On a family of binary completely transitive codes with growing covering radius.∗

J. Rifà1, V. A. Zinoviev2

February 6, 2014

Abstract

A new family of binary linear completely transitive (and, therefore, completely regular) codes is constructed. 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 with \( d = 3 \), covering radius \( \rho \) and length \( (4\rho^2) \) and \( (4\rho^2 + 2) \), 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 \( \text{Aut}(C) \) 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 \( \mathbf{v} \in \mathbb{F}^n \), where \( \mathbb{F} \) is the binary finite field, 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 \( \rho = \max_{\mathbf{v} \in \mathbb{F}^n} \{d(\mathbf{v}, C)\} \).

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

\[
C(i) = \{\mathbf{x} \in \mathbb{F}^n : d(\mathbf{x}, C) = i\}, \quad i = 1, 2, \ldots, \rho.
\]

∗This work has been partially supported by the Spanish MICINN grants MTM2009-08435; the catalan grant 2009SGR1224 and also by the Russian fund of fundamental researches 12 - 01 - 00905.

1J. Rifà is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain. (email: josep.rifa@uab.cat)

2V. Zinoviev is with the A.A. Kharkevich Institute for Problems of Information Transmission, Russian Academy of Sciences, Bol’shoi Karetnyi per. 19, GSP-4, Moscow, 127994, Russia (e-mail: zinov@iitp.ru).
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 $a_l = n - b_l - c_l$ 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 A linear code $C$ with covering radius $\rho = \rho(C)$ and automorphism group $\text{Aut}(C)$ is completely transitive, if the set of all cosets of $C$ is partitioned into $\rho + 1$ orbits under action of $\text{Aut}(C)$, where for any $x \in \mathbb{F}_n$ and $\varphi \in \text{Aut}(C)$ the group acts on a coset $x + C$ as $\varphi(x + C) = \varphi(x) + C$.

Let $\Gamma$ be a finite connected simple (i.e., undirected, without loops and multiple edges) graph with diameter $\rho$. Let $d(\gamma, \delta)$ be the distance between two vertices $\gamma$ and $\delta$. (i.e., a numbers of edges in the minimal path between $\gamma$ and $\delta$). Denote

$$\Gamma_i(\gamma) = \{\delta \in \Gamma : d(\gamma, \delta) = i\}.$$

Two vertices $\gamma$ and $\delta$ from $\Gamma$ are neighbors if $d(\gamma, \delta) = 1$. An automorphism of a graph $\Gamma$ is a permutation $\pi$ of the vertex set of $\Gamma$ 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 $\Gamma_i$ be a subgraph of $\Gamma$ with the same vertices, where an edge $(\gamma, \delta)$ is defined when the vertices $\gamma, \delta$ are at distance $i$ in $\Gamma$. The graph $\Gamma$ is called primitive if it is connected and and all $\Gamma_i$ ($i = 1, \ldots, \rho$) are connected, and imprimitive otherwise.

Definition 3 A simple connected graph $\Gamma$ 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 $\delta$ in $\Gamma_{i-1}(\gamma)$ and $b_i$ neighbors of $\delta$ in $\Gamma_{i+1}(\gamma)$. Furthermore, this graph is called distance transitive, if for any pair of vertices $\gamma, \delta$ at distance $d(\gamma, \delta)$ there is an automorphism $\pi \in \text{Aut}(\Gamma)$ which moves this pair to any other given pair $\gamma', \delta'$ 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 [2, 3, 5] and references there).

This paper is a natural continuation of our previous paper [6], 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 $n = \binom{m}{2}$, dimension $k = n - m + 1$, minimum distance 3 and covering radius $\rho = [m/2]$. A half of these codes are non-antipodal and this implies (using [1]), that the covering set $C(\rho)$ of $C$ is a coset of $C$. In
these cases 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 the constructed linear completely transitive codes, an infinite family of distance-transitive coset graphs with growing diameter.

2 Preliminary results.

Let $C$ be a binary linear completely regular code with covering radius $\rho$ and intersection array $(b_0, \ldots, b_{\rho-1}; c_1, \ldots c_{\rho})$. Let $\{D\}$ be the set of cosets of $C$. Define the graph $\Gamma_C$ (which is called the coset graph of $C$, taking all cosets $D = C + x$ 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., $v \in D$ and $v' \in D'$ with distance $d(v, v') = 1$.

Lemma 4 \[2, 7\]. Let $C$ be a linear completely regular code with covering radius $\rho$ and intersection array $(b_0, \ldots, b_{\rho-1}; c_1, \ldots c_{\rho})$ and let $\Gamma_C$ be the coset graph of $C$. Then $\Gamma_C$ is distance-regular of diameter $\rho$ with the same intersection array. If $C$ is completely transitive, then $\Gamma_C$ is distance-transitive.

Lemma 5 \[5\]. Let $C$ be a completely regular code with covering radius $\rho$ and intersection array $(b_0, \ldots, b_{\rho-1}; c_1, \ldots c_{\rho})$. Then $C(\rho)$ is a completely regular code too, with inverse intersection array $(b'_{\rho}, \ldots, b'_{\rho-1}; c'_1, \ldots c'_{\rho})$, i.e.,

$$b'_i = c_{\rho-i}, \quad \text{and} \quad c'_i = b_{\rho-i}.$$

The starting point for the results in this paper comes from \[6\], where a specific class of combinatoric binary linear codes was introduced. For a given natural number $m$ where $m \geq 3$ denote by $E^m_2$ 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 $E^m_2$ (i.e., each vector from $E^m_2$ 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 \[6\]. Let $m$ be a natural number, $m \geq 3$.

(i) The binary linear $[n, k, d]$ code $C = C^{(m)}$ has parameters:

$$n = \left(\begin{array}{c} m \\ \ell \end{array}\right), \quad k = n - m + 1, \quad d = 3, \quad \rho = \left\lfloor \frac{m}{2} \right\rfloor.$$

(ii) Code $C^{(m)}$ is completely transitive and, therefore, completely regular. The intersection numbers of $C^{(m)}$ for $i = 0, \ldots, \rho$ are:

$$b_i = \left(\begin{array}{c} m - 2i \\ 2 \end{array}\right), \quad c_i = \left(\begin{array}{c} 2i \\ 2 \end{array}\right).$$

(iii) Code $C^{(m)}$ is antipodal if $m$ is odd and non-antipodal if $m$ is even.
3 A new family of completely transitive codes

Codes constructed in Theorem[4] for even $m$ are non-antipodal and this implies (using [1]), that the covering set $C(\rho)$ of $C$ is a coset of $C$. In these cases the union $C \cup C(\rho)$ gives also a completely regular and completely transitive code.

Lemma 8 Let $C$ be a completely regular non-antipodal linear code with $0 \in C$. Then any coset $D = C + x$ of $C$ of weight $s$ is a translate of $C(\rho)$ of weight $\rho - s$.

Proof. Let $D = C + x$ be any coset of $C$ of weight $s$. We can take the representative $x$ of weight $s$.

We want to show that $D = C(\rho) + y$, where $y$ is a minimum weight vector in $D$ and $\text{wt}(y) = \rho - s$. Since $d(x, C) = s$, there exists a vector $v \in C(\rho)$, such that $d(x, v) = \rho - s$ [3]. Let $y = v - x$.

Since for any $v \in C(\rho)$ we have $C + 1 = C + v = C(\rho)$, we obtain

$$D = C + x = C + (v + y) = (C + v) + y = C(\rho) + y,$$

which finishes the proof. △

The next statement is very important for the results we obtain in this paper.

Theorem 9 Let $C$ be a non-antipodal code with $0 \in C$, and let $A = C \cup C(\rho)$.

(i) If $C$ is completely regular, then the code $A$ is completely regular code too.

(ii) If $C$ is completely transitive, then $A$ is completely transitive.

Proof. (i) Since $C$ is completely regular non-antipodal code, the set $C(\rho)$ is a translate of $C$, i.e., $C(\rho) = C + 1$ [1]. To show that $A$ is completely regular we check its intersection array, denoted by $(b_0^s, \ldots, b_{p-1}^s; c_1^s, \ldots, c_p^s)$, where $\rho_a = \lfloor \rho/2 \rfloor$ is the covering radius of $A$. Recall (Lemma [5]) that $C(\rho)$ is completely regular with intersection array $(b_0^s, \ldots, b_{p-1}^s; c_1^s, \ldots, c_p^s)$, where $b_i = c_{\rho-i}$ and $c_i^s = b_{\rho-i}$.

Now assume that $x \in A(s)$. Since $C(\rho)$ is a translate of $C$, we have for $c_a^s$ and $b_a^s$ in any case, i.e., when $x \in C(s)$ or $x \in C(\rho)(s)$:

$$
\begin{align*}
&c_a^s = c_s, &b_a^s = b_s &\text{if } s < \lfloor \rho/2 \rfloor, \\
&c_a^s = c_s + b_s, &b_a^s = 0 &\text{if } s = \rho/2, &\rho \text{ even}, \\
&c_a^s = 0, &b_a^s = b_s &\text{if } s = \lceil \rho/2 \rceil, &\rho \text{ odd}.
\end{align*}
$$

Therefore, these numbers $c_a^s$ and $b_a^s$ do not depend on the choice of the vector $x \in A(s)$. We conclude that $A$ is completely regular.
(ii) For the second statement we assume that $C$ is a (linear) completely transitive code. Clearly, the code $A = C \cup C(\rho)$ is a linear code with covering radius $\rho_a = \lfloor \rho/2 \rfloor$. Now we have to show that for any two different vectors $x, x' \in A(s)$, $1 \leq s \leq \rho_a$ there is an automorphism (a permutation) $\varphi \in \text{Aut}(A)$ which transforms the coset $B = A + x$ into the coset $B' = A + x'$.

We can assume that $x$ and $x'$ are representatives of minimum weight $s$ in both cosets $B, B'$, respectively. Since $C$ is completely transitive, the coset $D = C + x$ of $C$ can be transformed into the coset $D' = C + x'$ by applying some permutation $\varphi \in \text{Aut}(C)$. We claim that using the same $\varphi$ we transform $B$ to $B'$. Note that $\text{Aut}(C(\rho)) = \text{Aut}(C)$ (lemma [8]) and $\text{Aut}(C) \subseteq \text{Aut}(A)$.

Since $B = A + x = (C + x) \cup (C + 1 + x)$,
we obtain

\[
\varphi(B) = \varphi(A + x) = (\varphi(C + x)) \cup (\varphi(C + 1 + x))
= (C + \varphi(x)) \cup (C + 1 + \varphi(x))
= A + \varphi(x) = B'.
\]

$\triangle$

Since for even $m$ the code $C^{(m)}$ is non-antipodal, its covering set $C^{(m)}(\rho)$ is a translate of $C^{(m)}$ [1]. Hence, it makes sense to consider the new (linear) code

\[ C^{[m]} = C^{(m)} \cup C^{(m)}(\rho). \]

**Proposition 10** A generating matrix $G^{[m]}$ for code $C^{[m]}$ is:

\[
G^{(m)} = \left[ \begin{array}{cc}
I_{k-1} & H^T_{m-1} \\
0 \ldots 0 & 1 \ldots 1
\end{array} \right],
\]

where $H^T_{m-1}$ means the transpose matrix of $H_{m-1}$.

**Proof.** Parity check matrix of $C^{(m)}$ can be written as $(I_{m-1}|H_{m-1})$ and so, the generating matrix for $C^{(m)}$ is $(H^T_{m-1}|I_{n_{m-1}})$, where $n_{m-1} = k - 1$ is the length of the code $C^{(m-1)}$.

Code $C^{(m)}$ is non-antipodal, so it does not contain the all ones vector. We can add it to the generating matrix of $C^{(m)}$ to obtain $C^{[m]}$ which gives the matrix $G^{[m]}$. $\triangle$

Next theorem gives important properties for code $C^{[m]}$.

**Theorem 11** Let $m$ be even, $m \geq 6$ and let $C^{[m]} = C^{(m)} \cup C^{(m)}(\rho)$. Then:

(i) Code $C^{[m]}$ is a linear completely regular linear $[n,k,d]$ code with parameters

\[ n = m(m-1)/2, \quad k = n - m + 2, \quad d = 3, \quad \rho = \lfloor m/4 \rfloor. \]
(ii) The intersection numbers of $C^{[m]}$ for $m \equiv 0 \pmod{4}$ and $\rho = m/4$ are

$$b_i = \binom{m - 2i}{2} \quad \text{and} \quad c_i = \binom{2i}{2} \quad \text{for} \quad i = 0, 1, \ldots, \rho - 1, \quad c_\rho = 2 \binom{2\rho}{2},$$

and, for $m \equiv 2 \pmod{4}$ and $\rho = (m - 2)/4$, are

$$b_i = \binom{m - 2i}{2} \quad \text{and} \quad c_i = \binom{2i}{2} \quad \text{for} \quad i = 0, 1, \ldots, \rho.$$

(iii) Code $C^{[m]}$ is completely transitive.

Proof. This is a direct corollary of Theorem 9. \triangle

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, and therefore, it is not completely regular [2].

Now we go over the structure of the automorphism group of the above codes.

**Lemma 12** Let $C$ be a binary completely regular code with $0 \in C$ and let $\text{Aut}(C)$ be the automorphism group of $C$. If $C$ is not antipodal, then $\text{Aut}(C) = \text{Aut}(C(\rho))$.

Proof. Since $C$ is non-antipodal we have [1] that $C(\rho) = C + 1$, where $1 = (1,1,\ldots,1)$.

Now we have for any $\varphi \in \text{Aut}(C)$

$$\varphi(C(\rho)) = \varphi(C + 1) = \varphi(C) + \varphi(1) = C + 1 = C(\rho),$$

which finishes the proof. \triangle

**Proposition 13** For the code $C^{(m)}$ we have $\text{Aut}(C^{(m)}) = S_m$.

Proof. The automorphism groups of $C^{(m)}$ and its dual $C^{(m)\perp}$ coincides, so our argumentation is about the dual. It is easy to see that any permutation of the rows of $H_m$ gives the same code $C^{(m)\perp}$. A permutation of the rows in $H_m$ can be seen as a permutation on the columns of $H_m$, so an automorphism of $C^{(m)\perp}$. Hence, $S_m \subseteq \text{Aut}(C^{(m)\perp})$.

To show the reciprocal inclusion let us begin by the fact that all the codewords of weight $m - 1$ in $C^{(m)\perp}$ are the rows of the matrix $H_m$. Indeed, the rows of matrix $H_m$ generate $C^{(m)\perp}$ and so, any codeword of weight $m - 1$ in $C^{(m)\perp}$ is a linear combination of rows of $H_m$. If a linear combination $v$ of any $t$ rows is of weight $m - 1$ we will have $\text{wt}(v) = m - 1 = t(m - 1) - 2\binom{t}{2}$ (mod $2^m - 1$) and so, $(t - 1)(m - 1) = t(t - 1)$ (mod $2^m - 1$). Hence, $t = 1$ or $t = m - 1$. In the first case $v$ is a row of $H_m$, but also in the second case (the sum of all rows in $H_m$ is the zero codeword, and so the sum of $m - 1$ rows coincides with one row).
Now, we finish the proof of the statement. We want to prove that there are no more automorphisms in Aut($C(m)^\perp$) apart from these ones in $S_m$. Assume $\phi \in$ Aut($C(m)^\perp$). For all codewords $v \in C(m)^\perp$ of weight $m - 1$ we have $\phi(v) \in C(m)^\perp$ is also of weight $m - 1$. Hence, since the rows of $H_m$ are the only codewords of weight $m - 1$ in $C(m)^\perp$ we have that $\phi$ is a permutation of the rows in $H_m$ and, as we said before, a permutation on the columns of $H_m$ and $\phi \in S_m$. △

**Proposition 14** Let $m$ be even, $m \geq 6$.

1. For $m > 6$ we have $\text{Aut}(C[m]) = \text{Aut}(C(m))$.

2. For $m = 6$ we have $\text{Aut}(C[m]) = GL_4(F_2)$.

**Proof.** Generators matrix of $C(m)$ and $C[m]$ coincide, except that the second one has one more independent row, the all ones row $1$. Hence, all the coordinate permutations which fix $C(m)$ also fix $C[m]$ and, so, $\text{Aut}(C(m)) \subseteq \text{Aut}(C[m])$. For $m > 6$, let $\phi \in \text{Aut}(C[m])$ such that $\phi \notin \text{Aut}(C(m))$. Then, as the codewords of weight 3 generate $C(m)$ (straightforward from Proposition 10) there should exists a codeword $v \in C(m)$, of weight 3 such that $\phi(v) \in C(m) + 1$. Therefore, $\phi(v)$ should be of weight 3, but this contradicts Theorem 7. Hence, item 1 is proved.

For $m = 6$ code $C[m]$ is the Hamming code of length 15, and so its automorphism group is very well known. Indeed, it is the general linear group of degree 4. △

### 4 A new description of distance-transitive graphs

Denote by $\Gamma^{(m)}$ (respectively, $\Gamma^{[m]}$) the coset graph, obtained from the codes $C^{(m)}$ (respectively, $C^{[m]}$) by Lemma 4. From Theorems 7 and 11 we obtain the following results, which leads to new coset graphs.

**Theorem 15** (i) 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.

(ii) The intersection arrays of graphs $\Gamma^{(m)}$ and $\Gamma^{[m]}$ are the same as the intersection arrays of codes, given by Theorems 7 and 11.

(iii) Both graphs $\Gamma^{(m)}$ and $\Gamma^{[m]}$ are distance transitive.

(iv) The graphs $\Gamma^{(m)}$ are imprimitive and the graphs $\Gamma^{[m]}$ are primitive.

(v) The graph $\Gamma^{[m]}$ has eigenvalues: for $m \equiv 2 \pmod{4}$

$$\left\{ \binom{m}{2} - 16i(\rho + 1 - i), \; i = 0, 1, \ldots, \rho \right\}$$
and for \( m \equiv 0 \pmod{4} \)

\[
\left\{ \binom{m}{2} - 8i(2\rho + 1 - i), \ i = 0, 1, \ldots, \rho \right\}.
\]

The graph \( \Gamma^{(m)} \) is well known. This graph 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 [2, 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] J. Borges, J. Rifa, V.A. Zinoviev, “On non-antipodal binary completely regular codes”, Discrete Mathematics, 2008, vol. 308, 3508 - 3525.

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

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

[4] M. Giudici, C. E. Praeger, “Completely Transitive Codes in Hamming Graphs”. Europ. J. Combinatorics (1999) 20, pp. 647662.

[5] A. Neumaier, “Completely regular codes,” Discrete Maths., vol. 106/107, pp. 335-360, 1992.

[6] 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.

[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.