Constructions of perfect binary codes *

F.I. Solov'eva
Sobolev Institute of Mathematics
Koptyug pr. 4., Novosibirsk 630090, Russia
sol@math.nsc.ru

Abstract

We consider some constructions of perfect binary codes with the purpose to outline them and present the best known lower and upper bounds on the number of different perfect binary codes. Some nontrivial properties of perfect binary codes are discussed.

Contents

1 Introduction

The paper is devoted to single-error correcting perfect binary codes (also called close-packed codes); we briefly call them perfect codes. The problems of the construction and enumeration of perfect codes are significant and complicated. We don't know now neither the classification of perfect binary codes nor a satisfactory nontrivial upper bound on the number of nonequivalent perfect codes.

We consider some constructions of perfect codes with the purpose to discuss them and the bounds on the number of nonequivalent perfect codes. The best known lower

*This research was supported by the Russian Foundation for Basic Research under grant 97-01-01104

and upper bounds on the number of perfect codes of the given length are presented. We also consider some nontrivial properties of perfect binary codes such as the existence of nonsystematic perfect codes, the existence of kernels of all possible sizes for nonlinear perfect codes etc. Some unsolved problems will be discussed.

2 Necessary definitions

A *binary code* C of length n is a subset (not necessarily subspace) of the n-cube E^n (the vector space of dimension n over $GF(2)$). The elements of C are called codewords or vectors. *The Hamming distance* between two vectors $x, y \in C$, denoted by $d(x, y)$, is the number of coordinates in which the two vectors differ. *The Hamming weight* of the vector x is given by

$$wt(x) = d(x, \theta),$$

where θ denotes the all-zero word. A code distance is given by $d = min\ d(x, y) = min\ wt(x - y)$ for any different vectors $x, y \in C$. Two codes $C, C' \subset E^n$ are said to be *isomorphic* if there exists a permutation π of coordinates which maps the vectors of C into C'. Two codes $C, C' \subset E^n$ are *equivalent* if they are isomorphic or if the code C' is isomorphic to a translation of C, e.g. $C' = \{\pi(a) \oplus b : a \in C\}$, where π is the permutation and $b \in E^n$ is a fixed vector.

The union of spheres $K_t\{c\} = \{x \in E^n : d(c, x) \leq t\}$ of radius t with the centres c in the vectors of the set $M \subset E^n$ is called the *hull* of the set M and we denote this hull by $K_t(M)$. A set $C \subseteq E^n$ is called a perfect code of length n with code distance $d = 2t + 1$ if $K_t(C) = E^n$ and if $K_t\{v\} \cap K_t\{u\} = \emptyset$ for all $v, u \in C$.

In [34, 35, 36, 28] it is shown that nontrivial perfect binary codes exist only in the following two cases:

1) $d = 3$ and $n = 2^k - 1, k > 1$;

2) $d = 7$ and $n = 23$.

The well-known binary Golay code is a perfect code of length $n = 23$; up to equivalence this code is uniquely determined. If $d = 3$ and $n = 2^k - 1$ many constructions of perfect codes exist. We give a list of these constructions and describe some of them with the goal to develop bounds on the number of perfect codes and main approaches to the construction of perfect codes. ¿From now on we consider only the case $d = 3$.

3 Short summary of constructions

There exist two principal approches to the construction of perfect codes. One of them is an approach by switching and another by concatenation. More than 20 papers are devoted to the construction of perfect binary codes.

The well known Hamming codes are the only linear perfect codes (linear subspaces of the space E^n). In 1962 Vasil'ev [29] constructed a large number of nonequivalent perfect codes. In 1977 Heden [9] constructed perfect codes which are not equivalent to the Vasil'ev codes. The class of perfect codes described by Solov'eva in 1981 [22] (they are not equivalent to the Vasil'ev codes) contains the Heden codes properly. Two years later Phelps [16] independently discovered Solov'eva's construction and generalized it in 1984 [17]. Heden's construction properly contains the class of Laborde's (1983) codes [12], cf. [10]. A generalization of Vasil'ev's construction can be found in Mollard

(1986) [15]. In 1970 and 1988 Zinov'ev [33] gave two constructions of perfect codes with the method of concatenation. In 1989 Solov'eva [24] independently discovered last Zinov'ev's construction. In 1988 Solov'eva presented another class of perfect codes [23] and generalized it with Vasil'ev in 1995 [30]. In 1994 Vardy and Etzion described a class of perfect codes of full rank [8]. There are also three codes of length 15 (Bauer, Ganter and Hergert, 1983, [7]) and three codes of length 15 described by Heden in 1994 [10]. In 1995 Phelps and LeVan [18] presented perfect codes with all possible sizes of kernels. In 1996 Avgustinovich and Solov'eva [3] gave a construction of perfect codes which led to a new lower bound on the number of different perfect codes. In 1997 Lobstein and Zinov'ev generalized the "concatenation construction" of perfect codes [13] and in 1998 they modified it [14].

4 Upper bounds

Knowing the number of all perfect codes of a certain length n it is easy to calculate the number of nonequivalent perfect codes, therefore we will treat equivalent codes as different codes. There is only an upper bound on the number of different perfect codes close to a trivial bound. This bound follows immediately from the following nontrivial properties of perfect codes. Let $\mathbf{1}$ be the all-one vector, i.e. $\mathbf{1} = (1, 1, \ldots, 1)$.

Property 1. (Shapiro and Slotnik, [21].) *For every codeword $\alpha \in C$ we have $\alpha \oplus \mathbf{1} \in C$.*

Property 2. (Shapiro and Slotnik, [21].) *The number of codewords of weight $(n-1)/2$ of a perfect code of length n is equal to*

$$A_n = \left(\binom{n}{(n-1)/2} + n \binom{(n-1)/2}{(n-3)/4} \right) /(n+1).$$

Property 3. (Avgustinovich, [2].) *Every perfect code of length n is uniquely determined by its codewords of weight $(n-1)/2$.*

Denoting by T_n the number of all vectors of weight $(n-1)/2$ of the n-cube E^n, we obtain from these properties the following upper bound on the number N_n of different perfect codes

$$N_n \leq \binom{T_n}{A_n} \leq 2^{2^{n - \frac{3}{2}\log n + \log\log(en)}}.$$

Here and below $\log n$ is always the binary logarithm.

The trivial upper bound is

$$2^{2^{n - \log n + \log\log(n+1)}}.$$

We now discuss a switching approach, namely consider some switching constructions (Vasil'ev construction, Mollard codes, the method of $\tilde{\alpha}$-components). After that we consider concatenation constructions (the main idea of concatenation, Zinov'ev codes, Solov'eva codes, Phelps codes, generalized concatenation constructions given by Lobstein and Zinov'ev).

5 Vasil'ev codes, lower bound

Let V^p be a perfect code of length $p = 2^k - 1, k \geq 2$. Let λ be an arbitrary function from V^p to the set $\{0, 1\}$. For $\gamma \in E^p$ let $|\gamma| = \gamma_1 + \cdots + \gamma_p \pmod 2$, where $\gamma = (\gamma_1, \ldots, \gamma_p)$. Set $n = 2p + 1$.

Theorem 1. (Vasil'ev, [29].) *The set* $V^n = \{(\gamma, \gamma \oplus \beta, |\gamma| \oplus \lambda(\beta)) : \gamma \in E^p, \beta \in V^p\}$ *is a perfect code of length* n.

Since λ is an arbitrary function, we obtain (taking in account the previous iterative steps) the following lower bound on the number of different perfect codes:

$$N(V^n) \geq 2^{2^{\frac{n+1}{2} - \log(n+1)}} \cdot 2^{2^{\frac{n+5}{4} - \log(n+1)}},$$

where $N(V^n)$ denotes the number of Vasil'ev codes of length n.

This bound has been the best lower bound for a long time. The lower bounds given by Phelps [17] and Solov'eva [23] are of the form

$$2^{2^{\frac{n+1}{2}(1-\varepsilon_n)}},$$

where $\varepsilon_n \to 0$ if $n \to \infty$.

Some inessential improvement of $N(V^n)$ can be obtained by Mollard's construction [15]. We now consider his construction.

6 Mollard codes, lower bound

Let C^r and C^m be two perfect codes of length r and m respectively. Let

$$\alpha = (\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1m}, \alpha_{21}, \ldots, \alpha_{2m}, \ldots, \alpha_{r1}, \ldots, \alpha_{rm}) \in E^{rm}.$$

The generalized parity functions $p_1(\alpha)$ and $p_2(\alpha)$ are defined by $p_1(\alpha) = (\sigma_1, \sigma_2, \ldots, \sigma_r) \in E^r$, $p_2(\alpha) = (\sigma'_1, \sigma'_2, \ldots, \sigma'_m) \in E^m$, where $\sigma_i = \sum_{j=1}^{m} \alpha_{ij}$ and $\sigma'_j = \sum_{i=1}^{r} \alpha_{ij}$. Let f be an arbitrary function from C^r to E^m.

Theorem 2. (Mollard, [15].) *The set*

$$M^n = \{(\alpha, \beta \oplus p_1(\alpha), \gamma \oplus p_2(\alpha) \oplus f(\beta)) : \alpha \in E^{rm}, \beta \in C^r, \gamma \in C^m\}$$

is a perfect code of length $n = rm + r + m$.

In the case $m = 1$ Mollard's and Vasil'ev's constructions coincide. Solov'eva [26] has proved the existence of Mollard codes which are not Vasil'ev codes.

7 $\tilde{\alpha}$-components, lower bound

We now develop a switching approach (we shall call it the method of $\tilde{\alpha}$-components) and a lower bound on the number of different perfect codes of length n.

First some definitions. Let C be a perfect code in E^n, $n = 2^k - 1$, $k \geq 2$, and let M be a subset of C. Exchanging the bit in the i'th coordinate of all vectors of M with the opposite bit we obtain a new set, denoted by $M \oplus i$. If $C' = (C \setminus M) \cup (M \oplus i)$ is a perfect code, we call the set M an *i-component* of the code C and say that C' is obtained from C by a *translation* of an i-component M.

Let $\tilde{\alpha} \subseteq \{1, \ldots, n\}$. The set M is called an *$\tilde{\alpha}$-component* of the code C if it is an i-component for every $i \in \tilde{\alpha}$.

An i-component is *minimal* if it cannot be subdivided into smaller i-components. The concept of i-components (in the terminology of disjunctive normal forms) was introduced by Vasil'ev [29]. ¿From Vasil'ev's construction it is easy to see that the set $\{(\gamma, \gamma, |\gamma|) : \gamma \in E^p\}$ is always an n-component of V^n, $n = 2p + 1$.

It is known [23, 25] that upper and lower bounds on the number m of minimal i-components of an arbitrary perfect code of length n, $n = 2^k - 1$, are given by

$$2 \leq m \leq 2^{\frac{n+1}{2}}/(n+1).$$

Both of these bounds can be achieved, see [29, 23, 25]. The cardinality of the minimal i-components can vary from $2^{(n-1)/2}$ to $2^{n-1}/(n+1)$. Therefore choosing successively some of n coordinates and exchanging some of the components, we can obtain a great variety of perfect codes. Denote by H^* the set of all perfect codes obtained in this way from the Hamming code. The question of whether every perfect code can be obtained from a Hamming code in such a way was raised in [3]. Phelps and LeVan [20] presented a perfect code of length 15 and showed that it does not belong to H^*.

Now we give the description of the construction of Avgustinovich and Solov'eva [3, 6]. Let H^n be the Hamming code of length n (a linear perfect code). Let $\{i, j, k\}$ be the vector of H^n of weight 3 with only the i'th, j'th and k'th coordinates equal to 1 and $N_1 = 2^{\frac{n+5}{4} - \log(n+1)}$, $N_2 = 2^{\frac{n-3}{4}}$.

Proposition 1. *The Hamming code H^n can be partitioned in $\{i, j, k\}$-components R^t_{ijk} :*

$$H^n = \bigcup_{t=1}^{N_1} R^t_{ijk}.$$

Proposition 2. *Every $\{i, j, k\}$-component R^t_{ijk}, $t = 1, \ldots, N_1$, can be partitioned in i-components R^l_i :*

$$R^t_{ijk} = \bigcup_{l=1}^{N_2} R^l_i.$$

We now choose for every $\{i, j, k\}$-component R^t_{ijk} one of the coordinates i, j or k and divide the $\{i, j, k\}$-component into the components in the chosen coordinate. Thus the code H^n is split into the i-, j- and k-components with minimal cardinalities. This partitioning of the Hamming code allows us to construct cf. [3, 6] a large class of different perfect binary codes.

Theorem 3. *There are at least*

$$2^{2^{\frac{n+1}{2}-\log(n+1)}} \cdot 6^{2^{\frac{n+5}{4}-\log(n+1)}}$$

different perfect binary codes of length n.

This bound is better than the other known lower bounds.

It is not difficult to see that this construction method is possible for the Hamming code divided into some $\tilde{\alpha}$-components, where every $\tilde{\alpha}$-component is divided into $\tilde{\alpha'}$-components, $\tilde{\alpha'} \subseteq \tilde{\alpha}$. Such partitions yield complicated classes of perfect codes. We restrict ourselves to the case which gave us the maximal factor in the lower bound of theorem 3.

We do not know, if this lower bound can be raised.

¿From sections 5-7 it is clear that Vasil'ev and Mollard constructions can be described by the method of $\tilde{\alpha}$-components.

8 The main idea of concatenation constructions. Zinov'ev codes

Consider the main idea of concatenation construction presented by Zinoviev (1970). Below we use the notation (n, K, d) for a code of length n, cardinality K and code distance d. Let A be a q-ary $(n, |A|, d)$ code. Let B be a q'-ary $(N, |B|, d')$ code, with $|B| = q$. We label the codewords of B from 0 to $q-1$: $B = \{\mathbf{b}(0), \ldots, \mathbf{b}(q-1)\}$. For any codeword $\mathbf{a} = (a_1, \ldots, a_n) \in A$, we construct the vector $\mathbf{a}(B) = (\mathbf{b}(a_1)| \ldots |\mathbf{b}(a_n))$, where $|$ stands for concatenation. Now $C = \{\mathbf{a}(B) : \mathbf{a} \in A\}$ is a q'-ary code with length nN, size $|C| = |A|$ and minimum distance $d(C) \geq dd'$. The codes A, B and C are called, respectively, the *outer*, *inner* and *concatenated codes.*

Let now A be a q-ary perfect $(n, |A|, d)$ code, $q = 2^k$, $n = 2^k + 1$, and let $C_0, C_1, \ldots, C_r$ be any partition of the vector space E^r into perfect codes, $r = 2^k - 1$.

Theorem 4. (Zinov'ev, [33], see also [24].) *The set Z^N defined by*

$$Z^N = \{(c_0|c_1| \ldots |c_n) : c_i \in C_{a_i}, i = 0, 1, \ldots, n, (a_1, a_2, \ldots, a_n) \in A\}$$

is a perfect binary code of length $N = nr = 2^{2k} - 1$.

9 Solov'eva codes

Let $C_0, C_1, \ldots, C_n$ and $C'_0, C'_1, \ldots, C'_n$ be any partitions of the vector space E^n into perfect codes (constructions of nontrivial partitions of E^n can be found in [22]). Let π be a permutation on the set $\{0, 1, \ldots, n\}$.

Theorem 5. (Solov'eva, [22].) *The set*

$$C^{2n+1} = \{(x, y, |y|) : x \in C_i, y \in C'_{\pi(i)}, i = 0, 1, \ldots, n\} \tag{1}$$

is a perfect binary code of length $2n + 1$.

10 Phelps codes

Let $C_0^0, C_1^0, \ldots, C_n^0$ and $C_0^1, C_1^1, \ldots, C_n^1$ be any partitions of the even and odd weight vectors of E^{n+1} into extended perfect codes of length $n+1$ respectively. Now let C be an extended perfect code of length $m+1 = 2^p$ in E^{m+1}. For each vector $v \in C$, let $C(v)$ be a minimum distance 2 code of length $m+1$ over $GF(n+1)$, $|C(v)| = (n+1)^m$, $n+1 = 2^k$.

Theorem 6. (Phelps, [17].) *The set P^N defined by*

$$P^N = \{(c_0|c_1|\ldots|c_m) : c_i \in C_{j_i}^{v_i}, v = (v_0, v_1, \ldots, v_m) \in C,$$

$$(j_0, j_1, \ldots, j_m) \in C(v)\}$$

is an extended perfect binary code of length $N = (m+1)(n+1)$.

Puncturing any coordinate of the code P^N gives a perfect code of length $(m+1)(n+1) - 1$.

For $m = 1$, a code C is a trivial "extended perfect" code consisting of a vector $(0, 1)$. The code $C(v)$ is an $(n+1)$-ary code of length 2 with distance 2, which corresponds to a permutation π on $n+1$ elements

$$C(v) = \{(0, \pi(0)), (1, \pi(1)), \ldots, (n, \pi(n)), \}.$$

Thus Theorem 5 is a particular case of Theorem 6 and we obtain the construction (1).

The number of nonequivalent codes of length n given by Theorem 6 is at least

$$2^{2^{\frac{n+1}{2}(1-\varepsilon_n)}},$$

where $\varepsilon_n \to 0$ if $n \to \infty$.

11 Generalized concatenated codes. Lobstein and Zinov'ev codes.

Let B be a q_B-ary $(n_B, K_1, d_{B,1})$ code. Assume that the code B is partitioned into q_1 subcodes:

$$B = \bigcup_{i=0}^{q_1-1} B_i,$$

where B_i is a q_B-ary $(n_B, K_2, d_{B,2})$ code for $i = 0, 1, \ldots, q_1 - 1$.

Assume furthermore that each subcode B_i can be partitioned into q_2 subcodes: for $i = 0, 1, \ldots, q_1 - 1$,

$$B_i = \bigcup_{j=0}^{q_2-1} B_{i,j},$$

where $B_{i,j}$ is a q_B-ary $(n_B, K_3, d_{B,3})$ code, $|K_3| = q_3 - 1$.

Let any codeword $\mathbf{b} \in B$ has index k in $B_{i,j}$ then the triple

$$(i, j, k) \in \{0, \ldots, q_1 - 1\} \times \{0, \ldots, q_2 - 1\} \times \{0, \ldots, q_3 - 1\}$$

characterizes the vector $\mathbf{b}$ and one can note $\mathbf{b} = \mathbf{b}(i, j, k)$.

Consider, for $\ell = 1, 2, 3$, a q_ℓ-ary $(n_A, K_{A,\ell}, d_{A,\ell})$ code A_ℓ and a codeword $\mathbf{a}^\ell = (a_1^\ell, \dots, a_{n_A}^\ell) \in A_\ell$. For any $s = 1, \dots, n_A$ the triple (a_s^1, a_s^2, a_s^3) designates a codeword $\mathbf{b} = \mathbf{b}(a_s^1, a_s^2, a_s^3) \in B$.

Let

$$C = \{(\mathbf{b}(a_1^1, a_1^2, a_1^3)| \dots |\mathbf{b}(a_{n_A}^1, a_{n_A}^2, a_{n_A}^3)) : \mathbf{a}^\ell \in A_\ell, 1 \leq \ell \leq 3\}.$$

Theorem 7. (See [31, 32].) *The code C is a q_B-ary code of length $n_C = n_A n_B$, cardinality $K_{A,1}K_{A,2}K_{A,3}$ and distance*

$$d_C \geq \min\{d_{A,1}d_{B,1}, d_{A,2}d_{B,2}, d_{A,3}d_{B,3}\}.$$

Consider the binary case. Let $B = E^{n_B}$, $B = E_0^{n_B} \cup E_1^{n_B}$, where $E_0^{n_B}$ and $E_1^{n_B}$ are the all even and all odd weight vectors of B respectively, $n_B = 2^m$. Consider for $E_0^{n_B}$ and $E_1^{n_B}$ partitions into 2^m extended perfect codes of length n_B.

Let A_1 be a binary extended perfect code $(n_A, 2^{n_A-1-u}, 4)$, $n_A = 2^u$. Let A_2 be an n_B-ary $(n_A, n_B^{n_A-1}, 2)$ code and A_3 be a q_3-ary $(n_A, q_3^{n_A}, 1)$ code, where $q_3 = 2^{n_B-1-m}$.

Using the construction of Theorem 7 we obtain from (2) a binary extended perfect code C of length 2^{m+n}.

Theorem 8. (See [13].) *The code C is an extended perfect binary code of length 2^{m+n}.*

Special case of this basic construction were obtained in [33]. In turn this construction is a special case of a construction by Phelps described in [17] in a different way without mentioning concatenation construction (see above the section 10).

In [13, 14] Lobstein and Zinov'ev generalized Theorem 8 by permuting all n_B alphabet symbols of the second outer code A_2.

In [14] they modified further the resulting code by adding an $n_B \times n_A$ matrix to the codewords, using the interesting fact that this does not alter the distances between codewords. The fact allows them to get switching Vasil'ev codes from the concatenation construction.

The question of whether every switching construction can be described by concatenation or vice versa is still open.

12 Nonsystematic perfect codes

We now continue to describe some properties of perfect codes.

The technique of $\tilde{\alpha}$-components allowed Avgustinovich and Solov'eva [4, 5] to obtain nonsystematic perfect binary codes of length n for every $n = 2^k - 1, \ \ k \geq 8$. The question about the existence of nonsystematic perfect codes was posed by Hergert [11]. A perfect code C of length n is systematic if there are $n - \log(n+1)$ coordinates (called information symbols) such that the code C deleted in the remaining $\log(n+1)$ coordinates (called check symbols) coincides with $E^{n-\log(n+1)}$.

Proposition 3. *Let $n = 2^k - 1, \ \ k \geq 8$. There are n minimal components $M_1, \dots, M_n$ with minimal cardinalities in the Hamming code H^n such that the i'th component M_i is an i-component and the distance between two components M_i and M_j is more than 5 if $i \neq j$.*

This property allows us to exchange every i-component M_i in the i'th coordinate. With this we obtain

Theorem 9. (See [4, 5].) *The set*

$$C = (H^n \setminus (\bigcup_{i=1}^{n} M_i)) \cup (\bigcup_{i=1}^{n} (M_i \oplus i))$$

is a nonsystematic code of length n for every $n = 2^k - 1,\ \ k \geq 8$.

The existence of nonsystematic perfect codes of length $n = 2^k - 1,\ \ 5 \leq k \leq 7$, was proved by Phelps and LeVan [19].

13 Isometries of perfect codes

Let φ be an *isometric* map from C to C', i.e. a map between two perfect codes C and C' such that $d(x, y) = d(\varphi(x), \varphi(y))$ for every $x, y \in C$.

Theorem 10. (Avgustinovich, [1].) *Let $n > 15$ and C, C' be any two isometric perfect codes. Then they are isomorphic.*

It is also true if $n = 15$ but if $n = 7$ there exists the isometric map φ from H^7 to H^7 such that φ is not extendable to an isomorphism of the whole space E^7, see [27].

14 Kernels of perfect codes

Let $C \subseteq E^n$ be a code. The set K of all vectors $x \in E^n$, for which $C \oplus x = C$ is called the kernel of C.

In 1994 Heden [10] found three perfect codes of length 15 which have kernels of dimension 1, 2 and 3.

In 1995 Phelps and LeVan [18] established the following result

Theorem 11. *For all $k \geq 4$ there exists a nonlinear perfect code of length $n = 2^k - 1$ which has a kernel of dimension j if and only if $j \in \{1, 2, \ldots, 2^k - k - 3\}$.*

Studying kernels and $\tilde{\alpha}$-components may be helpful for the decision of the complicatedly seeming question if two given perfect codes are equivalent.

The author is grateful to Werner Heise and the anonymous referees for comments improving the presentation of the paper.

References

[1] *Avgustinovich S.V.*, On nonisometry of perfect binary codes, Proc. of Institute of Math. SO RAN 27 (1994) 3-5.

[2] *Avgustinovich S.V.,* On a property of perfect binary codes, Discrete Analysis and Operation Research 2 (1) (1995) 4-6.

[3] *Avgustinovich S.V., Solov'eva F.I.,* Construction of perfect binary codes by sequential translations of the i-components, Proc. of Fifth Int. Workshop on Algebraic and Comb. Coding Theory. Sozopol, Bulgaria. June (1996) 9-14.

[4] *Avgustinovich S.V., Solov'eva F.I.,* Existence of nonsystematic perfect binary codes, Proc. of Fifth Int. Workshop on Algebraic and Comb. Coding Theory, Sozopol, Bulgaria, June (1996) 15-19.

[5] *Avgustinovich S.V., Solov'eva F.I.,* On the nonsystematic perfect binary codes, Problems of Information Transmission 32 (3) (1996) 258-261.

[6] *Avgustinovich S.V., Solov'eva F.I.,* Construction of perfect binary codes by sequential translations of an $\tilde{\alpha}$-components, Problems of Information Transmission 33 (3) (1997) 202-207.

[7] *Bauer H., Ganter B., Hergert F.,* Algebraic techniques for nonlinear codes, Combinatorica 3 (1983) 21-33.

[8] *Etzion T., Vardy A.,* Perfect binary codes: Constructions, properties and enumeration, IEEE Trans. Inform. Theory 40 (3) (1994) 754-763.

[9] *Heden O.,* A new construction of group and nongroup perfect codes, Inform. and Control 34 (4) (1977) 314-323.

[10] *Heden O.,* A binary perfect code of length 15 and codimension 0, Designs, Codes and Cryptography 4 (1994) 213-220.

[11] *Hergert F.,* Algebraische Methoden fur Nichtlineare Codes, Thesis Darmstadt (1985).

[12] *Laborde J.-M.,* Une nouvelle famille de codes binaires, parfaits, non linéaires, C.R. Acad. Sc. Paris 297 (1) (1983) 67-70.

[13] *Lobstein A.C., Zinov'ev V.A.,* On new perfect binary nonlinear codes, Applicable Algebra in Engin. Comm. and Comput., 8 (1997) 415-420.

[14] *Lobstein A.C., Zinov'ev V.A.,* On some constructions of perfect binary nonlinear codes, Designs, Codes and Cryptography, submitted.

[15] *Mollard M.,* A generalized parity function and its use in the construction of perfect codes, SIAM J. Alg. Disc. Meth. 7 (1) (1986) 113-115.

[16] *Phelps K.T.,* A combinatorial construction of perfect codes, SIAM J. Alg. Disc. Meth. 4 (3) (1983) 398-403.

[17] *Phelps K.T.,* A general product construction for error correcting codes, SIAM J. Alg. Disc. Meth. 5 (2) (1984) 224-229.

[18] *Phelps K.T., LeVan M.J.,* Kernels of nonlinear Hamming codes, Designs, Codes and Cryptography 6 (1995) 247-257.

[19] *Phelps K.T., LeVan M.J.,* Non-systematic perfect codes, SIAM Journal of Discrete Mathematics, to appear.

[20] *Phelps K.T., LeVan M.J.,* Switching equivalence classes of perfect codes, Designs, Codes and Cryptography, submitted.

[21] *Shapiro G.S., Slotnik D.L.,* On the mathematical theory of error correcting codes, IBM J. Res. and Devel. 3 (1) (1959) 25-34.

[22] *Solov'eva F.I.,* On binary nongroup codes, Methody Discretnogo Analiza 37 (1981) 65-76. (in Russian).

[23] *Solov'eva F.I.,* Factorization of code-generating disjunctive normal forms, Methody Discretnogo Analiza 47 (1988) 66-88. (in Russian).

[24] *Solov'eva F.I.,* Class of close-packed binary codes generated by q-ary codes, Methody Discretnogo Analiza 48 (1989) 70-72. (in Russian).

[25] *Solov'eva F.I.,* Exact bounds on the connectivity of code-generating disjunctive normal forms, Inst. Math. of the Siberian Branch of Acad. of Sciences USSR, Preprint 10 (1990) 15 (in Russian).

[26] *Solov'eva F.I.,* A combinatorial construction of perfect binary codes, Proc. of Fourth Int. Workshop on Algebraic and Comb. Coding Theory, Novgorod, Russia. September (1994) 171-174.

[27] *Solov'eva F.I., Avgustinovich S.V., Honold T., Heise W.,* On the extendability of code isometries, Beitrage zu Geometrie und Algebra, Tu München 35 (1997), Obtainable through the web page http://www-lit.mathematik.tu-muenchen.de/veroeff/quel/971.94008.ps.gz.

[28] *Tietäväinen A.,* On the nonexistence of perfect codes over finite fields, SIAM J. Appl. Math. 24 (1973) 88-96.

[29] *Vasil'ev Y.L.,* On nongroup close-packed codes, Problems of Cybernetics 8 (1962) 375-378 (in Russian).

[30] *Vasil'ev Y.L., Solov'eva F.I.,* Interdependence between perfect binary codes and their projections, Proc. Seventh Joint Swedish-Russian Workshop on Information Theory, St.-Petersburg, Russia. June (1995) 239-242.

[31] *Zinov'ev V.A.,* On Generalized Concatenated Codes. Colloquia Mathematica Societatis Jànos Bolyai **16**, Topics in Information Theory, Keszthely, Hungary (1975) 587-592.

[32] *Zinov'ev V.A.,* Generalized Concatenated Codes. Problems of Information Transmission 12 (3) (1976) 23-31.

[33] *Zinov'ev V.A.,* A combinatorial methods for the construction and analysis of nonlinear error-correcting codes, Doc. D. Thesis, Moscow (1988) (in Russian).

[34] *Zinov'ev V.A., Leontiev V.K.,* A theorem on nonexistence of perfect codes over Galois fields, Inst. of Problems Information Transmission, Preprint, 1972 (in Russian).

[35] *Zinov'ev V.A., Leontiev V.K.,* On perfect codes, Problems of Control and Inform. Theory 1 (1972) 26-35.

[36] *Zinov'ev V.A., Leontiev V.K.,* Nonexistence of perfect codes over Galois fields, Problems of Control and Inform. Theory 2 (2) (1973) 123-132.