

Families of completely transitive codes and distance transitive graphs

J. Borges^a, J. Rifà^a, V. A. Zinoviev^b

^a*Dept. of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain.*

Email: {joaquin.borges, josep.rifa}@uab.cat. Tel. +34935811470.

^b*V. Zinoviev is with the Institute for Problems of Information Transmission, Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 127994, Russia.*

Email: zinov@iitp.ru

Abstract

In a previous work, the authors found new families of linear binary completely regular codes with the covering radius $\rho = 3$ and $\rho = 4$. In this paper, the automorphism groups of such codes are computed and it is proven that the codes are not only completely regular, but also completely transitive. From these completely transitive codes, in the usual way, i.e., as coset graphs, new presentations of infinite families of distance transitive coset graphs of diameter three and four, respectively, are constructed.

Keywords: Completely regular codes, completely transitive codes, distance regular graphs, distance transitive graphs

2000 MSC: 94B60, 94B25

1. Introduction

In a recent paper [1] we described completely regular codes which are halves of a binary Hamming code, obtained by adding one row to the parity check matrix of a Hamming code. As a result we obtained three new infinite

families of linear binary completely regular codes with covering radius $\rho = 3$ and 4.

This paper is an addendum to [1] and the purpose is to prove that all completely regular codes constructed in [1] are completely transitive. This is proved in Section 2. In the usual way, i.e., as coset graphs, we will see that new infinite families of completely transitive codes induce new presentations of infinite families of distance transitive coset graphs of diameter three and four. For the basic definitions and notation on completely regular codes and distance regular graphs we refer to [1].

2. Completely transitive codes and distance transitive graphs

For a binary code C , we denote by $\text{Aut}(C)$ the group of coordinate permutations that leaves C invariant.

Definition 2.1. [3, 7] *A binary linear code C with covering radius ρ is completely transitive if $\text{Aut}(C)$ has $\rho + 1$ orbits when acts on the cosets of C .*

Since two cosets in the same orbit should have the same weight distribution, it is clear that any completely transitive code is completely regular [7].

Definition 2.2. [2] *A connected graph Γ of diameter d is distance transitive if it admits an automorphism group which is transitive on each of the sets $\{(\gamma, \delta) \mid d(\gamma, \delta) = i\}$ for $0 \leq i \leq d$.*

A distance transitive graph is also distance regular [2].

Let H_m denote the parity check matrix of the Hamming code \mathcal{H}_m of length $n = 2^m - 1$, where the column \mathbf{h}_i of H_m is the binary representation of α^i , $i = 0, 1, \dots, n - 1$, through the polynomial base $\alpha^0, \alpha^1, \dots, \alpha^{n-1}$, where

α is a primitive element of the finite field \mathbb{F}_{2^m} . For a given even $m \geq 4$ and any $i_1, i_2 \in \{0, 1, 2, 3\}$, where $i_1 \neq i_2$, denote by $\mathbf{v}_{i_1, i_2} = (v_0, v_1, \dots, v_{n-1})$ the binary vector whose i -th position v_i is a function of the weight of the column \mathbf{h}_i :

$$v_i = \begin{cases} 1, & \text{if } \text{wt}(\mathbf{h}_i) \equiv i_1 \text{ or } i_2 \pmod{4}, \\ 0, & \text{otherwise.} \end{cases} \quad (1)$$

Let \mathbb{F} be the binary field. The vector \mathbf{v}_{i_1, i_2} can be seen as a boolean function f_{i_1, i_2} over $\mathbb{F}^m \setminus \{\mathbf{0}\}$, where:

$$f_{i_1, i_2}(\mathbf{x}) = \begin{cases} 1, & \text{if } \text{wt}(\mathbf{x}) \equiv i_1 \text{ or } i_2 \pmod{4} \\ 0, & \text{otherwise.} \end{cases}$$

It is well known [4] that the automorphism group $\text{Aut}(\mathcal{H}_m)$ of the Hamming code is isomorphic to the general linear group $GL(m, 2)$ of all the $m \times m$ nonsingular matrices over \mathbb{F} . This group $\text{Aut}(\mathcal{H}_m)$ acts 2-transitively over the set of coordinate positions (or columns of H_m) and has more powerful transitivity properties. It is well known, for example, that given any pair of ordered sets of m positions (corresponding to independent column vectors in H_m), there exists a permutation in $\text{Aut}(\mathcal{H}_m)$ moving one set to the other one.

Theorem 2.1. *Assume that $i_1 - i_2 \equiv 1 \pmod{2}$ and let H_m be the parity check matrix of the Hamming $[n, n - m, 3]$ code \mathcal{H}_m of length $n = 2^m - 1$, where m is even, and let $H_m(\mathbf{v}_{i_1, i_2})$ be obtained from H_m by adding one more row \mathbf{v}_{i_1, i_2} given by (1). Let $\mathcal{C} = \mathcal{C}_{i_1, i_2}$ be the $[n, n - m - 1, 3]$ code with the parity check matrix $H_m(\mathbf{v}_{i_1, i_2})$. Then, the group $\text{Aut}(\mathcal{C})$ coincides with the symplectic group $\text{Sp}(m, 2)$.*

Proof: In [6, Th. 2.2] it was proved that for any even m , $m \geq 4$, the function f_{i_1, i_2} is quadratic for $i_1 - i_2 \equiv 1 \pmod{2}$. In these cases we have:

$$\begin{aligned}
f_{2,3}(\mathbf{x}) &= \mathbf{x}Q\mathbf{x}^T, \\
f_{1,2}(\mathbf{x}) &= \mathbf{x}Q\mathbf{x}^T + L\mathbf{x}^T, \\
f_{0,1}(\mathbf{x}) &= \mathbf{x}Q\mathbf{x}^T + \epsilon, \\
f_{0,3}(\mathbf{x}) &= \mathbf{x}Q\mathbf{x}^T + L\mathbf{x}^T + \epsilon,
\end{aligned} \tag{2}$$

where Q is the all-one upper triangular binary $m \times m$ matrix with zeroes in the diagonal, L is the all-one binary vector of length m , $\epsilon = 1$ and $\mathbf{x} \in \mathbb{F}^m$.

Associated to f_{i_1, i_2} there is a symplectic form [4, Ch. 15. §2] defined by:

$$\mathcal{B}(\mathbf{u}, \mathbf{v}) = f_{i_1, i_2}(\mathbf{u} + \mathbf{v}) + f_{i_1, i_2}(\mathbf{u}) + f_{i_1, i_2}(\mathbf{v}) + \epsilon, \tag{3}$$

where $\mathbf{u}, \mathbf{v} \in \mathbb{F}^m$ and $\epsilon = 1$ or $\epsilon = 0$ when $0 \in \{i_1, i_2\}$ or $0 \notin \{i_1, i_2\}$, respectively.

From [4] we know that, $\text{Aut}(\mathcal{C}) = \text{Aut}(\mathcal{C}^\perp)$ and so, a permutation of the coordinate positions represented by the $n \times n$ matrix P is in $\text{Aut}(\mathcal{C})$ if and only if $H_m(\mathbf{v}_{i_1, i_2})P$ is again a parity check matrix for code \mathcal{C} . Moreover, following [5], the above condition happens if and only if $H_m(\mathbf{v}_{i_1, i_2})$ and $H_m(\mathbf{v}_{i_1, i_2})P$ are related by a linear transformation of coordinates, which we denote by K . This is the key point. This means that finding the automorphism group $\text{Aut}(\mathcal{C})$ is reduced to find all the nonsingular $m \times m$ matrices K preserving the symplectic form \mathcal{B} . So, such that $\mathcal{B}(K\mathbf{u}, K\mathbf{v}) = \mathcal{B}(\mathbf{u}, \mathbf{v})$. Hence, the automorphism group $\text{Aut}(\mathcal{C})$ is isomorphic to the symplectic group $\text{Sp}(m, 2)$. This proves the statement. \square

Now, we are ready to prove that the group $\text{Aut}(\mathcal{C})$ acts transitively over $\mathcal{C}(i) = \{\mathbf{x} + \mathcal{C} : \mathbf{x} \in \mathbb{F}^n, d(\mathbf{x}, \mathcal{C}) = i\}$, for any $i \in \{0, 1, 2, 3\}$.

Corollary 2.1. *The code $\mathcal{C} = \mathcal{C}_{i_1, i_2}$, constructed as in Theorem 2.1 is completely transitive.*

Proof: It is known from [1] that \mathcal{C} is a completely regular code with covering radius 3. Now, we have to prove that under action of $\text{Aut}(\mathcal{C})$ all cosets of \mathcal{C} are partitioned into 4 orbits. Since there is only one coset of weight 3 we have to consider only cosets of weights 1 and 2.

Consider cosets of weight 1. It is clear from the construction of $\text{Aut}(\mathcal{C})$ that there exists an automorphism swapping any two columns in H_m and so, moving a coset of weight 1 to any other one.

Consider cosets of weight 2, say, $D = \mathcal{C} + \mathbf{x}$, where $\text{wt}(\mathbf{x}) = 2$. Let $\text{supp}(\mathbf{x}) = \{j_1, j_2\}$. Since \mathbf{x} is not covered by weight 3 codewords, we conclude that $f_{i_1, i_2}(\mathbf{h}_{j_1} + \mathbf{h}_{j_2}) \neq f_{i_1, i_2}(\mathbf{h}_{j_1}) + f_{i_1, i_2}(\mathbf{h}_{j_2})$ and so, $\mathcal{B}(\mathbf{h}_{j_1}, \mathbf{h}_{j_2}) \neq \epsilon$. But, as $\text{Aut}(\mathcal{C})$ is constructed, any pair of columns $\mathbf{h}_{j_1}, \mathbf{h}_{j_2}$ such that $\mathcal{B}(\mathbf{h}_{j_1}, \mathbf{h}_{j_2}) \neq \epsilon$ can be moved to any other pair, with the same property, by some element in $\text{Aut}(\mathcal{C})$. Therefore any coset of weight 2 can be moved by the action of $\text{Aut}(\mathcal{C})$ to any other coset of weight 2. \square

As a consequence, we have the following result, which strengthen the corresponding result in [1].

Theorem 2.2. *Let H_m be the parity check matrix of the Hamming code \mathcal{H}_m of length $n = 2^m - 1$, where m is even, and let $H_m(\mathbf{v}_{i_1, i_2})$ be obtained from H_m by adding one more row \mathbf{v}_{i_1, i_2} given by (1). Let $\mathcal{C} = \mathcal{C}_{i_1, i_2}$ be the code with parity check matrix $H_m(\mathbf{v}_{i_1, i_2})$.*

- *If $\{i_1, i_2\} = \{0, 1\}$ or $\{0, 3\}$, then \mathcal{C} is a non antipodal completely transitive code with covering radius $\rho = 3$ and intersection array $(n, (n - 3)/2, 1; 1, (n - 3)/2, n)$.*
- *If $\{i_1, i_2\} = \{1, 2\}$ or $\{2, 3\}$, then \mathcal{C} is an antipodal completely transitive code with covering radius $\rho = 3$ and intersection array $(n, (n + 1)/2, 1; 1, (n + 1)/2, n)$.*

- If $\{i_1, i_2\} = \{0, 2\}$, then \mathcal{C} is an even part of the Hamming code, i.e., a completely transitive $[n, k - 1, 4]$ code with covering radius $\rho = 3$.
- If $\{i_1, i_2\} = \{1, 3\}$, then \mathcal{C} is the Hamming code \mathcal{H}_m .

Consider the extended codes from the ones obtained above. We give one lemma from [1], about dual weights of codes \mathcal{C}_{i_1, i_2}^* . By \mathcal{H}_m^* we denote an extended Hamming code of length 2^m and by \mathbf{v}_{i_1, i_2}^* the extended vector of \mathbf{V}_{i_1, i_2} .

Lemma 2.1. [1] *Let m be even. The weight distribution of the coset $\mathbf{v}_{i_1, i_2}^* + (\mathcal{H}_m^*)^\perp$ is:*

- $\{2^{m-1} \pm 2^{\frac{m}{2}-1}\}$, when $i_1 - i_2 = 1 \pmod{2}$.
- $\{0, 2^{m-1}\}$, when $\{i_1, i_2\} = \{1, 3\}$.
- $\{2^{m-1}, 2^m\}$, when $\{i_1, i_2\} = \{0, 2\}$.

Note that it is not the same to extend the code \mathcal{C}_{i_1, i_2} or to add a new row \mathbf{v}_{i_1, i_2} to the parity check matrix of the extended code \mathcal{C}^* . The next lemma will show us the difference.

Lemma 2.2. *Let $i_1 - i_2 \equiv 1 \pmod{2}$. We have that $(\mathcal{C}_{i_1, i_2})^* = (\mathcal{C}^*)_{i_1+1, i_2+1}$, where the addition of the indices is modulo 4, if and only if $0 \notin \{i_1, i_2\}$.*

Proof: Adding the row \mathbf{v}_{i_1, i_2} given by (1) to matrix H_m we obtain a parity check matrix for \mathcal{C}_{i_1, i_2} . Extending this code we obtain the same code as the one obtained after adding the row $\mathbf{v}_{i_1+1, i_2+1}$ to the parity check matrix H_m^* (matrix H_m^* is obtained from H_m adding a zero column and, later, the all-one row). The point is that this row $\mathbf{v}_{i_1+1, i_2+1}$ is of even weight (Lemma 2.1) and so, has a zero in the parity check position if and only if $1 \notin \{i_1 + 1, i_2 + 1\}$ or the same, if $0 \notin \{i_1, i_2\}$. \square

From [1] we know that the code \mathcal{C}_{i_1, i_2}^* is completely regular if and only if $0 \notin \{i_1, i_2\}$. In this case, since Lemma 2.2, it is the same to refer to the extension of \mathcal{C}_{i_1, i_2} or to refer to $(\mathcal{C}^*)_{i_1+1, i_2+1}$. Furthermore, the automorphism group of the extension depends on this situation.

Theorem 2.3. *Let $i_1 - i_2 \equiv 1 \pmod{2}$ and $0 \notin \{i_1, i_2\}$. Let \mathcal{C}^* be the extended code of $\mathcal{C} = \mathcal{C}_{i_1, i_2}$. Then:*

$$\text{Aut}(\mathcal{C}^*) = \text{Aut}(\mathcal{C}) \times \mathbb{F}^m = \text{Sp}(m, 2) \times \mathbb{F}^m.$$

Proof: Let $\mathbf{h}_1, \dots, \mathbf{h}_n \in \mathbb{F}^m$ be the columns of H_m , where $n = 2^m - 1$, and let \mathbf{h}_0 be the zero vector in \mathbb{F}^m . Vector \mathbf{h}_i represent the i th coordinate positions of the codewords in \mathcal{C} and also in \mathcal{C}^* (assuming that the parity check position corresponds to vector \mathbf{h}_0). For any $\mathbf{v} \in \mathbb{F}^m$, let $T_{\mathbf{v}} : \mathbb{F}^m \rightarrow \mathbb{F}^m$ be the translation on \mathbb{F}^m defined by $T_{\mathbf{v}}(\mathbf{x}) = \mathbf{x} + \mathbf{v}$, for any $\mathbf{x} \in \mathbb{F}^m$. We can also think of $T_{\mathbf{v}}$ as acting on \mathcal{C}^* by permuting the coordinates of the codewords in \mathcal{C}^* . More precisely, we can define $P_{\mathbf{v}} : \mathbb{F}^{n+1} \rightarrow \mathbb{F}^{n+1}$ such that for any $\mathbf{z} = (z_0, \dots, z_n) \in \mathbb{F}^{n+1}$, $P_{\mathbf{v}}(\mathbf{z}) = (y_0, \dots, y_n)$, where $y_j = z_i$ if $T_{\mathbf{v}}(\mathbf{h}_i) = \mathbf{v} + \mathbf{h}_i = \mathbf{h}_j$, for $i = 0, \dots, n$. As all the codewords in \mathcal{C}^* have even weight it is clear that $P_{\mathbf{v}}$ is in $\text{Aut}(\mathcal{C}^*)$. Indeed, let $\mathbf{a} = (a_0, \dots, a_n) \in \mathcal{C}^*$. This means that $\sum_{i=0}^n a_i \mathbf{h}_i = \mathbf{0}$. Now, $\sum_{i=0}^n a_i (\mathbf{h}_i + \mathbf{v}) = \sum_{i=0}^n a_i \mathbf{v} = \mathbf{0}$ and $P_{\mathbf{v}}(\mathbf{a}) \in \mathcal{C}^*$.

Furthermore, $\mathcal{P}_m = \{P_{\mathbf{v}} : \mathbf{v} \in \mathbb{F}^m\}$ is a normal subgroup in $\text{Aut}(\mathcal{C}^*)$. Indeed, for any $\phi \in \text{Aut}(\mathcal{C}^*)$ we have that $\phi P_{\mathbf{v}} \phi^{-1}$ is again a permutation $P_{\mathbf{w}}$, where $\mathbf{w} = \phi(\mathbf{v})$. For any element $\alpha \in \text{Aut}(\mathcal{C}^*)$, it is clear that we can find $\alpha' \in \text{Aut}(\mathcal{C}^*)$ fixing the extended coordinate and a vector $\mathbf{u} \in \mathbb{F}^m$, such that $\alpha = \alpha' P_{\mathbf{u}}$. Therefore, we have $\text{Aut}(\mathcal{C}^*)/\mathcal{P}_m \cong \text{Aut}(\mathcal{C})$ and so $\text{Aut}(\mathcal{C}^*)$

is the semidirect product of \mathbb{F}^m and $\text{Aut}(\mathcal{C})$ (obviously, we can identify \mathcal{P}_m with \mathbb{F}^m). This proves the statement. \square

Theorem 2.4. *The code \mathcal{C}_{i_1, i_2}^* is completely transitive with $\rho = 4$ and intersection array $(n + 1, n, \frac{n+1}{2}, 1; 1, \frac{n+1}{2}, n, n + 1)$ if and only if $0 \notin \{i_1, i_2\}$.*

Proof: From [1] we know that the code \mathcal{C}_{i_1, i_2}^* is completely regular if and only if $0 \notin \{i_1, i_2\}$ and also we know the intersection array for these cases. Therefore, if this condition is not satisfied, the code is not completely regular and neither completely transitive. Hence, we have to prove that the completely regular code $\mathcal{C}^* = \mathcal{C}_{i_1, i_2}^*$ is completely transitive. To do so, we prove that all the cosets with the same minimum weight are in the same orbit by the action of $\text{Aut}(\mathcal{C}^*)$.

The number of cosets of \mathcal{C}^* are twice the cosets of \mathcal{C} . Let 0 be the parity check position. If $\mathbf{v} + \mathcal{C}$ is a coset of \mathcal{C} , where \mathbf{v} is a representative vector of minimum weight then $(0|\mathbf{v}) + \mathcal{C}^*$ and $(1|\mathbf{v}) + \mathcal{C}^*$ are cosets of \mathcal{C}^* . There is only one coset of \mathcal{C}^* of weight 4, namely $(1|\mathbf{v}) + \mathcal{C}^*$, where $\mathbf{v} + \mathcal{C}$ is the only coset of weight three in \mathcal{C} . Clearly this coset is fixed under the action of $\text{Aut}(\mathcal{C}^*)$.

Now consider the cosets of \mathcal{C}^* of weight $r \in \{1, 2, 3\}$. They are of the form $(0|\mathbf{v}) + \mathcal{C}^*$, where $\mathbf{v} + \mathcal{C}$ is a coset of weight r of \mathcal{C} and of the form $(1|\mathbf{v}) + \mathcal{C}^*$, where $\mathbf{v} + \mathcal{C}$ is a coset of weight $r - 1$ of \mathcal{C} . Cosets of the same minimum weight in \mathcal{C} can be moved among them by $\text{Aut}(\mathcal{C})$ and so, as $\text{Aut}(\mathcal{C}) \subset \text{Aut}(\mathcal{C}^*)$ we need only to show that there exist an automorphism in $\text{Aut}(\mathcal{C}^*)$ moving $(0|\mathbf{v}) + \mathcal{C}^*$ to $(1|\mathbf{v}') + \mathcal{C}^*$, where \mathbf{v}, \mathbf{v}' are at distance r and $r - 1$ from \mathcal{C} , respectively. We further assume that $\text{supp}(\mathbf{v}') \subset \text{supp}(\mathbf{v})$ and so, $\text{supp}(\mathbf{v}) = \text{supp}(\mathbf{v}') \cup \{i\}$, for some coordinate position $i \neq 0$. The

existence of the wanted automorphism is straightforward from Theorem 2.3. The automorphism $T_{\mathbf{h}_i}$ (see the proof of Theorem 2.3) moves $(0|\mathbf{v}) + \mathcal{C}^*$ to $(1|\mathbf{v}'') + \mathcal{C}^*$, where $\text{supp}(\mathbf{v}'') = \{j + i : j \in \text{supp}(\mathbf{v}')\}$ and, finally, by using an automorphism from $\text{Aut}(\mathcal{C})$ we can move from $\mathbf{v}'' + \mathcal{C}$ to $\mathbf{v}' + \mathcal{C}$. \square

Given a linear code C , the coset graph of C is the graph whose vertices are the cosets $C + \mathbf{x}$ of C and such that two vertices are adjacent if the corresponding cosets contain neighbor vectors. Denote by Γ_{i_1, i_2} (respectively, Γ_{i_1, i_2}^*) the coset graph, obtained from the code \mathcal{C}_{i_1, i_2} (respectively \mathcal{C}_{i_1, i_2}^*). From Theorems 2.2 and 2.4 we obtain the following result, which gives a new description, as coset graphs, of some known graphs.

The next theorem was stated in [1] without explaining the property of transitivity of such graphs that we include here.

Theorem 2.5. *For any even m , $m \geq 4$ there exist imprimitive and antipodal distance transitive coset graphs $\Gamma_{0,1}$, $\Gamma_{1,2}$ with $v = 2^{m+1}$ vertices and $\Gamma_{1,2}^*$ with $v = 2^{m+2}$ vertices. Specifically:*

- $\Gamma_{0,1}$ has the intersection array $(n, \frac{n-3}{2}, 1; 1, \frac{n-3}{2}, n)$.
- $\Gamma_{1,2}$ has the intersection array $(n, \frac{n+1}{2}, 1; 1, \frac{n+1}{2}, n)$.
- $\Gamma_{1,2}^*$ has the intersection array $(n+1, n, \frac{n+1}{2}, 1; 1, \frac{n+1}{2}, n, n+1)$.
- The graphs $\Gamma_{0,1}$ and $\Gamma_{1,2}$ are Q -polynomial.

All the graphs $\Gamma_{0,1}$, $\Gamma_{1,2}$ and $\Gamma_{1,2}^*$ are known as can be seen in [1].

Acknowledgements

The authors are grateful to the anonymous referee for his/her helpful comments, which have improved the presentation of the results of this paper. This work has been partially supported by the Spanish MICINN grant

TIN2013-40524; the Catalan grant 2009SGR1224 and also by the Russian fund of fundamental researches 12-01-00905.

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] A.E. Brouwer, A.M. Cohen & A. Neumaier: *Distance Regular Graphs*, Springer, Berlin, (1989).
- [3] M. Giudici, C. E. Praeger: Completely Transitive Codes in Hamming Graphs. *Europ. J. Combinatorics* vol. 20, pp. 647-662, (1999).
- [4] F.J. MacWilliams & N.J.A. Sloane: *The Theory of Error Correcting Codes*. North-Holland, (1976).
- [5] F. J. MacWilliams: Error correcting codes for multiple level transmission. *Bell Syst. Tech. J.*, vol. 40, pp. 281-308, (1961).
- [6] J. Rifà, & V. A. Zinoviev: On a class of binary quadratic bent functions. Submitted to *Problems of Information Transmission*. (2012), arXiv:1211.5257v2.
- [7] P. Solé: Completely Regular Codes and Completely Transitive Codes. *Discrete Maths.*, vol. 81, pp. 193-201, (1990).