CONSTRUCTION OF SELF-DUAL BINARY CODES

Carolin Hannusch

University of Debrecen

carolin.hannusch@science.unideb.hu

Joint work with Piroska Lakatos

DIMA 2015

Minsk, Belarus, 14th September - 18th September 2015

Overview

Definitions - 1

Definition 1

Let p be prime. Let $K = GF(p) = \mathbb{F}_p$ 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. We will denote the Jacobson radical of $\mathscr{A}_{p,m}$ by $J_{p,m}$.

Definitions - 1

Definition 1

Let p be prime. Let $K = GF(p) = \mathbb{F}_p$ 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. We will denote the Jacobson radical of $\mathscr{A}_{p,m}$ by $J_{p,m}$.

Definition 2

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

Definitions - 2

Definition 3

A basis of a linear code is called visible, if there exists a member of the basis with the minimum (Hamming) weight of the space.

Definitions - 2

Definition 3

A basis of a linear code is called visible, if there exists a member of the basis with the minimum (Hamming) weight of the space.

Definition 4 ([2])

The code C in $J_{p,m}$ is said to be a monomial code if it is an ideal in $\mathscr{A}_{p,m}$ generated by some monomials of the form

$$X_1^{k_1} X_2^{k_2} \dots X_m^{k_m}, \text{ where } 0 \leq k_i \leq p-1.$$

Definitions - 3

Definition 5

The dual code of a linear code C is defined by

$$C^{\perp} = \{x \in \mathbb{F}_p^n | \sum_{i=1}^{n} x_i c_i = 0 \ \forall c \in C\}.$$

A linear code C is called self-dual if $C = C^{\perp}$.

Historical development

The class of codes in the radical of group algebra $\mathscr{A}_{p,m}$ are of important practical values. 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 [3] over an arbitrary finite field as the powers of the radical of a group algebra.

The radical of $\mathscr{A}_{p,m}$

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

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

The radical of $\mathscr{A}_{p,m}$

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, $GRM(k,m)^{\perp} = GRM(m(p-1)-k-1,m)$.

Self-dual RM-codes

A power of the radical of a modular group algebra is self-dual if and only if the nilpotency index of the radical is even. In our case (when G is elementary abelian of order p^m) the nilpotency index is even if and only if $p = 2$ and m is odd.

Self-dual RM-codes

A power of the radical of a modular group algebra is self-dual if and only if the nilpotency index of the radical is even. In our case (when G is elementary abelian of order p^m) the nilpotency index is even if and only if $p = 2$ and m is odd.
If m is odd, the binary RM-codes with parameters $[2^m, 2^{m-1}, 2^{\frac{m+1}{2}}]$ are self-dual and they are the $\frac{m+1}{2}$-th powers of the radical $\mathscr{A}_{2,m}$.

Self-dual RM-codes

A power of the radical of a modular group algebra is self-dual if and only if the nilpotency index of the radical is even. In our case (when G is elementary abelian of order p^m) the nilpotency index is even if and only if $p = 2$ and m is odd.
If m is odd, the binary RM-codes with parameters $[2^m, 2^{m-1}, 2^{\frac{m+1}{2}}]$ are self-dual and they are the $\frac{m+1}{2}$-th powers of the radical $\mathscr{A}_{2,m}$.
For $m = 2k$ where k is an arbitrary integer, we have a new method to construct a doubly-even class of binary self-dual C codes with parameters $[2^m, 2^{m-1}, 2^k]$. For this code C we have $\mathrm{RM}(k-1, 2k) \subset C \subset \mathrm{RM}(k, 2k)$.

Introduction of "complement free" sets

For $m = 2k$ denote the set of all k-subsets of $\{1, 2, \ldots, 2k\}$ by X. The elements of X can be described with binary sequences $(k_1, k_2, \ldots, k_m)$ consisting of k zeros and k ones in any order. Clearly the cardinality of the set X is $\binom{2k}{k}$.

Introduction of "complement free" sets

For $m = 2k$ denote the set of all k-subsets of $\{1, 2, \ldots, 2k\}$ by X. The elements of X can be described with binary sequences $(k_1, k_2, \ldots, k_m)$ consisting of k zeros and k ones in any order. Clearly the cardinality of the set X is $\binom{2k}{k}$.

Definition 6

We say that the subset Y of binary m-tuples in X is complement free if $y \in Y$ implies $\mathbf{1} - y \notin Y$, where $\mathbf{1} = (1, 1, \ldots, 1)$.

Introduction of "complement free" sets

For $m = 2k$ denote the set of all k-subsets of $\{1, 2, \ldots, 2k\}$ by X. The elements of X can be described with binary sequences $(k_1, k_2, \ldots, k_m)$ consisting of k zeros and k ones in any order. Clearly the cardinality of the set X is $\binom{2k}{k}$.

Definition 6

We say that the subset Y of binary m-tuples in X is complement free if $y \in Y$ implies $\mathbf{1} - y \notin Y$, where $\mathbf{1} = (1, 1, \ldots, 1)$.

Two monomials of the form $X_1^{k_1} X_2^{k_2} \ldots X_m^{k_m}$ are orthogonal, i.e. their product is zero, if for some $i : (1 \leq i \leq m)$ we have $k_i = 1$.

Introduction of "complement free" sets

For $m = 2k$ denote the set of all k-subsets of $\{1, 2, \ldots, 2k\}$ by X. The elements of X can be described with binary sequences $(k_1, k_2, \ldots, k_m)$ consisting of k zeros and k ones in any order. Clearly the cardinality of the set X is $\binom{2k}{k}$.

Definition 6

We say that the subset Y of binary m-tuples in X is complement free if $y \in Y$ implies $\mathbf{1} - y \notin Y$, where $\mathbf{1} = (1, 1, \ldots, 1)$.

Two monomials of the form $X_1^{k_1} X_2^{k_2} \ldots X_m^{k_m}$ are orthogonal, i.e. their product is zero, if for some $i : (1 \leq i \leq m)$ we have $k_i = 1$. Denote the maximal set of pairwise orthogonal monomials in $\mathscr{X}$ by $\mathscr{Y}$ and the corresponding exponents in X by Y. Clearly Y is a complement free subset of X with cardinality $\frac{1}{2}\binom{2k}{k}$.

Theorem 1 (P. Lakatos, C.H.)

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 a monomial binary code in the radical of group algebra $\mathscr{A}_{2,m}$, which has the property $J_{2,m}^{k+1} \subset C \subset J_{2,m}^{k}$, further C forms a $(2^{2k}, 2^{2k-1}, 2^k)$ self-dual doubly-even code and C has a visible basis.

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 [4].

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 [4]. 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 [4]. 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 [4]).

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 [4]. 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 [4]).

These codes are formally self-dual.

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 [4]. 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 [4]).

These codes are formally self-dual. For $m \geq 6$ these classes of codes are new.

More codes with visible basis

Theorem 2 (C.H.)

For arbitrary p the principal ideal

$$C_1 = \langle X_1^{b_1} X_2^{b_2} \dots X_m^{b_m} \mid 0 \le b_i \le p-1; (i = 1,2,\dots,m) \rangle$$

determines a $(p^m, (p-b_1)\cdot(p-b_2)\cdot\dots\cdot(p-b_m), d)$ cyclic code which has a visible basis, where $d = \prod_{i=1}^{m}(b_i+1)$. The set

$$\{\prod_{i=1}^{m} X_i^{k_i} | b_i \le k_i \le p-1\}$$

is a visible basis of C_1.

Codes with visible basis - 2

Theorem 3 (C.H.)

The monomial code

$$C_{m,k} = \langle \prod (X_i)^{b_i} \mid \prod_{i=1}^{m} b_i \geq k, \text{ where } 0 < k \leq (p-1)^m \rangle$$

has a visible basis.

Questions

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

Questions

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.

Questions

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.

THANK YOU FOR YOUR ATTENTION!

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.


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
Arch. Math. (Basel) 54, no. 3, 307-312, (1990)