Eleventh International Workshop on Algebraic and Combinatorial Coding Theory
June 16-22, 2008, Pamporovo, Bulgaria *pp. 292-299*

On mobile sets in the binary hypercube

Yu. L. Vasil'ev, S. V. Avgustinovich*, D. S. Krotov `krotov@math.nsc.ru`
Department of Mechanics and Mathematics, Novosibirsk State University
Pirogova Str. 2, Novosibirsk, 630090, RUSSIA

Abstract. If two distance-3 codes have the same neighborhood, then each of them is called a mobile set. In the $(4k+3)$-dimensional binary hypercube, there exists a mobile set of cardinality $2 \cdot 6^k$ that cannot be split into mobile sets of smaller cardinalities or represented as a natural extension of a mobile set in a hypercube of smaller dimension.

1 Introduction

By E^n we denote the metric space of all length-n binary words with the Hamming metric. The space E^n is called the binary, or unary, or Boolean hypercube. The basis vector with one in the ith coordinate and zeros in the other is denoted by e_i. A subset M of E^n is called a 1-code if the radius-1 balls with centers in M are disjoint. The union of the radius-1 balls with the centers in M is called the *neighborhood* of M and denoted by $\Omega(M)$, i.e.,

$$\Omega(M) = \{x \in E^n : d(x, M) \le 1\}.$$

If a 1-code M satisfies $\Omega(M) = E^n$, then it is called perfect, or a 1-*perfect code*. 1-Perfect codes exist only when the dimension has the form $n = 2^k - 1$. For $n = 7$, such a code is unique (up to isometries of the space), the linear Hamming code. For $n = 15$, the problem of characterization and enumeration of the 1-perfect codes is not solved yet, in spite of the increasing computation abilities (considerable results are obtained in [10, 2]). In this context, it is topical to study objects that generalize, in different senses, the concept of 1-perfect code and exist in intermediate dimensions, not only of type $n = 2^k - 1$. Examples of such objects are the perfect colorings (in particular, with two colors [1]), the centered functions [8], and the mobile sets, discussed in this paper.

A set $M \subseteq E^n$ is called *mobile* (*m.s.*) iff:
1) M is a 1-code;
2) there exists a 1-code M' disjoint with M and with the same neighborhood, i.e., $M \cap M' = \emptyset$ and $\Omega(M) = \Omega(M')$;

such a set M' will be called the *alternative* of M.

In other words, a 1-code is a m.s. iff it has an alternative.

For every odd $n = 2m+1$, we can construct a linear (i.e., closed with respect to coordinatewise modulo-2 addition) m.s. in E^n:

$$M = \{(x, x, |x|) : x \in E^m\}. \qquad (1)$$

*This author is partially supported by the RFBR grant 07-01-00248.

(Here and below $|x|$ denotes the modulo-2 sum of the coordinates of x.) Respectively,

$$M' = \{(x, x, |x| \oplus 1) : x \in E^m\}.$$

It is not difficult to check the conditions 1 and 2 for these M and M'.

Our main goal is to prove the following:

Theorem. *For all $n \geq 7$ congruent to 3 modulo 4, there exists an irreducible unsplittable mobile set in E^n.*

A nonempty m.s. M is called *splittable* (*unsplittable*), iff if can (respectively, cannot) be represented as the union of two nonempty m.s. The concept of reducibility, which will be defined in Section 4, reflects a natural reducibility of mobile sets to mobile sets in the hypercube of the two-less dimension.

A simple way to construct a m.s. in a hypercube of a code dimension $n = 2^k - 1$ is the following. Let C and C' are 1-perfect codes in E^n. Then $M = C \setminus C'$ is a m.s. Indeed, we can take $C' \setminus C$ as M'. The cardinality of this m.s. is $C - |C \cap C'|$. We study the existence of m.s. that cannot be reduced to code dimensions.

In Section 2 we define extended mobile sets; that concept is convenient for the description of our construction. In Section 3 we describe a connection between the mobile sets and the i-components, which were studied earlier. In Section 4 we describe a construction of increasing dimension for mobile sets; that construction leads to the natural concept of a reducible m.s. In Section 5 we give the main construction and prove Theorem. In the final section, we formulate several problems.

2 Extended mobile sets

Like as with 1-perfect codes, it is sometimes convenient to work with mobile sets extending them by the all-parity check to the next dimension. In some cases we get more symmetrical objects, which simplifies proofs and formulations of statements. And. Some statements become more simple and intuitive while being formulated for the extended case, although geometrical interpretations of extended objects can seem to be not so elegant and natural as for the original.

Recall that the *extension* of the set $M \subseteq E^n$ is the set $\overline{M} \subseteq E^{n+1}$ obtained by the addition of the all-parity-check bit to all the words of M:

$$\overline{M} = \{(x, |x|) : x \in M)\} \qquad \text{or} \qquad \overline{M} = \{(x, |x| \oplus 1) : x \in M)\}.$$

Puncturing the ith coordinate for some set of words in E^n means removing the ith symbol from all the words of the set (the result is in E^{n-1}). Obviously, the extension and puncturing the last coordinate lead to the original set; so, these operations are opposite to each other, in some sence.

A set $\overline{M} \subseteq E^n$ is called *extended mobile* (an *e.m.s.*) iff it can be obtained as the extension of some m.s.

We will use the following lemma, which gives alternative definitions of an e.m.s. As a usual m.s., an e.m.s. M can be defined together with some other e.m.s. M', which can also be referred as an *alternative* of M (usually, it is clear from the context what we are talking about, mobile sets or extended mobile sets). For the formulation of the lemma and further using, it is convenient to define the concept of the *spherical neighborhood*

$$\dot{\Omega}(M) = \Omega(M) \setminus M,$$

which, for the extended mobile sets, plays the role similar to the role of the usual ("ball") neighborhood for the m.s. In particular, part (c) of Lemma 1 defines an e.m.s. and an alternative similarly to the case of a m.s.

Lemma 1 (alternative definitions of an e.m.s.)**.** *Let M and M' be disjoint* 1*-codes in E^n, and let their vectors have the same parity* (*either all vectors are even, or odd*)*. Let $i \in \{1, \ldots, n\}$. The following conditions are equivalent and imply that M* (*as like as M'*) *is an e.m.s.*
(a) *The sets M_i and M'_i obtained from M and M' by puncturing ith coordinate are mobile and, moreover, are alternatives of each other.*
(b) *The* (*bipartite*) *distance-*2 *graph $G(M \cup M')$ of the union $M \cup M'$ has the degree $n/2$.*
(c) $\dot{\Omega}(M) = \dot{\Omega}(M')$. △

Taking into account (b) and the existence of a linear m.s., we have the following:

Corollary 1. *Nonempty m.s.* (*e.m.s.*) *exist in E^n if and only if n is odd* (*resp., even*).

3. i-Components

A m.s. M is called an *i-component* iff $\Omega(M) = \Omega(M \oplus e_i)$. Consider the set M_i obtained from M by puncturing the ith coordinate. Let us construct the so-called minimal-distance graph $G(M_i)$ with the vertex set M_i, connecting vertices at the distance 2 from each other. The proof of the following lemma is similar to Lemma 1, and we omit it.

Lemma 2. A 1-code M is an i-component if and only if the graph $G(M_i)$ is regular of degree $(n-1)/2$ and bipartite.

So, Lemmas 1 and 2 establish a correspondence between pairs of alternative m.s. in E^{n-1} and i-components in E^{n+1} (for fixed i, say, $i = n+1$). This correspondence is evident as both objects correspond to a set in E^n whose distance-2 graph is bipartite and has the degree $n/2$. In the first case, all the vertices of this set have the same parity. In the second case, this is not not necessary, but the subsets of different parity will correspond to a partition of the i-component into independent i-components, "i-even" and "i-odd". Formally, we can formulate the following.

Corollary 2. *Sets $M, M' \subseteq E^{n-1}$ are a m.s. and an alternative if and only if the set*

$$\{(x, |x|, 0) : x \in M\} \cup \{(x, |x|, 1) : x \in M'\}$$

is an i-component with $i = n + 1$.

Corollary 3. *A set $M \subseteq E^{n+1}$ is an i-component with $i = n + 1$ if and only if the sets*

$$M_a^b = \{x : (x, |x| \oplus a, b) \in M\}, \quad a, b \in \{0, 1\}$$

are m.s., where M_a^0 and M_a^1 are alternatives to each other (the sets M_0^0 and M_0^1 correspond to the "i-even" part of the i-component; M_1^0 and M_1^1, to the "i-odd"; each of these parts can be empty; and if both are nonempty, then the i-component is splittable).

An example of i-component is the linear m.s. (1), $i = n$. Formerly [4, 5] many examples of nonlinear i-components were constructed. Each of them is embeddable to a 1-perfect codes and has the cardinality, divisible by the cardinality of the linear component. Moreover, it was only proved that these i-components cannot be split into smaller i-components. Their splittability onto mobile sets are still questionable. So, in spite of the fact that the researches are devoted to common problems and a common approach, the lines are slightly different and the results do not overlap but complement each other: we give the embeddability to 1-perfect codes up (which is a weakening) but deal with a stronger splittability and a wider specter of dimensions.

4 Reducibility

Lemma 3 (on the linear extension of a m.s.)**.** *Let $M \subseteq E^n$ be an e.m.s. and let $M' \subseteq E^n$ be an alternative of M. Then the set*

$$R = \{(x, 0, 0) : x \in M\} \cup \{(x, 1, 1) : x \in M'\} \tag{2}$$

is an e.m.s. with an alternative

$$R' = \{(x, 1, 1) : x \in M\} \cup \{(x, 0, 0) : x \in M'\}.$$

Proof. Condition (b) of Lemma 1 for M and M' implies the validity of this condition for R and R'. $\triangle$.

An e.m.s. $R \in E^n$ is called *reducible* iff it can be obtained by the construction (2) and applying some isometry of the space (i.e., a coordinate permutation and the inversion in some coordinates). A m.s. is called *reducible* iff the corresponding e.m.s. is reducible.

So, the existence of reducible m.s. is reduced to the existence of m.s. in smaller dimensions. From this point of view, the formulation of the main theorem is natural.

Remark. As we can see from Corollary 3, any i-component is either reducible m.s. or can be split into two i-components ("i-even" and "i-odd"), which are reducible m.s. In particular, the linear m.s. (1) is reducible. Moreover, the linear e.m.s., up to a coordinate permutation, can be obtained from the trivial e.m.s. $\{00\}$ in E^2 by sequential applying the construction from Lemma 3.

5 Proof of Theorem

Let us fix n divisible by 4: $n = 4k$. Partition the coordinate numbers into k groups with 4 numbers in each group; rename the corresponding orts as follows: $e_0^1, e_1^1, e_2^1, e_3^1, e_0^2, \ldots, e_3^k$. In each quadruple of type $\{e_0^i, e_1^i, e_2^i, e_3^i\}$ we chose arbitrarily (there exist 6 possibilities) a pair of different orts e_j^i and e_t^i; by the index of the pair we shell mean the number $p\{j,t\}$ where

$$p\{0,1\} = p\{2,3\} = 0, \qquad p\{0,2\} = p\{1,3\} = 1, \qquad p\{0,3\} = p\{1,2\} = 2.$$

Summarizing the chosen pairs for all $i = 1, 2, \ldots, k$, we get a vector of weight $2k$, which will be called *standard*. Totally, there exist 6^k standard vectors. By the index $I(v)$ of a standard vector v we shell mean the modulo-3 sum of the indexes of all the pairs of orts that constitute v.

Let us partition the set of standard vectors into disjoint subsets S_0, S_1, and S_2 in compliance with the indexes of the vectors.

Claim 1. *Let $i \neq j$, $i, j \in \{0, 1, 2\}$. Then the distance-two graph $G(S_i \cup S_j)$ induced by the set $S_i \cup S_j$ is bipartite and regular of degree $2k$.*

We first note that the graphs $G(S_i)$ and $G(S_j)$ are empty. Indeed, consider two vectors $v, u \in S_i$. Either v and u differ in exactly one quadruple of coordinates, and thus $d(v,u) = 4$, because $I(u) = I(v)$; or v and u differ in more than one quadruples, and thus $d(v,u) \geq 4$, because the distance between standard vectors is even in every quadruple. So, $G(S_i \cup S_j)$ is bipartite.

Further, it is easy to see that every vector of index i has exactly two distance-2 neighbors in S_j. This means that the graph degree is $2k$. Claim 1 is proved.

So, S_0 (for example) is an e.m.s. of cardinality $2 \cdot 6^{k-1}$.

Claim 2. *The e.m.s. S_0 is unsplittable.* Assume that $P \subseteq S_0$ and $Q = S_0 \backslash P$ are nonempty e.m.s. Then P and Q have alternative, say P' and Q'.

We will first show that

(*) P' (*similarly, Q'*) *consists of only standard vectors*, i.e., such vectors that contains exactly two ones in every quadruple. Indeed, otherwise P' contains a vector with non-standard quadruple; consequently, $\dot\Omega(P')$ contains a vector with two non-standard quadruples. But $\dot\Omega(P)$ consists of vectors with exactly one non-standard quadruple and, thus, cannot coincide with $\dot\Omega(P')$, which contradicts to Lemma 1. (*) is proved.

The following is another simple statement we will use:
(**) *The distance-two graph* $G(S_i \cup S_j)$ *is connected* $(i, j \in \{0, 1, 2\},\ i \neq j)$.
Let us show this by induction on k. For $k = 2$ the the statement can be checked directly. Let $k > 2$. It is sufficient to show that arbitrary u and v from $S_i \cup S_j$ belong to the same connected component. If u and v coincide in some coordinate quadruple, then this fact follows from the inductive assumption (fixing this quadruple, we get a subgraph isomorphic to a graph considered in the previous inductive step). Otherwise, there exists a word w in $S_i \cup S_j$ that coincide with u in the first quadruple and with v in the second quadruple (the values in the other quadruples are chosen to make the index of w being i or j). Similarly to the considered case, u, w and v belong to the same connected component. (**) is proved.

Since P' and Q' consist of standard vectors, they are included in $S_1 \cup S_2$. Denote

$$P_1 = P' \cap S_1, \qquad P_2 = P' \cap S_2, \qquad Q_1 = Q' \cap S_1, \qquad Q_2 = Q' \cap S_2.$$

If $P_1 = Q_1 = \emptyset$, then, as follows from Lemma 1(b), $P \cup P_2$ and $Q \cup Q_2$ correspond to connected components of $G(S_0 \cup S_2)$, which contradicts to (**). Similarly, $P_2 = Q_2 = \emptyset$ is impossible.

We have:

$$\dot\Omega(P_1 \cup P_2) \cup \dot\Omega(Q_1 \cup Q_2) = \dot\Omega(P) \cup \dot\Omega(Q) = \dot\Omega(S_0).$$

Further, $\dot\Omega(S_1) = \dot\Omega(S_0)$; thus,

$$\dot\Omega(S_1 \setminus (P_1 \cup Q_1)) = \dot\Omega(P_2 \cup Q_2).$$

Similarly,

$$\dot\Omega(S_2 \setminus (P_2 \cup Q_2)) = \dot\Omega(P_1 \cup Q_1).$$

So, S_1 is partitioned into two nonempty sets with alternatives in S_2. It follows from Lemma 1(b) that the graph $G(S_1 \cup S_2)$ is not connected, which contradicts to (**) and proves Claim 2.

Claim 3. *The e.m.s.* S_0 *is irreducible.*

Note that in the construction (2) the sum of the last two coordinates is 0 for every word in R. Taking into account coordinate permutations and symbol inversions, we can claim that for any reducible e.m.s. there exist two coordinates whose sum is either 0 or 1 simultaneously for all words of the e.m.s. It is easy to see that S_0 does not satisfy this condition: in every two coordinates there occur all four combinations of 0 and 1. Claim 3 is proved. The theorem is proved.

6. Conclusion

We have constructed an infinite class of unsplittable irreducible m.s. Our construction generalizes the example mentioned in [7]. In conclusion, we formulate several problems, which are naturally connected with the study of mobile sets and with the problem of characterization of their variety.

For constructing m.s., one can apply the generalized concatenation principle which works for 1-perfect codes [9]. In particular, the construction from Section 5 can be treated in such terms. Unsplittable m.s. constructed in such the way will have non-full rank, i.e., for all the words of the set the coordinates will satisfy some linear equation.

Problem 1. Construct an infinite family of full-rank unsplittable m.s.

Example. Consider the four words

$$\begin{pmatrix} 100 \\ 110 \\ 010 \end{pmatrix}, \quad \begin{pmatrix} 011 \\ 110 \\ 000 \end{pmatrix}, \quad \begin{pmatrix} 101 \\ 001 \\ 011 \end{pmatrix}, \quad \begin{pmatrix} 001 \\ 100 \\ 111 \end{pmatrix},$$

in E^9, listed, for convenience, as 3×3 arrays, and all the words obtained from them by cyclic permutations of rows and/or columns of the array. We get full-rank unsplittable m.s. of cardinality 36. An alternative can be obtained by the inversion of all the words.

Problem 2. Construct a rich class of transitive unsplittable m.s., e.m.s. A set $M \subseteq E^n$ is called transitive iff the stabilizer $\mathrm{Stab}_I(M)$ of M in the group I of isometries of the hypercube acts transitively on the elements of M; i.e., for every x, y from M there exists an isometry $\sigma \in \mathrm{Stab}_I(M)$ such that $\sigma(x) = y$. For example, it is not difficult to see that the m.s. constructed in the current paper are transitive. There are several constructions of transitive 1-perfect and extended 1-perfect codes, see [6, 3] for the last results.

Problem 3. Study the embeddability of m.s. into 1-perfect codes: the existence of nonembeddable m.s. in the code dimensions $n = 2^k - 1$; the existence of m.s. that cannot be embedded with help of the linear extension (Lemma 3) into a 1-perfect code in a larger dimension. In particular, for m.s. constructed in Section 5, the embedding questions are open provided $n \geq 11$.

Problem 4. Estimate the maximal cardinality of an unsplittable m.s.

Problem 5. Estimate the minimal cardinality of a nonlinear m.s. (the construction of Section 5 together with Lemma 3 give the upper bound $1{,}5L(n)$, where $L(n) = 2^{(n-1)/2}$ is the cardinality of the linear m.s.), of an irreducible unsplittable m.s. (the construction gives the upper bound $1{,}5^{(n-3)/4}L(n)$), unsplittable m.s. of full rank.

Problem 6. Study mobile sets in other spaces, in particular, in q-ary Hamming spaces where $q > 2$ is an arbitrary integer, not necessarily a prime power.

References

[1] D. G. Fon-Der-Flaass, Perfect 2-colorings of a hypercube, *Sib. Math. J.*, 48, 2007, 740-745. dx.doi.org/10.1007/s11202-007-0075-4, DOI:10.1007/s11202-007-0075-4 transl. from Sib. Mat. Zh. 48, 2007, 923-930.

[2] S. A. Malyugin, On enumeration of nonequivalent perfect binary codes of length 15 and rank 15, *J. Appl. Ind. Math.* 1, 2007, 77-89, dx.doi.org/10.1134/S1990478907010085, DOI: 10.1134/S1990478907010085 transl. from Diskr. Anal. Issled. Oper., Ser. 1 13, 2006, 77-98.

[3] V. N. Potapov, A lower bound for the number of transitive perfect codes. *J. Appl. Ind. Math.* 1, 2007, 373-379, dx.doi.org/10.1134/S199047890703012X, DOI: 10.1134/S199047890703012X transl. from Diskr. Anal. Issled. Oper. Ser. 1, 13, 2006, 49-59.

[4] F. I. Solov'eva, On the factorization of code-generating d.n.f. *Met. Diskr. Anal. Issled. Funkts. Sistem* 47, Inst. Math. SB AS USSR, Novosibirsk, 1988, 66-88 (in Russian).

[5] F. I. Solov'eva, Structure of i-components of perfect binary codes, *Discr. Appl. Math.* 111, 2001, 189-197. dx.doi.org/10.1016/S0166-218X(00)00352-8, DOI: 10.1016/S0166-218X(00)00352-8.

[6] F. I. Solov'eva, On the construction of transitive codes, *Probl. Inform. Transm.* 41, 2005, 204-211. dx.doi.org/10.1007/s11122-005-0025-3, DOI: 10.1007/s11122-005-0025-3, transl. from Probl. Peredachi Inf. 41, 2005, 23-31.

[7] Yu. L. Vasil'ev, F. I. Solov'eva, Codegenerating factorization on n-dimensional unite cube and perfect binary codes, *Probl. Inform. Transm.* 33, 1997, 64-74, transl. from Probl. Peredachi Inf. 33, 1997, 64-74.

[8] A. Yu. Vasil'eva, A representation of perfect binary codes, *Proc. Seventh Intern. Workshop ACCT*, Bansko, Bulgaria, 2000, 311-315.

[9] V. A. Zinoviev, A. Lobstein, On generalized concatenated constructions of perfect binary nonlinear codes, *Probl. Inform. Transm.* 36, 2000, 336-348.

[10] V. A. Zinoviev, D. V. Zinoviev, Binary extended perfect codes of length 16 and rank 14, *Probl. Inform. Transm.* 42, 2006, 123-138, dx.doi.org/10.1134/S0032946006020062, DOI:10.1134/S0032946006020062 transl. from Probl. Peredachi Inf. 42, 2006, 63-80.