Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 243-247*

On binary linear completely regular and completely transitive codes with arbitrary covering radius[1]

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 $\mathbb{F}^n$, the code C is a *linear* code denoted $[n, k, d]$, where $N = 2^k$.

Given any vector $\mathbf{v} \in E^n$, 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

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

We assume that a code C always contains the zero vector. Let $D = C + \mathbf{x}$ be a *translate* of C. The *weight* $\mathrm{wt}(D)$ of D is the minimum weight of the codewords of D. For an arbitrary translate D of weight $i = \mathrm{wt}(D)$ 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 $\mu_i(D) = |D_i|$.

[1]This 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 ρ 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 $i = wt(D)$.*

2 Definitions and preliminary results

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

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

For any vector $\mathbf{x} \in E^n$ denote by $S(\mathbf{x})$ the sphere of radius one near $\mathbf{x}$, i.e. $S(\mathbf{x}) = \{\mathbf{y} \in E^n : d(\mathbf{x}, \mathbf{y}) = 1\}$.

Definition 2 *Let C be a code of length n with covering radius ρ. 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 $\mathbf{v} \in E^n$*

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

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

For any vector $\mathbf{x} \in E^n$ denote by $W_i(\mathbf{x})$ the sphere of radius i near $\mathbf{x}$, i.e. $W_i(\mathbf{x}) = \{\mathbf{y} \in E^n : d(\mathbf{x}, \mathbf{y}) = i\}$. Denote $W_1(\mathbf{x}) = W(\mathbf{x})$.

We say that two vectors $\mathbf{x}$ and $\mathbf{y}$ are *neighbors* if $d(\mathbf{x}, \mathbf{y}) = 1$. 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 $\mathbf{v} \in E^n$, $\mathbf{v} = (v_1, \ldots, \ v_n)$ is $supp(\mathbf{v}) = \{ \ \ell \mid v_\ell \neq 0 \ \}$. Say that a vector $\mathbf{v}$ *covers* a vector $\mathbf{z}$ 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. η_i 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 η'_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 ρ, 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 $\mathrm{Perm}(C)$ be its permutation stabilizer group. For any $\theta \in \mathrm{Perm}(C)$ and any translate $D = C + \mathbf{x}$ of C define the action of θ on D as: $\theta(D) = C + \theta(\mathbf{x})$.

Definition 4 *[13] Let C be a binary linear code with covering radius ρ. The code C is called* completely transitive*, if the set $\{C+\mathbf{x} : \mathbf{x} \in \mathbb{F}^n\}$ of all different cosets of C is partitioned under action of* $\mathrm{Perm}(C)$ *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 $\ell = 0, \ldots, \rho$:*

$$\begin{aligned} a_\ell &= 2\,\ell \cdot (m - 2\ell), \\ b_\ell &= \binom{m-2\ell}{2}, \\ c_\ell &= \binom{2\,\ell}{2}. \end{aligned}$$

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 ℓ) above works only in three following cases. For given natural number m where $m \geq 3$ define by E_ℓ^m the set of all binary vectors of length m and weight ℓ.

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_ℓ^m (i.e. each vector from E_ℓ^m 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

[1] L. A. Bassalygo, G. V. Zaitsev, V. A. Zinoviev, Uniformly packed codes, *Probl. Inform. Transm.* 10, 1974, 9-14.

[2] L. A. Bassalygo, V. A. Zinoviev, Remark on uniformly packed codes, *Probl. Inform. Transm.* 13, 1977, 22-25.

[3] J. Borges, J. Rifa, On the nonexistence of completely transitive codes, *IEEE Trans. Inform. Theory* 46, 2000, 279-280.

[4] J. Borges, J. Rifa, V. A. Zinoviev, Nonexistence of completely transitive codes with error-correcting capability $e > 3$, *IEEE Trans. Inform. Theory* 47, 2001, 1619-1621.

[5] J. Borges, J. Rifa, V. A. Zinoviev, On non-antipodal binary completely regular codes, *Discr. Math.*, 2008, to appear.

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

[7] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.* 10, 1973.

[8] J. M. Goethals, H. C. A. Van Tilborg, Uniformly packed codes, *Philips Res.* 30, 1975, 9-36.

[9] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, New York, 1977.

[10] A. Neumaier, Completely regular codes, *Discr. Math.* 106/107, 1992, 335-360.

[11] J. Rifa, V. A. Zinoviev, On new completely regular q-ary codes, *Probl. Inform. Transm.*, 43, 2007.

[12] N. V. Semakov, V. A. Zinoviev, G. V. Zaitsev, Uniformly packed codes, *Probl. Inform. Transm.* 7, 1971, 38-50.

[13] P. Solé, Completely regular codes and completely transitive codes, *Discr. Math.* 81, 1990, 193-201.