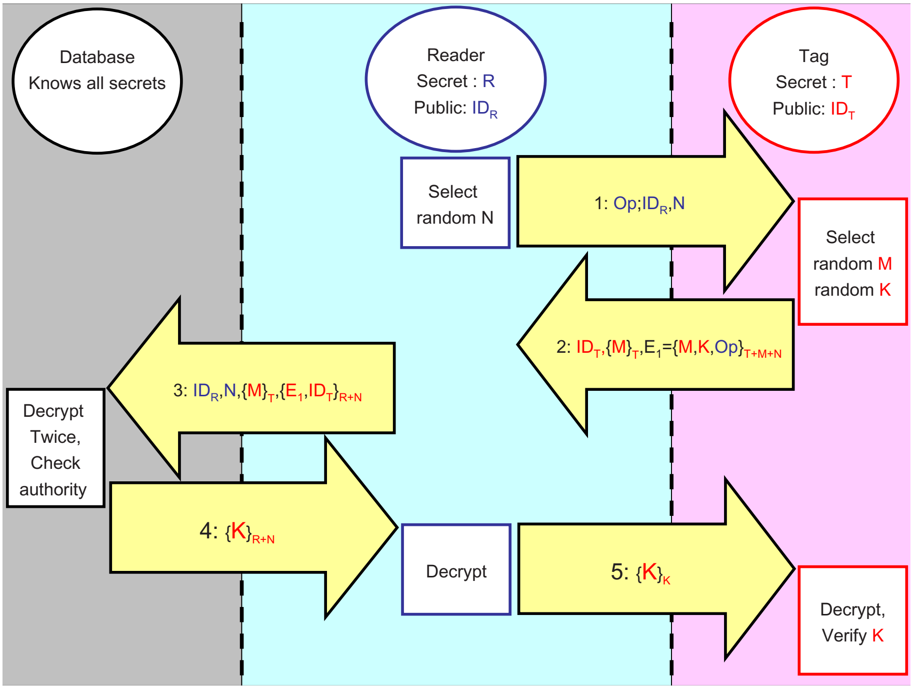


Fig. 4. An authentication and key exchange protocol for lightweight devices [2]. The reader and the tag have public identities $\mathrm{ID_R}$ and $\mathrm{ID_T}$, respectively. Each of these devices has a secret key, R and T, known only to the device itself and to the database. N, M, and K are nonces chosen at random and without reuse. The protocol has five steps: 1) The reader selects nonce N, and sends the intended operation Op, its own identity $\mathrm{ID_R}$, and the nonce N to the tag, 2) The tag generates nonces M and K and sends a packet to the reader consisting of (i) its own identity $\mathrm{ID_T}$, (ii) the nonce M encrypted by T, and (iii) $\mathrm{E_1} = (\mathrm{M}, \mathrm{K}, \mathrm{Op})$ encrypted by $\mathrm{T{+}M{+}N}$. 3) The reader sends a packet to the database consisting of $\mathrm{ID_T}, \mathrm{N}, \mathrm{Op}$, the cryptogram [M encrypted by T] received from the tag, and $(\mathrm{E_1}, \mathrm{ID_T})$ encrypted by $\mathrm{R} + \mathrm{N}$. 4) The database now can resolve all the cryptograms and if the cryptograms match (i. e. the keys are correct) and the reader is authorized to perform the requested operation, sends the response packet consisting of K encrypted by $\mathrm{R}+\mathrm{N}$. If this packet is received, the reader at this point knows that the tag is legitimate. 5) The reader now sends K encrypted by K to the tag. If the tag recognizes K, the reader is considered authenticated and authorized. The ciphers are intended to be stream ciphers. For a feasibility study, the stream cipher Pomaranch has been implemented on a passive sensor device.

Stream ciphers are in general simple to implement and may provide solutions to some of the security challenges in communication on inductively coupled channels. In [2] the authors proposed an authentication protocol for such channels, based on stream ciphers and relying on reader access to a "big brother" database server that knows secret keys of all devices in the system. The protocol is shown in Figure 4.

4 Summary and Disclaimer

In this paper I have attempted to address some issues in coding theory and cryptography that are encountered when designing communication systems for inductively coupled channels. In the talk at *2ICMCTA* I intend to elaborate on these issues. Please note that among the applications that use inductively coupled channels, there are many for which other additional considerations must be made. This, notably, includes multiple access channel allocation issues for medium range communications, and many security related issues.

Acknowledgments. The research behind this paper was supported by the Norwegian Research Council under the ICC:RASC project. The author would like to thank Ángela I. Barbero, Greg D. Horler, Sasha Kholosha, Eirik Rosnes, and the Tigre for stimulating discussions that have forwarded his own understanding of these matters.

References

1. Adler, R.L., Coppersmith, D., Hassner, M.: Algorithms for sliding block codes - an application of symbolic dynamics to information theory. IEEE Transactions on Information Theory IT-29(1), 5–22 (1983)
2. Barbero, Á.I., Horler, G.D., Kholosha, A., Ytrehus, Ø.: Modulation codes for reader-tag communication on inductively coupled channels. In: Proc. The IET Conference on Wireless, Mobile and Multimedia Networks, Mumbai, January 2008, pp. 294–297 (2008)
3. Barbero, Á.I., Horler, G.D., Rosnes, E., Ytrehus, Ø.: Modulation codes for reader-tag communication on inductively coupled channel. In: ISITA 2008 (submitted, 2008)
4. Funk, G.: Determination of Best Shortened Linear Codes. IEEE Transactions on Communications 44(1), 1–6 (1996)
5. Glover, B., Bhatt, H.: RFID Essentials. O'Reilly, Sebastopol (2006)
6. Horler, G.D.: Private communication
7. Immink, K.A.S., Siegel, P.H., Wolf, J.K.: Codes for digital recorders. IEEE Transactions on Information Theory 44(6), 2260–2299 (1998)
8. Marcus, B.H., Roth, R.M., Siegel, P.H.: Constrained systems and coding for recording channels. In: Pless, V., Huffman, W.C. (eds.) Handbook of Coding Theory, pp. 1635–1764. North-Holland, Amsterdam (1998)
9. Shannon, C.E.: A mathematical theory of communication. Bell System Tech. J. 27, 379–423, 623-656 (1948)
10. http://www.epcglobalinc.org/
11. ISO/IEC JTC1/SC17 N3391, Ballot on ISO/IEC CD, 3-2.2 (Revision), http://wg8.de/
12. http://www.cs.vu.nl/~ast/ov-chip-card/

Author Index