数理解析研究所講究録 1476 巻 2006 年 111-119

Finite groups and codes

Kanat Abdukhalikov
Institute of Mathematics,
Pushkin Str 125, Almaty 480100, Kazakhstan
and
Graduate School of Mathematics, Kyushu University,
Hakozaki 6-10-1, Higashi-ku, Fukuoka 812-8581, Japan

1 Introduction

Let $G$ be a doubly transitive group on a finite set $\Omega$. Consider the permutation module $F^{\Omega}=\{f \mid f:\Omega\rightarrow F\}$, where $F$ is a ring or a field. We are interesting to find all $G$-invariant $F$-submodules in $F^{\Omega}$. In case of finite field $F$ it means that we are looking for $G$-invariant codes, and in case $F=\mathbb{Z}$ we will have $G$-invariant lattices. Many known codes and lattices can be constructed by such a construction: quadratic residue codes, Reed-Muller codes, Golay codes, Leech and Barnes-Wall lattices. Recently constructed quaternary Kerdock, Preparata, Goethals, Goethals-Delsarte, Delsarte-Goethals codes are also covered by this construction, if we take $F=\mathbb{Z}_4$.

We will write elements of $f\in F^{\Omega}$ in the form $f=\sum_{\alpha\in\Omega}a_{\alpha}\chi_{\alpha}$, where $\chi_{\alpha}$ is a characteristic function. The natural action of an element $g\in G$ on $F^{\Omega}$ is given by $g(\sum_{\alpha\in\Omega}a_{\alpha}\chi_{\alpha})=\sum_{\alpha\in\Omega}a_{\alpha}\chi_{g(\alpha)}$. This action of $G$ preserves the natural bilinear form defined by

$$(\sum a_{\alpha}\chi_{\alpha},\sum b_{\alpha}\chi_{\alpha})=\sum a_{\alpha}b_{\alpha}.$$

There are two natural submodules in $F^{\Omega}$:

$$M=\langle\sum\chi_{\alpha}\rangle,$$

the set of constant functions, and its orthogonal complement

$$M^{\perp}=\{\sum a_{\alpha}\chi_{\alpha}\mid\sum a_{\alpha}=0\}.$$

If $F$ is a field and the characteristic of $F$ does not divide the order of $G$ then $M$ and $M^{\perp}$ are the only nontrivial $G$-invariant $F$-submodules of $F^{\Omega}$. Also $M\leq M^{\perp}$ precisely when the characteristic of the field $F$ divides the degree $|\Omega|$ of the group $G$.

2 Doubly transitive groups

If $G$ is a doubly transitive group on $\Omega$, $H$ is the socle of $G$ then O'Nan-Scott theorem and the classification of finite simple groups implies that only two cases are possible:

1. $H$ is a nonregular nonabelian simple group, $G\leq Aut(H)$;

2. $H$ is a regular elementary abelian $p$-group for some prime $p$, $|\Omega|=p^{n}=|H|$, $G\leq AGL_{n}(p)$.

All possible groups for the case 1 are listed in the Table 1 [9].

H	$\vert\Omega\vert$	Remarks
A_n, $n \geq 5$	n	Two representations if $n = 6$
$PSL_n(q)$, $n \geq 2$	$(q^n - 1)/(q - 1)$	$(n, q) \neq (2, 2), (2, 3)$ Two representations if $n > 2$
$PSU_3(q)$	$q^3 + 1$	$q > 2$
${}^2B_2(q)$ (Suzuki)	$q^2 + 1$	$q = 2^{2f+1} > 2$
${}^2G_2(q)$ (Ree)	$q^3 + 1$	$q = 3^{2f+1} > 3$
$Sp_{2n}(2)$	$2^{2n-1} + 2^{n-1}$	$n > 2$
$Sp_{2n}(2)$	$2^{2n-1} - 2^{n-1}$	$n > 2$
$PSL_2(11)$	11	Two representations
$PSL_2(8)$	28	
A_7	15	Two representations
M_{11} (Mathieu)	11	
M_{11} (Mathieu)	12	
M_{12} (Mathieu)	12	Two representations
M_{22} (Mathieu)	22	
M_{23} (Mathieu)	23	
M_{24} (Mathieu)	24	
HS (Higman-Sims)	176	Two representations
Co_3 (Conway)	276	

Table 1: Non-abelian socles of doubly transitive groups

In the affine case we have $G \leq A\Gamma L_m(q) = V \cdot \Gamma L_m(q)$, $q = p^t$, $G = V \cdot G_0$, and one of the following cases hold:

(i) $SL_m(q) \leq G_0 \leq \Gamma L_m(q)$;
(ii) $Sp_m(q) \leq G_0 \leq \Gamma L_m(q)$;
(iii) $G_2(2^t) \leq G_0 \leq \Gamma L_6(2^t)$;
(iv) Several exceptions [11, 13].

3 Invariant submodules for groups with nonabelian socle

Starting point in our considerations is the Mortimer's paper [16]. He defines the heart over the field F of the group G acting on the set Ω as the G-module $M^{\perp}/(M \cap M^{\perp})$. The Table 2 from [16] describes the cases when heart is reducible. In fact, this result points out the cases when it is possible to get nontrivial codes and lattices.

In case $G = PSL_2(q)$, $|\Omega| = q + 1$, $F \geq \mathbb{F}_2$ for $q \equiv \pm 1 \pmod 8$ and $F \geq \mathbb{F}_4$ for $q \equiv \pm 3 \pmod 8$, all the G-invariant nontrivial subspaces in F^{Ω} are M, $M^{\perp}$ and two more subspaces, C_1 and C_2, where $\mathrm{PGL}_2(q)$ permutes them. These subspaces C_1 and C_2 give realizations of quadratic residue codes of length $q + 1$.

Studying $PSL_2(13)$-invariant lattices in $M^{\perp}$, $F = \mathbb{Q}(\sqrt{-3})$, we get a construction [2] of the unique hermitian unimodular rootless lattice of rank 13 over the Eisenstein numbers (of course in this case we have to take hermitian form in place of bilinear form). Its automorphism group is isomorphic to $\mathbb{Z}_6 \times \mathrm{PSp}_6(3)$.

The structure of permutation modules for $Sp_{2n}(2)$ over a field was studied in [17]. There is no clear classification of submodules, and description is done through some filtrations.

Group, G	Degree $\|\Omega\|$	Transitivity	Conditions under which the heart of G over F is reducible (F a field of characteristic p)
S_n, $n \geq 3$	n	n	always simple
A_n, $n \geq 5$	n	$n-2$	always simple
$G \leq A\Gamma L_n(q)$ containing the translations	q^n	2 or 3	p divides q
$PSL_n(q) \leq G \leq P\Gamma L_n(q)$, $n \geq 3$	$(q^n-1)/(q-1)$	2	p divides q
$PSL_2(q) \leq G \leq P\Sigma L_2(q)$	$q+1$	2	$F \geq \mathbb{F}_2$ if $q \equiv \pm 1 \pmod 8$ $F \geq \mathbb{F}_4$ if $q \equiv \pm 3 \pmod 8$
G, a 3-transitive subgroup of $P\Gamma L_2(q)$	$q+1$	3	always simple
$PSU_3(q) \leq G \leq P\Gamma U_3(q)$	q^3+1	2	p divides $q+1$
${}^2B_2(q) \leq G \leq Aut({}^2B_2(q))$	q^2+1	2	p divides $q+1+\sqrt{2q}$
${}^2G_2(q) \leq G \leq Aut({}^2G_2(q))$	q^3+1	2	p divides $(q+1)(q+1+\sqrt{3q})$ and perhaps if p divides $(q+1)(q+1-\sqrt{3q})$
$Sp_{2n}(2)$, $n \geq 2$	$2^{2n-1}+2^{n-1}$	2	$p=2$
$Sp_{2n}(2)$, $n \geq 3$	$2^{2n-1}-2^{n-1}$	2	$p=2$
$A_4 = AGL_1(4)$	4	2	$F \geq \mathbb{F}_4$
$PSL_2(11)$	11	2	$p=3$
$G = A_7 < PGL_4(2)$	15	2	$p=2$
M_{11} (Mathieu)	11	4	always simple
M_{11} (Mathieu)	12	3	$p=3$
M_{12} (Mathieu)	12	5	always simple
M_{22} (Mathieu)	22	3	$p=2$
M_{23} (Mathieu)	23	4	$p=2$
M_{24} (Mathieu)	24	5	$p=2$
HS (Higman-Sims)	176	2	$p=2, 3$
Co_3 (Conway)	276	2	perhaps if $p=2$ or 3

Table 2: Reducibility of the hearts of some 2-transitive groups

The unitary group $PSU_3(q)$ acts 2-transitively on the points Ω of the hermitian unital of order q, which is a $2-(q^3+1, q+1, 1)$ design. Suzuki group ${}^2B_2(q)$, $q = 2^{2r+1}$, is an automorphism group of an inversive plane of order q, that is, of a $3-(q^2+1, q+1, 1)$ design. Ree group ${}^2G_2(q)$, $q = 3^{2r+1}$, acts 2-transitively on the points Ω of the Ree unital, which is a $2-(q^3+1, q+1, 1)$ design. In these three cases design modules give examples of G-invariant codes over a field F of corresponding characteristic (see Table 2). However the list of all submodules is not known. The dimensions of design modules of the Ree unital is calculated in [12].

The group $PSL_2(11)$ and Mathieu groups produce codes related to Golay codes. For the Higman-Sims group some invariant codes are presented in [8].

Projective groups $PGL_n(q)$ are studied only in the case $q = p$, they produce projective generalized Reed-Muller codes [4] (over field $\mathbb{F}_p$ and $\mathbb{Z}_{p^m}$). Invariant lattices for these groups are studied in [6].

When we consider G-invariant codes and lattices in F^Ω we get codes of length $|\Omega|$ and lattices of rank $|\Omega|$. If we consider invariant sublattices in $M^\perp$ ($F = \mathbb{Z}$) we get lattices of rank $|\Omega| - 1$.

Let W be a rational module over a finite group G. Recall [14] that number of similarity classes of invariant lattices in W is finite if and only if G acts absolutely irreducible on W. In this case on the vector space W there exists unique (up to scalar factor) G-invariant symmetric positive definite bilinear form. Denote by $\mathrm{Aut}(\Lambda)$ the group of isometries of Λ with respect to this form.

Now we take $W = \mathbb{Q}M^{\perp}$. Then W is absolutely irreducible G-module. We can assume that G is a minimal doubly transitive group (that is, any proper subgroup of G is no longer doubly transitive). If it is the case then G is simple, except for $G = {}^2G_2(3) \cong P\Gamma L_2(8) = PSL_2(8) : 3$.

We have the following theorem [5].

Theorem 1 *Let G be a minimal doubly transitive group with nonabelian socle, Λ be a G-invariant $\mathbb{Z}$-lattice in the module W. Then one of the following assertions holds:*

1) $\mathbb{Z}_2 \times G \leq \mathrm{Aut}(\Lambda) \leq \mathbb{Z}_2 \times \mathrm{Aut}(G)$.
2) $\mathrm{Aut}(\Lambda) \cong \mathbb{Z}_2 \times S_\Omega$.
3) $G = PSL_2(7)$, $|\Omega| = 8$, $\mathrm{Aut}(\Lambda) \cong \mathbb{Z}_2 \times AGL_3(2)$, $\mathbb{Z}_2 \times Sp_6(2)$ *or* $\mathbb{Z}_2^7 : S_7$.
4) $G = PSL_2(11)$, $|\Omega| = 11$, $\mathrm{Aut}(\Lambda) \cong \mathbb{Z}_2 \times M_{11}$.
5) $G = PSL_2(11)$, $|\Omega| = 12$, $\mathbb{Z}_2 \times M_{12} \leq \mathrm{Aut}(\Lambda) \leq \mathbb{Z}_2 \times M_{12} : 2$.
6) $G = M_{11}$, $|\Omega| = 12$, $\mathbb{Z}_2 \times M_{12} \leq \mathrm{Aut}(\Lambda) \leq \mathbb{Z}_2 \times M_{12} : 2$ *or* $\mathrm{Aut}(\Lambda) = \mathbb{Z}_2^{11} : S_{11}$.
7) $G = A_7$, $|\Omega| = 15$, $\mathbb{Z}_2 \times A_8 \leq \mathrm{Aut}(\Lambda) \leq \mathbb{Z}_2 \times S_8$.
8) $G = PSL_2(23)$, $|\Omega| = 24$, $\mathrm{Aut}(\Lambda) \cong \mathbb{Z}_2 \times M_{24}$.
9) $G = PSU_3(3)$, $|\Omega| = 28$, $\mathrm{Aut}(\Lambda) \cong \mathbb{Z}_2 \times Sp_6(2)$.
10) $G = {}^2G_2(3)$, $|\Omega| = 28$, $\mathbb{Z}_2 \times A_9 \leq \mathrm{Aut}(\Lambda) \leq \mathbb{Z}_2 \times S_9$ *or* $\mathrm{Aut}(\Lambda) \cong \mathbb{Z}_2 \times Sp_6(2)$.

A similar consideration for the group $G = ASL_2(5)$ gives a construction of the Leech lattice as a G-invariant lattice.

4 Invariant submodules for groups with abelian socle

Let $G = V \cdot Sp_{2m}(q)$. This case is studied only for odd prime values $q = p$. Let $F = \mathbb{F}_p$. Then G-invariant subcodes of F^Ω are C^0, C^1, ..., $C^{2m(p-1)}$, and, if $m \geq 2$, two more codes C^+ and C^-, where

$$C^0 \supset C^1 \supset \cdots C^{m(p-1)} \supset C^{m(p-1)+1} \supset \cdots \supset C^{2m(p-1)},$$
$$C^+ + C^- = C^{m(p-1)},$$
$$C^+ \cap C^- = C^{m(p-1)+1}.$$

Now let $F = \mathbb{Z}$, $\Lambda = M^{\perp}$, so $\mathrm{rank}(\Lambda) = p^{2m} - 1$. Then there are G-invariant basic sublattices Λ^k, $1 \leq k \leq 2m(p-1)$; Λ^+; Λ^-; $\Lambda^{k,s,r}$, $1 \leq r \leq p-1$, $1 \leq s \leq 2m-1$, $1 \leq k < (2m-s)(p-1)/2$, such that any invariant sublattice will be a linear combination of these basic lattices:

$$\Lambda = \sum p^i \Lambda_i.$$

Here Λ^k, Λ^+ and Λ^- are defined as the minimal lattices Γ, such that $(\Gamma + p\Lambda)/p\Lambda$ is isomorphic to C^k, C^+ or C^- respectively. Furthermore, $\Lambda^{2m(p-1)-k} + p^s\Lambda^k \supset \Lambda^{k,s,r} \supset \Lambda^{2m(p-1)-k+1} + p^s\Lambda^{k+1}$ and $\Lambda^{k,s,r}/(\Lambda^{2m(p-1)-k+1} + p^s\Lambda^{k+1}) \cong C^k/C^{k+1}$.

If $p = 5$, $m = 1$, $k = 1$, $s = 1$, then $\Lambda^{k,s,r}$ is isometric to the Leech lattice (in this case we have $ASp_2(5) \cong ASL_2(5)$).

If we consider invariant lattices in $F^\Omega = \mathbb{Z}^V$, we will have additional invariant lattices Λ^0; $\Lambda^{0,s,r}$, $1 \leq r \leq p-1$, $s \geq 1$.

Permutation module for the group $Sp_{2m}(p)$ is studied also in [18].

Now we are coming to the most interesting case, the affine group $G = AGL_n(q) = V \cdot GL_n(q)$. We have here $\Omega = V$. First we consider the group $G_1 = AGL_1(p^n) = V \cdot GL_1(p^n)$. Let $\mathbb{F}_{p^n}$ be a finite field of p^n elements. Consider F^{Ω} as group algebra $A = F[V]$ of the abelian group $V = \mathbb{F}_{p^n}^+$ over a ring F:

$$A = \left\{ \sum_{v \in V} a_v X^v \mid a_v \in F \right\}.$$

So we write X^v in place of χ_v. Operations in A are given by:

$$\sum a_v X^v + \sum b_v X^v = \sum (a_v + b_v) X^v,$$

$$c \sum a_v X^v = \sum c a_v X^v, \quad c \in F,$$

$$\left(\sum a_v X^v\right) \cdot \left(\sum b_v X^v\right) = \sum_{u,v} a_u b_v X^{u+v} = \sum_w \left(\sum_u a_u b_{w-u} \right) X^w.$$

The element X^0 is the unity of the algebra A and A is a module over F of rank p^n with basis $\{X^v \mid v \in V\}$.

The affine group $G_1 = AGL_1(p^n) = V \cdot GL_1(p^n)$ is a semidirect product of the abelian group V and the multiplicative group $GL_1(p^n) = \mathbb{F}_{p^n}^*$ of the field $\mathbb{F}_{p^n}$ and it acts on A:

$$\widehat{u}(X^v) = X^u \cdot X^v = X^{u+v}, \quad u \in V,$$

$$\widehat{g}(X^v) = X^{gv}, \quad g \in \mathbb{F}_{p^n}^*.$$

So V-invariant F-submodules in A are exactly ideals of F-algebra A.

G_1-invariant submodules of A are called affine invariant codes, and $GL_1(p^n)$-invariant codes in

$$A' = \{ \sum_{v \neq 0} a_v X^v \mid a_v \in F \}$$

are cyclic codes. If C is a cyclic code in A', then the extended cyclic code $\hat{C}$ is obtained by embedding:

$$\sum_{v \neq 0} a_v X^v \mapsto (-\sum_{v \neq 0} a_v) X^0 + \sum_{v \neq 0} a_v X^v.$$

We recall some facts and definitions for the case when F is a field. A cyclic code C of length $p^n - 1$ over F is an ideal in the quotient ring $F[Y]/(Y^{p^n - 1} - 1)$, and the code C is uniquely determined by its generating polynomial $f(Y)$. Let θ be a primitive element of the field $\mathbb{F}_{p^n}$. Then the set T of all numbers s, such that $0 < s \leq p^n - 1$ and $f(\theta^s) = 0$, is called the defining set of C. Note that we consider the defining set of a cyclic code in the range $0 < s \leq p^n - 1$, rather than $0 \leq s < p^n - 1$, as usually defined; this allows us later to consider 0 as an element of the defining set of the extended code.

Consider the following F-linear map of A (resp. A'):

$$\varphi_s(\sum a_\alpha X^\alpha) = \sum a_\alpha \alpha^s,$$

where $0 \leq s \leq p^n - 1$ (resp. $0 < s \leq p^n - 1$). If $C \subseteq A'$ is a cyclic code then

$$T = \{ s \mid \varphi_s(c) = 0 \ \forall c \in C \}$$

is the defining set of C. In this case $T \cup \{0\}$ can be considered as the defining set of $\hat{C}$.

For s, $0 \leq s \leq p^n - 1$, the p-adic expansion is

$$s = \sum_{i=0}^{n-1} s_i p^i, \quad (0 \leq s_i \leq p-1).$$

The partial order relation $\prec$ on $\{0, 1, \dots, p^n - 1\}$ is defined as follows:

$$\forall s, r \in \{0, 1, \dots, p^n - 1\}: \ s \prec r \Longleftrightarrow s_i \leq r_i, \ 0 \leq i \leq n-1.$$

The following result is well-known [15].

Theorem 2 *Let T be the defining set of an extended cyclic code C. Then C is affine invariant if and only if the condition $s \in T$ implies $r \in T$ for any $r \prec s$.*

The group G_1 is contained in the group $G_m = AGL_m(q) = V \cdot GL_m(q)$, where $n = mt$ and $q = p^t$ (consider $V = \mathbb{F}_{p^n}^+$ as m-dimensional space over $\mathbb{F}_q$).

Theorem 3 *Let T be the defining set of an extended cyclic code C of length p^n over a field F. Then C is invariant under G_m, $n = mt$, if and only if the following two conditions hold:*
(i) $s \in T$, $r \prec s \Rightarrow r \in T$;
(ii) $s = \sum_{i=0}^{n-1} s_i p^i \in T$ $(0 \leq s_i \leq p-1)$, $s_j > 0 \Rightarrow (s - p^j + p^{j+tl})_{\bmod p^n - 1} \in T$ *for* $l = 1, \dots, m-1$.

General situation ($AGL_m(q)$-invariant codes over the ring $\mathbb{Z}_{p^e}$ and $AGL_m(q)$-invariant lattices) was considered in [1, 3]. Note that remarkable Barnes-Wall lattices are also covered by this construction. Permutation modules for $GL_m(q)$ are studied also in [7].

5 Codes over $\mathbb{Z}_4$

In this section we consider extended cyclic codes of length 2^n over the ring $\mathbb{Z}_4$ of integers modulo 4. The ambient space will be

$$A = \left\{ \sum_{v \in V = \mathbb{F}_{2^n}} a_v X^v \mid a_v \in \mathbb{Z}_4 \right\}.$$

Let C be an extended cyclic code over $\mathbb{Z}_4$ in A (i.e. invariant under $GL_1(2^n)$). There are two canonical subcodes of C:

$$C_1 = (C + 2A)/2A \quad \text{(residue code)},$$

$$C_2 = C \cap 2A = \{c \in C \mid 2c = 0\} \quad \text{(torsion code)}.$$

They can be considered as linear codes over $\mathbb{F}_2$. We say that (T_1, T_2) is the defining set of C if T_1 and T_2 are the defining sets of C_1 and C_2 respectively. Assuming that C_i is naturally embedded in A mod 2, we have

$$C_1 \subseteq C_2, \quad T_1 \supseteq T_2.$$

We will say that a quaternary code is affine invariant if it is invariant under $AGL_1(2^n)$. We have the following theorem [1].

Theorem 4 *Let (T_1, T_2) be the defining set of an extended cyclic code $C$ of length 2^n over $\mathbb{Z}_4$. Then $C$ is affine invariant if and only if the following two properties hold:*

(i) $s \in T_d$, $r \prec s \Rightarrow r \in T_d$ *for* $d = 1, 2$;

(ii) $s = s_0 + \dots + s_i \cdot 2^i + 0 \cdot 2^{i+1} + 1 \cdot 2^{i+2} + \dots \in T_2 \Rightarrow s_0 + \dots + s_i \cdot 2^i + 1 \cdot 2^{i+1} + 0 \cdot 2^{i+2} + \dots \in T_1$.

(Subscripts and superscripts mod$n$.*)*

Now we show that all known good series of quaternary codes [10] are affine invariant. Note that if $s = s_0 \cdot 2^0 + s_1 \cdot 2^1 + \dots + s_{n-1} \cdot 2^{n-1} \in T_d$ then $s \cdot 2 \bmod (2^n - 1) = s_{n-1} \cdot 2^0 + s_0 \cdot 2^1 + \dots + s_{n-2} \cdot 2^{n-1} \in T_d$, so we will denote by $Cl(s_0, s_1, \dots, s_{n-1}) = Cl(s_0 + s_1 \cdot 2^1 + \dots + s_{n-1} \cdot 2^{n-1})$ the cyclotomic coset of the number $s = s_0 \cdot 2^0 + s_1 \cdot 2^1 + \dots + s_{n-1} \cdot 2^{n-1}$, that is, numbers $s$, $s \cdot 2 \bmod (2^n - 1)$, $s \cdot 2^2 \bmod (2^n - 1)$,..., $s \cdot 2^{n-1} \bmod (2^n - 1)$.

Preparata code is given by the defining set (T_1, T_2), where

$$T_1 = T_2 = \{Cl(0, \dots, 0), Cl(1, 0, \dots, 0)\}.$$

It is clear that conditions of Theorem 4 are satisfied, so this $\mathbb{Z}_4$-code is affine invariant. For odd $n$, the Gray image of the $\mathbb{Z}_4$-Preparata code determines binary $(2^{n+1}, 2^{2^{n+1}-2n-2}, 6)$ code. (Gray map sends elements $0, 1, 2, 3$ of $\mathbb{Z}_4$ to the binary combinations $00, 01, 11, 10$ respectively).

Kerdock code is the dual code to Preparata code, considered as $\mathbb{Z}_4$-code. It is given by the following defining set:

$$T_1 = T_2 = \{0, 1, 2, \dots, p^n - 1\} \setminus \{Cl(1, \dots, 1), Cl(0, 1, \dots, 1)\}.$$

For odd $n$, the Gray image of the $\mathbb{Z}_4$-Kerdock code is binary $(2^{n+1}, 4^n, 2^n - 2^{(n-1)/2})$ code.

Quaternary Preparata and Kerdock codes are particular cases of **quaternary Reed-Muller codes** $QRM(r, n)$, defined by

$$T_1 = T_2 = \{Cl(s_0, \dots, s_{n-1}) \mid s_0 + \dots + s_{n-1} \leq n - 1 - r\}.$$

Quaternary Reed-Muller codes are also affine invariant. Codes $QRM(n-2, n)$ and $QRM(1, n)$ are Preparata and Kerdock codes respectively. Note that $QRM(r, n)$ is a lifted Reed-Muller code, in the sense that $T_1 = T_2$ and T_1 determines binary Reed-Muller code $RM(r, n)$. Similarly one can define lifted Reed-Muller $\mathbb{Z}_{2^k}$-codes ($k \geq 3$), and lifted Generalized Reed-Muller codes for odd characteristic $p > 2$. However these codes will not be affine invariant [4].

Goethals codes are determined by the defining sets

$$T_2 = \{Cl(0, \dots, 0), Cl(1, 0, \dots, 0)\},$$

$$T_1 = T_2 \cup \{Cl(1, 1, 0, \dots, 0)\}.$$

They define binary codes with parameters $(2^{n+1}, 2^{2^{n+1}-3n-8}, 8)$.

Helleseth, **Kumar** and **Shanbhag** define a quaternary code which determines binary code with the same parameters as Goethals code:

$$T_2 = \{Cl(0, \dots, 0), Cl(1, 0, \dots, 0)\},$$

$$T_1 = T_2 \cup \{Cl(1, 0, \dots, 0, 1, 0, \dots, 0)\} = T_2 \cup Cl(2^r + 1),$$

where $(r, n) = 1$.

Goethals-Delsarte codes are defined by:

$$T_2 = \{Cl(0, \dots, 0), Cl(1, 0, \dots, 0)\},$$

$$\begin{aligned} T_1 &= T_2 \cup \{Cl(1,1,0,\ldots,0), Cl(1,0,1,0,\ldots,0), \ldots Cl(1,0,\ldots,0,1,0,\ldots,0)\} \\ &= T_2 \cup \{Cl(1+2^1), Cl(1+2^2), \ldots, Cl(1+2^r)\}, \end{aligned}$$

where $1 \leq r \leq (n-1)/2$.

Similarly, **Delsarte-Goethals** and **Calderbank-McGuire codes** are also affine invariant.

Finally, we show the connection between defining sets and parity check matrices of quaternary codes. If a quaternary code C has the defining set

$$T_2 = \{Cl(0), Cl(s_1), \ldots, Cl(s_a)\},$$

$$T_1 = T_2 \cup \{Cl(r_1), \ldots, Cl(r_b)\},$$

then the parity check matrix of the code C will be

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \xi^{s_1} & \xi^{2s_1} & \ldots & \xi^{(q-2)s_1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 1 & \xi^{s_a} & \xi^{2s_a} & \ldots & \xi^{(q-2)s_a} \\ 0 & 2 & 2\xi^{r_1} & 2\xi^{2r_1} & \ldots & 2\xi^{(q-2)r_1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 2 & 2\xi^{r_b} & 2\xi^{2r_b} & \ldots & 2\xi^{(q-2)r_b} \end{pmatrix}$$

(where $q = 2^n$ and ξ is the Teichmüller representative of a primitive generator θ of $\mathbb{F}_{2^n}$, see [10] for details).

References

[1] K. S. Abdukhalikov, Defining sets of extended cyclic codes invariant under the affine group. *J. Pure Appl. Algebra* **196** (2005), 1–19.

[2] K. S. Abdukhalikov, Unimodular hermitian lattices in dimension 13. *J. Algebra* **272** (2004), no. 1, 186–190.

[3] K. S. Abdukhalikov, Lattices invariant under the affine general linear group. *J. Algebra* **276** (2004), no. 2, 638–662.

[4] K. S. Abdukhalikov, Projective Generalized Reed-Muller Codes over p-adic Numbers and Finite Rings. In: Jungnickel, Dieter (ed.) et al., Finite fields and applications. Proceedings of the fifth international conference on finite fields and applications F_{q^5}, 1–13, University of Augsburg, Germany, August 2-6, 1999. Berlin: Springer. 1–13 (2001).

[5] K. S. Abdukhalikov, Doubly transitive groups and lattices. *J. Math. Sci. (New York)* **93** (1999), no. 6, 809– 823.

[6] K. S. Abdukhalikov, Modular permutation representations of PSL(n,p) and invariant lattices. *Mat.* Sb. **188** (1997), no. 8, 3–12. English transl. in *Sb. Math.* **188** (1997), no. 8, 1107–1117.

[7] M. Bardoe, P. Sin, The permutation modules for GL$(n+1, \mathbb{F}_q)$ acting on $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{F}_q^{n+1}$, *J. London Math. Soc.* (2) 61 (2000), no.1, 58–80.

[8] A. R. Calderbank, D. B. Wales, A global code invariant under the Higman-Sims group. *J. Algebra* **75** (1982) 233–260.

[9] P. G. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981) 1–22.

[10] R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* 40, No. 2 (1994), 301–319.

[11] C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order. *Geometriae Dedicata* **2** (1974), 425–460.

[12] G. Hiss, On the incidence matrix of the Ree unital. *Des. Codes Cryptogr.* **10** (1997), 57–62.

[13] B. Huppert, Zweifach transitive, auflösbare Permutationsgruppen. *Math. Z.* **68** (1957) 126–150.

[14] D. N. Ivanov, Orthogonal decompositions of Lie algebras of types A_{p-1} and D_n with a finite number of classes of similar invariant sublattices, *Vestnik Moskov. Univ. Ser. I Mat. Mekh* 1989, No.2, 40–43. English transl. in *Moscow Univ. Math. Bull.* 44 (1989).

[15] T. Kasami, S. Lin and W. W. Peterson, Some results on cyclic codes which are invariant under the affine group and their applications, *Inform. and Control* **11** (1967), 475–496.

[16] B. Mortimer, The modular permutation representations of the known doubly transitive groups, *Proc. London Math. Soc.* **41** (1980) 1–20.

[17] N. S. N. Sastry, P. Sin, On the doubly transitive permutation representations of $\mathrm{Sp}(2n, \mathbb{F}_2)$. *J. Algebra* **257** (2002) 509–527.

[18] P. Sin, The permutation representation of $\mathrm{Sp}(2m, \mathbb{F}_p)$ acting on the vectors of its standard module. *J. Algebra* **241** (2001), 578–591.