ON SELF-DUAL BINARY CODES

Carolin Hannusch

University of Debrecen

carolin.hannusch@science.unideb.hu

Joint work with Piroska Lakatos

Austrian-Hungarian Conference

Győr, Hungary, 25th August - 27th August 2015

Overview

Introduction

Monomial codes in the radical of $\mathscr{A}_{p,m}$

Construction of codes with given distance

New classes of self-dual binary codes

Open Problems

Codes from group algebras

Definition 1

Let p be prime. Let $K = GF(p)$ and G be an elementary abelian p-group $G = \langle x_1, \ldots, x_m \rangle$ of rank m. We consider the p^k-dimensional subspaces C of the modular group algebra $K[G] = \mathscr{A}_{p,m}$ as linear codes.

Codes from group algebras

Definition 1

Let p be prime. Let $K = GF(p)$ and G be an elementary abelian p-group $G = \langle x_1, \ldots, x_m \rangle$ of rank m. We consider the p^k-dimensional subspaces C of the modular group algebra $K[G] = \mathscr{A}_{p,m}$ as linear codes.

Definition 2

If the minimum (Hamming) weight of the k-dimensional subspace is d then the linear code C is referred to as a (p^m, p^k, d)-code.

Historical development

The structure of a group algebra behind a linear code is of important practical value. For abelian G Berman [1] initiated the study of the Jacobson radical of the group algebra $\mathscr{A}_{p,m}$. For $\mathscr{A}_{2,m}$ he proved that the well known Reed-Muller (RM)-codes are the powers of the radical of the group algebra. The Generalized Reed-Muller (GRM) codes were introduced by Kasami, Lin, and Peterson [4] over an arbitrary finite field as the powers of the radical of a group algebra.

GRM-codes

For $0 \leq r \leq m(p-1)$, the rth order generalized Reed-Muller code of length p^m is

$$GRM(r,m) := \langle \prod_{i=1}^{m} (x_i - 1)^{b_i} \mid \sum_{i=1}^{m} b_i \leq r \rangle.$$

GRM-codes

For $0 \leq r \leq m(p-1)$, the rth order generalized Reed-Muller code of length p^m is

$$GRM(r,m) := \langle \prod_{i=1}^{m} (x_i - 1)^{b_i} \mid \sum_{i=1}^{m} b_i \leq r \rangle.$$

Let us denote the radical of $\mathscr{A}_{p,m}$ by J. With the notation $X_i = x_i - 1$ the powers of $J_{p,m}$ are defined by

$$J_{p,m}^k = GRM(m(p-1)-k,m) = \langle \prod_{i=1}^{m} X_i^{b_i} \mid \sum_{i=1}^{m} b_i \geq k \rangle,$$

where $0 \leq b_i \leq p-1$ and $1 \leq k \leq m(p-1)$.
This follows from the fact that the dual of a GRM-code is a GRM-code, $GRM(k,m)^{\perp} = GRM(m(p-1)-k-1,m)$.

Construction of codes with given distance

Drensky and Lakatos asked the following question in ([2], Problem 2.6):
Does there exist an abelian group of order 2^n for arbitrary $n \in \mathbb{N}$, such that for $1 \leq d \leq \left[\frac{n+1}{2}\right]$ and for a field K of characteristic 2 one of the powers of the Jacobson radical of $\mathscr{A}_{2,n}$ is a $(2^n, 2^{n-1}, 2^d)$ self-dual code. In [3] a proof of the positive answer of this problem is written down.

Outline of the proof

The main tool in our proof is Berman's formula for the minimum distance of a code (see [1] and [3] for details). Our proof is constructive. To construct the required codes it is enough to take abelian groups which are direct product of cyclic groups of at most 3 different orders. It is easy to see that if G is a 2-group, then some power of the radical of $K[G \times C_2]$ or $K[G]$ is self-dual. This fact suggests to take abelian groups with one factor of order two. It turned out that in the decomposition of above mentioned group G with cyclic components C_2 and C_{2^2} satisfy the above mentioned property. This does not mean that there are no other groups with this property.

These codes are constructed for abelian groups G with decomposition

$$G = C_{2^{a_1}}^{s_1} \times C_{2^2}^{s_2} \times C_2^{s_3} \text{ i.e. } n = s_1 a_1 + 2s_2 + s_3,$$

where $a_1 \geq 3$ and $s_i \geq 0$ $(1 \leq i \leq 3)$. The main idea of the proof is to fix the values n, a_1, r and s_1 or s_2. Then we increase (by the smallest possible steps) the value s_1 or s_2. We consider only those situations, when the corresponding value of d is increasing or decreasing at most by 1.
Proof is divided into four intervals:

1. $\left[\frac{n}{4}\right] + t + 1 \leq d \leq \left[\frac{n+1}{2}\right]$, where $t = 1$ if $n \equiv 3,6 \pmod 8$, and $t = 0$
2. $1 \leq d \leq \left[\frac{n+1}{5}\right]$
3. $\left[\frac{n+1}{5}\right] < d \leq \left[\frac{n}{4}\right] - \left[\frac{n+40}{64}\right]$
4. $\left[\frac{n}{4}\right] + 1 - \left[\frac{n+40}{64}\right] \leq d \leq \left[\frac{n}{4}\right] + t$, where $t = 1$, if $n \equiv 3,6 \pmod 8$, otherwise $t = 0$

How to construct new self-dual binary codes

We say that the set Y of binary vectors in X is *complement free* if $\mathbf{c} \in X$ implies $\mathbf{1} - \mathbf{c} \notin X$.
Denote by $\mathscr{Y}$ the maximal set of pairwise orthogonal monomials in $\mathscr{X}$ and Y by the corresponding exponents in X. Clearly Y is a complement free subset of X with cardinality $\frac{1}{2}\binom{2k}{k}$.

How to construct new self-dual binary codes

We say that the set Y of binary vectors in X is *complement free* if $\mathbf{c} \in X$ implies $\mathbf{1} - \mathbf{c} \notin X$.
Denote by $\mathscr{Y}$ the maximal set of pairwise orthogonal monomials in $\mathscr{X}$ and Y by the corresponding exponents in X. Clearly Y is a complement free subset of X with cardinality $\frac{1}{2}\binom{2k}{k}$.

Theorem 1

Let G be an elementary abelian group of order 2^m, where $m = 2k$, $k \geq 2$.
Let $C = \langle J_{2,m}^{k+1} \bigcup \mathscr{Y} \rangle$, be the subspace of the radical of the group algebra $\mathscr{A}_{2,m}$ generated by the union of $J_{2,m}^{k+1}$ and $\mathscr{Y}$.
Then C is self-dual binary code with parameters $(2^{2k}, 2^{2k-1}, 2^k)$ in the radical of group algebra $\mathscr{A}_{2,m}$, which has the property $J_{2,m}^{k+1} \subset C \subset J_{2,m}^{k}$.

Particular case of the code C

In particular, in Theorem 1. we get $(16, 8, 4)$ self-dual codes for $m = 4$. These codes are extremal doubly-even codes. Using the SAGE computer algebra software we checked the classification of binary self-dual codes listed in [5].

Particular case of the code C

In particular, in Theorem 1. we get $(16, 8, 4)$ self-dual codes for $m = 4$. These codes are extremal doubly-even codes. Using the SAGE computer algebra software we checked the classification of binary self-dual codes listed in [5]. There are two cases

1. If the elements of Y generate a hyperplane of X, then we have the direct sum of $E_8 \oplus E_8$, where E_8 is the extended Hamming code.

Particular case of the code C

In particular, in Theorem 1. we get $(16, 8, 4)$ self-dual codes for $m = 4$. These codes are extremal doubly-even codes. Using the SAGE computer algebra software we checked the classification of binary self-dual codes listed in [5]. There are two cases

1. If the elements of Y generate a hyperplane of X, then we have the direct sum of $E_8 \oplus E_8$, where E_8 is the extended Hamming code.
2. elsewhere we get an indecomposable $(16, 8, 4)$-code (which is denoted by E_{16} in [5]).

Open problems

1. How many non-isomorphic self-dual binary codes exist for fixed m and p ?

Open problems

1. How many non-isomorphic self-dual binary codes exist for fixed m and p ?
2. Compare the automorphism groups of C with the automorphism group of GRM-codes.

Open problems

1. How many non-isomorphic self-dual binary codes exist for fixed m and p ?
2. Compare the automorphism groups of C with the automorphism group of GRM-codes.
3. Find decoding algorithms for C.

Support

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318202.

References


Berman, S.D. (1967)
On the theory of group codes
Kibernetika 3(1), 31 – 39.


Drensky, V., Lakatos, P. (1989)
Monomial ideals, group algebras and error correcting codes
Lecture Notes in Computer Science, Springer Verlag 357, 181 – 188.


Hannusch, C., Lakatos, P. (2012)
Construction of self-dual radical 2-codes of given distance
Discrete Mathematics, Algorithms and Applications 4.


Kasami, T. , Lin, S, Peterson, W.W. (1968)
New generalisations of the Reed-Muller codes
IEEE Trans. Inform. Theory II 14, 189 – 199.


Pless, V. (1972)
A classification of self-orthogonal codes over GF(2)
Discrete Mathematics 3, 209–246


Ward, Harold N. (1990)
Visible codes