Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 85–90*

On nested completely regular codes and distance regular graphs[1]

J. Borges quim@deic.uab.cat
J. Rifà josep.rifa@autonoma.edu
Department of Information and Communications Engineering, Autonomous University of Barcelona, Spain
V. A. Zinoviev zinov@iitp.ru
A.A. Kharkevich Institute for Problems of Information Transmission, Moscow, Russia

Abstract. Infinite families of linear binary nested completely regular codes with covering radius ρ equal to 3 and 4 are constructed. In the usual way, i.e., as coset graphs, infinite families of embedded distance-regular coset graphs of diameter $D = 3$ or 4 are constructed. In some cases, the constructed codes are also completely transitive codes and the corresponding coset graphs are distance-transitive.

1 Introduction

Let $\mathbb{F}_q$ be the finite field of order $q \geq 2$ and C be a binary linear $[n, k, d]$ code of length n, dimension k and minimum distance d. The automorphism group $\mathrm{Aut}(C)$ of C consists of all permutations of the n coordinate positions which send C into itself. $\mathrm{Aut}(C)$ acts in a natural way over the set of cosets of C: $\pi(C + \boldsymbol{v}) = C + \pi(\boldsymbol{v})$ for every $\boldsymbol{v} \in \mathbb{F}_2^n$ and $\pi \in \mathrm{Aut}(C)$.

For any $\boldsymbol{v} \in \mathbb{F}_2^n$ its *distance* to the code C is $d(\boldsymbol{v}, C) = \min_{\boldsymbol{x} \in C}\{d(\boldsymbol{v}, \boldsymbol{x})\}$ and the *covering radius* of the code C is $\rho = \max_{\boldsymbol{v} \in \mathbb{F}_2^n}\{d(\boldsymbol{v}, C)\}$. Let $J = \{1, 2, \ldots, n\}$ be the set of coordinate positions of vectors from $\mathbb{F}_2^n$. Denote by $\mathrm{Supp}(\boldsymbol{x})$ the *support* of the vector $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, i.e., $\mathrm{Supp}(\boldsymbol{x}) = \{j \in J : x_j \neq 0\}$. Say that two vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^n$ are *neighbors* if $d(\boldsymbol{x}, \boldsymbol{y}) = 1$ and also say that vector $\boldsymbol{x}$ *covers* vector $\boldsymbol{y}$ if $\mathrm{Supp}(\boldsymbol{y}) \subseteq \mathrm{Supp}(\boldsymbol{x})$.

For a given binary code C such that $\mathbf{0} \in C$ and with covering radius ρ define $C(i) = \{\boldsymbol{x} \in \mathbb{F}_2^n : d(\boldsymbol{x}, C) = i\}$, $i = 1, 2, \ldots, \rho$.

Definition 1. *A code C with covering radius ρ 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 $a_l = (q-1)n - b_l - c_l$ and note that $c_0 = b_\rho = 0$.*

For a completely regular code, define $(b_0, \ldots, b_{\rho-1}; c_1, \ldots, c_\rho)$ as the intersection array of C.

[1]This work has been partially supported by the Spanish MICINN grant TIN2013-40524-P and the Catalan AGAUR grant 2014SGR-691 and by the Russian fund of fundamental researches (under the project No. 12-01-00905).

Definition 2. [8] *A binary linear code C with covering radius ρ is completely transitive if* $\mathrm{Aut}(C)$ *has $\rho+1$ orbits when acts on the cosets of C.*

Clearly any completely transitive code is completely regular.

Existence and enumeration of completely regular and completely transitive codes are open hard problems (see [3, 6, 8] and references there). The purpose of this paper is to construct nested infinite families of completely regular codes with covering radius ρ equal to 3 and 4. When m is growing the length of the chain of these nested codes (with constant covering radius) is also growing. For length $n = 2^m - 1$, where $m = 2u$, each family is formed by u nested completely regular codes of length n with the same covering radius $\rho = 3$. The last code in the nested family, so the code with the smallest cardinality is a $1/2^u$-th part of a Hamming code of length n. These last codes are known to be completely regular codes due to Calderbank and Goethals [4]. These nested families of completely regular codes and their extended codes induces infinite families of embedded distance-regular coset graphs with diameters 3 and 4, which also give interesting families of embedded covering graphs. We point out that in some cases such completely regular codes are also completely transitive and hence the corresponding coset graphs are also distance transitive.

2 Preliminary results

Let Γ be a finite connected simple graph (i.e., undirected, without loops and multiple edges). Let $d(\gamma,\delta)$ be the distance between two vertices γ and δ (i.e., the number of edges in the minimal path between γ and δ). The *diameter* D of Γ is its largest distance. Two vertices γ and δ from Γ are *neighbors* if $d(\gamma,\delta)=1$. Denote $\Gamma_i(\gamma) = \{\delta \in \Gamma : \ d(\gamma,\delta) = i\}$.

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 the graph with the same vertices of Γ, where an edge (γ,δ) is defined when the vertices γ,δ are at distance i in Γ. Clearly, $\Gamma_1 = \Gamma$. The graph Γ is called *primitive* if Γ and all Γ_i $(i = 2,\dots,D)$ are connected. Otherwise, Γ is called *imprimitive*. A graph is called *complete* (or a *clique*) if any two of its vertices are adjacent.

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 (γ,δ) to any other given pair γ',δ' of vertices at the same distance $d(\gamma,\delta) = d(\gamma',\delta')$.*

The sequence $(b_0, b_1, \dots, b_{D-1}; c_1, c_2, \dots, c_D)$, where D is the diameter of Γ, is called the *intersection array* of Γ. Clearly $b_0 = k$, $b_D = c_0 = 0$, $c_1 = 1$.

Let C be a linear completely regular code with covering radius ρ and intersection array $(b_0, \dots, b_{\rho-1}; c_1, \dots c_\rho)$. Let $\{B\}$ be the set of cosets of C. Define the graph Γ_C, which is called the *coset graph of* C, taking all different cosets $B = C + \mathbf{x}$ as vertices, with two vertices $\gamma = \gamma(B)$ and $\gamma' = \gamma(B')$ adjacent, if and only if the cosets B and B' contain neighbor vectors, i.e., there are $\mathbf{v} \in B$ and $\mathbf{v}' \in B'$ such that $d(\mathbf{v}, \mathbf{v}') = 1$.

Lemma 1. [3, 7] *Let C be a linear completely regular code with covering radius ρ and intersection array $(b_0, \dots, b_{\rho-1}; c_1, \dots c_\rho)$ and let Γ_C be the coset graph of C. Then Γ_C is distance-regular of diameter $D = \rho$ with the same intersection array as the code C. If C is completely transitive, then Γ_C is distance-transitive.*

Given a code C with $d = 2e + 1$, denote by C^* the extended code, i.e., the code obtained from C by adding an overall parity checking position. Now we give a lemma, which is an strengthening of a result from [1].

Lemma 2. *Let C be a completely regular linear code of length $n = 2^m - 1$ with minimum distance $d = 3$, covering radius $\rho = 3$ and intersection array $(n, b_1, 1; 1, c_2, n)$. Let the orthogonal code $C^\perp$ have nonzero weights w_i, $i = 1, 2, 3$. Then the extended code C^* is completely regular with covering radius $\rho^* = 4$ and intersection array $(n+1, n, b_1, 1; 1, c_2, n, n+1)$, if and only if $w_1 + w_3 = 2w_2 = n + 1$.*

3 Completely regular nested codes

Present the elements of $\mathbb{F}_{2^m}$ as elements in a quadratic extension of $\mathbb{F}_{2^u}$. Let $\beta = \alpha^r$ be a primitive element of $\mathbb{F}_{2^u}$ and let $\mathbb{F}_{2^m} = \mathbb{F}_{2^u}[\alpha]$. Every element $\gamma \in \mathbb{F}_{2^m}$ can be presented as $\gamma = \gamma_1 + \gamma_2\alpha \in \mathbb{F}_{2^u}[\alpha]$, where $\gamma_1, \gamma_2 \in \mathbb{F}_{2^u}$. The parity check matrix of the Hamming code $\mathcal{H}_m$ of length $n = 2^m - 1$, which we denote by H_m, can also be written as the binary matrix of size $(2u \times n)$, where the columns are binary presentations of $[\gamma_i, \gamma_j]$ with $\gamma_i, \gamma_j \in \{0, \beta^1, \dots, \beta^{q-1}\}$.

Let E_m be the binary representation of the matrix $[\alpha^{0r}, \alpha^r, \dots, \alpha^{(n-1)r}]$. Take the matrix P_m as the vertical join of H_m and E_m. It is well known [4] that the code $C^{(u)}$ with parity check matrix P_m is a cyclic binary completely regular code with covering radius $\rho = 3$, minimum distance $d = 3$ and dimension $n - (m + u)$. The generator polynomial of $C^{(u)}$ is $g(x) = m_\alpha(x)m_{\alpha^r}(x) \in \mathbb{F}_2[x]$, where $m_{\alpha^i}(x)$ means the minimal polynomial associated to α^i.

Denote by $\boldsymbol{e}_i$ the vector with only one nonzero coordinate of value 1 in ith position. Binary vectors $\boldsymbol{v} \in \mathbb{F}_2^n$ can be written as $\boldsymbol{v} = \sum_{i \in I_{\boldsymbol{v}}} \boldsymbol{e}_i$, where $I_{\boldsymbol{v}} = \mathrm{Supp}(\boldsymbol{v})$. The elements in $\mathbb{F}_{2^m}$ can also be seen as elements in $\mathbb{F}_{2^u}[\alpha]$. The positions of vectors in $\mathbb{F}_2^n$ can be enumerated by using the nonzero elements in $\mathbb{F}_{2^m}$, or as elements in $\mathbb{F}_{2^u}[\alpha]$ by substituting any $\alpha^i \in \mathbb{F}_{2^m}$ with the corresponding $\alpha^i = \gamma_{i1} + \gamma_{i2}\alpha \in \mathbb{F}_{2^u}[\alpha]$, where $\gamma_{i1}, \gamma_{i2} \in \mathbb{F}_{2^u}$.

For any $\boldsymbol{v} = \sum_{i \in I_{\boldsymbol{v}}} \boldsymbol{e}_i \in \mathbb{F}_2^n$, denote $S(\boldsymbol{v}) = \sum_{i \in I_{\boldsymbol{v}}} \gamma_{i1}\gamma_{i2} \in \mathbb{F}_{2^u}$. The next lemma gives a new description for the code $C^{(u)}$.

Lemma 3. *The code $C^{(u)}$ consists of elements $\boldsymbol{v} \in \mathbb{F}_2^n$, with syndromes $H_m \boldsymbol{v}^T = 0$ and $S(\boldsymbol{v}) = 0$.*

The code $C^{(u)}$ is a binary $[n = 2^m - 1, k = n - m - u]$ code and it is a subcode of the $[2^m - 1, n - m]$ Hamming code $\mathcal{H}_m$. The number of cosets $C^{(u)} + \boldsymbol{v}$, of weight three, is $2^u - 1$. Indeed, their syndromes $S(\boldsymbol{v})$ are the nonzero elements of $\mathbb{F}_{2^u}$. For $i \in \{0, \ldots, u\}$, taking $u - i$ cosets $C^{(u)} + \boldsymbol{v}_1, \ldots, C^{(u)} + \boldsymbol{v}_{u-i}$ with independent syndromes $S(\boldsymbol{v}_1), \ldots, S(\boldsymbol{v}_{u-i})$ (independent, means that they are independent binary vectors in $\mathbb{F}_2^u$) we can generate a linear binary code $C^{(i)} = \langle C^{(u)}, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{u-i} \rangle$.

The dimension of the code $C^{(u)}$ is $\dim(C^{(u)}) = n - m - u$ and, in general, $\dim(C^{(i)}) = u - i + \dim(C^{(u)})$. Note that the maximum number of independent syndromes we can take is u, so the biggest code we can obtain is of dimension $u + \dim(C^{(u)}) = n - m$, which is the Hamming code $C^{(0)} = \mathcal{H}_m$. All the constructed codes contains $C^{(u)}$ and they are contained in the Hamming code $C^{(0)}$.

Theorem 1. *Let $i \in \{0, 1, u\}$ for $m = 2u \geq 8$ and $i \in \{0, 1, 2, 3\}$ for $m = 6$. The codes $C^{(i)}$ and $C^{(i)*}$ are completely transitive.*

We conjecture that codes $C^{(i)}$ and $C^{(i)*}$ are completely transitive if and only if $i = 0, i = 1, i = u$ or $2^i \leq u + 1$, for $i \in \{2, \ldots, u - 1\}$.

Theorem 2. *Let $i \in \{0, \ldots, u\}$ and $m = 2u$. The codes $C^{(i)}$ and $C^{(i)*}$ are completely regular with intersection arrays $(2^m - 1, 2^m - 2^{m-i}, 1; 1, 2^{m-i}, 2^m - 1)$ and $(2^m, 2^m - 1, 2^m - 2^{m-i}, 1; 1, 2^{m-i}, 2^m - 1, 2^m)$, respectively.*

4 Nested antipodal distance regular graphs of diameter 3 and 4

A graph Γ with diameter $D \geq 3$ is called *antipodal* if all vertices at distance D from a given vertex are at distance D from each other [3], i.e., graph Γ_D is a disjoint union of cliques. Such a graph is imprimitive by definition. In this case, the *folded graph, or antipodal quotient* of Γ is defined as the graph $\bar{\Gamma}$, whose vertices are the maximal cliques (which are called *fibres*) of Γ_D, with two adjacent if and only if there is an edge between them in Γ. If, in addition, each vertex γ has the same valency as its image under folding, then Γ is called an *antipodal covering graph* of $\bar{\Gamma}$. If, moreover, all fibres of Γ_D have the same size r, then Γ is also called an *antipodal r-cover* of $\bar{\Gamma}$.

Denote by $\Gamma^{(i)}$ (respectively, $\Gamma^{(i)*}$) the coset graph, obtained from the code $C^{(i)}$ (respectively $C^{(i)*}$). Since all cosets of weight 3 (respectively, of weight 4) of the Hamming code $\mathcal{H}_m$ (respectively, of the extended Hamming code $\mathcal{H}_m^*$) belong to this code, we conclude that all graphs $\Gamma^{(i)}$ (respectively, $\Gamma^{(i)*}$) are antipodal.

Lemma 4. [5] *Let Γ be an antipodal distance-regular graph of diameter three. Then Γ is a r-fold covering graph of K_n, for some r and n and recall that c_2 is the number of common neighbors of two vertices in Γ at distance two. Then the intersection array of Γ is $(n-1,(r-1)c_2,1;1,c_2,n-1)$.*

As a direct result of Theorem 2 and taking into account [5, 7] we obtain the following new distance-regular and distance-transitive coset graphs.

Theorem 3. *For any $m=2u\geq 4$, there exist a family of embedded antipodal distance-regular coset graphs $\Gamma^{(i)}$ with 2^{2u+i} vertices and diameter 3, for $i=1,\ldots,u$. Graph $\Gamma^{(0)}$ has diameter 1, i.e., it is a complete graph $K_n, n=2^m-1$. Specifically:*
(i) $\Gamma^{(i)}$, $i=1,\ldots,u$ *has intersection array* $(2^m-1,2^m-2^{m-i},1;1,2^{m-i},2^m-1)$.
(ii) $\Gamma^{(i)}$ *is a subgraph of* $\Gamma^{(i+1)}$ *for all* $i=0,1,\ldots,u-1$.
(iii) $\Gamma^{(i)}$ *covers* $\Gamma^{(j)}$ *with parameters* $(2^m-1,2^{i-j},2^{2u-i+j})$, *for* $j\in\{0,...,i-1\}$.
(iv) $\Gamma^{(i)}$ *is distance-transitive for* $i\in\{0,1,u\}$ *when* $m\geq 8$ *and for* $i\in\{0,1,2,3\}$ *when* $m=6$.

Theorem 4. *For any $m=2u\geq 4$ and $i=0,1,\ldots,u$ there exist a family of embedded antipodal distance-regular coset graphs $\Gamma^{(i)*}$ with 2^{m+i+1} vertices and diameter 4. Specifically:*
(i) $\Gamma^{(i)*}$ *has intersection array* $(2^m,2^m-1,2^m-2^{m-i},1;1,2^{m-i},2^m-1,2^m)$.
(ii) $\Gamma^{(i)*}$ *is a subgraph of* $\Gamma^{(i+1)*}$ *for all* $i=0,1,\ldots,u-1$.
(iii) $\Gamma^{(i)*}$ *covers* $\Gamma^{(j)*}$, *where* $j=0,1,\ldots,i-1$ *with the size of the fibre* $r_{i,j}=2^{i-j}$.
(iv) $\Gamma^{(i)*}$ *is distance-transitive for* $i=0,1,u$ *when* $m\geq 8$ *and* $i=0,1,2,3$ *when* $m=6$.

We conjecture that the graphs $\Gamma^{(i)}$ and $\Gamma^{(i)*}$ are distance-transitive for $i\in\{2,\ldots,u-1\}$ and $2^i\leq u+1$.

The first graphs $\Gamma^{(1)}$ and $\Gamma^{(1)*}$ are well known distance-transitive graphs (see [1, 2] and references there). Graphs $\Gamma^{(u)}$ and $\Gamma^{(u)*}$ are also known. The corresponding codes $C^{(u)}$ and $C^{(u)*}$ have been presented in a very symmetric form by Calderbank and Goethals [4]. They proved that these codes form association schemes, which immediately implies the existence of the corresponding distance-regular graphs $\Gamma^{(u)}$ and $\Gamma^{(u)*}$ [3, Ch. 11]. All graphs $\Gamma^{(i)}$ for $i=0,1,\ldots,u$ have been constructed by Godsil and Hensel using the Quotient Construction [5]. But it was not mentioned in all references above that some

of these graphs are completely transitive. Besides, except for the graphs $\Gamma^{(u)}$, it was not stated that these graphs can be constructed as coset graphs. We could not found the graphs $\Gamma^{(i)*}$ for $i = 2, \ldots, u-1$ in the above mentioned literature.

References

[1] J. Borges, J. Rifa, V.A. Zinoviev, "New families of completely regular codes and their corresponding distance regular coset graphs", *Designs, Codes and Cryptography*, (2014), vol.70, pp:139-148. DOI 10.1007/s10623-012-9713-3.

[2] J. Borges, J. Rifa, V.A. Zinoviev, "New families of completely transitive codes", *Discrete Mathematics*, 2014, to appear.

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

[4] A.M. Calderbank, J.-M. Goethals, *Three-weights codes and association schemes*, Philips J. Res., vol. 39, 143-152, 1984.

[5] C.D. Godsil, A.D. Hensel, "Distance regular covers of the complete graph", *J. Comb. Theory, Ser. B*, 1992, vol. 56, 205 - 238.

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

[7] 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.

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