Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 282–286*

A family of binary completely transitive codes and distance-transitive graphs[1]

J. Rifà josep.rifa@autonoma.edu
Universitat Autònoma de Barcelona, Spain
V. A. Zinoviev zinov@iitp.ru
A.A. Kharkevich Institute for Problems of Information Transmission, Moscow, Russia

Abstract. In this paper we construct new family of binary linear completely transitive (and, therefore, completely regular) codes. The covering radius of these codes is growing with the length of the code. In particular, for any integer $\rho \geq 2$, there exist two codes in the constructed class of codes with $d = 3$, covering radius ρ and length $\binom{4}{2}^{\rho}$ and $\binom{4}{2}^{\rho+2}$, respectively. These new completely transitive codes induce as coset graphs a family of distance-transitive graphs of growing diameter.

1 Introduction

We use the standard notation $[n, k, d]$ for a binary linear code C of length n, dimension k and minimum distance d. The automorphism group $\mathrm{Aut}(C)$ coincides with the subgroup of the symmetric group S_n consisting of all $n!$ permutations of the n coordinate positions which send C into itself.

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 $\rho = \max_{\mathbf{v}\in\mathbb{F}_q^n}\{d(\mathbf{v}, C)\}$.

For a given code C with covering radius $\rho = \rho(C)$ define

$$C(i) \;=\; \{\mathbf{x} \in \mathbb{F}_q^n :\; d(\mathbf{x}, C) = i\}, \quad i = 1, 2, ..., \rho.$$

Definition 1. *A code C with covering radius $\rho = \rho(C)$ is completely regular, if for all $l \geq 0$ every vector $x \in C(l)$ 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 $c_0 = b_\rho = 0$. Define the intersection array of C as $(b_0, \ldots, b_{\rho-1}; c_1, \ldots, c_\rho)$.*

Definition 2. [9] *A linear code C with covering radius $\rho = \rho(C)$ and automorphism group $\mathrm{Aut}(C)$ is completely transitive, if the set of all cosets of C is partitioned into $\rho + 1$ orbits under the action of $\mathrm{Aut}(C)$, where for any $\mathbf{x} \in \mathbb{F}_2^n$ and $\varphi \in \mathrm{Aut}(C)$ the group acts on a coset $\mathbf{x} + C$ as $\varphi(\mathbf{x} + C) \;=\; \varphi(\mathbf{x}) + C$.*

[1]This work has been partially supported by the Spanish MICINN grants MTM2009-08435; PCI2006-A7-0616; the catalan grant 2009SGR1224 and also by the Russian fund of fundamental researches 12 - 01 - 00905-a.

Let Γ be a finite connected simple (i.e. undirected, without loops and multiple edges) graph. Let $d(\gamma,\delta)$ be the distance between two vertices γ and δ. Denote $\Gamma_i(\gamma) = \{\delta \in \Gamma : d(\gamma,\delta) = i\}$.

Two vertices γ and δ from Γ are *neighbors* if $d(\gamma,\delta) = 1$. An *automorphism* of a graph Γ is a permutation π of the vertex set of Γ such that, for all $\gamma,\delta \in \Gamma$ we have $d(\gamma,\delta) = 1$, if and only if $d(\pi\gamma,\pi\delta) = 1$. Let Γ_i be a subgraph of Γ with the same vertices, where an edge (γ,δ) is defined when the vertices γ,δ are at distance i in Γ. The graph Γ is called *primitive* if it is connected and and all Γ_i $(i = 1,\ldots,D)$ are connected, and *imprimitive* otherwise.

Definition 3. [3] *A simple connected graph Γ is called* distance-regular*, if it is regular of valency k, and if for any two vertices $\gamma,\delta \in \Gamma$ at distance i apart, there are precisely c_i neighbors of δ in $\Gamma_{i-1}(\gamma)$ and b_i neighbors of δ in $\Gamma_{i+1}(\gamma)$. Furthermore, this graph is called* distance transitive*, if for any pair of vertices γ,δ at distance $d(\gamma,\delta)$ there is an automorphism π from $\mathrm{Aut}(\Gamma)$ which move this pair to any other given pair γ',δ' of vertices at the same distance $d(\gamma,\delta) = d(\gamma',\delta')$.*

Completely regular and completely transitive codes are classical subjects in algebraic coding theory, which are closely connected with graph theory, combinatorial designs and algebraic combinatorics. Existence and enumeration of all such codes are open hard problems (see [3, 4, 6] and references there).

This paper is a natural continuation of our previous paper [7], where we describe a wide class of new binary linear completely regular and completely transitive codes for which the covering radius is growing with the length of the code. The parameters of the main family of the codes depend only on one integer parameter $m \geq 4$. The resulting code C has length $n = \binom{m}{2}$, the number of information symbols is $k = n - m + 1$, the minimum distance is 3 and the covering radius is $\rho = \lfloor m/2 \rfloor$. A half of these codes are non-antipodal and this implies (using [2]), that the covering set $C(\rho)$ of C is a coset of C. In this case the union $C \cup C(\rho)$ gives also a completely regular and completely transitive code. Our purpose here is to describe the resulting completely transitive codes. We give as a corollary of existing linear completely transitive codes, an infinite family of distance-transitive coset graphs with growing diameter.

2 Preliminary results

Let C be a linear completely regular code with covering radius ρ and intersection array $(b_0,\ldots,b_{\rho-1};c_1,\ldots c_\rho)$. Let $\{D\}$ be a set of cosets of C. Define the graph Γ_C (which is called the *coset graph of* C, taking all cosets $D = C+\mathbf{x}$ as vertices, with two vertices $\gamma = \gamma(D)$ and $\gamma' = \gamma(D')$ adjacent, if and only if the cosets

D and D' contains neighbor vertices, i.e. $\mathbf{v} \in D$ and $\mathbf{v}' \in D'$ with distance $d(\mathbf{v}, \mathbf{v}') = 1$.

Lemma 4. [3,8]. *Let C be a linear completely regular code with covering radius ρ and intersection array $(b_0, \ldots, b_{\rho-1}; c_1, \ldots c_\rho)$ and let Γ_C be the coset graph of C. Then Γ_C is distance-regular of diameter ρ with the same intersection array. If C is completely transitive, then Γ_C is distance-transitive.*

Lemma 5. [6] *Let C be a completely regular code with covering radius ρ and intersection array $(b_0, \ldots, b_{\rho-1}; c_1, \ldots c_\rho)$. Then $C(\rho)$ is a completely regular code too, with intersection array $(c_\rho, \ldots, c_1; b_{\rho-1}, \ldots b_0)$.*

3 Main results

We start by defining a specific class of binary linear codes. For a given natural number m where $m \geq 3$ denote by E_2^m the set of all binary vectors of length m and weight 2.

Definition 6. *Let H_m be the binary matrix of size $m \times m(m-1)/2$, whose columns are exactly all the vectors from E_2^m (i.e. each vector from E_2^m occurs once as a column of H_m). Now define the binary linear code $C^{(m)}$ whose parity check matrix is the matrix H_m.*

Theorem 7. [7] *Let m be a natural number, $m \geq 3$.*
(i) The binary linear $[n, k, d]$ code $C = C^{(m)}$ has parameters: $n = \binom{m}{\ell}$, $k = n - m + 1$, $d = 3$, $\rho = \lfloor \frac{m}{2} \rfloor$. (ii) Code $C^{(m)}$ is completely transitive and, therefore, completely regular. The intersection numbers of $C^{(m)}$ for $i = 0, \ldots, \rho$ are: $b_i = \binom{m-2i}{2}$, $c_i = \binom{2i}{2}$.
(iii) Code $C^{(m)}$ is antipodal if m is odd and non-antipodal if m is even.

Since for even m the code $C^{(m)}$ is non-antipodal, its covering set $C^{(m)}(\rho)$ is a translate of $C^{(m)}$ [2]. Hence, it makes sense to consider the new (linear) code $C^{[m]} = C^{(m)} \cup C^{(m)}(\rho)$. The generating matrix $G^{[m]}$ of this code has a very symmetric structure:

$$G^{[m]} = \left[\begin{array}{c|c} I_{k-1} & H^t_{m-1} \\ \hline 0 \ldots 0 & 1 \ldots 1 \end{array}\right].$$

Using Lemma 5 and the fact that $C^{(m)}(\rho) = C^{(m)} + (1, 1, \ldots, 1)$, we obtain the following result.

Theorem 8. *Let m be even, $m \geq 6$ and let $C^{[m]} = C^{(m)} \cup C^{(m)}(\rho)$. Then:*

- *Code* $C^{[m]}$ *is completely regular linear* $[n, k, d]$ *code with parameters* $n = m(m-1)/2$, $k = n - m + 2$, $d = 3$, $\rho = \lfloor m/4 \rfloor$.
- *The intersection numbers of* $C^{[m]}$ *for* $m \equiv 0 \pmod 4$ *and* $\rho = m/4$ *are* $b_i = \binom{m-2i}{2}$ *and* $c_i = \binom{2i}{2}$ *for* $i = 0, 1, \ldots, \rho - 1$, $c_\rho = 2\binom{2\rho}{2}$, *and, for* $m \equiv 2 \pmod 4$ *and* $\rho = (m-2)/4$, *are* $b_i = \binom{m-2i}{2}$ *for and* $c_i = \binom{2i}{2}$ *for* $i = 0, 1, \ldots, \rho$.
- *Code* $C^{[m]}$ *is completely transitive.*

We note that the extension of the code $C^{[m]}$ (i.e. adding one more overall parity checking position) is not uniformly packed in the wide sense (see [1] for the definition of this concept), and therefore, it is not completely regular.

Denote by $\Gamma^{(m)}$ (respectively, $\Gamma^{[m]}$) the coset graph, obtained from code $C^{(m)}$ (respectively, $C^{[m]}$). From Theorems 7 and 8 we obtain the following results.

Theorem 9.

- *For any even* $m \geq 6$ *there exist two embedded double covers* $\Gamma^{(m)}$ *and* $\Gamma^{[m]}$ *of complete graph* K_n, $n = \binom{m}{2}$, *on* 2^{m-1} *and* 2^{m-2} *vertices, respectively, and with covering radius* $m/2$ *and* $\lfloor m/4 \rfloor$, *respectively.*
- *The intersection arrays of graphs* $\Gamma^{(m)}$ *and* $\Gamma^{[m]}$ *are the same as those of the respective codes, given by Theorems 7 and 8.*
- *Both graphs* $\Gamma^{(m)}$ *and* $\Gamma^{[m]}$ *are distance transitive.*
- *The graphs* $\Gamma^{(m)}$ *are imprimitive and the graphs* $\Gamma^{[m]}$ *are primitive.*
- *The graph* $\Gamma^{[m]}$ *has eigenvalues* $\{\binom{m}{2} - 8i(2\rho + 1 - i),\ i = 0, 1, \ldots, \rho\}$ *for* $m \equiv 2 \pmod 4$ *and* $\{\binom{m}{2} - 8i(2\rho - i),\ i = 0, 1, \ldots, \rho\}$ *for* $m \equiv 0 \pmod 4$.

The graph $\Gamma^{(m)}$ is well known. It can be obtained from the even weight binary vectors of length m, adjacent when their distance is 2. It is the halved m-cube and is a distance-transitive graph, uniquely defined from its intersection array [3, p. 264]. Since the graph $\Gamma^{(m)}$ is antipodal, the graph $\Gamma^{[m]}$ (which has twice less vertices) can be seen as its folded graph, obtained by collapsing antipodal pairs of vertices.

References

[1] L.A. Bassalygo, G.V. Zaitsev & V.A. Zinoviev, "Uniformly packed codes," *Problems Inform. Transmiss.,* vol. 10, no. 1, pp. 9-14, 1974.

[2] J. Borges, J. Rifa & V.A. Zinoviev, "On non-antipodal binary completely regular codes", *Discrete Mathematics*, 2008, vol. 308, 3508 - 3525.

[3] A.E. Brouwer, A.M. Cohen & A. Neumaier, *Distance-Regular Graphs*, Springer, Berlin, 1989.

[4] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Reports Supplements, vol. 10, 1973.

[5] D.G. Fon-Der-Flaass, "Perfect 2-coloring of hypercube", *Siberian Math. J.*, 2007, vol. 48, pp. 923-930.

[6] A. Neumaier, "Completely regular codes," *Discrete Maths.*, vol. 106/107, pp. 335-360, 1992.

[7] J. Rifà & V.A. Zinoviev, "On a class of binary linear completely transitive codes with arbitrary covering radius", *Discrete Mathematics*, 2009, vol. 309, pp. 5011 - 5016.

[8] J. Rifà, J. Pujol, "Completely transitive codes and distance transitive graphs," *Proc, 9th International Conference, AAECC-9*, no. 539 LNCS, 360-367, Springer-Verlag, 1991.

[9] P. Solé, "Completely Regular Codes and Completely Transitive Codes," *Discrete Maths.*, vol. 81, pp. 193-201, 1990.