Com^{2}MaC LECTURE NOTE SERIES 13

ON PERFECT CODES AND RELATED TOPICS

Faina I. Soloveva

Combinatorial and Computational Mathematics Center
Pohang University of Science and Technology

Series of lecture notes from the lectures held at Com^{2}MaC in POSTECH.

2000 *Mathematics Subject Classification*: ?????

Faina I. Soloveva
Sobolev Institute of Mathematics
pr. Koptyuga 4
Novosibirsk 630090, Russia
Email: sol@math.nsc.ru

Editors :

Sungpyo Hong
Department of Mathematics
POSTECH
Pohang, 790--784
Korea

Sung-Yell Song
Department of Mathematics
Iowa State University,
Ames, Iowa 50011
U. S. A.

Mar. 2004 Combinatorial and Computational Mathematics Center
Pohang University of Science and Technology (POSTECH)

ON PERFECT CODES AND RELATED TOPICS

Faina I. Soloveva

Sobolev Institute of Mathematics
pr. Koptyuga 4
Novosibirsk 630090, Russia
Email: sol@math.nsc.ru

This work is partially supported by Com^{2}MaC-KOSEF, Korea.

To Ivan and Maria

Preface

Some results on perfect codes and related topics are discussed. The main methods to construct perfect codes such as the switching method and the concatenation approach and their implementations to solve some important problems are analyzed. The solution of ranks and kernels problem, the lower and upper bound of the automorphism group order of a perfect code, spectral properties, and isometries of perfect codes and codes close to them by close-packed properties are considered.

The topic of perfect codes is one of the most fascinating topics in the theory of error-correcting codes. The class of perfect binary codes is very complicated, large and intensively studied by many researches, see the list of references. The investigation of nontrivial properties of perfect codes is important both from coding point of view (for the solution of the classification problem for such codes) and for combinatorics, graph theory, group theory, geometry. Many constructions and properties, for example, for perfect binary codes can be applied for codes with different parameters (lengths, sizes, distances) or for nonbinary cases.

There are several surveys devoted to perfect codes, see [24, 75, 77, 76, 12]. We discuss in these lectures some results on perfect binary codes and some related correspondence between perfect codes and Steiner triple systems or codes with other parameters (length or distance).

The lectures are organized as follows: first we give necessary definitions and notations (Chapter 1), then we consider the Hamming code and its properties (Chapter 2), the well known Vasil'ev codes and their properties (Chapter 3), and some properties and constructions of Steiner triple systems (Chapter 4). Properties of linear codes are considered in Chapter 5, for the concatenation approach and its implementations to get solutions of some important problems, see Chapter

6, the main methods to construct perfect codes such as the switching method and its implementations to establish some interesting nontrivial properties of perfect codes are presented in Chapter 7, and in Chapter 8 we discuss several spectral properties of perfect codes (see Sections 8.1 and 8.3), upper bound on the number of perfect binary codes (Section 8.2), automorphism groups of perfect codes (Section 8.4), the solution of ranks and kernels problem (Section 8.5), and isometries of perfect codes and codes close to them by close-packed properties (Section 8.6). We discuss some results in more details, others we only concern. It should be noted that the lecture notes are organized in such a way that in the first reading each chapter can be considered independently from other chapters taking only into account Chapter 1.

Contents

Preface **v**

1 Necessary definitions **1**

2 The Hamming code and its properties **5**
2.1 Decoding of the Hamming code 7

3 Vasil'ev codes **9**

4 Steiner triple systems **13**
4.1 The Assmuss and Mattson construction of Steiner triple systems 14

5 On one property of linear codes **19**

6 Concatenation approach **23**
6.1 The main idea of the concatenation approach 23
6.2 Solov'eva codes – 1981 25
6.3 Romanov codes 29
6.4 Hämäläinen codes 31
6.5 Zinov'ev's concatenation construction – 1988 33
6.6 Phelps codes 34
6.7 Generalized concatenated codes. Lobstein and Zinov'ev codes 36

7 Switching approach **39**
7.1 Mollard codes, lower bound 39
7.2 Method of α-components 41

7.3 Combining construction 44
7.4 Method of i-components 47

8 Some properties of perfect binary codes 51
8.1 Spectral properties. Part I. 51
8.2 Upper bound on the number of perfect binary codes . . . 56
8.3 Spectral properties. Part II. 59
8.4 Automorphism groups of perfect codes 61
8.5 Ranks and kernels problem 64
8.6 Metrical rigidity 68

Bibliography 71

Index 80

Chapter 1

Necessary definitions

A binary code C of length n is a subset of the n-dimensional metric space E^n over the Galois field $GF(2)$ with the Hamming metric.

The Hamming distance $d(x, y)$ between vectors $x, y \in E^n$ is a number of coordinates in which x and y differ.

The Hamming weight of $x \in E^n$ is defined as $wt(x) = d(x, \mathbf{0^n})$, where $\mathbf{0^n}$ is the all-zero vector of length n. Let $\mathbf{1^n}$ be the all-one vector of length n.

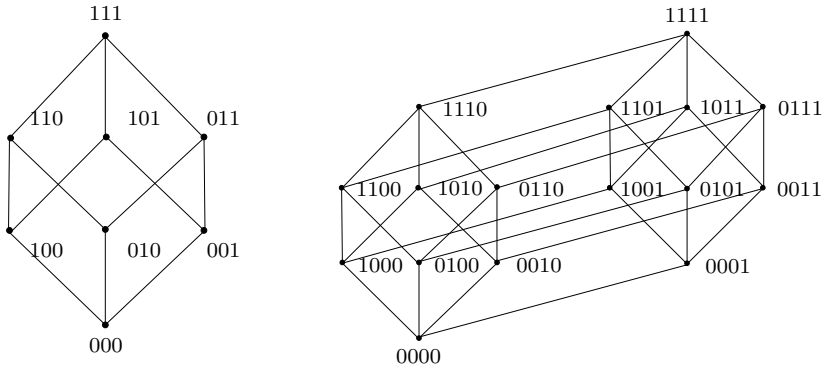

Figure 1.1: 3-dimensional, 4-dimensional cubes.

We put all vectors of the same weight i, on the i-th level of the n-cube E^n, $i \in \{0, 1, 2, \ldots, n\}$, see Figures 1.1 and 1.2.

A code distance is defined as $d = min\, d(x, y)$ for any two different

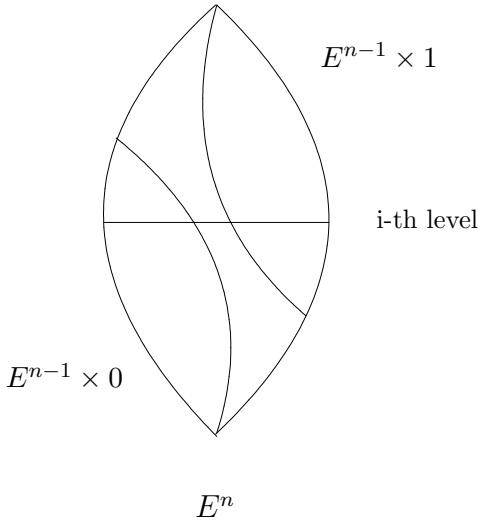

Figure 1.2: n-dimensional cube.

codewords x, y from the code C.

Two codes $C, C' \subset E^n$ are said to be *isomorphic* if there exists a permutation π such that $C' = \pi(C) = \{\pi(x) : x \in C\}$.

Codes $C, C' \subset E^n$ are *equivalent* if there exists a vector $b \in E^n$ and a permutation π such that $C' = b + \pi(C) = \{b + \pi(x) : x \in C\}$.

A neighborhood $K(C)$ of a set C in E^n is the union of spheres of radius 1 with centers at the vectors of C.

A code C is *perfect* if $K(C) = E^n$ and $K(x) \cap K(y) = \emptyset$ for any $x, y \in C$. This definition gives us a close-packed property: the whole space E^n is partitioned by spheres of radius one with centers in the codewords. The definition is equivalent to the following: a code C is perfect if for any vector $z \in E^n$ there exists exactly one vector $x \in C$ such that $d(z, x) \leq 1$.

In [92, 93, 82] the following important theorem is proved:

Theorem 1. *Nontrivial perfect codes of length n exist only in the following three cases:*

1) $d = 3$ and $n = (q^m - 1)/(q - 1), m > 1$, $q = p^k$, where p is a prime number;

2) $d = 7$ and $n = 23$, $q = 2$;

3) $d = 5$ and $n = 11$, $q = 3$.

The well-known binary and ternary Golay codes are perfect codes

of lengths 23 and 11 respectively; up to equivalence these codes are uniquely determined. If $d = 3$ and $n = (q^m - 1)/(q - 1)$ many constructions of perfect codes exist, especially for the binary case. We give a list of these constructions and describe some of them with the goal to establish bounds on the number of perfect binary codes and to show the main approaches to the construction of such codes. We also consider some nontrivial properties of perfect codes. From now on if it will not be otherwise stated we only consider perfect binary codes with distance $d = 3$ (we briefly call them perfect codes) because the binary case is usually typical and very often it is possible to generalize a construction developed for the binary case to a q-ary case, $q > 2$ taking into account the structure of the Galois field $GF(q)$.

Chapter 2

The Hamming code and its properties

To define a binary Hamming code, which was presented by Hamming in 1949 we would remind the following theorem.

Theorem 2. *If H is the parity check matrix of a linear code of length n, then the code has minimum distance d if and only if every $d-1$ columns of H are linearly independent and some d columns are linearly dependent.*

Now we are going to construct a perfect binary group code with distance 3.

Using a proof of the well known Varshamov and Gilbert bound Theorem, see [46], chapter 1, for any natural number m we have to take binary vectors of length m satisfying Theorem 2 for the case when the code distance equals 3. We have to construct a parity check matrix such that any two columns are linearly independent and some three vectors are linearly dependent. Excluding the all-zero vector $\mathbf{0^m}$ we can take in this case all vectors from the vector space E^m. As a result we have a group code with distance 3 defined by its parity check matrix. It is called the Hamming code. We will further denote it by H^n.

The parameters of the Hamming code H^n are the following

$$[n = 2^m - 1, k = n - \log(n+1), d = 3],$$

$m = \log(n+1)$ (here and below $\log(n+1)$ is always a binary logarithm if not stated otherwise) we use here the same notations as in the book of MacWilliams and Sloane [46]: n stands for the code length, k – for the dimension of the code and d – for the distance.

Proposition 1. *The Hamming code H^n is perfect.*

Proof. This code corrects one error according to the definition of the code. The size of the code is

$$|H^n| = 2^k = \frac{2^n}{n+1}.$$

Therefore the code reaches the Hamming bound and is perfect.

Proposition 2. *The Hamming code H^n is unique up to equivalence.*

Proof. One Hamming code presented by its parity check matrix differs from another one only by a permutation π of its parity check matrix columns. This permutation gives the same permutation π of n coordinates positions, which transforms one code to another.

Examples of the Hamming codes of length 7.

Let us consider the following three different presentations of the Hamming code of length 7.

1) It can be done in the standard form, see [46], chapter 1, which means that last three columns define the identity matrix of order 3, for example the parity check matrix is

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

2) A code C of length n is *cyclic* if the word $(x_2, x_3, \ldots, x_n, x_1) \in C$ for any codeword $x = (x_1, x_2, \ldots, x_n) \in C$.

The Hamming code H^7 presented by its parity check matrix given in the cyclic form is the following:

$$H = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

3) In many cases it is useful to define the Hamming code by its parity check matrix given in the lexicographic order of increasing binary numbers:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

2.1 Decoding of the Hamming code

Decoding of the Hamming code is very easy. Let us consider a presentation of the Hamming code H^n in the lexicographic order of increasing binary numbers:

$$H_m = [B(1), B(2), \ldots, B(n)],$$

here H_m is a parity check matrix of the code H^n, $m = \log(n+1)$, $B(i)$ is the binary presentation of an integer i. Using the parity check matrix H_m we can formulate the following definition of the Hamming code:
$H^n = \{x = (x_1, \ldots, x_n) : x \in E^n$ and $\sum_{i=1}^{n} B(i) \times x_i = \mathbf{0^m}.\}$
If there is a single error in the i-th coordinate and we receive a vector y from the channel we can calculate the syndrome

$$S = Hy^\top = He_i = B(i),$$

which shows the error position i in the vector y. Here e_i is the vector of weight one with 1 only in the i-th coordinate position.

Later we consider the construction of a Hamming code over the Galois field $GF(q)$ for any q.

Exercises.

1. Find the different numbers of bases in the n-cube E^n.

2. Find the different numbers of linear binary codes of length n and cardinality k.

3. Let us receive the vector $y = (01101101)$. Find the input codeword if it was used the binary extended Hamming code of length 8 given by its parity check matrix in the lexicographic presentation.

Chapter 3

Vasil'ev codes

Before defining the main switching approach to construct perfect codes (see chapter 7), we are going to consider the first switching construction of perfect codes given by an analytic formula. Further we will show that this construction is really a switching construction. This well known construction was presented by Vasil'ev in 1962, see [84].

In 1959 Shapiro and Slotnik, see [69], conjectured that there is no nonlinear perfect code. Vasil'ev constructed a very large class of perfect binary nonlinear codes and showed that this conjecture was false.

Let $C^{(n-1)/2}$ be a perfect code of length $(n-1)/2 = 2^m - 1, m \geq 2$, and λ be an arbitrary function from $C^{(n-1)/2}$ to the set $\{0,1\}$. For $x = (x_1, \ldots, x_{(n-1)/2}) \in E^{(n-1)/2}$ let $|x| = x_1 + \ldots + x_{(n-1)/2} (\mathrm{mod} 2)$.

Theorem 3. (Vasil'ev, 1962, see [84].) *The set*

$$V^n = \{(x+y, |x| + \lambda(y), x) : x \in E^{(n-1)/2}, y \in C^{(n-1)/2}\}$$

is a perfect binary code of length n.

Proof. We have to check the code parameters: code length, size of the code and code distance.

1. It is easy to check that the length satisfies the condition $n = 2^{m+1} - 1$:

$$n = 2 \cdot (n-1)/2 + 1 = 2 \cdot 2^m - 1.$$

2. The size of the code is

$$|V^n| = |E^{(n-1)/2}| \cdot |C^{(n-1)/2}| = 2^{(n-1)/2} \cdot 2^{(n-1)/2} / ((n-1)/2+1) = 2^n/(n+1).$$

3. Now we are going to check that the distance between two arbitrary codewords

$$u = (x + y, |x| + \lambda(y), x),$$
$$v = (x' + y', |x'| + \lambda(y'), x')$$

is at least 3.

There are the following three cases:

3a. If $y = y'$ and $x \neq x'$ then

$$d(u, v) = d((x, |x|, x), (x', |x'|, x')) \geq 3$$

because $x, x' \in E^{(n-1)/2}$ and $d(x, x') \geq 1$.

3b. Suppose $y \neq y\prime$ and $x = x'$. Vectors y, y' are from $C^{(n-1)/2}$ therefore $d(y, y') \geq 3$ and we get

$$d(u, v) \geq d(y, y') \geq 3.$$

3c. Assume $y \neq y\prime$ and $x \neq x'$ then for

$$d(x, x') \geq 1, 2, 3, \ldots$$

we have

$$d(x + y, x' + y') \geq 2, 1, 0, \ldots$$

respectively. Adding these distances we obtain

$$d(u, v) \geq 3.$$

The proof is done.

Corollary 1. *If $\lambda \equiv 0$ and $C^{(n-1)/2} = H^{(n-1)/2}$ we get the Hamming code*

$$H^n = \{(x + y, |x|, x) : x \in E^{(n-1)/2}, y \in H^{(n-1)/2}\}$$

of length n.

Corollary 2. *Assume $\lambda(y)+\lambda(y') \neq \lambda(y+y')$ for some $y, y' \in C^{(n-1)/2}$. Then we get a nonlinear perfect code of length n from Vasil'ev's construction.*

Since λ is an arbitrary function, taking into account all previous iterative steps we obtain the following statement.

Corollary 3. *The number D_n of different Vasil'ev codes of length n satisfies the lower bound*

$$D_n \geq 2^{2^{\frac{n+1}{2}-\log(n+1)}} \cdot 2^{2^{\frac{n+5}{4}-\log(n+1)}} \cdot 2^{2^{\frac{n+9}{8}-\log(n+1)}} \cdot \ldots$$

Knowing the number of all perfect codes of a certain length n it is easy to calculate the number of nonequivalent perfect codes. One has to only divide this number by the number $2^n \cdot n!$, where 2^n stands for the different possible translates in E^n and there are $n!$ valuable permutations of all the coordinate positions. Therefore it is possible to treat equivalent codes as different codes. It is not difficult to see from Corollary 3 the following statement:

Corollary 4. *The number N_n of nonequivalent Vasil'ev codes of length n satisfies the lower bound*

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

for n sufficiently large.

This bound has been the best lower bound for a long time. The lower bounds on the number of nonequivalent perfect codes of length n given by other researches till 1996 were of the form

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

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

How to get better than the Vasil'ev lower bound on the number of nonequivalent perfect binary codes see below Section 7.2.

For $n = 7$ there exists only one perfect code, for $n = 15$ there are 11 nonequivalent Vasil'ev codes, see [33] and at least 963 nonequivalent perfect codes of length 15, see Phelps [61].

Exercise. Prove Corollary 4 using the Stirling formula

$$n^n e^{-n}\sqrt{2n\pi} \leq n! \leq n^n e^{1-n}\sqrt{2n\pi}.$$

Open problem

Find the classification of all perfect binary codes of length 15.

Chapter 4

Steiner triple systems

There is a close relation between perfect codes and Steiner triple systems.

A Steiner triple system of order n (briefly $STS(n)$) is a family of 3-element blocks (subsets or triples) of the set $N = \{1, 2, \ldots, n\}$ such that each not ordered pair of elements of N appears in exactly one block.

Two STS-s of order n are called *isomorphic* if there exists a permutation on the set N which transforms them into one another.

It is well known that $STS(n)$ exists if and only if $n \equiv 1$ or $3 \pmod 6$. It is easy to calculate that the number of blocks in $STS(n)$ is $|STS(n)| = n(n-1)/6$.

Further we will identify any vector $x = (x_1, \ldots, x_n) \in E^n$ with its block presentation $(i_1, \ldots, i_k)$, where $i_1, \ldots, i_k$ are only the coordinate positions of the vector x equaled to 1. This correspondence is one-to-one and further every time when we consider a block presentation of a vector x it will be clear what is the length of this vector. A vector $x + \mathbf{1^n}$ is called a *compliment* to the vector x.

Example. Let us consider a Steiner triple system of order 7

$$STS(7) = \{(1,2,3), (1,4,5), (2,4,6), (3,4,7), (1,6,7), (2,5,7), (3,5,6)\}.$$

It is not difficult to see that this set with its complement blocks of weight 4 in E^7 together with $\mathbf{0}^7$ and $\mathbf{1}^7$ gives the Hamming code H^7 of length 7.

Theorem 4. *Let a perfect code C^n of length n contain the all-zero vector. Then all its codewords of weight 3 form an $STS(n)$.*

Proof. By the condition of the theorem $\mathbf{0}^n \in C^n$. By the close-packed property of the code C^n each not ordered pair (i, j), where $i, j \in N$, belongs to some triple (i, j, k) from C^n. It is easy to show that this pair belongs to only one triple. Suppose there exists another triple $(i, j, t), t \neq k$ from C^n containing the pair (i, j). Then

$$d((i, j, k), (i, j, t)) = 2,$$

which contradicts to the fact that the code distance in C^n is 3. The proof is done.

Let $E_i^n = \{x = (x_1, \ldots, x_n) : x \in E^n \text{ and } w(x) = i\}$. We consider without proofs the following two theorems.

Theorem 5. (See [45].) *For any $n \equiv 1$ or 3 (mod 6), $n > 7$, there exists a partition of E_3^n into $n - 2$ disjoint STS-s of order n.*

Theorem 6. *The number $N(n)$ of nonisomorphic Steiner triple systems of order n satisfies the following bounds*

$$(e^{-5}n)^{\frac{n^2}{6}} \leq N(n) \leq (e^{-1/2}n)^{\frac{n^2}{6}}.$$

The lower bound was proved by Egorychev in 1980 using the result on permanents of double stochastic matrices, see [25, 26], the upper bound is straightforward.

4.1 The Assmuss and Mattson construction of Steiner triple systems

Assmuss and Mattson obtained the following constructon for $STS(n)$, $n \equiv 1, 3 \pmod 6$ using Vasil'ev's construction for perfect codes:

Theorem 7. (Assmuss and Mattson, 1966, see [2].) *Let $S_{(n-1)/2}$ be $STS((n-1)/2)$ defined on the set $N = \{1, \ldots, (n-1)/2\}, n \equiv 1, 3$*

(mod 6) *and* λ *be any function from* $S_{(n-1)/2}$ *to the set* $\{0,1\}$. *Then the set* S_n *is an STS of order* n *defined by the following rules:*

1) the triples $(i,(n+1)/2,i+(n+1)/2)$ *are in* S_n *for any* $i \in N$;

2a) if $(i,j,k) \in S_{(n-1)/2}$ *and* $\lambda(i,j,k)=0$ *then*

$$(i,j,k),(i,j+\frac{n+1}{2},k+\frac{n+1}{2}),(i+\frac{n+1}{2},j,k+\frac{n+1}{2}),$$

$$(i+\frac{n+1}{2},j+\frac{n+1}{2},k) \in S_{2n+1};$$

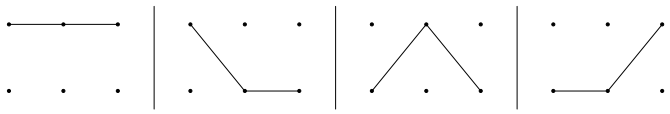

Figure 4.1: An illustration to $\lambda(i,j,k)=0$

2b) if $(i,j,k) \in S_{(n-1)/2}$ *and* $\lambda(i,j,k)=1$ *then*

$$(i+\frac{n+1}{2},j+\frac{n+1}{2},k+\frac{n+1}{2}),(i+\frac{n+1}{2},j,k),(i,j+\frac{n+1}{2},k),$$

$$(i,j,k+\frac{n+1}{2}) \in S_{2n+1}.$$

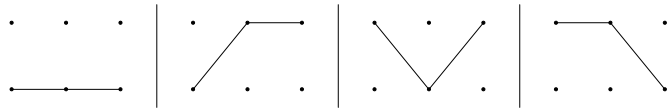

Figure 4.2: An illustration to $\lambda(i,j,k)=1$

In Figures 4.1 and 4.2 in every matrix three points in the first (second) line stands for i,j and k $(i+\frac{n+1}{2},j+\frac{n+1}{2},k+\frac{n+1}{2})$ respectively.

It is not difficult to check from the construction that every not ordered pair (i,j) of elements from the set $\{1,\ldots,n\}$ is exactly in one block.

Theorem 8. *An Assmuss and Mattson $STS(n)$ of order $n = 2^m - 1$ is a Steiner triple system $STS(V^n)$ obtained from the Vasil'ev code V^n when $\mathbf{0}^n \in V^n$.*

Before to prove the theorem we consider an example for $n = 7$, in the case the Vasil'ev code of length 7 coincides with the Hamming code H^7. From Vasil'ev's construction using $(x, |x|, x) \in H^7, w(x) = 1$ we immediately get the following triples in the code H^7:

$$(1, 4, 5), (2, 4, 6), (3, 4, 7).$$

If $\lambda(1, 2, 3) = 0$, where $(1, 2, 3) \in H^3$ then we have the following blocks

$$(1, 2, 3), (1, 6, 7), (2, 5, 7), (3, 5, 6)$$

in the code H^7; if $\lambda(1, 2, 3) = 1$ then we have in H^7 the blocks

$$(5, 6, 7), (2, 3, 5), (1, 3, 6), (1, 2, 7).$$

Proof. Let us consider any $n = 2^m - 1, m > 2$. From Vasil'ev's construction we have $(x, |x|, x) \in V^n$. If $x = e_i$ we get the block $(i, (n + 1)/2, i + (n + 1)/2)$ in V^n and therefore in $STS(V^n)$ for each $i \in \{1, \ldots, (n - 1)/2\}$.

Suppose $y = (i, j, k) \in V^{(n-1)/2}$ and $\lambda(y) = 0$. Then by Vasil'ev construction we have the following blocks: if $x = \mathbf{0}^{(n-1)/2}$ then $(x + y, |x| + \lambda(y), x) = (y, \mathbf{0}^{(n+1)/2}) \in V^n$ and we get the triple (i, j, k) in $STS(V^n)$.

If $x = (i, j)$ then

$$(x + y, |x| + \lambda(y), x) = (k, (n + 1)/2 + i, (n + 1)/2 + j)$$

in V^n and therefore in $STS(V^n)$. Analogous considerations for the pairs (j, k) and (i, k) give us the blocks

$$(i, j + (n + 1)/2, k + (n + 1)/2), (i + (n + 1)/2, j, k + (n + 1)/2)$$

respectively in $STS(V^n)$.

The case $\lambda(y) = 1$ is analogous. It is easy to see that the triples we have constructed are different from each other. The number of all triples is

$$\frac{n-1}{2} + 4 \cdot \frac{\binom{(n-1)/2}{2}}{3} = \frac{n(n-1)}{6}.$$

It is the correct number of all blocks in STS of order n. By this construction and the previous theorem it is clear that the Assmuss and Mattson STS of order n is $STS(V^n)$.

Exercises.

1. Prove that the number of all blocks in any Steiner triple system of order n is $n(n-1)/6$.

2. Construct $STS(15)$ by the Assmuss and Mattson construction using some nontrivial function $\lambda : STS(7) \to \{0,1\}$.

3. Prove that all codewords of weight 4 in any extended perfect code of length n containing the all-zero vector form a Steiner quadruple system. Remind that *a Steiner quadruple system* of order n is a family of 4-element blocks (subsets or quadruples) of the set $N = \{1, 2, \ldots, n\}$ such that each not ordered triple of elements of N appears in exactly one block.

Open problem

Improve the lower and upper bounds on the number of nonisomorphic Steiner triple systems presented in Theorem 6.

Chapter 5

On one property of linear codes

Further in this chapter the set of rows of a generator matrix of a code will be called *base set of codewords* or shortly a *base set*.

Theorem 9. (Glagolev, 1976, see [42].) *For any linear* $[n, k, d]$ *code* C *there exists a linear code* C' *with the same parameters such that its base set consists of codewords of minimal weight* d.

Proof. Let us take the set

$$T_d \cup T_{d+1} \cup \ldots \cup T_{d+p}$$

as a base set of the code C. Here the set T_d is a maximal linearly independent set of codewords of weight d, $T_d \subset C$, then we add the set T_{d+1} of codewords of weight $d+1$. It is the maximal possible linearly independent subset of codewords of weight $d+1$ which can be found in the code C such that $T_d \cup T_{d+1}$ is a maximal linearly independent set of codewords of weight not more than $d+1$. And we go on till the set T_{d+p}. Therefore we have

$$C =< T_d \cup T_{d+1} \cup \ldots \cup T_{d+p} > .$$

Further we will use the following obvious observation:

If G is a linear code with distance d and if there exists a vector x such that $d(G, x) \geq d$ then the set $G \cup (G + x)$ is a linear code with code distance d.

Consider any vector $y \in T_{d+1}$. A distance between y and any codeword from T_d is more than d: $d(T_d, y) > d$. If it is not true and there exists a vector $z \in T_d$ such that $d(y, z) = d$ then $w(y + z) = d$ and by the linearity of the code C we have $y + z \in C$ and $y + z \notin T_d$. Hence we get the subset $T_d \cup (y + z)$ in the code C which is a linearly independent set of codewords of weight d, a contradiction to the construction of the set T_d. Therefore

$$d(T_d, y) \geq d + 1. \tag{5.1}$$

Then we can take a vector y' of weight d such that $y' \prec y$, which means that all coordinates equal to one of the vector y' are between coordinates equal to one of the codeword y. Using (5.1) we obtain

$$d(T_d, y) > d(T_d, y') \geq d.$$

We can produce now a new set $T_d \cup \{y'\}$ which gives us a linear code $T_d \cup (T_d + y')$ with distance d according to the observation given at the beginning of the proof of this theorem. After that we use the set T_{d+1} further and in the same way we produce a new vector y'' and a new set $T_d \cup \{y', y''\}$, which is again a linear code with distance d and so on, going from the set T_{d+1} to the set T_{d+p}, in not more than k steps we design a new linear $[n, k, d]$ code C' with a base set consisting of codewords of minimal weight d. The proof is done.

Remark.

In 1992 Simonis [70] proved that for any q each linear code over the Galois field $GF(q)$ with length n, dimension k and code distance d can be transformed into a q-ary code D with the same parameters such that D possesses a basis of weight d vectors.

The next statement follows immediately from Proposition 2 about the uniqueness of the Hamming code and from Glagolev's Theorem:

Corollary 5. *There exists a base set consisting of codewords of weight 3 for a Hamming code.*

Proof.

The statement follows immediately from Proposition 2 about the uniqueness of the Hamming code and Glagolev's Theorem.

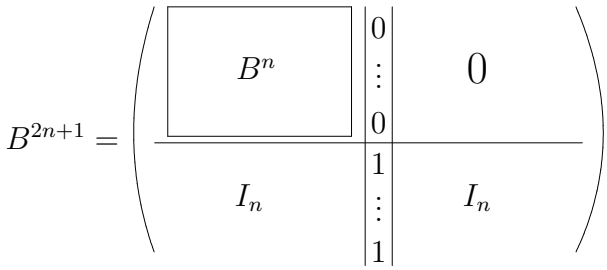

Figure 5.1: An illustration to Corollary 5

But Glagolev's Theorem does not give the way how to construct such base set. It can be easily produced from the presentation of the Hamming code by Vasil'ev's construction. Now we are going to develop a constructive proof of this corollary using induction by m, where $m = \log(n+1)$. For the aim we consider the Hamming code given by Vasil'ev's construction:

$$H^n = \{(x + y, |x|, x) : x \in E^{(n-1)/2}, y \in H^{(n-1)/2}\}. \tag{5.2}$$

If $m = 2$ then the Hamming code of length 3 is obviously generated by the all-one codeword of length 3.

Let B_n be a basis of the Hamming code H^n,

$$|B_n| = n - \log(n+1).$$

Let us consider the set

$$B_{2n+1} = B'_n \cup \bigcup_{i=1}^{n} (e_i + e_{n+1} + e_{n+1+i}),$$

where

$$B'_n = \{(y, \mathbf{0^{n+1}}) : y \in B_n\}.$$

According to (5.2)

$$e_i + e_{n+1} + e_{n+1+i} \in H^{2n+1}$$

for any $i = 1, \ldots, n$. It is easy to see that B_{2n+1} consists of linearly independent codewords of H^{2n+1} of weight 3, see an illustration in Figure 5.1.

The equality

$$|B_{2n+1}| = |B_n| + n = 2n - \log(n+1)$$

shows that B_{2n+1} is the required set of codewords of the code H^{2n+1}.

The proof is done.

Chapter 6

Concatenation approach

6.1 The main idea of the concatenation approach

There are a lot of concatenation constructions, see, for example, surveys [24, 75]. First we remind the definition of a q-ary Hamming code using the parity check matrix.

q-ary Hamming code

The main idea to design the parity check matrix for the $q > 2$ case is the same as for $q = 2$. We have to take such columns that any two of them are linearly independent and there exist three linearly dependent columns. But in the case $q > 2$ we cannot use all nonzero m-tuples because some of them can be linearly dependent. For example, vectors (11011) and (22022) are linearly dependent over $GF(3)$. To guarantee linear independence for any two columns we take as columns all nonzero vectors of length m over $GF(q)$ with first nonzero entry equal to 1. The total number of nonzero vectors of length m over $GF(q)$ is $q^m - 1$, it is clear that among them we have

$$(q^m - 1)/(q - 1)$$

vectors with the prescribed property. Therefore the code length of the Hamming code with m parity check symbols is $n = (q^m - 1)/(q - 1)$,

the size of the code is q^{n-m} and by the construction the code distance is 3. So we obtain the code with parameters

$$(n = (q^m - 1)/(q - 1), q^{n-m}, d = 3)_q.$$

This code will be denoted by H_q^n.

Example.

Let us consider the Hamming code over $GF(3)$ with two check symbols. A parity check matrix in the standard form is

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}.$$

Therefore we get a ternary Hamming code H_3^4 of length 4. Going from this parity check matrix to the generator matrix in the standard form

$$G = \begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

we construct all codewords of the type

$$\alpha_1 x_1 + \alpha_2 x_2,$$

where x_1, x_2 are rows from G and $\alpha_1, \alpha_2 \in \{0, 1, 2\}$:

$$\text{information blocks} \Longrightarrow \text{codewords}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 2 \\ 1 & 0 \\ 1 & 1 \\ 1 & 2 \\ 2 & 0 \\ 2 & 1 \\ 2 & 2 \end{pmatrix} \Longrightarrow \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 2 & 1 & 2 \\ 1 & 0 & 2 & 2 \\ 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \\ 2 & 0 & 1 & 1 \\ 2 & 1 & 0 & 2 \\ 2 & 2 & 2 & 0 \end{pmatrix}$$

The main idea of the concatenation construction

The construction was presented by Zinoviev in 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 $\mathbf{a}(B) = \big(\mathbf{b}(a_1)| \ldots |\mathbf{b}(a_n)\big)$, where $|$ stands for concatenation. The set $C = \{\mathbf{a}(B) : \mathbf{a} \in A\}$ is a q'-ary code. It is easy to check the code parameters:

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*.

6.2 Solov'eva codes – 1981

To define the concatenation construction presented in [71] we need partitions of E^n into perfect codes.

Partitions of E^n into perfect codes

Let us consider any perfect code C of length n. By the close packed property of a perfect code it is easy to get the following trivial partition of E^n into "cosets" of any (even nonlinear) perfect code C:

$$E^n = C \cup (C + e_1) \cup \ldots \cup (C + e_n).$$

We are going to construct a large class of nontrivial partitions of E^n into perfect codes of any admissible length $n > 7$ using Vasil'ev's construction. We will denote the class by $\mathbf{P}^n$.

Theorem 10. (Solov'eva, 1981, see [71].) *There exists a class* $\mathbf{P}^n$ *of different partitions of* E^n *into perfect codes of length* $n > 15$*, where*

$$|\mathbf{P}^n| \geq 2^{2^{(n-1)/2}}.$$

Proof. The proof will be done by induction on $m, m = \log(n+1)$.

For $m = 2$ and 3 there exist only trivial partitions because for $n = 3$ and $n = 7$ there exist only linear perfect codes H^3 and H^7.

Let us take any partition of $E^{(n-1)/2}$, $m = (n-1)/2$, into some perfect codes of length $(n-1)/2$:

$$E^{(n-1)/2} = \bigcup_{i=0}^{(n-1)/2} C_i^{(n-1)/2}.$$

Let us consider the case $m+1$. Using Vasil'ev's construction and $C_i^{(n-1)/2}$ for each $i \in \{0, 1, \ldots, (n-1)/2\}$ we construct the following two perfect codes of length n.

The first code is

$$C_i^n = \{(x+y, |x| + \lambda_i(y), x) : x \in E^{(n-1)/2}, y \in C_i^{(n-1)/2}\},$$

the second one is

$$C^n_{i+(n+1)/2} = C_i^n + e_{(n+1)/2},$$

where, as it was defined in Vasil'ev's construction, the function λ_i is any function from $C_i^{(n-1)/2}$ to the set $\{0, 1\}$. It is easy to show that any two perfect codes in the partition do not intersect.

The number of different partitions is not less than the number of choices of different functions $\lambda_i(y)$ for each $i = 0, 1, \ldots, (n-1)/2$. So we get

$$|P^n| \geq (2^{|C_i^{(n-1)/2}|})^{\frac{n+1}{2}} \geq (2^{\frac{2^{(n+1)/2}}{n+1}})^{\frac{n+1}{2}} = 2^{2^{(n-1)/2}},$$

This concludes the proof.

Theorem 11. (Solov'eva, 1981, see [71].) *Let*

$$E^n = \bigcup_{i=0}^{n} C_i^n, \; E^n = \bigcup_{i=0}^{n} D_i^n$$

be any two partitions of E^n into perfect codes of length n and π be any permutation on n positions. Then the set

$$C = \{(x, y, |y|) : x \in C_i^n, y \in D^n_{\pi(i)}, i = 0, 1, \ldots, n\}$$

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

Proof. It is clear that the number of coordinate positions is $2n+1 = 2^{m+1}-1$ if $n = 2^m - 1$.

The cardinality of the code is

$$\begin{aligned} |C| &= (n+1)\cdot|C_i^n|\cdot|D_i^n| = (n+1)\cdot(|C_i^n|)^2 \\ &= (n+1)\cdot\frac{2^{2n}}{(n+1)^2} = \frac{2^{2n+1}}{(2n+1)+1}. \end{aligned}$$

Finally we have to check if the code distance of the code C is 3. Let $u = (x, y, |y|)$ and $v = (x', y', |y'|)$ be any two codewords from C. There are three cases.

1. If $x = x', y \neq y', x \in C_i^n, i = 0, 1, \ldots, n$ then $y, y' \in D_{\pi(i)}^n$ and $d(y, y') \geq 3$ and therefore $d(u, v) \geq 3$.

2. The case $x \neq x', y = y'$ is analogous to the previous case.

3a. Suppose $x \neq x', y \neq y'$ and $x, x' \in C_i^n$. Then $d(x, x') \geq 3$ and therefore $d(u, v) \geq 3$.

3b. Assume $x \neq x', y \neq y'$ and $x \in C_i^n$, $x' \in C_j^n$, where $i, j \in \{0, 1, \ldots, n\}$ and $i \neq j$. Then $y \in D_{\pi(i)}^n$ and $y' \in D_{\pi(i)}^n$. If $|y| = |y'|$ then $d(y, y') \geq 2$, $d(x, x') \geq 1$ and therefore $d(u, v) \geq 3$. If $|y| \neq |y'|$ then $d(y, y') \geq 1$, $d((y, |y|), (y', |y'|) \geq 2$, $d(x, x') \geq 1$ and again $d(u, v) \geq 3$.

The proof is done.

This construction can be easily generalized to extended perfect codes.

Remarks.

1. It can be shown that this construction is the concatenation construction, see, for example, below sections 6.7 and 6.6 (remark 2), it is the reason why we call it the concatenation construction. It can also be called X-4 construction, see [46], chapter 18.

2. It should be noted that using this concatenation construction it is possible to construct partitions of E^n into perfect binary codes, see, for example, [71, 14].

3. The class of perfect codes described in the last theorem is not equivalent to the class of Vasil'ev codes and contains Heden codes properly. Two years later Phelps [55] in 1983 independently discovered

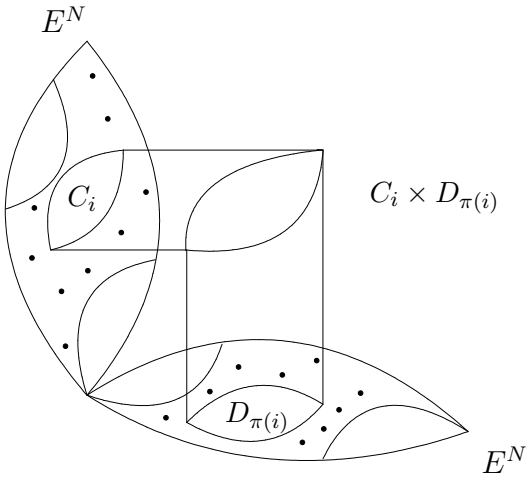

Figure 6.1: An illustration to theorem 11, the case of extended perfect codes

Solov'eva's construction and generalized it in 1984 [56], see Section 6.6. Heden's construction properly contains the class of Laborde (1983) codes [43], cf. [30].

4. The investigation of perfect binary codes of length 15 given by the concatenation construction from [71, 55] is done by Phelps in [61]. It is shown that there exist at least 963 and at most 15408 inequivalent such codes.

5. Exploiting the same concatenation construction, see Theorem 11, lower and upper bounds on the number of intersection matrices given by different partitions of the space E^n into perfect binary codes are given in [14]. The following problem is considered: given two partitions of E^n into perfect codes, their *intersection matrix* provides the cardinalities of the pairwise intersections of the subsets of these partitions. It is established that the number of different, or nonequivalent, intersection matrices given by partitions of extended perfect binary codes of length n is at least 2^{cn^2} and at most $2^{c'n^3}$, where n is large and c, c' are positive constants. The problem of the construction of partitions of E^n is also considered in [28].

It should be mentioned that the problem of enumerating the different partitions of the n-cube E^n is closely related to the problem of enumerating all perfect codes of length n, because the number of partitions is closely connected to the number of different perfect codes. For

example, double logarithms of these numbers are asymptotically equal.

Exercises.

1. Prove that $C_i^n \cap C_j^n = \emptyset$ for any $i, j \in \{1, 2, \ldots, (n-1)/2\}$, $i \neq j$ in Theorem 10.

2. Construct a class of partitions using Theorem 11.

3. Generalize the concatenation construction from Theorem 11 to extended perfect codes.

4. How to construct the Hamming code by the construction from Theorem 11?

6.3 Romanov codes

Let us consider an application of the concatenation construction for codes, which are not perfect. We are going to present a code of length 16 with the best known cardinality correcting a single error.

It is well known that there exists a partition of E_3^9 into seven STS-s of order 9. Denote these STS-s by $S_i, i = 1, \ldots, 7$:

$$E_3^9 = \bigcup_{i=1}^{7} S_i.$$

Let us consider also a partition of E^7 into cosets of the Hamming code H^7:

$$E^7 = \bigcup_{i=0}^{7} (H^7 + e_i).$$

Let S_i' be the set of all compliment words of the set S_i in E^9 :

$$S_i' = \{z + \mathbf{1}^9 | z \in S_i\}.$$

Theorem 12. (Romanov, 1983, see [65].) *The set* C^{16} *defined by*

$$\{(x, y) : x \in S_i \cup S_i',\ y \in H^7 + e_i,\ i = 1, \ldots, 7 \text{ or } x \in \{\mathbf{0}^7, \mathbf{1}^7\},\ y \in H^7\}$$

is a single error-correcting code of length 16 and cardinality 2720.

We omit the proof because it is analogous to the proof of Theorem 11.

The construction can be useful to get a class of good codes of length $2^m \leq n \leq 2^m + 2^{m-4}$ exploiting the well known Plotkin's construction. For the aim to show it we remind Plotkin's construction.

It is easy to prove the following proposition.

Proposition 3. *For any words a and b from E^n it is true*

$$w(a+b) \geq w(a) - w(b).$$

Theorem 13. (Plotkin, 1960, see [46].) *Let C be an (n, M_1, d_1) code and D be an (n, M_2, d_2) code. Then the set*

$$C^{2n} = \{(x, x+y) : x \in C, y \in D\}$$

is an $(n, M_1 \times M_2, d = min\{2d_1, d_2\})$ code.

Proof. Let

$$u = (x, x+y), \;\; v = (x', x'+y')$$

be distinct codewords of the code C^{2n}, where $x, x' \in C$, $y, y' \in D$.
If $y = y'$ then

$$d(u,v) = d((x,x),(x',x')) = 2d(x,x') = 2d_1.$$

If $y \neq y'$ then using the previous proposition we obtain

$$d(u,v) = w(x-x') + w(x+y-x'-y') \geq$$

$$w(x-x') + w((y-y') + (x-x')) \geq$$

$$w(x-x') + w(y-y') - w(x-x') = w(y-y') = d_2.$$

The proof is done.

Taking an even weight code D of length 17 and the extended Romanov code C of length 17 in Plotkin's construction one can build up a class of codes with good parameters:

$$D : (17,\, 2^{16},\, 2), \;\; C : (17,\, \frac{85}{64} \times 2^{11},\, 4) \;\; \Longrightarrow \;\; (34,\, \frac{85}{64} \times 2^{27},\, 4).$$

Shortening the code obtained we get the two following codes

$$(34, \frac{85}{64} \times 2^{27}), 4) \implies (33, \frac{85}{64} \times 2^{27}, 3) \implies (32, \frac{85}{64} \times 2^{26}, 3)$$

with good parameters.

Starting with these codes we obtain by induction on $m = \log n$ the following result:

Theorem 14. (Romanov, 1983, see [65].) *For any block length n satisfying $2^m \leq n \leq 2^m + 2^{m-4} - 1$ there exists a nonlinear $(n, \lambda \times 2^{n-m-1}, 3)$ code, where $\lambda = \frac{85}{64}$.*

For codes of length more than 16 it should be mentioned that there exist known codes with good parameters, for example, Etzion code of length 17, cardinality 5312, distance 3 or Hämäläinen code of length 18, cardinality 10496 and distance 3, see [32]. One can get, using these codes and the same Plotkin's construction an infinite class of codes with good parameters. We consider Hämäläinen's construction in Section 6.4 below.

6.4 Hämäläinen codes

The main idea of Hämäläinen's construction is the following: first find a good subcode over a four element subalphabet in the Hamming code with parameters $(6, 5^4, 3)_5$, then apply to this subcode a concatenation construction. Now we are going to develop this construction in more details.

Consider the Hamming code H_q^n of length $n = 6$ over the Galois field $GF(5)$, so $q = 5$. Let us take the following generator matrix of the code in standard form

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 4 \\ 0 & 1 & 0 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

we construct all codewords of a type

$$\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 + \alpha_4 x_4,$$

where x_1, x_2, x_3, x_4 are rows from G and $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \{0, 1, 2, 3, 4\}$. The size of the code is 5^4. Let us fix an element $k \in \{1, 2, 3, 4\}$. Using inclusion and exclusion method eliminate from the code H_5^6 all codewords containing a coordinate equal to k :

$$5^4 + \sum_{i=1}^{4} (-1)^i \begin{pmatrix} 6 \\ i \end{pmatrix} 5^{4-i} - 1 = 164,$$

here there exists only one vector with five coordinates equal to k, for example, if $k = 4$, the vector is $(4, 2, 4, 4, 4, 4)$. The resulting subcode is a restriction of the Hamming code H_5^6 to the subcode with 164 codewords over the four element subalphabet $\{0, 1, 2, 3\}$ with code distance 3.

To get a code of length 18 we apply the following concatenation construction for the subcode:

instead of 0 we take the Hamming binary code H^3 of length 3:

$$0 \to \{000, 111\};$$

every element from the set $\{1, 2, 3\}$ we replace by a coset of the Hamming code H^3 such that any two different elements will be replaced by different cosets. At the end of the procedure we get a binary code with parameters $(18, 10496, 3)$, that means code length 18, size

$$164 \times 2^6 = 10496$$

and code distance 3.

Deleting one coordinate in this code one can easily get a code with parameters $(17, 5248, 3)$.

So we prove the following statement:

Theorem 15. (Hämäläinen, 1988, see [32], see also [34].) *There exist* $(18, 10496, 3)$ *and* $(17, 5248, 3)$ *binary codes.*

Exercises.

1. Prove Proposition 3.

2. Prove Theorems 12 and 14.

3. Prove that a subcode of the Hamming code with parameters $(6, 5^4, 3)_5$ over a four element subalphabet $\{1, 2, 3, 4\}$, which does not contain the element 0 consists of 160 codewords.

6.5 Zinov'ev's concatenation construction – 1988

Let us consider a more complicated concatenation construction, which was presented by Zinov'ev in 1988, see [96]. In fact the construction can be considered as a generalization of Hämäläinen's construction.

Let now A be a q-ary perfect $(n, |A|, 3)$ code, $q = 2^k$, $n = 2^k + 1$, for example, we can take the Hamming code over $GF(2^k), k > 1$ with two check symbols. 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 16. (Zinov'ev, 1988, see [96].) *The set C^N defined by*

$$C^N = \bigcup_{(x_1,x_2,\ldots,x_n)\in A} C_{x_1} \times C_{x_2} \times \ldots \times C_{x_n}$$

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

Proof. The length of the code is

$$N = n(q-1) = (2^k + 1)(2^k - 1) = 2^{2k} - 1.$$

The size of the code is

$$\begin{aligned} |C^N| &= |H_q^n| \times |C_0|^n = 2^{k2^k - k}(2^{2^k - 1 - k})^{2^k + 1} \\ &= 2^{k2^k - k} \times 2^{2^2 k - 1 - k2^k - k} = 2^{N - \log(N+1)}, \end{aligned}$$

where $N = 2^{2k} - 1$.

Let us check the code distance. Consider any two different codewords

$$x = (x_1, x_2, \ldots, x_n),$$
$$y = (y_1, y_2, \ldots, y_n)$$

from A.

If $x \neq y$ then $d(x, y) \geq 3$ and there exist at least three coordinate positions i, j, k, where x and y differ. Therefore there are at least three pairs of codes in the partition E^n such that

$$d(C_{x_i}, C_{y_i}) \geq 1, \quad d(C_{x_j}, C_{y_j}) \geq 1, \quad d(C_{x_k}, C_{y_k}) \geq 1$$

and we get

$$d(C_{x_1} \times C_{x_2} \times \ldots \times C_{x_n}, C_{y_1} \times C_{y_2} \times \ldots \times C_{y_n}) \geq 3.$$

Assume $x = y$. Then we get the set

$$C_{x_1} \times C_{x_2} \times \ldots \times C_{x_n}$$

and taking into account that every C_{x_i} is a perfect binary code we have the distance between any two vectors of the set at least three.

Remark

The construction was independently presented in 1989 in [72].

6.6 Phelps codes

Let $C_1^0, C_2^0, \ldots, C_r^0$ and $C_1^1, C_2^1, \ldots, C_r^1$ be any partitions of the even and odd weight vectors of E^r into extended perfect codes of length r respectively, C^m be an extended perfect code of length m in E^m, in this section $r = 2^k$, $m = 2^p$. For each vector $\mu \in C^m$, let C_μ be a minimum distance 2 code of length m over $GF(r)$, $|C_\mu| = r^{m-1}$, (C_μ is an MDS code). Remind that an MDS code C of length m, size $|C|$ and distance d over $GF(r)$ is a code, which reaches the Singleton bound $m - \log_r |C| \leq d - 1$.

Theorem 17. (Phelps, 1984, see [56].) *The set C^n defined by*

$$C^n = \{(c_1|c_2|\ldots|c_m) : c_i \in C_{j_i}^{\mu_i}, \mu = (\mu_1, \mu_2, \ldots, \mu_m) \in C^m,$$

$$j = (j_1, j_2, \ldots, j_m) \in C_\mu\}$$

is an extended perfect binary code of length $n = mr$.

We will further call the code C^m a *base code*.

Proof. Another way to write the construction of the code is

$$C^n = \bigcup_{\mu \in C^m} \bigcup_{j \in C_\mu} C_{j_1}^{\mu_1} \times \ldots \times C_{j_m}^{\mu_m}.$$

We will use this presentation of the code to prove this theorem.

It is obvious that the length of the code is $n = mr$.

The size of the code is

$$|C^n| = |C^{\mu_i}_{j_i}|^m \times |C_\mu| \times |C^m| = (2^{r-\log r-1})^m \times r^{m-1} \times 2^{m-\log m-1} = 2^{n-\log n-1},$$

here $n = mr$.

Let us check that the code distance satisfies

$$d = d(C^{\mu_1}_{j_1} \times \ldots \times C^{\mu_m}_{j_m}, C^{\mu'_1}_{j'_1} \times \ldots \times C^{\mu'_m}_{j'_m}) \geq 4$$

for any $\mu, \mu' \in C^m$ and $j, j' \in C_\mu$.

There are some cases.

1) The case $\mu = \mu'$, $j = j'$ is trivial.

2) Assume $\mu = \mu'$, $j \neq j'$.

Then $d(j, j') \geq 2$ and there exist coordinate positions s, t such that $j_s \neq j_{s'}$, $j_t \neq j_{t'}$. From this inequalities taking into account that $C^{\mu_s}_{j_s}$ and $C^{\mu_s}_{j'_s}$ are both even or odd weight perfect codes (analogous for the codes $C^{\mu_t}_{j_t}$ and $C^{\mu_t}_{j'_t}$) we have $d(C^{\mu_s}_{j_s}, C^{\mu_s}_{j'_s}) \geq 2$ and $d(C^{\mu_t}_{j_t}, C^{\mu_t}_{j'_t}) \geq 2$. Therefore

$$d(C^{\mu_1}_{j_1} \times \ldots \times C^{\mu_s}_{j_s} \times C^{\mu_t}_{j_t} \times \ldots \times C^{\mu_m}_{j_m},$$

$$C^{\mu_1}_{j'_1} \times \ldots \times C^{\mu_s}_{j'_s} \times C^{\mu_t}_{j'_t} \times \ldots \times C^{\mu_m}_{j'_m}) \geq 4.$$

3) Let $\mu \neq \mu'$, $j = j'$.

The vectors $\mu \neq \mu'$ are from the base code C^m, then $d(\mu, \mu') \geq 4$ and there exist four coordinate positions t, s, e and l where μ and μ' differ. Therefore there are four pairs of perfect codes $C^{\mu_i}_{j_i}$ and $C^{\mu'_i}_{j_i}$, $i \in \{t, s, e, l\}$ such that

$$d(C^{\mu_i}_{j_i}, C^{\mu'_i}_{j_i}) \geq 1.$$

As a consequence we have the inequality $d \geq 4$.

4) Let $\mu \neq \mu'$, $j \neq j'$. The proof $d \geq 4$ is the same as in the case 3 and this finishes the proof.

Remarks.

1. Puncturing any coordinate of the extended perfect binary code C^n gives us a perfect binary code of length $mr - 1$.

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

$$C(v) = \{(1, \pi(1)), (2, \pi(2)), \ldots, (r, \pi(r))\}.$$

Thus Theorem 11 is a particular case of this theorem.

3. 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 $n \to \infty$.

4. The generalization of the construction was done by Krotov in [38], see below Section 7.3.

6.7 Generalized concatenated codes. Lobstein and Zinov'ev codes

Let B be a q_B-ary $\left(n_B, K_1, d_{B,1}\right)$ 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 $\left(n_B, K_3, d_{B,3}\right)$ code, $K_3 = q_3$.

Let any codeword $\mathbf{b} \in B$ have 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 $\left(n_A, K_{A,\ell}, d_{A,\ell}\right)$ code A_ℓ and a codeword $\mathbf{a}^\ell = (a_1^\ell, \ldots, a_{n_A}^\ell) \in A_\ell$. For any $s = 1, \ldots, n_A$ 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

$$C = \{\left(\mathbf{b}(a_1^1, a_1^2, a_1^3)|\ldots|\mathbf{b}(a_{n_A}^1, a_{n_A}^2, a_{n_A}^3)\right) : \mathbf{a}^\ell \in A_\ell, 1 \le \ell \le 3\}. \quad (6.1)$$

Theorem 18. (See [94, 95].) *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*

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

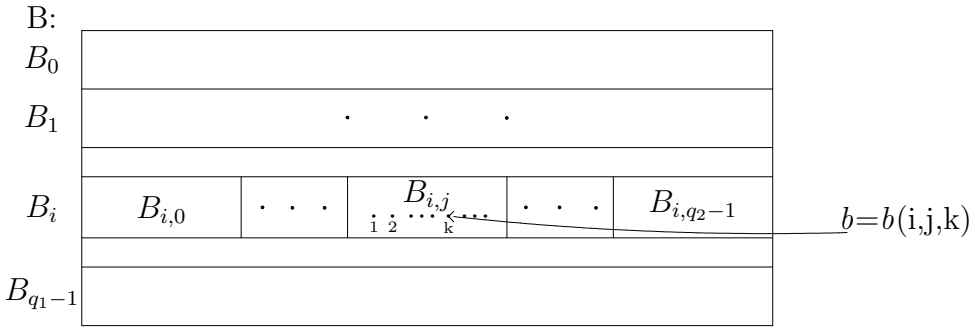

Figure 6.2: An illustration of the generalized concatenated approach

Consider the binary case. Let $B = E^{n_B}$, $B = E_\bullet^{n_B} \cup (E^n \setminus E_\bullet^{n_B})$, where $E_\bullet^{n_B}$ are the all even vectors of B, $n_B = 2^m$. Consider for $E_\bullet^{n_B}$ and $E^n \setminus E_\bullet^{n_B}$ 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 a n_B-ary $(n_A, n_B^{n_A-1}, 2)$ code (it is an MDS code with distance 2) 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 from the last theorem we obtain from (6.1) a binary extended perfect code C of length 2^{m+n}.

Theorem 19. (See [97].) *The code C is an extended perfect binary code of length 2^{m+n}.*

In [97, 98] Zinov'ev and Lobstein generalized last theorem by permuting all n_B alphabet symbols of the second outer code A_2.

In [98] they modified further the resulting code by adding an $n_B \times n_A$ matrix to the codewords, using the fact that this does not alter the distances between codewords. The fact allows them to get switching Vasil'ev codes from this modified concatenation construction. Some other concatenation constructions were done by Zinov'ev and Lobstein in [99].

Remarks

1. The enumeration of binary extended perfect codes of length 16 obtained by a generalized concatenation construction was presented in [100]. It is shown that there exist 285 such inequivalent codes.

2. A special case of this basic construction was obtained in [96]. In turn this construction is a special case of a construction by Phelps described in [56] in a different way without mentioning concatenation construction (see above the section 6.6). It should be mentioned that a class of Phelps codes – 1984 (see above Section 6.6) can be described by generalized concatenated approach given by Zinov'ev in 1975, see [94], but in the paper [94] there is no the information about parameters of the codes used in the generalized concatenation construction which lead us to the perfect codes.

Chapter 7

Switching approach

7.1 Mollard codes, lower bound

Let us now consider Mollard's construction, which is a generalization of Vasil'ev's construction.

Let C^r and C^m be two perfect codes of length r and m respectively, here $r = 2^k - 1$, $m = 2^p - 1$. Let

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

The generalized parity functions $p_1(x)$ and $p_2(x)$ are defined by

$$p_1(x) = (\sigma_1, \sigma_2, \ldots, \sigma_r) \in E^r,$$

$$p_2(x) = (\sigma'_1, \sigma'_2, \ldots, \sigma'_m) \in E^m,$$

where $\sigma_i = \sum_{j=1}^{m} x_{ij}$ and $\sigma'_j = \sum_{i=1}^{r} x_{ij}$. Let f be an arbitrary function from C^r to E^m.

Theorem 20. (Mollard, see [53].) *The set*

$$C^n = \{(x, y \oplus p_1(x), z \oplus p_2(x) \oplus f(y)) : x \in E^{rm}, y \in C^r, z \in C^m\}$$

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

Proof. It is easy to check that the code length is $n = rm + r + m$ and the size of the code is

$$|C^n| = |E^{rm}| \times |C^r| \times |C^m| = 2^{rm} \times \frac{2^r}{r+1} \times \frac{2^m}{m+1} = \frac{2^n}{n+1}.$$

Let

$$u = (x, y \oplus p_1(x), z \oplus p_2(x) \oplus f(y)),$$
$$u' = (x', y' \oplus p_1(x'), z' \oplus p_2(x') \oplus f(y'))$$

be any two different vectors from the code C^n. We have to show that $d(u, u') \geq 3$.

There are some cases.

1) If $x = x'$ then $p_1(x) = p_1(x')$, $p_2(x) = p_2(x')$ and

$$d(u, u') = d(y, y') + d(z, z') \geq 3.$$

2) If $d(x, x') = 1$ then

$$d(p_1(x), p_1(x')) = d(p_2(x), p_2(x')) = 1.$$

If $y \neq y'$ then

$$d(y \oplus p_1(x), y' \oplus p_1(x')) \geq 2$$

and again $d(u, u') \geq 3$.

If $y = y'$ then

$$d(y \oplus p_1(x), y' \oplus p_1(x')) = 1,$$

$d(z \oplus p_2(x) \oplus f(y), z' \oplus p_2(x') \oplus f(y')) = d(z \oplus p_2(x), z' \oplus p_2(x') \geq 1$ and therefore the result is $d(u, u') \geq 3$.

3) If $d(x, x') = 2$ then $d(p_1(x), p_1(x'))$ and $d(p_2(x), p_2(x'))$ are 0 or 2 but both can not be zero at the same time. From this fact we have

$$y \oplus p_1(x) = y' \oplus p_1(x') \text{ and } z \oplus p_2(x) \oplus f(y) = z' \oplus p_2(x') \oplus f(y')$$

are not compatible and therefore $d(u, u') \geq 3$.

Remarks

1. In the case $m = 1$ Mollard's and Vasil'ev's constructions coincide.

2. It is proved in [73] that there exist Mollard codes which are not Vasil'ev codes.

3. In Mollard construction the function f is a constant value function.

4. A generalization of Mollard construction was done by Krotov in [35].

$$\begin{array}{ccc|c} x_{11} & \cdot\ \cdot\ \cdot & x_{1m} & \sum_{i=1}^{m} x_{1i} + z_1 + f(y_1) \\ x_{21} & \cdot\ \cdot\ \cdot & x_{2m} & \sum_{i=1}^{m} x_{2i} + z_2 + f(y_2) \\ \cdot & & \cdot & \cdot\ \cdot\ \cdot \\ \cdot & & \cdot & \\ x_{n1} & \cdot\ \cdot\ \cdot & x_{nm} & \sum_{i=1}^{m} x_{ni} + z_n + f(y_n) \\ \hline \sum_{j=1}^{n} x_{j1} + y_1 & \cdot\ \cdot\ \cdot & \sum_{j=1}^{n} x_{jm} + y_m & \end{array}$$

Figure 7.1: An illustration to Theorem 20

7.2 Method of α-components

Switching methods (the method of α-components and the method of i-components) allow to construct complicated and large classes of perfect codes with different properties, see the survey [76]. Let us first consider the method of α-components. It was introduced and developed in [7, 8]. The main idea is the following.

Let M be a subset in a perfect code C. By a *switch* of the set M we mean the exchange of the bit in the ith coordinate of all vectors of a set M with the opposite bit. We get a new set, denoted by $M + e_i$, where e_i is the word with ones only in the i-th coordinate. A set M is an *i-component* of the perfect code C if $K(M) = K(M + e_i)$. As a result we have a new perfect code $C' = (C \setminus M) \cup (M + e_i)$, which can be or can not be equivalent to the starting perfect code. We say that C' is obtained from the code C by a *switching* (or a *translation*) of an i-component M.

Next we take $\alpha \subseteq \{1, \ldots, n\}$. The set M is called an *α-component* of the perfect code C if it is an i-component for every $i \in \alpha$. First for every α-component we choose an element i in the set α and make a switch of any numbers of i-components from this α-component into new i-components of the same cardinality. After that one can switch the obtained α-components with new α-components using switchings by not utilized coordinates from the set α. The resulting code is perfect but different or even inequivalent to the starting perfect code.

The method of α-components is effectively suitable to the Hamming code because it is possible to destroy the group structure of the Hamming code in such a way that we can get the code with prescribed prop-

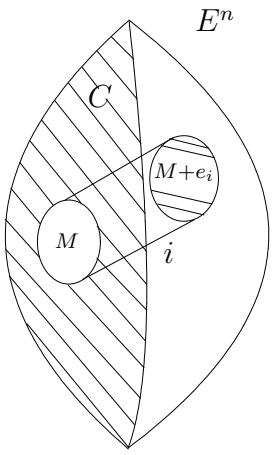

Figure 7.2: An illustration to the definition of i-components

erties. The method allows to construct complicated and large classes of perfect codes with different properties, see the survey [76]. The first essential improvement of the lower bound on the number of well known Vasil'ev codes (which was the best from 1962 till 1996) was achieved by this switching approach.

Now we give a sketch of the description of the construction of Avgustinovich and Solov'eva, see all details in [7, 8]. 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 4. *The Hamming code H^n can be partitioned into $\{i,j,k\}$-components R^t_{ijk} :*

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

Proposition 5. *Every $\{i,j,k\}$-component R^t_{ijk}, $t = 1,\dots,N_1$, can be partitioned into 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 one to construct a large class of different perfect binary codes.

Theorem 21. (Avgustinovich, Solov'eva, 1996, see [7, 8].) *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.

In fact we counted the lower bound on the number of different perfect codes of ranks not more than $n-\log(n+1)+2$. Here the *rank* $r=r(C)$ of a code C is the dimension of the subspace $<C>$ spanned by the code C. To get the bound for different numbers of perfect codes of ranks more than $n-\log(n+1)+2$ the method described above can be implied, for example, to any partition of the Hamming code into α-components, where $|\alpha|>3$.

The first modification of the method was done by Malyugin [49]. He proposed to exchange any (i,j,k)-component in the Hamming code with an isomorphic (i,j,k)-component and after that switch nonintersecting i and j components. The modification allows to get a great variety of perfect codes and as a consequence the following lower bound:

Theorem 22. (Malyugin, 1999, see [49].) *There are at least*

$$2^{2^{\frac{n+1}{2}-\log(n+1)}} \cdot 2^{2^{\frac{n-3}{4}}}$$

different perfect binary codes of length n.

A further development was achieved by Krotov [36] again for the class of perfect codes of ranks not more than $n-\log(n+1)+2$ using simultaneously the α-components method and Phelps's [56] construction (see also Section 7.3. below).

Theorem 23. (Krotov, 2000, see [36].) *There are at least*

$$2^{2^{\frac{n+1}{2}-\log_2(n+1)}} \cdot 3^{2^{\frac{n-3}{4}}} \cdot 2^{2^{\frac{n+5}{4}-\log_2(n+1)}} \tag{7.1}$$

different perfect binary codes of length n.

The last bound is better than the other known lower bounds. It is not difficult to see that Vasil'ev's [84] and Mollard's [53] constructions can be described by the method of α-components. See Section 7.4, where we show that "one step" Vasil'ev codes can be represented by the method of i-components. "One step" means that the code $C^{(n-1)/2}$ in Vasil'ev's construction is any perfect code of length $(n-1)/2$. For the "two steps" Vasil'ev's construction we can take the code $C^{(n-1)/2}$, as we did it in Corollary 3, represented again by Vasil'ev's construction. For the description of such codes we can use the method of α-components.

Phelps and LeVan [60] presented the perfect code of length 15 which does not belong to the Hamming switching class. That means it does not belong to the set of all perfect codes obtained by switchings from the Hamming code. Malyugin [48] enumerated all perfect codes of length 15 obtained from the Hamming code by simultaneous switchings of nonintersecting components using different coordinates. The number of such different codes is 131224432. All these codes are included in the Hamming switching class. The question of the enumeration of all perfect codes of length 15 is still open (see also Chapter 3). It is not even known how many switching classes there are for perfect codes of length 15.

7.3 Combining construction

Let us consider the combining construction from [38] as one of the most promising constructions because the particular case of the construction gives the best lower bound on the number of different perfect binary codes and allows to get the asymptotic bound on the number of inequivalent perfect binary codes of length n of rank $n - \log(n+1) + 2$ (see the end of Section 8.3). The construction can be considered as a combination of switching [53, 8] and concatenation approaches [56, 97, 98]. First we have to define a μ-component as a generalization of the notion of an α-component.

Let $n = rm$, in this section again r and m are powers of two: $m = 2^p$ and $r = 2^k$ for any $p, k > 2$ and let

$$x = (x_{11}, x_{12}, \ldots, x_{1m}, x_{21}, \ldots, x_{2m}, \ldots, x_{m1}, \ldots, x_{rm})$$

be any vector from E^n. The generalized parity function $p(x)$ is defined like in Mollard's construction [53] by

$$p(x) = (\sigma'_1, \sigma'_2, \ldots, \sigma'_m) \in E^m,$$

where $\sigma'_j = \sum_{i=1}^{r} x_{ij}$.

Let $\mu \in E^m$. A subset K_μ in E^n is called a *μ-component* of the space E^n if $|K_\mu| = 2^{n-m-\log_2(n/m)}$, $p(x) = \mu$ for any $x \in K_\mu$ and $d(x, x') \geq 4$ for any different $x, x' \in K_\mu$, here $n = rm$ is a power of two.

Theorem 24. (Combining construction, Krotov, 2000, see [38].) *Let C^m be an extended perfect binary code of length s and K_μ be a μ-component for any $\mu \in C^m$. Then the set*

$$C = \bigcup_{\mu \in C^m} K_\mu$$

is an extended perfect binary code of length $n = rm$.

As follows from this theorem we have first to define a base code C^m of length m and for any codeword $\mu \in C^m$ take a μ-component K_μ, which construction depends upon the word μ. Three cases to construct μ-components are presented in [38]. Let us consider one of them, which gives us the best lower bound on the number of perfect binary codes.

Let us turn to Phelps's construction, see Section 6.6. Let us consider the following application of this construction:

Theorem 25. *The set*

$$C^n = \{(c_1|c_2|\ldots|c_m) : c_i \in C_{ij_i}^{\mu_i}, \mu = (\mu_1, \mu_2, \ldots, \mu_m) \in C^m,$$

$$j = (j_1, j_2, \ldots, j_m) \in B\}$$

is an extended perfect binary code of length $n = mr$.

Here C^m is a base code (an extended perfect binary code of length n), B – r-ary code of cardinality r^{m-1} with distance 2 and length m, $B \subset \{1, \ldots, r\}^m$ (a MDS code). For each coordinate $i \in \{1, \ldots, m\}$ we take r disjoint perfect even weight codes

$$C^0_{i1}, \ldots, C^0_{ir}$$

of length r and r disjoint perfect odd weight codes

$$C^1_{i1}, \ldots, C^1_{ir}$$

of length r (existence of such partitions see in [71, 14] and also Section 6.2). So, we have the following $2m$ partitions, m of these partitions for the m coordinates given by even weight extended perfect binary codes (these partitions are given in columns):

$$\begin{array}{ccc} C^0_{11}, & \ldots, & C^0_{m1} \\ C^0_{12}, & \ldots, & C^0_{m2} \\ \ldots & \ldots & \ldots \\ C^0_{1r}, & \ldots, & C^0_{mr} \end{array}$$

and m partitions (in columns) given by odd weight extended perfect binary codes:

$$\begin{array}{ccc} C^1_{11}, & \ldots, & C^1_{m1} \\ C^1_{12}, & \ldots, & C^1_{m2} \\ \ldots & \ldots & \ldots \\ C^1_{1r}, & \ldots, & C^1_{mr} \end{array}$$

We can write the construction of the code in the folowing way

$$C^n = \bigcup_{\mu \in C^m} \bigcup_{j \in B} C^{\mu_1}_{1j_1} \times \ldots \times C^{\mu_m}_{mj_m}.$$

It should be noted that in Phelps's construction only two partitions $C^0_1, \ldots, C^0_r$ and $C^1_1, \ldots, C^1_r$ are used, first of them for even weight extended perfect codes, the second one – for odd.

Let for each $i \in \{1, \ldots, m\}$ and fixed $v = (v_1, \ldots, v_m) \in E^m$, r disjoint perfect codes $C_{i1}, \ldots, C_{ir}$ of length r be given where the codes are even weight if $v_i = 0$ and odd weight if $v_i = 1$.

Theorem 26. *The set*

$$K^\mu = \{(c_1|c_2|\ldots|c_m) : c_i \in C_{ij_i}, j = (j_1, j_2, \ldots, j_m) \in B\} =$$

$$\bigcup_{j \in B} C_{1j_1} \times \ldots \times C_{mj_m}.$$

is a μ-component.

The proof is straightforward.

Since the codes C_{ij} are only used in the construction of the μ-component and can be chosen independently for each μ, from Theorem 24 and 26 one can get the following construction, which generalizes Theorem 25.

Let C^m be an extended perfect binary code of length m. For each $\mu \in C^m$ let $B(\mu)$ be an r-ary code of length m, cardinality r^{m-1} and distance 2. Let us take for every $\mu \in C^m$ and each $i \in \{1, \ldots, m\}$ r disjoint perfect codes $C^\mu_{i1}, \ldots, C^\mu_{ir}$ (even weight or odd weight codes if μ_i is 0 or 1 respectively).

Theorem 27. *The set*

$$C^n = \bigcup_{\mu \in C^m} \bigcup_{j \in B(\mu)} C^\mu_{1j_1} \times \ldots \times C^\mu_{mj_m}.$$

is an extended perfect binary code of length $n = mr$.

For $r = 4$ varying the choice of the codes $B(\mu)$ (such codes are in an one-to-one correspondence with $(m-1)$-quasigroups of order 4), Krotov obtained the best lower bound on the number of perfect binary codes, see Theorem 23.

7.4 Method of i-components

The method of i-components or the method of switching non-intersecting components by disjoint coordinates is very close to the method of α-components but different because there are some situations where we can use i-components approach but can not use α-components

method. The method of i-components was exploited by different authors, see this section below and the first who introduced the concept of i-components (in the terminology of disjunctive normal forms) was Vasil'ev [84, 85]. The method of switching nonintersecting components allowed Avgustinovich and Solov'eva [6] to construct a class of nonsystematic perfect binary codes of length n for every $n = 2^k - 1, \ \ k \geq 8$. The problem about the existence of nonsystematic perfect codes was posed in 1985 by Hergert [33]. A perfect code C of length n is systematic if there are $n - \log(n+1)$ coordinates such that the code C deleted in the remaining $\log(n+1)$ coordinates coincides with $E^{n-\log(n+1)}$.

Proposition 6. *Let $n = 2^k - 1, \ \ k \geq 8$. There are n minimal components $M_1, \ldots, M_n$ 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 greater than 4 if $i \neq j$.*

This property allows us to switch every i-component M_i in the i-th coordinate. Thus we obtain

Theorem 28. (Avgustinovich, Solov'eva 1996, see [6].) *The set*

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

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

For $n \leq 127$ nonsystematic perfect codes were investigated by Phelps and LeVan [59] and for $n = 15$ by Romanov [67]. Malyugin [51] proved the following result:

Theorem 29. (Malyugin, see [51].) *Minimal number of i-components necessary to switch in the Hamming code in order to get a nonsystematic perfect code is equal to 7 independently of the code length.*

There are some other papers devoted to switching construction or using it, see [27, 58, 66, 68].

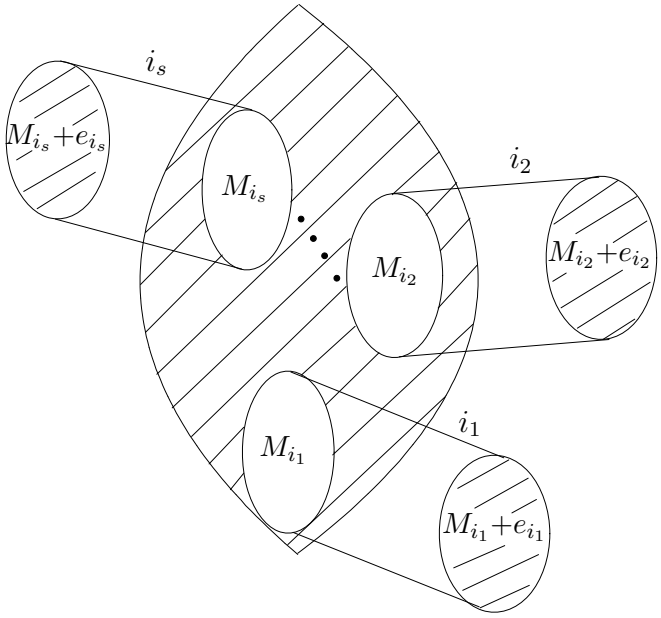

Figure 7.3: An illustration to Theorem 28

Let us show that Vasil'ev's construction is a switching construction. Consider Vasil'ev's construction

$$V^n = \{(x + y, |x| + \lambda(y), x) : x \in E^p, y \in C^p\},$$

where $n = 2p + 1$. It is easy to see that the set

$$M_{p+1} = \{(x, |x|, x) : x \in E^p\}$$

is the $(p+1)$-component of V^n of cardinality 2^p and Vasil'ev's construction is the switching construction.

Let $K(M_{p+1})$ and $K(M_{p+1} \oplus e_{p+1})$ be neighborhoods of M_{p+1} and $M_{p+1} \oplus e_{p+1}$ respectively. It is easy to see that

$$K(M_{p+1}) = K(M_{p+1} \oplus e_{p+1}).$$

Therefore M_{p+1} is a $(p + 1)$-component by the definition and the set

$$(V^n \setminus M_{p+1}) \cup (M_{p+1} \oplus e_{p+1})$$

is a perfect code. Analogously

$$V^n \setminus (\bigcup_{y \in V_1^p} M_{p+1}^y)) \cup (\bigcup_{y \in V_1^p} (M_{p+1}^y \oplus e_{p+1})$$

is a perfect binary code of length n, here V_1^p is a subcode of the code C^p such that $\lambda(y) = 1$ iff $y \in V_1^p$, e_{p+1} is as earlier a vector of length n with one only in $(p+1)$-th coordinate,

$$M_{p+1}^y = M_{p+1} \oplus (y, \mathbf{0^{p+1}}).$$

The structure of i-components of a perfect code was investigated in [5, 80]. It is very complicated and various. We call an i-component *indecomposable* if it can not be divided into i-components of smaller cardinality. The existence of perfect codes with i-components of different cardinalities was established in [5]. In [80] it was proved that there exists a class of perfect codes of length $n-1$ with minimal i-components of cardinality $h2^{n-h}/n$ for every $n = 2^m, m > 2$ and $h = 2^p$, where $p = 2, \ldots, m-1$. The existence of maximal cardinality nonisomorphic i-components of different perfect codes of length n for all $n = 2^m - 1, m > 3$ is proved in [80].

Chapter 8

Some properties of perfect binary codes

8.1 Spectral properties. Part I.

A code is *distance-invariant* if the number $A_i(n)$ of all codewords at distance i from a fixed codeword does not depend on the choice of the codeword.

In 1957 Lloyd [44] and independently in 1959 Shapiro and Slotnik [69] proved a perfect binary code to be distance-invariant. We are going to consider some nice theorems due to Shapiro and Slotnik.

Theorem 30. (Shapiro and Slotnik, see [69].) *Let C be a perfect code. Then the number of codewords at distance r from a given codeword $x \in C$ does not depend on the choice of the word x and on the choice of the code.*

Proof. Let us denote the number of codewords at distance k from a codeword x by A_k. Without loss of generality we can consider $x = \mathbf{0^n}$, where n is the length of the code C. Let us compose a system of linear equations for A_k, $k = 0, \ldots, n$. All numbers A_k can be calculated from the equations.

Let us consider the k-th level E_k^n in E^n. By the close packed property of the code C all vectors from E_k^n are partitioned into three subsets:

1) A_k codewords of weight k;

2) vectors, which belong to spheres surrounding all codewords from E^n_{k-1}. There are $(n-k+1) \times A_{k-1}$ such vectors;

3) vectors, which belong to spheres with centers in codewords from E^n_{k+1}. There are $(k+1) \times A_{k+1}$ such vectors.

So we get the following system of $n+1$ linear equations with $n+1$ unknown values:

$$A_0 = 1, A_1 = A_2 = 0,$$

$$\left(\begin{array}{c} n \\ k \end{array} \right) = (k+1)A_{k+1} + A_k + (n-k+1)A_{k-1},$$

$$k = 2, 3, \ldots, n.$$

It should be noted that negatively indexed A_k are to be interpreted as zero.

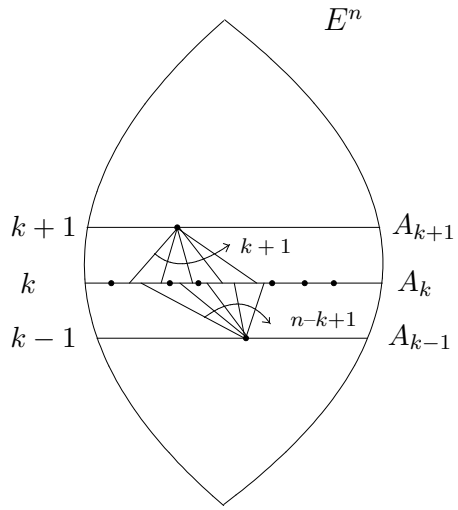

Figure 8.1: An illustration to Theorem 30

Using a generating function

$$A_0 + A_1 t + \ldots A_n t^n$$

it is possible to find an explicit form of the numbers A_k, $k = 0, 1, \ldots, n$:

$$A_{2k} = \frac{1}{n+1} \left(\left(\begin{array}{c} n \\ 2k \end{array} \right) + (-1)^k n \left(\begin{array}{c} (n-1)/2 \\ k \end{array} \right) \right);$$

$$A_{2k+1} = \frac{1}{n+1}\left(\begin{pmatrix} n \\ 2k+1 \end{pmatrix} + (-1)^{k+1} n \begin{pmatrix} (n-1)/2 \\ k \end{pmatrix}\right).$$

The proof is done.

Adding the last equation to the previous one, one can get

$$A_{2k} + A_{2k+1} = \frac{\begin{pmatrix} n \\ 2k \end{pmatrix} + \begin{pmatrix} n \\ 2k+1 \end{pmatrix}}{n+1}$$

and conclude it in the following result:

Corollary 6. *A perfect code of length n containing the all-zero vector has uniform distribution by pairs of neighboring levels E^n_{2k} and E^n_{2k+1}, $k = 0, \ldots, \frac{n-1}{2}$.*

Immediately from this theorem we get the following very important properties of perfect codes.

Corollary 7. *For every codeword $x \in C$, where C is a perfect code of length n, it is true that the compliment vector $x \oplus \mathbf{1^n}$ belongs to the code C.*

This property appeared to be very useful to investigate nontrivial properties of perfect binary codes, see, for example, sections 8.3, 8.4.

Corollary 8. *The number of codewords of weight $(n-1)/2$ of a perfect code of length n is equal to*

$$A_{(n-1)/2} = \frac{1}{n+1}\left(\begin{pmatrix} n \\ (n-1)/2 \end{pmatrix} + n \begin{pmatrix} (n-1)/2 \\ (n-3)/4 \end{pmatrix}\right).$$

Theorem 31. (Shapiro and Slotnik, see [69].) *The only perfect codes with distance 7 are the Golay code of length 23 and the trivial code of length 7.*

Proof. If there exists a perfect code of length n, cardinality k and distance 7 then

$$2^n : \left(1 + \begin{pmatrix} n \\ 1 \end{pmatrix} + \begin{pmatrix} n \\ 2 \end{pmatrix} + \begin{pmatrix} n \\ 3 \end{pmatrix}\right) = 2^k$$

and therefore

$$1 + \left(\begin{array}{c} n \\ 1 \end{array} \right) + \left(\begin{array}{c} n \\ 2 \end{array} \right) + \left(\begin{array}{c} n \\ 3 \end{array} \right) = 2^r,$$

where $r = n - k$. Multiplying by 6 and simplifying the left side factors, we get

$$(n^2 - n + 6)(n + 1) = 3 \cdot 2^{r+1}.$$

Hence, one or another of the left-hand factors is a multiple of 3.

There are two cases.

1) Assume $3|(n^2 - n + 6)$. Here

$$n + 1 = 2^l, \;\; n^2 - n + 6 = 3 \cdot 2^{r-l+1},$$

whence,

$$(2^l - 1)^2 - (2^l - 1) + 6 = 3 \cdot 2^{r-l+1}$$

and

$$2^{2l} - 3 \cdot 2^l + 8 = 3 \cdot 2^{r-l+1}. \tag{8.1}$$

If $l = 3$ we have a trivial code of length $n = 7$. So $l > 3$ and $n > 7$. From (8.1) we have

$$2^3(2^{2l-3} - 3 \cdot 2^{l-3} + 1) = 3 \cdot 2^{r-l+1}.$$

The first factor of the left-hand factors is equivalent to 0 (mod 2), the second one is equivalent to 1 (mod 2). Analyzing the right-hand factors we conclude $2^3 = 2^{r-1+l}$ and therefore $r - 1 + l = 3$. Then

$$n^2 - n + 6 = 3 \cdot 2^3,$$

which contradicts $n > 7$ as well as n is an integer.

2) Assume $3|(n + 1)$. Here

$$n + 1 = 3 \cdot 2^l, \;\; n^2 - n + 6 = 2^{r+l-1},$$

whence,

$$(3 \cdot 2^l - 1)^2 - (3 \cdot 2^l - 1) + 6 = 2^{r-l+1}$$

and

$$9 \cdot 2^{2l} - 9 \cdot 2^l + 8 = 2^{r-l+1},$$

$$2^3(9\cdot 2^{2l-3} - 9\cdot 2^{l-3} + 1) = 2^{r-l+1},$$
$$9\cdot 2^{2l-3} - 9\cdot 2^{l-3} + 1 = 2^{r-l-2},$$
$$9\cdot 2^{2l-3} - 9\cdot 2^{l-3} = 2^{r-l-2} - 1.$$

Left hand side is an even number, but at the same time the right hand side is odd, whence there is only the possibility $2^{l-3} = 1$. So $l = 3$ and $n + 1 = 3\cdot 2^3 = 24$. This leads to the code of length 23 with distance 7 and completes the proof.

The next theorem will show by a non-constructive elegant way that the number of perfect codes with distance more than 4 is finite. The proof of the theorem is a consequence of the following deep result of Siegel from Number Theory.

Lemma 1. *(Siegel) Let $f(x)$ be any polynomial, which takes integer values when x is an integer. Then unless $f(x)$ is a constant times a power of a linear polynomial, the largest prime factor of $f(n)$ increases without limits as $n \to \infty$.*

Theorem 32. (Shapiro and Slotnik, [69].) *If $t \geq 2$ then the number of perfect codes of length n with distance $d \geq 5$ is finite.*

Proof. To deduce the theorem from Lemma 1 we have to verify that the polynomial $f(x)$ defined by

$$f(x) = 1 + \begin{pmatrix} x \\ 1 \end{pmatrix} + \ldots + \begin{pmatrix} n \\ t \end{pmatrix} \tag{8.2}$$

is not a power of a linear polynomial if $t \geq 2$ (here $1 + \begin{pmatrix} x \\ 1 \end{pmatrix} + \ldots + \begin{pmatrix} n \\ t \end{pmatrix}$ is the number of vectors in a sphere of radius t in the x-dimensional cube E^x). Then according to Lemma 1 and (8.2) the number $f(n)$ has a prime factor more than 2 for n sufficiently large and therefore it cannot be 2 and $2^n/f(n) \neq 2^k$ for some k, which means we cannot reach the Hamming bound and there is no perfect code of length n with distance t.

The theorem will be proved by contradiction. Suppose

$$f(x) = a(b + cx)^t, \tag{8.3}$$

where a, b, c are some rational numbers. Let us count $f(0)$ from the last equation:

$$f(0) = 1 = ab^t,$$

so we may write

$$f(x) = (1 + r\cdot x)^t, \tag{8.4}$$

where $r = c/b$ is rational.

Substituting $x = 1$ into (8.3) we get

$$f(1) = 1 + \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 2.$$

On the other hand from (8.4) we have

$$f(1) = (1 + r)^t.$$

Then $(1 + r)^t = 2$, so that $1 + r = \sqrt[t]{2}$ is rational. This contradiction establishes the proof of the theorem.

8.2 Upper bound on the number of perfect binary codes

There is only an upper bound on the number of different perfect codes close to a trivial bound, but the proof of this bound is far from trivial. This bound follows from the following nice property of perfect codes.

Proposition 7. (Avgustinovich, [4].) *A perfect binary code of length n is uniquely determined by its codewords of weight $(n-1)/2$.*

Proof. As earlier we denote all vectors of weight k by E_k^n and consider the set $X_{\frac{n-1}{2}} = C \cap E^n_{\frac{n-1}{2}}$ of all codewords of weight $(n-1)/2$ in a perfect code C containing $\mathbf{0^n}$. First of all it should be noted that if we know the set $X_{\frac{n-1}{2}}$ then according to Corollary 7 the set $\overline{X}_{\frac{n-1}{2}}$ is a

subset of the code C, where $\overline{X}_{\frac{n-1}{2}}$ is the set of all compliment vectors to the set $X_{\frac{n-1}{2}}$.

Let us have at least two extensions of the set $X_{\frac{n-1}{2}} \cup \overline{X}_{\frac{n-1}{2}}$ to perfect codes:

$$C = A \cup X_{\frac{n-1}{2}} \cup \overline{X}_{\frac{n-1}{2}} \cup \overline{A}, \tag{8.5}$$

$$C' = B \cup X_{\frac{n-1}{2}} \cup \overline{X}_{\frac{n-1}{2}} \cup \overline{B},$$

where $A \neq B$.

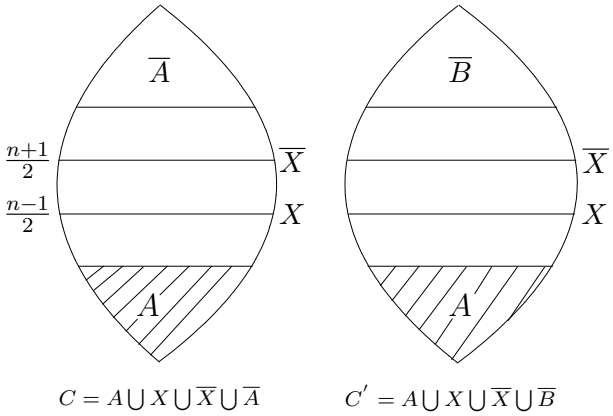

Figure 8.2: An illustration to Proposition 7

It is easy to see that $d(A, \overline{B}) \geq 3$. Using this fact we can get a perfect code

$$D = A \cup X_{\frac{n-1}{2}} \cup \overline{X}_{\frac{n-1}{2}} \cup \overline{B}, \tag{8.6}$$

see Figure 8.2.

From $A \neq B$ we have $\overline{A} \neq \overline{B}$ and therefore there exists a vector $y \in \overline{B}$ such that $y \notin \overline{A}$. From this fact and from (8.5) we get $\overline{y} \notin A$. But according to Corollary 7 from $y \in \overline{B}$ and (8.6) it follows $\overline{y} \in A$, a contradiction. The proof is done.

Using this property one can get the following upper bound on the number N_n of different perfect codes of length n.

Theorem 33. (Avgustinovich, 1995, see [4].) *There are not more than*

$$N_n \le 2^{2^{n-\frac{3}{2}\log n+\log\log(en)}}$$

different perfect binary codes of length n.

Proof. From Proposition 7 it is easy to obtain the following upper bound on the number of different perfect binary codes of length n :

$$N_n \le \left(\begin{array}{c} |E^n_{(n-1)/2}| \\ |E^n_{(n-1)/2} \cap C^n| \end{array} \right).$$

Using twice the Stirling formula

$$n^n e^{-n}\sqrt{2\pi n}e^{-n} \le n! \le n^n e^{1-n}\sqrt{2\pi n}$$

and Corollary 8 we can estimate this bound

$$N_n \le \left(\begin{array}{c} |E^n_{(n-1)/2}| \\ A_{\frac{n-1}{2}} \end{array} \right) \le \left(\begin{array}{c} 2^n/\sqrt{n} \\ 2^n/n\sqrt{n} \end{array} \right) \le 2^{2^{n-\frac{3}{2}\log n+\log\log(en)}}. \qquad (8.7)$$

The proof is done.

Remarks.

1. Comparing this upper bound with the best lower bound from Theorem 23 we see the big gap between both bounds.

2. It should be noted that the trivial upper bound is

$$2^{2^{n-\log n}}.$$

3. Further developing of the results presented in this section see at the end of Section 8.3.

Exercises.

1. Prove using the Stirling formula the inequality

$$\left(\begin{array}{c} n \\ (n-1)/2 \end{array} \right) \le \frac{2^n}{\sqrt{n}}.$$

2. Prove using the Stirling formula that the number $A_{\frac{n-1}{2}}$ from Corollary 8 satisfies the inequality

$$A_{\frac{n-1}{2}} \leq \frac{2^n}{n\sqrt{n}}.$$

3. Prove the last inequality in (8.7) using the Stirling formula.

Open problem

Find new upper and lower bounds on the number of different perfect binary codes of length $n \geq 15$.

8.3 Spectral properties. Part II.

A binary code of length n is called *distance-regular* if for any codewords x, y and any integers $i, j \in \{1, \ldots, n\}$ the number of codewords z such that $d(x, z) = i,\ \ d(y, z) = j$, does not depend on the choice of x, y but only depends on $d(x, y)$.

Theorem 34. (See [9].) *Among the perfect binary codes with distance 3 only the Hamming codes of length 3 and 7 are distance-regular.*

Between these two properties the following interesting metrical property of a perfect code introduced in [90] takes place.

A perfect binary code is *strongly distance-invariant* if the number of codeword pairs at distance d, where one codeword of the pair is at distance i from a codeword x and the other one at distance j from x, depends only on the numbers i, j, d and does not depend on the choice of x.

Theorem 35. (Vasil'eva, see [90].) *All perfect binary codes are strongly distance-invariant.*

A subset F of all vectors in E^n with fixed $n-k$ coordinates is called a *k-dimensional face.*

The following generalization of well known results of Lloyd, Shapiro and Slotnik (the distance-invariance of perfect codes, see, for example, Theorem 30), Delsart, Pulatov (every perfect binary code of length n has uniform distribution in k-dimensional faces of E^n, $k \geq (n+1)/2$) is presented in the following theorem:

Theorem 36. (Vasil'eva, see [87].) *The weight distribution of the codewords of a perfect binary code in any face of E^n depends only on the number of the codewords of this face.*

The notion of the local spectrum of a perfect binary code is defined in [89] as the weight spectrum of the subcode of the perfect code in a face which contains this subcode.

Theorem 37. (Vasil'eva, see [89, 90].) *The local spectrum of a perfect binary code in any face is uniquely determined by the local spectrum of the code in the orthogonal face.*

The notion of a centered characteristic function is introduced in [88]. Let

$$v^C : E^n \to \{0, 1\}$$

be the characteristic function of a perfect binary code C, i. e. $v^C(x) = 1$ iff $x \in C$.

The function

$$v^C(x) - 1/(n+1)$$

is called a *centered characteristic function* of the code C.

The function is considered as a vector of length 2^n. The following two results are presented in [88]. The centered characteristic functions of all perfect binary codes are eigenvectors of all incidence matrices of the Hamming associated scheme and, therefore, belong to a certain eigensubspace of the Euclidean 2^n-space. The centered characteristic function of a perfect binary code can be presented as a linear combination of centered characteristic functions of a class of equivalent perfect binary codes.

The notion of a K-centered function as a generalization of the notion of the centered characteristic function is introduced in [13]. A real-valued function defined on E^n is called *K-centered* if the sum of its values in any sphere of radius 1 equals K. A perfect code characteristic function is the 1-centered function on E^n for appropriate n with values from $\{0, 1\}$ and vice versa. Remind that in 1995 Avgustinovich [4] showed that every perfect binary code is uniquely determined by its codewords of weight $(n-1)/2$; see Section 8.2. The following generalization of the result is obtained for centered functions:

Theorem 38. (Avgustinovich S. V., Vasil'eva A.Y., see [13, 21].) *The values of a centered function on all vertices of the n-cube are uniquely determined by values on the middle level of the n-cube.*

The explicit formula is presented.

8.4 Automorphism groups of perfect codes

The automorphism group $Aut(C)$ of a code C of length n consists of all the isometries of E^n which transform the code into itself $A^v_\pi(C) = C$ or $\pi(C) + v = C$. It is known that each isometry E^n is defined by a mapping

$$A^v_\pi : x \to \pi(x) + v,$$

where π is a permutation of the n coordinate positions, and $v \in E^n$. Let

$$Sym(C) = \{A^{\mathbf{0}}_\pi : A^{\mathbf{0}}_\pi(C) = C\}$$

denote *the permutational automorphism group* of the code C, and

$$Ker(C) = \{A^v_e : A^v_e(C) = C\}$$

the set of all its *periods* (remind that here $\mathbf{0}$ is the all-zero vector of E^n, e – the identity permutation of length n). It is called the *kernel* $K(C)$ of a code C. Since C (see for instance perfect nonlinear binary Z_4-linear codes in [37]) may possess an automorphism $A^v_\pi(C) = C$ such that $\pi(C) \neq C$ and $v + C \neq C$, it is clear that not always

$$Aut(C) = Sym(C) \times Ker(C)$$

(here and later in this section $\times$ denotes semidirect product). This means that it is not enough to investigate separately $Ker(C)$ and $Sym(C)$. Obviously for any linear code C, $Aut(C) = Sym(C) \times Ker(C)$.

There are not too many papers devoted to the investigation of the automorphism group of perfect codes. It is well known that for the Hamming code H^n of length n the permutational automorphism group is equivalent to $GL(\log(n+1), 2)$ and therefore for the automorphism group of the Hamming code it holds

$$Aut(H^n) \cong GL(\log(n+1), 2) \times H^n$$

and

$$|Aut(H^n)| = 2^{n-\log(n+1)} N_1,$$

where

$$\begin{aligned} N_1 &= |GL(\log_2(n+1), 2)| \\ &= n(n-1)(n-2^2+1)(n-2^3+1)\ldots(n-(n-1)/2). \end{aligned}$$

The first result about the permutational automorphism group of perfect binary codes was given by Phelps in [57]:

Theorem 39. (Phelps, [57].) *Every finite group is isomorphic to the permutational automorphism group of some perfect code.*

Unfortunately this interesting result does not give full information about the structure of the automorphism group of a perfect code of any length $n = 2^m - 1$, $m > 3$. Some research on the full automorphism group of a perfect code has been done in [10, 47]:

Theorem 40. (Avgustinovich, Solov'eva, [10].) *For any $n \geq 255$ there exists a perfect binary code of length n with a trivial automorphism group of order 2, and this code is full rank nonsystematic.*

Theorem 41. (Malyugin, [47].) *For any $n \geq 31$ there exists a systematic perfect binary code of length n with a trivial automorphism group of order 2.*

If a perfect code contains $\mathbf{0}^n$ it always contains the all-one vector of E^n, see Corollary 7. So the last two theorems show that the lower bound is achievable.

An upper bound on the order of the automorphism group of a perfect binary code was established in [78, 79, 50]. Let us remind that all codewords of weight 3 of a perfect binary code including $\mathbf{0}$ define a Steiner triple system. That is why the automorphism group of a perfect code is very closely related to the automorphism group of its Steiner triple system. The automorphism group $Aut(STS(n))$ of any $STS(n)$ consists of all the permutations of the set N, which transform $STS(n)$ into itself.

Theorem 42. (See [29, 78, 79].) *If the order of the automorphism group of a Steiner triple system of order n is equal to the order of the full linear group $GL(\log(n+1), 2)$ then it is a Hamming system, and it is unique up to isomorphism.*

The proof in [29] is algebraic, in [78, 79] combinatorial and shorter. In [78] an upper bound on the order of the automorphism group of any Steiner system $S(t, t+1, n)$ was obtained.

It is proved in [78] that

$$|Aut(C)| = |T(C)| \cdot |Sym(C)|$$

for a code C, where $T(C)$ is the set of all vectors $v \in E^n$ for which there exists a permutation $\pi_v \in S_n$ such that

$$\pi_v(C) + v = C.$$

Here π_v is not always from $Sym(C)$.

First the following theorem was proved.

Theorem 43. (Solov'eva, Topalova, [78].) *The order of the automorphism group of any perfect binary code of length n is not greater than the order of the automorphism group of the Hamming code of the same length.*

Then next results appeared independently using different approaches.

Theorem 44. (Solov'eva, Topalova, [79].) *Any perfect binary code with an automorphism group of maximal order is equivalent to the Hamming code of the same length.*

Theorem 45. (Malyugin, [50].) *The order of the automorphism group of any nonlinear perfect binary code is at least twice less than the order of the automorphism group of the Hamming code of the same length.*

Analogous results can be extended to Steiner quadruple systems of order $n = 2^m$ and extended perfect binary codes. Remind that a *Steiner quadruple system* is a collection of 4-element subsets (*blocks*) of N, such that each not ordered 3-element subset of N is contained in exactly one block.

Theorem 46. (See [79], [50].) *There is a unique Steiner quadruple system $S(3,4,n)$ with an automorphism group of the maximal possible order and it is contained in the extended Hamming code of the same length.*

Theorem 47. (See [79], [50].) *Any extended perfect binary code with an automorphism group of maximal order is equivalent to the extended Hamming code of the same length.*

Open problem

Clarify whether a perfect binary code of length 15 with a trivial automorphism group exists or not.

8.5 Ranks and kernels problem

The definition of the kernel can also be done in the following way: the *kernel* $Ker(C)$ of a code C is defined as the set of all its *periods* (all codewords $x \in C$ such that $x + C = C$). The dimension of the kernel is denoted by $k = k(C)$.

Heden [30] constructed perfect codes of length 15 with kernels of dimension $1, 2, 3$. In 1994 Etzion and Vardy [27] found perfect codes of length $n \geq 15$ of all admissible ranks using switchings of nonintersecting minimal i-components. The same approach allowed Phelps and LeVan [58] to establish the existence of a nonlinear perfect code of length $n \geq 15$ with a kernel of dimension k for each $k \in \{1, 2, \ldots, n-m-2\}$, where $n = 2^m - 1$. See also [67].

In 1998 Etzion and Vardy [28] proposed to clarify which pairs of numbers (r, k) are attainable as the rank r and kernel dimension k of some perfect code of length n. It will be mentioned further as the *ranks and kernels problem*. Let $\delta(r)$ be such minimal number that

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

Denote by $U(n,r)$ the following

$$U(n,r) = n - \log(n+1) - \delta(r).$$

Theorem 48. (Etzion and Vardy, 1995, see [28].) *For full rank perfect codes for every $n \geq 2^m - 1, m > 3$, it is true $k(C) \leq U(n,r)$. The bound is tight for full rank perfect codes for each $n \geq 2^{10} - 1$.*

Using the same approach as Etzion and Vardy did in [28] Phelps and Villanueva [62] established the upper bound of pairs (r,k) for a perfect code of length $n \geq 15$ for not full rank codes and proved that all such pairs are attainable.

Denote by $L(n,r)$ the following

$$L(n,r) = \begin{cases} 2^{n-r}, & \text{if } r > n - \log(n+1) + 1, \\ 2^{n-r} - 1, & \text{if } r = n - \log(n+1) + 1. \end{cases}$$

Theorem 49. (Phelps and Villanueva, 2001, see [62].) *The bound $L(n,r)$ is the exact lower bound of kernel dimension of a perfect code for length $n \geq 15$ and rank r.*

For $r < 15$ perfect codes of length 15 for all possible pairs (r,k) are given in [61]. For $n = 15$ full rank perfect codes with any kernel dimension k, $1 \leq k \leq 5$ are known, see [30, 54, 28], for $k \geq 6$ full rank perfect codes do not exist [28, 83].

In this section we are going to present the following theorem:

Theorem 50. (Avgustinovich, Heden, Solov'eva, 2002, see [19, 20].) *Let n and r be natural numbers such that $n = 2^m - 1$, $m > 10$, $n - \log(n+1) \leq r \leq n$. Then for any natural number k such that $L(n,r) \leq k \leq U(n,r)$ there exists a perfect code of length n and rank r with kernel dimension k.*

Let us consider the construction. Let H^n be the Hamming code of length n defined by its parity check matrix with columns given in lexicographic order. Remind some definitions. A linear subspace R_i^0 of the code H^n is a linear span of all vectors of weight 3 with the i-th coordinate equal to 1, $i \in \{1, \ldots, n\}$. It is called reduced i-component. For any vector $v \in H^n$ a set $R_i^v = R_i^0 + v$ is called an i-component with the representative v, see the beginning of Chapter 7.

Let us consider a set of pairs $F = \{(u_1, i_1), (u_2, i_2), ..., (u_s, i_s)\}$, where $u_t \in H^n$, $i_t \in \{1, 2, ..., n\}$. We call a family F *separable* if the following conditions hold:

1. the set of vectors of length $\log(n+1)$ corresponding to the binary representation of natural numbers $i_1, i_2, ..., i_s$ is linearly independent over $GF(2)$;

2. $\mathbf{0} \notin R_{i_t}^{u_t}$, $i_t \in \{1, 2, ..., n\}$;

3. for all $t \neq l$ it is true that $R_{i_t}^{u_t} \cap R_{i_l}^{u_l} = \emptyset$.

The number s of pairs in the family F is the *size* of the family. A separable family F is called *full rank family* if $s = \log(n+1)$. Let $M = \{L_1, L_2, \ldots, L_s\}$ be a set of arbitrary linear subspaces of the code H^n. A family F is called *M-separable* if in addition to conditions 1 and 2 the following condition is valid

$3^\star$. for all $t \neq l$ it holds $(R_{i_t}^{u_t} + L_t) \cap (R_{i_l}^{u_l} + L_l) = \emptyset$.

Let all spaces L_i in the set M coincide with some space L. Unless otherwise stated in this case we will call an M-separable family *L-separable*. Let us consider the set

$$C(F, M) = H^n \setminus \bigcup_{t=1}^{s} (R_{i_t}^{u_t} \oplus L_t) \cup \bigcup_{t=1}^{s} (R_{i_t}^{u_t} \oplus L_t \oplus e_{i_t}),$$

where e_{i_t} is the vector with one in only the i_t-th coordinate. Let $K(F, M) = \bigcap_{t=1}^{s} (R_{i_t}^0 \oplus L_t)$. Using the same approach as in [58] the following fact can be proved:

Theorem 51. *Let F be an M-separable family of size s. Then the set $C(F, M)$ is a perfect code of rank $n - \log(n+1) + s$ with kernel $K(F, M)$.*

Corollary 9. *Let F be an L-separable family of size s. Therefore there exist perfect codes of length n of rank $n - \log(n+1) + l$ with any kernel dimension from $dim(K(F))$ to $dim(K(F, L))$.*

The last theorem shows that to prove Theorem 50 it is necessary to construct an L-separable family of pairs for appropriate subspaces L. A basis of the construction is given by the following three propositions.

Proposition 8. *For all admissible $n > 7$ there exist separable families of any size s, where $s = 1, \ldots, \log(n+1)$.*

Proposition 9. *Let F be a separable family of pairs of size s of the code $H^{(n-1)/2}$ and $v \in H^{(n-1)/2} \setminus \bigcup_{t=1}^{s} R_{i_t}^{u_t}, v \notin \{\mathbf{0}, \mathbf{1}\}$. Then the family $F' = F \cup (v, n)$ is an $R_n^{\mathbf{0}}$-separable family of pairs of size $s+1$ of the code H^n.*

Proposition 10. *Let F be an L-separable family of pairs of size s of the code $H^{(n-1)/2}$ and $v \in H^{(n-1)/2} \setminus \bigcup_{t=1}^{s}(R_{i_t}^{u_t} \oplus L), v \notin L$. Then the family $F' = F \cup (v, n)$ is a $(R_n^{\mathbf{0}} \oplus L)$-separable family of pairs of size $s+1$ of the code H^n.*

To prove Theorem 50, it remains to collate Theorem 51 and Propositions 8–10. Propositions 8–10 and Theorem 51 provide the existence of perfect codes of any rank s with minimal possible kernel and, respectively, kernel of dimension at least $(n-1)/2$. A possibility to choose any linear subspace of the space L for the set M gives a continuous variation (adding one with every step) of kernel dimension from the minimum to the maximum.

In [15] the classification of perfect codes of length n and rank $n - m + 2$ is reduced to the description of MDS-codes with distance 2 over an alphabet with four symbols. It is not difficult to show that if the rank of a perfect code C is $n - m + 1$ then C is a Vasil'ev code.

Theorem 52. (See [15].) *If the rank is $n - m + 2$ then a perfect code of length n for any admissible length $n > 7$ can be described by a Hamming code of length $(n-3)/4$ and a set of MDS-codes of length $(n-3)/4$ with distance 2 over an alphabet with four symbols using Phelps's construction* [56].

Krotov and Potapov [41] investigated such MDS-codes, every MDS-code of length $(n+1)$ with distance 2 over an alphabet with four symbols is equivalent to n-quasigroup of order 4. They proved that the asymptotic number of such n-quasigroups is

$$3^{n+1}2^{2^n+1}\left(1 + O\left(\frac{1}{3^n}\right)\right).$$

From this bound, Theorem 52 and Theorem 23 one can obtain the asymptotic estimate for the number of perfect codes of length n and rank $n - m + 2$. So using [15] and [41] we have a preclassification of perfect codes of rank $n - m + 2$.

Heden [31] has shown the following theorem.

Theorem 53. (Heden, 2002, see [31].) *Any perfect code with rank less than n is equivalent to a Krotov code obtained by the combining construction (see Theorem 24).*

Open problem

Find a solution of the ranks and kernels problem for full rank perfect codes for pairs (n, k), where

$$15 < n < 2^{10} - 1,\ k \in \{U(n), U(n) - 1\}.$$

8.6 Metrical rigidity

A code C in the n-dimensional vector space E^n over $GF(2)$ is called *metrically rigid* if every isometry $I : C \to E^n$ with respect to the Hamming metric is extendable to an isometry of the whole space E^n. A notion of the metrical rigidity is closely and naturally connected with the well known in classical geometry notion of a rigidity. Remind that every isometry of E^n is defined by a mapping $A^v_\pi : x \to \pi(x) + v$, where π is a permutation of coordinates and $v \in E^n$. A code C is *reduced* if it contains the all-zero vector.

The metrical rigidity of the following classes of codes has been established in [3, 74]:

Theorem 54. (Avgustinovich, see [3]; Solov'eva, Avgustinovich, Honold, Heise, see [74].) *Perfect q-ary codes for $q \geq 2$, are metrically rigid with the exception of the binary Hamming code of length 7 and the ternary Hamming code of length 4.*

Theorem 55. (Solov'eva, Avgustinovich, Honold, Heise, see [74].) *The following codes are metrically rigid:*

1) the binary even-weight code of length n with the exception of the case of $n = 4$;

2) q-ary $(n, n-1)$ MDS codes with the exception of several codes of small length;

3) full constant-weight codes.

Let $N = \{1, 2, \ldots, n\}$. A subset $D \subset E^n$ of weight k vectors is called a *2-(n, k, λ)-design* if the number of vectors in D with ones in the i-th and j-th coordinates is equal to λ for all different $i, j \in N$.

Theorem 56. (Avgistinovich, Solov'eva, see [18]. *Any reduced binary code of length n containing a 2-(n, k, λ)-design is metrically rigid for n large enough.*

The class of such codes includes for sufficiently large code length all the families of uniformly packed codes satisfying the condition $d-\rho \geq 2$, where d is the code distance and ρ is the covering radius, all primitive extended BCH-codes and all codes containing $t-(n, k, \lambda)$-designs.

Two codes C_1, C_2 are called *weakly isometric* if there exists such a map $J : C_1 \to C_2$ that the equality $d(\alpha, \beta) = 3$, $\alpha, \beta \in C_1$ is true iff $d(J(\alpha), J(\beta)) = 3$. It is clear that isometric codes are weakly isometric.

Theorem 57. (Avgustinovich, see [11].) *Any two weakly isometric perfect binary codes are equivalent.*

The result was announced by Avgustinovich in 1994, see [3].

(Temporary) Concluding remarks

The aim of these Lecture Notes was to introduce the beautiful theory of perfect codes to any reader with a basic background in coding theory and combinatorics. Of course the selection of the material presented here reveals the author's taste and inclinations. We followed the strong relation with combinatorics (for example, to the fascinating correspondence between perfect binary codes and Steiner triple systems, or the geometry of the n-dimensional cube), other topics of coding theory, group theory, graph theory, classical geometry.

The present state of the manuscript is by far not complete, and there will be more to come, especially about the structure of perfect codes, about q-ary perfect codes, about a generalization of the results for codes with parameters different from parameters of perfect codes (ternary codes, codes with parameters of Reed-Muller codes and so on).

It should be noted that there are some other interesting and beautiful recent results devoted to perfect codes and related topics such as classifications of Z_4-linear perfect and Hadamard codes [37, 40], results on perfect codes in distance regular graphs [1], constructions of perfect ternary constant weight codes [81, 39], results about propelinear perfect codes, see [64] and others.

I express my deep sense of gratitude to Professor Hyun Kwang Kim from Com^{2}MaC center, POSTECH, South Korea for inviting me to visit the center, present 8 lectures on perfect codes and related topics, for his kind hospitality and for making these lecture notes possible. Special thanks to the people in Com^{2}MaC center, especially to Sangmok Kim and his family for making my stay in Pohang very pleasant. I am very grateful to Svetla Topalova for her kind help, which allowed to improve the presentation of the text and Jong Yoon Hyun and Natasha Tokareva, who helped to accompany the text of the lecture notes with nice figures.

Bibliography

[1] *Ahlswede R., Aydinian H., Khachatrian L.,* On perfect codes and related concepts, Des., Codes and Cryptogr. 22 (2001) 221–237.

[2] *Assmus E. F., Jr., and Mattson H. F., Jr.,* On tactical configurations and error correcting codes, J. Comb.Theory 2 (1967) 243–257.

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

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

[5] *Avgustinovich S.V., Solov'eva F.I.,* On projections of perfect binary codes, Proc. Seventh Joint Swedish-Russian Workshop on Information Theory, St.-Petersburg, Russia. June (1995) 25–26.

[6] *Avgustinovich S.V., Solov'eva F.I.,* On the nonsystematic perfect binary codes, Problems of Inform. Transm. 32 (3) (1996) 258–261.

[7] *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.

[8] *Avgustinovich S.V., Solov'eva F.I.,* Construction of perfect binary codes by sequential translations of an α-components, Problems of Inform. Transm. 33 (3) (1997) 202–207.

[9] *Avgustinovich S.V., Solov'eva F.I.,* On distance regularity of perfect binary codes, Problems of Inform. Transm. 34 (3) (1998) 47–49 (in Russian).

[10] *Avgustinovich S.V., Solov'eva F.I.,* Perfect binary codes with trivial automotphism group, Proc. of Int. Workshop on Information Theory, Killarney, Ireland. June (1998) 114–115.

[11] *Avgustinovich S.V.,* To minimal distance graph structure of perfect binary $(n, 3)$-codes, Discrete Analysis and Operation Research 1 (5) 4 (1998) 3–5 (in Russian).

[12] *Avgustinovich S. V., Solov'eva F. I.,* New constructions and properties of perfect codes, Proc. of Int. Workshop on Discrete Analysis and Operation Research, Novosibirsk, Russia. June (2000) 5–10 (in Russian).

[13] *Avgustinovich S. V., Vasil'eva A. Y.,* On reconstruction of centered function, Proc. of Int. Workshop on Discrete Analysis and Operation Research, Novosibirsk, Russia. June (2000) 5–10 (in Russian).

[14] *Avgustinovich S. V., Lobstein A., Solov'eva F. I.,* Intersection matrices for partitions by binary perfect codes, IEEE Trans. on Inform. Theory (47) 4 (2001) 1621–1624.

[15] *Avgustinovich S. V., Heden O., Solov'eva F. I.,* The classification of some perfect codes, Stockholm: Royal Inst. of Technology, 2001. (Preprint / Trita-mat.–2001-9).

[16] *Avgustinovich S. V., Heden O., Solov'eva F. I.,* On ranks and kernels of perfect codes, Stockholm: Royal Inst. of Technology, 2001. (Preprint / Trita-mat.–2001-13).

[17] *Avgustinovich S. V., Heden O., Solov'eva F. I.,* Full rank perfect codes with big dimension kernels, Discrete Analysis and Operation Research 1 (8) 4 (2001) 3–8.

[18] *Avgustinovich S. V., Solov'eva F. I.,* On the metrical rigidity of binary codes, Proc. of Workshop on Coding and Cryptography WCC'2001, Paris, France. January (2001) 35–42.

[19] *Avgustinovich S. V., Heden O., Solov'eva F. I.,* On ranks and kernels problem of perfect codes, Proc. Eighth Int. Workshop on Algebraic and Comb. Coding Theory. Tsarskoe Selo, Russia. September (2002) 14–17.

[20] *Avgustinovich S. V., Solov'eva F. I., Heden O.,* On the ranks and kernels problem for perfect codes, Problems of Inform. Transm. 39 (4) (2003) 30–34.

[21] *Avgustinovich S. V., Vasil'eva A. Y.,* Evaluating of centered function by its values on the middle level of bulean cube, Discrete Analysis and Operation Research 1 (10) 2 (2003) 3–16 (in Russian).

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

[23] *Blokh E.L., Zyablov V.V.,* Coding of generalized concatenation codes, Problems of Inform. Transm. (10) 3 (1974) 45–50.

[24] *Cohen G., Honkala I., Lobstein A., Litsyn S.,* Covering codes, Elsevier, 1998.

[25] *Egorychev G. P.,* Solution of the van der Waerden problem for permanents, Preprint IFSO-13 M Akad. Nauk SSSR Sibirsk. Otdel., Inst. Fiz., Krasnoyarsk, 1980, 12 pp.

[26] *Egorychev G. P.,* The solution of the van der Waerden problem for permanents, Adv. in Math. (42) 3 (1981) 299–305.

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

[28] *Etzion T., Vardy A.,* On perfect codes and tilings: problems and solutions, SIAM J. Disc. Math. (11) 2 (1998) 205–223.

[29] *Hall M.,* Automorphisms of Steiner triple systems, IBM Journal of Research and Development 4 (1960) 460–472.

[30] *Heden O.,* A binary perfect code of length 15 and codimension 0, Des., Codes and Cryptogr. 4 (1994) 213–220.

[31] *Heden O.,* Private communication.

[32] *Handbook on coding theory,* Amsterdam: North-Holland, 1998.

[33] *Hergert F.,* Algebraische Methoden fur Nichtlineare Codes, *Hergert F.* Algebraische Methoden fur Nichtlineare Codes, Thesis Darmstadt. 1985.

[34] *Kabatyanskij G. A., Panchenko V. I.,* Packing and covering of the Hamming space by balls of unit radius, Problems of information Transm. (4) 24 (1988) 3–16 (in Russian).

[35] *Krotov D. S.,* On universal perfect code containing all given perfect codes, Discrete Analysis and Operation Research 1 (7) 1 (2000) 40–48.

[36] *Krotov D. S.* Lower bounds on the number of m-quasigroups of order 4 and the number of perfect binary codes, Discrete Analysis and Operation Research 1 (7) 2 (2000) 47–53.

[37] *Krotov D. S.,* Z_4-linear perfect codes, Discrete Analysis and Operation Research 1 (7) 4 (2000) 78–90.

[38] *Krotov D. S.,* Combining construction of perfect binary codes, Problems of Inform. Transm. (36) 4 (2000) 74–79.

[39] *Krotov D. S.,* Inductive construction of perfect ternary weighted codes, Problems of Inform. Transm. (37) 1 (2001) 3–11.

[40] *Krotov D. S.,* Z_4-linear Hadamard and extended perfect codes, Proceedings of the International Workshop on Coding and Cryptography, Paris, France. January (2001) 329–334.

[41] *Krotov D. S., Potapov V. N.,* On the reconstruction of n-quasigroups of order 4 and the upper bounds on their number, Proc. of Intern. Conf. devoted to 90th annivesary of A.A.Lyapunov, Novosibirsk, Russia. October (2000) 323–327.

[42] *Kurlyandchik Ya. M.,* On logariphm asysmptotic of length of maximal sparce cycle $r > 2$, Methody Discretnogo Analiza 19 (1971) 48–55 (in Russian).

[43] *Laborde J.-M.,* Une nouvelle famille de codes binaires, parfaits, non lineares, C. R. Acad. Sci. Paris. 1983. V. 297. N 1. P. 67–70.

[44] *Lloyd S. P.,* Binary block coding, Bell Syst. Tech. J. 36 (1957) 517–535.

[45] *Luc Teirlinck,* A completion of Lu/s determination of the spectrum for large sets of disjoint STS, J. of Comb. Theory, A (57) 2 (1991) 302–305.

[46] *MacWilliams, F. J. and Sloane, N. J. A.,* The theory of error-correcting codes, Amsterdam: North-Holland, 1977.

[47] *Malyugin S. A.,* Perfect codes with trivial automorphism group, Proc. of II Int. Workshop on Optimal Codes, Sozopol, Bulgaria. June (1998) 163–167.

[48] *Malyugin S. A.,* On enumeration of perfect binary codes of length 15, Discrete Analysis and Operation Research 1 (6) 2 (1999) 1 (6) 2 (1999) 48–73 (in Russian).

[49] *Malyugin S. A.,* On lower bound on the number of perfect binary codes, Discrete Analysis and Operation Research 1 (6) 4 (1999) 44–48 (in Russian).

[50] *Malyugin S. A.,* On the order of automorphism group of perfect binary codes, Discrete Analysis and Operation Research 1 (7) 4 (2000) 91–100 (in Russian).

[51] *Malyugin S. A.,* Nonsystematic perfect binary codes, Discrete Analysis and Operation Research 1 (8) 1 (2001) 55–76 (in Russian).

[52] *Malyugin S. A.,* Private communication.

[53] *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.

[54] *Näslund M.,* Steiner triple systems and perfect codes, Master of Sci. thesis, 1993, Royal Institute of Technology, Stockholm, Sweden.

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

[56] *Phelps K. T.,* A General Product Construction for Error Correcting Codes, SIAM J. Algebraic and Discrete Methods 5 (1984) 224–228.

[57] *Phelps K.T.,*, Every finite group is the automorphism group of some perfect code. J. of Combin. Theory, A 43 (1) (1986) 45–51.

[58] *Phelps K.T., LeVan M.J.,* Kernels of nonlinear Hamming codes, Des., Codes and Cryptogr. 6 (1995) 247–257.

[59] *Phelps K.T., LeVan M.J.,* Non-systematic perfect codes, SIAM J. Alg. Disc. Math. 12 (1) (1999) 27–34.

[60] *Phelps K.T., LeVan M.J.,* Switching equivalence classes of perfect codes, Des., Codes and Cryptogr. (16) 2 (1999) 179–184.

[61] *Phelps K. T.,*, An enumeration of 1-perfect binary codes of length 15, Australasian Journal of Combinatorics 21 (2000) 287–298.

[62] *Phelps K.T., Villanueva M.,*, On perfect codes: rank and kernel, Designs, Codes and Cryptogr. (27) 3 (2002) 183–194.

[63] *Phelps K.T., Rifa J., Villanueva M.,* The switching construction and kernels of q-ary perfect codes, Proc. Eighth Int. Workshop on Algebraic and Comb. Coding Theory. Tsarskoe Selo, Russia. September (2002) 222–225.

[64] *Rifa J., Pujol J.,* Translation-invariant propelinear codes, IEEE Trans. on Inform. Theory 43 (2) (1997) 590–598.

[65] *Romanov A. M.,* New binary codes with minimal distance three, Problems of Inform. Transm. (19) 3 (1983) 101–102.

[66] *Romanov A. M.,* On the construction of nonlinear perfect binary codes by inversion of symbols, Discrete Analysis and Operation Research 1 (4) 1 (1997) 46–52 (in Russian).

[67] *Romanov A. M.,* On nonsystematic perfect codes of length 15, Discrete Analysis and Operation Research 1 (4) 4 (1997) 75–78 (in Russian).

[68] *Romanov A. M.,* Perfect binary codes with trivial kernel, Discrete Analysis and Operation Research (4) 4 (1999) 75–78 (in Russian).

[69] *Shapiro G.S. and Slotnik D.S.,* On the mathematical theory of error correcting codes, IBM Journal of Research Development 3 (1959) 68–72.

[70] *Simonis J.,* On generator matrices of codes, IEEE Trans. on Inform.Theory (38) 2 (1992) 516.

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

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

[73] *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.

[74] *Solov'eva F.I., Avgustinovich S.V., Honold T., Heise W.,* On the extendability of code isometries, J. of Geometry 61 (1998) 3–16.

[75] *Solov'eva F. I.,* Constructions of perfect binary codes, Preprint 98-042, Universität Bielefeld, Sonderforschungsbereich 343 Discrete Structuren in der Mathematik (1998) 12 p.

[76] *Solov'eva F. I.,* Switchings and perfect codes, Numbers, Information and Complexity, Kluwer Academic Publisher (2000) 311–324.

[77] *Solov'eva F. I.,* Perfect binary codes: bounds and properties, Discrete Math. 213 (2000) 283–290.

[78] *Solov'eva F. I., Topalova S. T.,* On the automorphism groups of perfect binary codes and Steiner triple systems, Problems of Inform. Transm. (36) 4 (2000) 53–58.

[79] *Solov'eva F. I., Topalova S. T.,* Perfect codes and Steiner triple systems with maximal automorphism group order, Discrete Analysis and Operation Research 1 (7) 4 (2000) 101–110 (in Russian).

[80] *Solov'eva F. I.* Structure of i-components of perfect binary codes, Discrete Appl. of Math. (111) 1–2 (2001) 189–197.

[81] *Svanström M.* Ternary codes with weight constraints. Ph. Dissertation, N. 572. Linköping Univ. 1999.

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

[83] *Vardy A.* Private communication.

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

[85] *Vasil'ev Y.L.,* On comparing of complexity of deadlock and minimal disjunctive normal forms, Problems of Cybernetics 10 (1963) 5–61 (in Russian).

[86] *Vasil'ev Y.L., Solov'eva F.I.,* Codegenerating factorization on n-dimensional unite cube and perfect codes. Problems of Inform. Transm. 33 (1) (1997) 64–74.

[87] *Vasil'eva A.Y.,* Spectral properties of perfect binary (n,3)-codes, Dickrete Analysis and Operation Research (2) 2 (1995) 16–25 (in Russian).

[88] *Vasil'eva A.Y.,* On centered characteristic functions of perfect binary codes, Proc. of Sixth Int. Workshop on Algebraic and Combin. Coding Theory, Pskov, Russia. September (1998) 224–227.

[89] *Vasil'eva A.Y.,* Local spectra on perfect binary codes, Dickrete Analysis and Operation Research 1 (6) 1 (1999) 3–11 (in Russian).

[90] *Vasil'eva A.Y.,* Local and Interweight Spectra of Perfect Binary Codes, Proceedings of International Symposium on Information Theory ISIT-2000, Sorrento, Italy. June (2000) 474.

[91] *Vasil'eva A.Y.,* Strong distance invariance of perfect binary codes, Dickrete Analysis and Operation Research 1 (9) 4 (2002) 33–40 (in Russian).

[92] *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).

[93] *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.

[94] *Zinoviev V. A.,* On Generalized Concatenated Codes. Colloquia Mathematica Societatis Jànos Bolyai, V. 16, Topics in Information Theory, Keszthely, Hungary (1975) 587–592.

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

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

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

[98] *Zinov'ev V. A., Lobstein A. C.,* Constructions of perfect binary nonlinear codes. Proc. Sixth Int. Workshop on Algebraic and Comb. Coding Theory. Pskov, Russia. September (1998) 249–254.

[99] *Zinov'ev V.A., Lobstein A.S.,* On generalized concatenation constructions of nonlinear perfect binary codes, Problems of Inform. Transm. (36) 4 (2000) 59–73.

[100] *Zinov'ev V.A., Zinov'ev D.V.,* Binary extended perfect codes of length 16 by generalized concatenation construction, Proc. Eighth Int. Workshop on Algebraic and Comb. Coding Theory. Tsarskoe Selo, Russia. September (2002) 268–271.

Index

K-centered, 60
L-separable, 66
M-separable, 66
μ-component, 45
i-component, 41
k-dimensional face, 59
α-component, 41
2-(n, k, λ)-design, 69

automorphism group, 61

base code, 34
base set, 19
base set of codewords, 19
blocks, 63

centered characteristic function, 60
code
  concatenated, 25
  inner, 25
  outer, 25
code distance, 1
compliment, 13
cyclic, 6

distance-invariant, 51
distance-regular, 59

equivalent, 2

full rank family, 66

Hamming distance, 1
Hamming weight, 1

indecomposable, 50
intersection matrix, 28
isomorphic, 2, 13

kernel, 61, 64

metrically rigid, 68

neighborhood, 2

perfect, 2
periods, 61, 64
permutational automorphism group, 61

rank, 43
ranks and kernels problem, 64
reduced, 68

separable, 65
size, 66
Steiner quadruple system, 17
Steiner quadruple system, 63
Steiner triple system, 13
strongly distance-invariant, 59
switch, 41
switching, 41

translation, 41

weakly isometric, 69

Combinatorial and Computational Mathematics Center
Pohang University of Science and Technology

San 31, Hyoja-dong, Namgu, Pohang, 790-784, Korea.
http://com2mac.postech.ac.kr