On binary linear completely regular and completely transitive codes with arbitrary covering radius

Josep Rifà
josep.rifa@uab.es
Dept. of Information and Communications Engineering,
Autonomous University of Barcelona, 08193-Bellaterra, SPAIN

Victor Zinoviev
zinov@iitp.ru
Institute for Information Transmission Problems, Russian Academy of Sciences,
Bol’shoi Karetnyi per. 19, GSP-4, Moscow, 101447, RUSSIA

Abstract. An infinite class of binary linear completely regular and completely transitive codes is given. The covering radius of these codes is growing with the length of the code.

1 Introduction

Let $E$ be a binary alphabet. A binary $(n, N, d)$-code $C$ is a subset of $E^n$ where $n$ is the length, $d$ is the minimum distance and $N = |C|$ is the cardinality of $C$. For the case when $C$ is a $k$-dimensional linear subspace of $F^n$, the code $C$ is a linear code denoted $[n, k, d]$, where $N = 2^k$.

Given any vector $v \in E^n$, its distance to the code $C$ is

$$d(v, C) = \min_{x \in C} \{d(v, x)\}$$

and the covering radius of the code $C$ is

$$\rho = \max_{v \in E^n} \{d(v, C)\}.$$

We assume that a code $C$ always contains the zero vector. Let $D = C + x$ be a translate of $C$. The weight $\text{wt}(D)$ of $D$ is the minimum weight of the codewords of $D$. For an arbitrary translate $D$ of weight $i = \text{wt}(D)$ denote by $\mu(D) = (\mu_0(D), \mu_1(D), ..., \mu_n(D))$ its weight distribution, where $\mu_i(D)$ denotes the number of words of $D$ of weight $i$. Denote by $C_j$ (respectively, $D_j$) the subset of $C$ (respectively, of $D$), formed by all words of the weight $j$. In this terminology $\mu_i(D) = |D_i|$.

1This work was partially supported by Catalan DURSI Grant 2004PIV1-3, and also was partly supported by Russian fund of fundamental researches (the number of project 06 - 01 - 00226)
Definition 1 A binary code $C$ with covering radius $\rho$ is called completely regular if the weight distribution of any its translate $D$ is uniquely defined by the minimum weight of $D$, i.e. by the number $i = \text{wt}(D)$.

2 Definitions and preliminary results

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

$$C(i) = \{ x \in E^n : d(x, C) = i \}, \ i = 1, 2, ..., \rho.$$ 

For any vector $x \in E^n$ denote by $S(x)$ the sphere of radius one near $x$, i.e.

$$S(x) = \{ y \in E^n : d(x, y) = 1 \}.$$ 

Definition 2 Let $C$ be a code of length $n$ with covering radius $\rho$. We say that $C$ is uniformly packed in the wide sense, i.e. in the sense of [1], if there exist rational numbers $\alpha_0, \ldots, \alpha_\rho$ such that for any $v \in E^n$

$$\sum_{k=0}^\rho \alpha_k f_k(v) = 1,$$ 

where $f_k(v)$ is the number of codewords at distance $k$ from $v$.

For any vector $x \in E^n$ denote by $W_i(x)$ the sphere of radius $i$ near $x$, i.e.

$$W_i(x) = \{ y \in E^n : d(x, y) = i \}.$$ 

Denote $W_1(x) = W(x)$.

We say that two vectors $x$ and $y$ are neighbors if $d(x, y) = 1$. We use also the definition of completely regularity given in [10].

Definition 3 A code $C$ is a completely regular code 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 $c_0 = b_\rho = 0$. Define by $\{ b_0, \ldots, b_{\rho-1}; c_1, \ldots, c_\rho \}$ the intersection array of $C$.

The support of $v \in E^n$, $v = (v_1, \ldots, v_n)$ is $\text{supp}(v) = \{ \ell : v_\ell \neq 0 \}$. Say that a vector $v$ covers a vector $z$ if the condition $z_i \neq 0$ implies $z_i = v_i$.

For a binary $(n, N, d)$ code $C$ with zero codeword let $(\eta_0, \ldots, \eta_n)$ be its distance distribution, i.e. $\eta_\ell$ is the number of ordered pairs of codewords at a distance $i$ apart, divided by $N$. Let $(\eta'_0, \ldots, \eta'_n)$ be the MacWilliams transform of $(\eta_0, \ldots, \eta_n)$ and assume this vector has $s = s(C)$ nonzero components $\eta'_i$ for $1 \leq i \leq n$. We call $s$ the external distance of $C$. If $C$ is a linear code, then $s(C)$ is the number of different nonzero weights of codewords in the dual code $C^\perp$. 
Lemma 1 [7] For any code \( C \) with covering radius \( \rho(C) \) and external distance \( s(C) \)

\[ \rho(C) \leq s(C). \]

The case of equality above implies existence of uniformly packed code in the wide sense.

Lemma 2 [2] Let \( C \) be a code with minimum distance \( d = 2e + 1 \), covering radius \( \rho \), and external distance \( s \). Then the code \( C \) is uniformly packed in the wide sense, if and only if \( \rho = s \).

For a binary code \( C \) let \( \text{Perm}(C) \) be its permutation stabilizer group. For any \( \theta \in \text{Perm}(C) \) and any translate \( D = C + x \) of \( C \) define the action of \( \theta \) on \( D \) as: \( \theta(D) = C + \theta(x) \).

Definition 4 [13] Let \( C \) be a binary linear code with covering radius \( \rho \). The code \( C \) is called completely transitive, if the set \( \{C + x : x \in \mathbb{F}^n\} \) of all different cosets of \( C \) is partitioned under action of \( \text{Perm}(C) \) into exactly \( \rho + 1 \) orbits.

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

It has been conjectured for a long time that if \( C \) is a completely regular code and \( |C| > 2 \), then \( e \leq 3 \). For the special case of linear completely transitive codes, the problem of existence is solved in [3, 4] in the sense that for \( e \geq 4 \) such nontrivial codes do not exist.

3 Main results

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 5 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 \( H^{(m)} \).

For a fixed natural number \( m \) and any \( i \in \{1, 2, \ldots, m\} \) define \( f_i(m) \) as the weight of the vector sum of any \( i \) rows of \( H^{(m)} \). Note that \( f_i(m) \) is well defined and it does not depend on the specific rows taken in the computation as be can see in the next lemma.

Lemma 3 For any natural number \( m \geq 3 \) the value \( f_i(m) \) does not depend on the choice of \( i \) rows of \( H^{(m)} \) and \( f_i(m) = i \cdot (m - i) \) for \( i \in \{1, 2, \ldots, m\} \).
Lemma 4 For any natural number \( m \geq 3 \) the code \( C^{(m)} \) has the external distance \( s(m) = \lfloor m/2 \rfloor \) and the covering radius \( \rho(m) = \lfloor m/2 \rfloor \).

Thus, the code \( C^{(m)} \) has the same external distance and covering radius: \( s(m) = \rho(m) \). By Lemma 2 the code \( C^{(m)} \) is uniformly packed in the wide sense. The following statements shows that \( C^{(m)} \) is, in fact, a completely transitive code and, so, a completely regular code too.

Theorem 1 For any natural number \( 3 \leq m \) the code \( C^{(m)} \) is a completely transitive \([n, k, d]\)-code with the following parameters:
\[
n = \binom{m}{2}, \quad k = n - m + 1, \quad d = 3, \quad \rho = \lfloor m/2 \rfloor.
\]

Theorem 2 For any natural number \( 3 \leq m \) the code \( C^{(m)} \) is a completely regular \([n, k, d]\)-code with intersection numbers, for \( \ell = 0, \ldots, \rho \):
\[
a_\ell = 2 \ell \cdot (m - 2\ell),
b_\ell = \binom{m - 2\ell}{2},
c_\ell = \binom{2\ell}{2}.
\]

The interesting fact is that generalization of this idea (i.e. using as a parity check matrix all possible binary vectors of length \( m \) and weight \( \ell \)) above works only in three following cases. For given natural number \( m \) where \( m \geq 3 \) define by \( E^{m}_\ell \) the set of all binary vectors of length \( m \) and weight \( \ell \).

Definition 6 Denote by \( H^{(m,\ell)} \) the binary matrix of size \( m \times \binom{m}{\ell} \), whose columns are exactly all vectors from \( E^{m}_\ell \) (i.e. each vector from \( E^{m}_\ell \) occurs once as a column of \( H^{(m,\ell)} \)). Define the binary linear code \( C^{(m,\ell)} \), whose parity check matrix is the matrix \( H^{(m,\ell)} \).

Theorem 3 Let \( C^{(m,\ell)} \) be the code defined above. Let \( \ell \geq 3 \). Let \( C^{(m,\ell)} \) be a completely regular code. Then we are in one of the following three cases:
1. \( m = 5 \) and \( \ell = 3 \). The code \( C^{(5,3)} \) is the \([10, 5, 4]\)-code with covering radius \( \rho = 3 \) and with intersection array \((10, 9, 4; 1, 6, 10)\).
2. \( m = 6 \) and \( \ell = 4 \). The code \( C^{(6,4)} \) is the \([15, 10, 3]\)-code with covering radius \( \rho = 3 \) and with intersection array \((15, 8, 1; 1, 8, 15)\).
3. \( m = 7 \) and \( \ell = 4 \). The code \( C^{(7,4)} \) is the \([35, 29, 3]\)-code with covering radius \( \rho = 2 \) and with intersection array \((35, 16; 1, 20)\).
Furthermore, all these three codes are completely transitive.
References


