Helsinki University of Technology Department of Communications and Networking
Teknillinen korkeakoulu Tietoliikenne- ja tietoverkkotekniikan laitos
Espoo 2009 Report 3/2009

PERFECT BINARY CODES: CLASSIFICATION AND PROPERTIES

Olli Pottonen

TEKNILLINEN KORKEAKOULU
TEKNISKA HÖGSKOLAN
HELSINKI UNIVERSITY OF TECHNOLOGY
TECHNISCHE UNIVERSITÄT HELSINKI
UNIVERSITE DE TECHNOLOGIE D'HELSINKI

Helsinki University of Technology Department of Communications and Networking
Teknillinen korkeakoulu Tietoliikenne- ja tietoverkkotekniikan laitos
Espoo 2009 Report 3/2009

PERFECT BINARY CODES: CLASSIFICATION AND PROPERTIES

Olli Pottonen

Dissertation for the degree of Doctor of Science in Technology to be presented with due permission of the Faculty of Electronics, Communication and Automation, for public examination and debate in Auditorium S4 at Helsinki University of Technology (Espoo, Finland) on 21st of August, 2009, at 12 noon.

Helsinki University of Technology
Faculty of Electronics, Communications and Automation
Department of Communications and Networking

Teknillinen korkeakoulu
Elektroniikan, tietoliikenteen ja automaation tiedekunta
Tietoliikenne- ja tietoverkkotekniikan laitos

Distribution:
Helsinki University of Technology
Department of Communications and Networking
P.O. Box 3000
FIN-02015 TKK
Tel. +358-9-451 5300
Fax +358-9-451 2474

ISBN 978-952-248-010-1
ISBN 978-952-248-011-8 (pdf)
ISSN 1797-478X
ISSN 1797-4798 (pdf)

Multiprint Oy
Espoo 2009

HELSINKI UNIVERSITY OF TECHNOLOGY P.O.BOX 1000, FI-02015 TKK http://www.tkk.fi	ABSTRACT OF DOCTORAL DISSERTATION

Author Olli Mikael Pottonen

Name of dissertation
Perfect Binary Codes: Classification and Properties

Date of manuscript 16.3.2009	Date of the dissertation 21.8.2009
Form of dissertation Article dissertation (summary + original articles)	
Faculty	Faculty of Electronics, Communication and Automation
Department	Department of Communications and Networking
Field of Research	Information theory
Opponent	Prof. Jeffrey Dinitz (University of Vermont)
Supervisor	Prof. Patric Östergård

Abstract

An r-perfect binary code is a subset of $\mathbb{Z}_2^n$ such that for any word, there is a unique codeword at Hamming distance at most r. Such a code is r-error-correcting. Two codes are equivalent if one can be obtained from the other by permuting the coordinates and adding a constant vector. The main result of this thesis is a computer-aided classification, up to equivalence, of the 1-perfect binary codes of length 15.

In an extended 1-perfect code, the neighborhood of a codeword corresponds to a Steiner quadruple system. To utilize this connection, we start with a computational classification of Steiner quadruple systems of order 16. This classification is also used to establish the nonexistence of Steiner quintuple systems $S(4, 5, 17)$.

The classification of the codes is used for computational examination of their properties. These properties include occurrences of Steiner triple and quadruple systems, automorphisms, ranks, structure of i-components and connections to orthogonal arrays and mixed perfect codes.

It is also proved that extended 1-perfect binary codes are equivalent if and only if their minimum distance graphs are isomorphic.

Keywords: Classification, Exact cover problem, Extended perfect code, Isomorph rejection, Minimum distance graph, Perfect code, Steiner system

ISBN (printed)	978-952-248-010-1	ISBN (pdf)	978-952-248-011-8
ISSN	1797-478X	ISSN (pdf)	1797-4798
Language	English	Number of pages	viii+19
Publisher	Helsinki University of Technology, Dept. of Communications and Networking		
The dissertation can be read at http://lib.tkk.fi/Diss/2009/isbn9789522480118			

TEKNILLINEN KORKEAKOULU P.L. 1000, 02015 TKK http://www.tkk.fi/	VÄITÖSKIRJAN TIIVISTELMA
Tekijä Olli Mikael Pottonen	
Väitöskirjan nimi Täydelliset binäärikoodit: luokittelu ja ominaisuuksia	
Käsikirjoituksen jättämispäivämäärä 16.3.2009	Väitöstilaisuuden ajankohta 21.8.2009
Väitöskirjan muoto Yhdistelmäväitöskirja (yhteenveto+erillisartikkelit)	
Tiedekunta Elektroniikan, tietoliikenteen ja automaation tiedekunta Laitos Tietoliikenne- ja tietoverkkotekniikan laitos Tutkimusala Informaatioteoria Vastaväittäjä Prof. Jeffrey Dinitz (University of Vermont) Työn valvoja Prof. Patric Östergård	

Tiivistelmä

Avaruuden $\mathbb{Z}_2^n$ osajoukko on r-täydellinen binäärikoodi, jos jokaisesta vektorista Hamming-etäisyyden r sisällä on yksikäsitteinen koodisana. Tällainen koodi on r virhettä korjaava. Kaksi koodia ovat ekvivalentteja, jos yksi niistä voidaan saada toisesta uudelleenjärjestämällä koordinaatit ja lisäämällä vakiovektori. Väitöskirjan päätulos on 1-täydellisten 15 pituisten binäärikoodien tietokoneavusteinen luokittelu ekvivalenssia vaille.

Laajennetussa 1-täydellisessä koodissa koodisanan naapurusto vastaa Steinerin nelikkosysteemiä. Hyödyntääksemme tätä yhteyttä aloitamme luokittelemalla laskennallisesti Steinerin nelikkosysteemit kertaluvulla 16. Tätä luokittelua käytetään myös todistamaan, ettei Steinerin systeemiä $S(4, 5, 17)$ ole olemassa.

Koodien luokittelua käytetään niiden ominaisuuksien laskennalliseen tutkimiseen. Näihin ominaisuuksiin kuuluu Steinerin kolmikko- ja nelikkojärjestelmien esiintymiset, automorfismit, rankit, i-komponenttirakenteet ja yhteydet ortogonaalisiin taulukoihin sekä täydellisiin sekakoodeihin.

Lisäksi työssä todistetaan, että laajennetut 1-täydelliset binäärikoodit ovat ekvivalentteja jos ja vain jos niiden minimietäisyysgraafit ovat isomorfisia.

Avainsanat: isomorfiakarsinta, laajennettu täydellinen koodi, luokittelu, minimietäisyysgraafi, Steinerin systeemi, täsmällinen peitto, täydellinen koodi			
ISBN (painettu)	978-952-248-010-1	ISBN (pdf)	978-952-248-011-8
ISSN	1797-478X	ISSN (pdf)	1797-4798
Kieli	englanti	Sivumäärä	viii+19
Julkaisija	Teknillinen korkeakoulu, Tietoliikenne- ja tietoverkkotekniikan laitos		
Väitöskirja luettavissa verkossa osoitteessa http://lib.tkk.fi/Diss/2009/isbn9789522480118			

Contents

Preface

In some sense this thesis is the latest step on a path that began in summer 2000 when I entered high school. Around that time I started to show serious interest in mathematics and related fields. Around that time I also entered a community of like-minded students, whose friendship and encouragement have been of enormous value ever since.

Work directly related to this thesis began in 2004 when I was studying for my Master's degree. For that summer I worked in the Communications laboratory[1] of Helsinki University of Technology TKK as a research assistant. The actual research was carried out in 2005 and 2007–2009, when I was hired by the Communications laboratory to continue my earlier work. The job was interesting as I was working on the two fields I found most interesting: mathematics and computer science.

Of the people who have been involved in this work, I first and foremost thank my supervisor Professor Patric Östergård for the guidance and encouragement that I have received during these years. I also thank Dr. Petteri Kaski for cooperation and many useful discussions, and my other coauthors, Prof. Kevin Phelps, Ivan Mogilnykh and Prof. Faina Solov'eva for their contribution to this work.

Numerous other people have helped my work less directly, and it is not possible to enumerate all of them. I thank the group of people who have reviewed this work. I have gained a lot from stimulating lectures of mathematics and computer science and interesting discussions with my colleagues.

This work was funded by the Graduate School in Electronics, Telecommunications and Automation GETA and the Academy of Finland as well as personal grants by the Finnish Foundation for Technology Promotion and the Nokia Foundation. Significant computing resources were provided by the TKK Computing Centre. I am grateful for all this support.

Last but not the least, I thank my family and friends for everything.

Otaniemi, 2.7.2009 Olli Pottonen

[1] Today Department of Communications and Networking

List of publications

This thesis consists of this summary and the following articles.

[P1] Petteri Kaski, Patric R. J. Östergård, and Olli Pottonen. The Steiner quadruple systems of order 16. *Journal of Combinatorial Theory. Series A*, 113(8):1764–1770, 2006.

[P2] Patric R. J. Östergård and Olli Pottonen. There exist Steiner triple systems of order 15 that do not occur in a perfect binary one-error-correcting code. *Journal of Combinatorial Designs*, 15(6):465–468, 2007.

[P3] Patric R. J. Östergård and Olli Pottonen. There exists no Steiner system $S(4, 5, 17)$. *Journal of Combinatorial Theory. Series A*, 115(8):1570–1573, 2008.

[P4] Patric R. J. Östergård and Olli Pottonen. The Perfect Binary One-Error-Correcting Codes of Length 15: Part I–Classification. *IEEE Transactions on Information Theory*, to appear.

[P5] Patric R. J. Östergård, Olli Pottonen and Kevin T. Phelps. The Perfect Binary One-Error-Correcting Codes of Length 15: Part II–Properties. Helsinki University of Technology, Department of Communications and Networking. Report 2/2009, Espoo, 2009.

[P6] Ivan Yu. Mogilnykh, Patric R. J. Östergård, Olli Pottonen, Faina I. Solov'eva. Reconstructing Extended Perfect Binary One-Error-Correcting Codes from Their Minimum Distance Graphs. *IEEE Transactions on Information Theory*, 55(6):2622–2625, 2009.

The author of the thesis is the main author of [P3] [P4] and [P6], wrote the first version of [P1] and took part in writing [P2] and [P5]. In [P1], [P2], [P3], [P4], and [P5] the author was responsible for designing the algorithms in detail and implementing them, and in [P6] the results in Sections III-V are mostly due to the author.

1 Introduction

In 1950 Richard Hamming published one of the first results concerning error-tolerant transmission and storage of data [21]. Since then coding theory has advanced immensely, and now techniques like low-density parity check codes and turbo codes [48] can transmit information at rates very close to the theoretical bound derived by Claude Shannon [59]. Nevertheless the Hamming codes have not been obsoleted.

Consider digital communication where a string of n symbols is transmitted, each symbol being an element of an alphabet of size q. Such strings are modeled as words of $\mathbb{Z}_q^n$, or if q is prime power we can use the vector space $\mathbb{F}_q^n$ over a finite field. Most common, and simplest, is the binary case with $q = 2$.

The *Hamming distance* between two words is the number of coordinates in which they differ. Some errors may be introduced to a codeword during transmission, but we may reasonable expect that the resulting word is rather close, in Hamming distance, to the original one. It is obviously desirable to be able to recover the original codeword.

An erroneous word can only be corrected if it is not close to more than one codeword. More precisely, up to r errors can always be corrected if the distance between any two codewords is at least $2r + 1$, or equivalently, if the balls of radius r around the codewords are nonintersecting. At the extreme these balls cover the entire ambient space, which leads to maximum transmission capability for the length and minimum distance in question. Codes with this property are called *perfect*, or r-perfect. The Hamming codes are 1-perfect.

An obvious necessary condition for the existence of r-perfect codes is that the cardinality of a ball of radius r divides the cardinality of the space. For example a binary 1-perfect code of length n may exist only if $(n+1)|2^n$. The Hamming codes prove that this condition is also sufficient: 1-perfect binary codes exist for lengths $n = 2^m - 1$.

Are there any other perfect codes? Yes; there are families of trivial codes with $r = 0$, $r = n$, and $r = (n + 1)/2$ for odd length n. In his remarkable half page paper Golay [19] described a 3-perfect binary code of length 23, a 2-perfect ternary code of length 11, and Hamming codes

over alphabets of prime size. Hamming codes further generalize over any finite field alphabet. In 1971 Tietäväinen and Perko [69] proved that every perfect binary code must have the same parameters—length, cardinality and minimum distance—as some aforementioned code. Two years later van Lint [70] and Tietäväinen [68] generalized the result for perfect codes over alphabets of prime power size—every perfect code has the same parameters as a Hamming code, a Golay code or a trivial code. The same result was independently proved by Zinov'ev and Leontiev [74]. For other alphabet sizes the matter is not completely settled, but in this case the nonexistence of nontrivial r-perfect codes has been proved for $r \geq 3$. Progress towards this result was started by Bannai [6], the cases $r = 3, 4, 5$ were solved by Reuvers [57], $r = 7$ and $r \geq 9$ by Best [7] and finally $r = 6, 8$ by Hong [27].

Now we know the possible parameters of perfect codes of prime power alphabets, but do we know all codes? It turns out that the Golay codes are (up to equivalence) the only codes with their parameters [13, 55, 61]. The same holds for Hamming codes of length 3 and 7; the former case is trivial and the latter was proved by Zaremba [73]. Originally it was thought that this would be the case for all lengths [60], but Vasil'ev [71] constructed nonlinear perfect codes, that are not equivalent to the linear Hamming codes. Nonbinary nonlinear codes were constructed by Schönheim [58] and Lindström [39].

The binary Hamming codes exist for lengths $n = 2^m - 1$. The lengths 3 and 7 are not very interesting, as the only codes are the Hamming codes, and there are not many interesting properties to study. For length 31 there are at least $2^{1854}3^{128} \approx 10^{619}$ codes [25], each consisting of 2^{26} codewords. Consequently computational study of these codes is hardly feasible. This makes length 15 the only interesting case for computational study, and indeed this specific case has gathered a lot of attention [23, 41, 42, 52, 53, 75, 76]

Different analytical constructions yield numerous nonequivalent codes, but not a complete catalog of the codes. However an exhaustive computer search based on the connection between Steiner systems and codes turns out to be possible, and is described in this thesis. A complete classification enables further study of the codes. All these results are computational. Indeed, computational methods allow us to solve problems which are beyond the reach of traditional mathematics. This approach requires knowledge of computer science in addition to mathematics, and special consideration should be given to correctness of the results.

1.1 Contribution of the thesis

The main result of this thesis is a classification of the perfect binary one-error-correcting codes of length 15 [P4] and the subsequent computational study of miscellaneous properties of these codes [P5], especially the nonex-

istence of codes which contain certain Steiner triple systems [P2, P5]. The classification relies on the classification of Steiner quadruple systems of order 16 [P1]. The classification of these quadruple systems is also utilized in proving that no Steiner system $S(4, 5, 17)$ exists [P3]. In addition it is proved that extended 1-perfect codes are equivalent if and only if they have isomorphic minimum distance graphs [P6].

1.2 Basic concepts

A binary code of length n is a nonempty subset of $\mathbb{Z}_2^n$. The Hamming distance $d(\mathbf{x}, \mathbf{y})$ between the words $\mathbf{x}$ and $\mathbf{y}$ is the number of coordinates in which they differ, the Hamming weight $\mathrm{wt}(\mathbf{x})$ of a word $\mathbf{x}$ is the number of its nonzero coordinates, and the support $\mathrm{supp}(\mathbf{x})$ of $\mathbf{x}$ is the set of these coordinates. Formally, $\mathrm{supp}(\mathbf{x}) = \{i : x_i \neq 0\}$, $\mathrm{wt}(\mathbf{x}) = |\mathrm{supp}(\mathbf{x})|$ and $d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} - \mathbf{y})$. The *minimum distance* of a code is the minimum amongst distances between distinct codewords. An r-perfect code is a code such that the balls $B(\mathbf{x}, r) = \{\mathbf{y} : d(\mathbf{x}, \mathbf{y}) \leq r\}$ form a partition of the space $\mathbb{Z}_2^n$.

A permutation π of $\mathbb{Z}_n$ acts on a word $\mathbf{x}$ of $\mathbb{Z}_2^n$ by permuting the coordinates, $\pi(\mathbf{x}) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})$, and another word $\mathbf{z}$ acts additively, giving $\mathbf{z}+\mathbf{x}$. A pair $(\pi, \mathbf{z})$ acts on a codeword $\mathbf{x}$ as $(\pi, \mathbf{z})(\mathbf{x}) = \pi(\mathbf{z}+\mathbf{x})$. Two codes C_1, C_2 are *isomorphic* if $\pi(C_1) = C_2$ for some π, and they are *equivalent* if $(\pi, \mathbf{z})(C_1) = C_2$. The *automorphism group* of a code C is defined as

$$\mathrm{Aut}(C) = \{(\pi, \mathbf{z}) : (\pi, \mathbf{z})(C) = C\}.$$

Two important subgroups of the automorphism group are the *kernel* and the *group of symmetries*, which are obtained by imposing the additional conditions $\pi = e$ (the identity mapping) or $\mathbf{z} = \mathbf{0}$ (the all-zero word), respectively.

An (n, M, d) code is a code of length n with M codewords and minimum distance d. A binary code is 1-perfect if and only if it is has parameters

$$n = 2^m - 1, \quad M = 2^n/(n+1) = 2^{2^m-m-1}, \quad d = 3.$$

A code can be *extended* by adding a coordinate. Unless stated otherwise, the value of the new coordinate is chosen so that each codeword gets even weight. Since this does not decrease distances and results in them being even, an extended 1-perfect code has minimum distance 4. The inverse operation of extending is *puncturing*, which means removing a coordinate. Note that a code has a unique extension, but can be punctured at several different coordinates. A code is an extended 1-perfect code if and only if it has parameters

$$n = 2^m, \quad M = 2^{n-1}/n = 2^{2^m-m-1}, \quad d = 4.$$

2 Designs and codes

Consider a 1-perfect binary code C with $\mathbf{0} \in C$. For any word $\mathbf{z}$ with weight 2 there is a unique codeword at distance 1. This means that the (supports) of the codewords with weight 3, which can be considered as the neighborhood of the codeword $\mathbf{0}$, form a combinatorial design called a *Steiner triple system*. The definition of Steiner systems and related results are presented in Section 2.1 and subsequent sections. For more information the reader is referred to [8, 10, 11].

2.1 Steiner systems

A *Steiner system* $S(t, k, v)$ with $t \leq k \leq v$ is a pair $(V, \mathcal{B})$ where V is a set of v *points* and $\mathcal{B}$ is a set of *blocks* such that each block consists of k points, and any set of t points occurs in a unique block. The parameter v is called the order of the design. Of special interest are the *Steiner triple systems* and *Steiner quadruple systems*, which are $S(2, 3, v)$ and $S(3, 4, v)$ designs, respectively. These are denoted as $\mathrm{STS}(v)$ and $\mathrm{SQS}(v)$ for short.

For a code C with minimum distance 3 we define the *neighborhood triple system* of a codeword $\mathbf{x} \in C$ as

$$\mathrm{NTS}(\mathbf{x}, C) = \{\mathrm{supp}(\mathbf{x} - \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, d(\mathbf{x}, \mathbf{y}) = 3\}.$$

By the reasoning above the neighborhood triple system of any codeword of a 1-perfect code is a Steiner triple system. Also the converse holds: a (nonempty) binary code is perfect if the neighborhood triple system of every codeword is an STS [54].

The *derived design* of $(V, \mathcal{B})$ induced by x is the design $(V', \mathcal{B}')$ with

$$V' = V \setminus \{x\}, \quad \mathcal{B}' = \{B \setminus \{x\} : x \in B \in \mathcal{B}\}.$$

The derived design of an $S(t, k, v)$ is an $S(t-1, k-1, v-1)$.

For codes with minimum distance 4 we can consider neighborhood quadruple systems, defined in the obvious fashion. The neighborhood quadruple systems of an extended perfect code are Steiner quadruple systems. By puncturing the extended code and considering neighborhood triple systems one gets derived triple systems of the neighborhood quadruple systems.

If all neighborhood quadruple systems of a nonempty code are Steiner quadruple systems, puncturing the code yields a code in which all neighborhood triple systems are Steiner systems. By the earlier result this code must be a perfect code. Hence the original code must be an extended perfect code.

There are also other connections between codes and designs. For example the codewords of weight 8 of the extended binary Golay code form the unique Steiner system $S(5, 8, 24)$, and the codewords of weight 5 of the extended ternary Golay code form the unique $S(5, 6, 12)$ [40, Chapter 20]. Other connections between codes and t-designs are analyzed in [1] and [40, Chapter 6].

Clearly Steiner triple systems exist for $v = 2^k - 1$ as they can be obtained from perfect codes, but also other orders are admissible. Counting the total number of blocks and the number of blocks containing given element show that the requirement $v \equiv 1, 3 \pmod 6$ is necessary. One of the earliest results in design theory was proving the sufficiency of this condition [33].

2.2 Derived designs

It is not known whether all Steiner triple systems are derived. For order 15 they are, as constructions by Diener, Schmitt and de Vries [16] and earlier results show. Already the next case, STS(19), is open. A related question is whether every STS($2^k - 1$) is a neighborhood triple system—being a derived design is a necessary, but not sufficient condition. In [P2] this is answered in negative for $k = 4$. However, Avgustinovich and Krotov [4] showed that an STS, or any 1-error-correcting code, occurs in a perfect code of greater length.

Since some STS(15) does not occur in a perfect code, none of the SQS(16) containing it as a derived design occurs in an extended perfect code. This result is not new, as Hergert had found a SQS(16) which is not a neighborhood quadruple system [26]. In [P5] it is concluded that exactly 33 of the 80 nonisomorphic STS(15) and 15,590 of the 1,054,163 nonisomorphic SQS(16) occur in perfect and extended perfect codes, respectively.

Steiner quadruple systems exist for $v \equiv 2, 4 \pmod 6$. Again simple counting arguments show that the requirement is necessary, and constructions by Hanani show that it is sufficient [22]. Note that this gives an alternative proof for the existence of Steiner triple systems, as they are derived designs of quadruple systems. For $S(4, 5, v)$ the matter is more difficult. The condition $v \equiv 3, 5 \pmod 6$ is necessary, but not sufficient, as neither $S(4, 5, 9)$, $S(4, 5, 15)$ nor $S(4, 5, 17)$ exists [46, P3]. No general sufficient conditions are known.

2.3 Classification

This section briefly surveys classification approaches for designs; for a comprehensive introduction to classification algorithms, the reader is referred to [31].

There are two basic approaches to classification of Steiner systems and other designs. One can construct the designs either point by point or block by block. It is also possible to mix these approaches [65] or use other techniques. In any case efficient isomorph rejection is essential; although it is in principle possible to iterate over generated designs and reject each that is isomorphic to an earlier one, this is very inefficient in terms of processing time, memory and parallelizability.

When proceeding point by point, isomorph rejection is typically accomplished by a technique called *orderly generation*, which was pioneered independently by Faradžev [17] and Read [56]. The basic idea is to require that all intermediate objects are canonical. There are several examples of this approach being applied for classification of Steiner systems [66] and similar designs [14, 15, 29, 49].

Progressing block by block has lately been accompanied by isomorph rejection with *generation by canonical augmentation*, which was discovered by McKay [45]. In typical application of this isomorph rejection technique one starts with a set of incomplete objects, called seeds, which are augmented to complete designs. To decide whether a designs is to be rejected or not, one does not only consider the design but also its relation to the seed. More generally generation by canonical augmentation may contain several augmentation and isomorph rejection steps.

The block by block approach has been used for classification of Steiner triple system, starting with the early manual [12, 72] and later computerized [20] classification of STS(15). Also SQS(14) have been classified with this type of approach [46]. More recenly the STS(19) have been classified with this type of approach [30], as have been the STS(21) with nontrivial automorphisms [28].

In [P1] the SQS(16) are classified using a block by block approach. The 80 nonisomorphic STS(15) are extended to quadruple systems in all possible ways with a straightforward computer search. Isomorphic designs are pruned with generation by canonical augmentation.

After advancing from a classification of STS(15) to a classification of SQS(16), it seems natural to take one step further and classify the quintuple systems $S(4, 5, 17)$. This is accomplished with a two-phase computer search [P3]. In the first phase, pairs of SQS(16) are combined to get potential pairs of derived designs, and in the second one a straightforward search attempts to extend those to complete designs. It turns out that none exist.

Once a classification has been achieved, it is definitely worthwhile to

run a consistency check on the results. The main method used in this work is a double counting check, which apparently was first used by Lam and Thiel [37]. A survey of correctness checks appears in [31, Chapter 10].

We will now demonstrate the check for extended 1-perfect codes. The same idea works just as well for other codes and Steiner systems. If $\mathcal{C}$ is the set of equivalence class representatives of the codes, the total number of codes is given by orbit-stabilizer theorem:

$$\sum_{C \in \mathcal{C}} \frac{|G|}{\mathrm{Aut}(C)}. \tag{2.1}$$

Here G is the group of pairs $(\pi, \mathbf{x})$, so $|G| = 16! \cdot 2^{16}$.

The orbit-stabilizer theorem can also be used as follows. Each code can be obtained by extending an SQS(16). Let the set $\mathcal{S}$ contain isomorphism class representatives of the quadruple systems, and let $N(S)$ be the number of extensions of the quadruple system S. Each code can be obtained by extending any of its 2048 neighborhood quadruple systems. Thus the total number of codes is

$$\frac{1}{2048} \sum_{S \in \mathcal{S}} \frac{|G| \cdot N(S)}{\mathrm{Aut}(S)} \tag{2.2}$$

The values of (2.1) and (2.2) are equal. By computing both of them from the classification data and verifying that they agree, we can gain more confidence in the correctness of the data.

3 Constructions of perfect binary codes

One of the central themes in the research on perfect codes has been constructing codes, the goal being to prove the existence of a code with a certain property or to produce a family of such codes. This chapter surveys some of the constructions.

We start with Hamming codes. Let H_m be an $m \times (2^m - 1)$ matrix, the columns of which contain every nonzero vector of $\mathbb{Z}_2^m$. The Hamming code of length $n = 2^m - 1$ is the set

$$C_n = \{\mathbf{x} \in \mathbb{Z}_2^n : H_m\mathbf{x} = \mathbf{0}\}.$$

In the nonbinary case the parity check matrix H has dimensions $m \times (q^m - 1)/(q - 1)$ and it contains one vector from each one-dimensional subspace of $\mathbb{F}_q^m$ as a column.

3.1 Increasing length

Let C_n be a perfect code of length n, let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be an arbitrary function and define the parity function as $\sigma(\mathbf{x}) = \sum_{i=1}^n x_i$, with addition carried out modulo 2. Now the following construction by Vasil'ev [71] gives a perfect code of length $2n + 1$:

$$C_{2n+1} = \{(\mathbf{x}|\mathbf{x} + \mathbf{y}|\sigma(\mathbf{x}) + f(\mathbf{y})) : \mathbf{x} \in \mathbb{Z}_2^n, \mathbf{y} \in C_n\}.$$

If $f(\mathbf{0}) = 0$ and f is nonlinear, then $\mathbf{0} \in C_{2n+1}$ and C_{2n+1} is nonlinear, which implies that it is not equivalent to the Hamming code. Note that since all admissible lengths are of the form $n = 2^m - 1$, the above construction produces codes of all such (lengths except the shortest one.) However for $n \leq 3$ it is not possible to choose nonlinear f with $f(\mathbf{0}) = 0$.

One of the most general constructions is due to Krotov [35], and is a generalization of Phelps's work [51]. Heden [24] proved that this construction produces all non-full-rank codes; the *rank* of a code is the dimension of the linear space it spans (we assume that the code contains the word $\mathbf{0}$). This

construction is most conveniently expressed for extended perfect codes. Let $n = st$ where both s and t are powers of 2. We consider vectors of $\mathbb{Z}_2^n$ as concatenations of s vectors of length t, $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_s) \in \mathbb{Z}_2^n$, $\mathbf{x}_i \in \mathbb{Z}_2^t$. The parity function σ is defined above, and the generalized parity function is $\boldsymbol{\sigma} : \mathbb{Z}_2^n \to \mathbb{Z}_2^s, (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_s) \mapsto (\sigma(\mathbf{x}_1), \ldots, \sigma(\mathbf{x}_t))$.

A *Krotov component* or $\boldsymbol{\mu}$*-component* $K_{\boldsymbol{\mu}}$ is a subset of $\mathbb{Z}_2^n$ with minimum distance 4 and cardinality $2^{n-s-\log_2 t}$ such that that each word has even weight and $\boldsymbol{\sigma}(\mathbf{x}) = \boldsymbol{\mu}$ for every $\mathbf{x} \in K_{\boldsymbol{\mu}}$. When C_s is an extended perfect code of length s, then

$$C_n = \bigcup_{\boldsymbol{\mu} \in C_s} K_{\boldsymbol{\mu}}$$

is an extended perfect code.

In a series of papers Zinov'ev and Zinov'ev [75, 76, 77] classified the non-full-rank extended perfect codes of length 16. These papers use independently discovered techniques instead of utilizing Krotov's work, and in any case finding all possible Krotov components is a difficult problem. The work in [75] corresponds to $t = s = 4$, $C_s = \{0000, 1111\}$, and the work in [77] to $t = 8$, $s = 2$ and $C_s = \{00\}$. The latter case is presented as a doubling constructing for extended perfect codes of length 8.

3.2 Translating components

Some general techniques employ i-components and α-components. An i-*component* is a subset of a code such that switching the value of the ith coordinate in the subset does not decrease the minimum distance of the entire code. An α-*component* is an i-component for each $i \in \alpha$. It is not difficult to prove that each 1-perfect code consists of at least two i-components [62]. For length 15 all possible structures of i-components and α-components are tabulated in [P5]. Malyugin has classified the perfect codes obtained from the Hamming code with a certain kind of i-component switches [41, 42].

The best known lower bound for the number of distinct perfect codes was obtained by Krotov [36] by switching α-components and using Phelps's [51] construction. The lower bound for length n is

$$2^{2^{(n+1)/2-\log(n+1)}} 3^{2^{(n-3)/4}} 2^{2^{(n+5)/4-\log(n+1)}}.$$

It turns out [P5] that all perfect codes of length 15 can be obtained by combining Krotov's construction and switching i-components. However, there is no good explanation for this fact, and it is not known whether the same holds for larger lengths.

3.3 Codeword-by-codeword search

When constructing general one-error-correcting codes computationally, we can consider a graph where the vertices correspond to potential codewords, and edges connect pairs of codewords with Hamming distance at least three. Now cliques correspond to the codes, and maximum cliques to optimal codes. This approach is succesfully employed in [50], although without explicit graph theoretical terminology.

In search of perfect codes we can utilize the additional constraint that the entire space must be covered by the balls of radius one around the codewords, and in [P4] 1-perfect codes are constructed computationally by searching for partitions of the space $\mathbb{Z}_2^{15}$ into such balls. In computer science the task of partitioning a set by using given collection of its subsets is called the *exact cover problem*. This problem was one of the first that were proven to be NP-complete, and the best known algorithm is a brute force search with some optimization heuristics. Knuth has suggested clever data structures very suitable for this task [34]. The idea is to use double linked lists which allows fast insertion and removal of elements. The implementation used in this work is the libexact library [32].

Some additional information is needed to make the exact cover search feasible. As stated in Chapter 2, the neighborhood of a codeword in an extended perfect code corresponds to a Steiner quadruple system, and a complete classification of SQS(16) is available [P1]. This way we get all (up to isomorphism) possible combinations of codewords with weight at most 4, which restricts the search immensely making it very fast.

4 Equivalence of codes

Once a family of codes has been constructed, equivalent codes need to be rejected in order to obtain a classification. This kind of isomorph rejection problems have been encountered several times in the literature [31]. In many isomorph rejection methods the objects are labelled canonically using the graph isomorphism software nauty [43, 44]. A code can be transformed into graph by creating a vertex for each codeword and for each pair of coordinate and alphabet symbol. A codeword is adjacent to the pairs corresponding to the values it has at different coordinates, and pairs with the same coordinate form a clique. For small codes this works well [50], but for 1-perfect codes of length 15 it results in graphs that nauty can not process within reasonable time [P4, 52].

Phelps [52] used a canonical labeling method that is based on considering the code as the kernel and its cosets. The kernel can be computed quickly [38], and the kernel and canonical coset representatives can be handled with nauty.

In the classification of perfect codes [P4] the following method is employed. A canonical isomorphism class representative $c_I(C)$ of the code C is computed with nauty—this is reasonably fast. Canonical equivalence class representative is defined as $c_E(C) = \min_{\mathbf{x}\in C} c_I(C + \mathbf{x})$, where the minimum is taken with respect to some total order.

Some methods have been tailored for codes obtained by a specific construction. For example Zinov'ev and Zinov'ev used this approach [77].

No matter which method is used, suitable invariants can speed up the computation. For example one can count some configurations in the Steiner triple and quadruple systems contained in the code. Moreover it may be of use to consider automorphisms of the code.

4.1 Minimum distance graphs

Phelps and LeVan [53] made use of the fact that equivalent codes have isomorphic minimum distance graphs; the *minimum distance graph* has the codewords as vertices. Two vertices are adjacent if the corresponding codewords have Hamming distance equal to the minimum distance of the code.

It turns out that canonical labeling of these graphs is rather fast.

Isomorphism of minimum distance graphs is connected to isometricity; two codes are *isometric* if some distance-preserving functions maps one code onto the other. Clearly equivalence implies isometricity, and only isometries of the entire space are the pairs $(\pi, \mathbf{x})$ considered in Section 1.2. Isometricity does not in general imply equivalence, but for several families of codes it does [5, 64].

Since the neighborhood of a vertex corresponds to the neighborhood triple (quadruple) system of the codeword, for (extended) 1-perfect codes the minimum distance graphs are regular. However, they are not strongly regular.

Spielman [67] proved that STS(v) with $v \geq 19$ can be reconstructed from their block intersection graphs by considering the maximum cliques. By applying the same idea for the neighborhood triple system, Avgustinovich proved that 1-perfect binary codes with length strictly greater than 15 are equivalent if and only if they have isomorphic minimum distance graphs [2]. The same holds also for length 15; also this result was proved by Avgustinovich [3]. The proof relies on the fact that these codes are isometric if they have isomorphic minimum distance graphs, and on a tedious analysis by Solov'eva and others [64] showing that most (not necessarily binary) perfect codes are equivalent if they are isometric.

Also (extended) Preparata codes have isomorphic minimum distance graphs only if the codes are equivalent. This was independently proved by Fernández-Córboda and Phelps [18] and Mogilnykh [47]. Fernández-Córboda and Phelps demonstrated that by considering the maximum cliques and their connections the code can be reconstructed. Mogilnykh proved that codes with isomorphic minimum distance graphs are isometric. The general result by Avgustinovich and Solov'eva [5] show that isometricity of these codes imply equivalence for large enough length.

Extended 1-perfect codes with isomorphic minimum distance graphs are isometric [P6], and a the work of Avgustinovich and Solov'eva [5] show that isometricity of these codes imply equivalence for length $n \geq 256$. A more careful analysis shows that the isomorphism of minimum distance graphs implies equivalence for smaller lengths as well [P6], and furthermore automorphism groups of the codes and of the graphs are isomorphic for $n \geq 16$. It appears that the proof is most difficult for $n = 16$.

The proof in [P6] relies on the fact that neighborhood quadruple system of a codeword can be reconstructed, up to isomorphism, from the graph. Once that is done, the rest of the code can be reconstructed inductively. The quadruple systems are reconstructed by showing that maximum cliques in their block intersection graphs have useful combinatorial interpretation. Similar ideas have been used in most of the works cited above.

5 Conclusions

The 1-perfect binary codes of length 15 have now been classified [P4]. This classification has enabled a broad computational study of the properties of the codes; these properties include automorphisms, occurrences of Steiner systems, i-components and α-components, systematicity, embedded codes, defining sets and connections to orthogonal arrays and mixed perfect codes [P5].

Now the work of studying these codes computationally appears to be mostly completed, although there are still some interesting problems which might admit at least a partial computational solution. These include classifying the partitions of $\mathbb{Z}_2^{15}$ with nonintersecting perfect codes, finding all possible cardinalities of intersections of perfect codes, and determining whether each $(13, 512, 3)$ code can be obtained by shortening a prefect code; for $(14, 1024, 3)$ codes the answer is affirmative, as shown by Blackmore [9]. It appears unlikely that computational research could be continued by a complete classification for length 31.

A closely related topic of further research is the classification of nonbinary 1-perfect codes using an analogous approach. In this case the neighborhood of a codeword corresponds to a generalized Steiner triple system.

Prior to this work 11 was the largest length for which classification of optimal binary one-error-correcting codes was known [50]. Now classification is known for $n = 14, 15$ [P4], but the cases $n = 12, 13$ remain open.

The classifications of Steiner quadruple systems and perfect codes fall within the scope of combinatorial classification, and rely on techniques typically encountered there. Although the techniques are already mature and sophisticated, there is still room for further work, especially with software tools. Also answers to some deep theoretical questions, such as whether NP = P, are of great interest.

Finally, the correctness of results should be addressed, as complex computer programs are likely to contain errors. Accordingly attempts to detect erroneous results should be made on all levels: software implementation, algorithm designs and mathematical analysis. In the author's experience a double counting consistency check has proven really useful for this purpose.

Bibliography

[1] E. F. Assmus, Jr. and J. D. Key. *Designs and their codes.* Cambridge University Press, Cambridge, 1992.

[2] S. V. Avgustinovich. On isometry of close-packed binary codes [Translation of *Discrete analysis (Russian)*, 3–5, Izdat. Ross. Akad. Nauk Sibirsk. Otdel. Inst. Mat., Novosibirsk, 1994]. *Siberian Adv. Math.*, 5(3):1–4, 1995.

[3] S. V. Avgustinovich. Perfect binary $(n, 3)$ codes: the structure of graphs of minimum distances. *Discrete Appl. Math.*, 114:9–11, 2001.

[4] S. V. Avgustinovich and D. Krotov. Embedding in a perfect code. *J. Combin. Des.*, to appear.

[5] S. V. Avgustinovich and F. I. Solov′eva. On the metric rigidity of binary codes. *Problemy Peredachi Informatsii*, 39(2):23–28, 2003. English translation in *Probl. Inf. Transm.*, 39:178–183, 2003.

[6] E. Bannai. On perfect codes in the Hamming schemes $H(n, q)$ with q arbitrary. *J. Combin. Theory Ser. A*, 23(1):52–67, 1977.

[7] M. R. Best. *A Contribution to the Nonexistence of Perfect Codes.* Ph.D. thesis, University of Amsterdam, 1982.

[8] T. Beth, D. Jungnickel, and H. Lenz. *Design theory. Vol. II.* Cambridge University Press, Cambridge, second edition, 1999.

[9] T. Blackmore. Every binary $(2^m-2, 2^{2^m-2-m}, 3)$ code can be lengthened to form a perfect code of length $2^m - 1$. *IEEE Trans. Inform. Theory*, 45:698–700, 1999.

[10] C. J. Colbourn and J. H. Dinitz, editors. *The CRC Handbook of Combinatorial Designs.* CRC Press, Boca Raton, FL, second edition, 2006.

[11] C. J. Colbourn and A. Rosa. *Triple systems.* The Clarendon Press Oxford University Press, New York, 1999.

[12] F. N. Cole, L. D. Cummings, and H. S. White. The complete enumeration of triad systems in 15 elements. *Proc. Nat. Acad. Sci. U.S.A.*, 3:197–199, 1917.

[13] P. Delsarte and J.-M. Goethals. Unrestricted codes with the Golay parameters are unique. *Discrete Math.*, 12:211–224, 1975.

[14] P. C. Denny and P. B. Gibbons. Case studies and new results in combinatorial enumeration. *J. Combin. Des.*, 8:239–260, 2000.

[15] P. C. Denny and R. Mathon. A census of t-$(t+8, t+2, 4)$ designs, $2 \leq t \leq 4$. *J. Statist. Plann. Inference*, 106:5–19, 2002.

[16] I. Diener, E. Schmitt, and H. L. de Vries. All 80 Steiner triple systems on 15 elements are derived. *Discrete Math.*, 55:13–19, 1985.

[17] I. A. Faradžev. Constructive enumeration of combinatorial objects. In *Problèmes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976)*, volume 260 of *Colloq. Internat. CNRS*, pages 131–135. CNRS, Paris, 1978.

[18] C. Fernández-Córboda and K. T. Phelps. On the minimum distance graph of an extended Preparata code. arXiv:0902.1351v1.

[19] M. J. E. Golay. Notes on digital coding. *Proc IRE*, 37:657, 1949.

[20] M. Hall, Jr. and J. D. Swift. Determination of Steiner triple systems of order 15. *Math. Tables Aids Comput.*, 9:146–152, 1955.

[21] R. W. Hamming. Error detecting and error correcting codes. *The Bell System Tech. J.*, 26:147–160, April 1950.

[22] H. Hanani. On quadruple systems. *Canad. J. Math.*, 12:145–157, 1960.

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

[24] O. Heden. On the classification of perfect binary 1-error-correcting codes. TRITA-MAT-2002-1, Kungliga Tekniska högskolan, 2002.

[25] O. Heden. A survey of perfect codes. *Adv. Math. Commun.*, 2:223–247, 2008.

[26] F. Hergert. *Algebraische Methoden für nichtlineare Codes*. Ph.D. thesis, Technische Universität Darmstadt, 1985.

[27] Y. Hong. On the nonexistence of unknown perfect 6- and 8-codes in Hamming schemes $H(n, q)$ with q arbitrary. *Osaka J. Math.*, 21:687–700, 1984.

[28] P. Kaski. Isomorph-free exhaustive generation of designs with prescribed groups of automorphisms. *SIAM J. Discrete Math.*, 19:664–690, 2005.

[29] P. Kaski and P. R. J. Östergård. Miscellaneous classification results for 2-designs. *Discrete Math.*, 280:65–75, 2004.

[30] P. Kaski and P. R. J. Östergård. The Steiner triple systems of order 19. *Math. Comp.*, 73:2075–2092, 2004.

[31] P. Kaski and P. R. J. Östergård. *Classification Algorithms for Codes and Designs.* Springer-Verlag, Berlin, 2006.

[32] P. Kaski and O. Pottonen. libexact user's guide, version 1.0. Technical Report HIIT TR 2008-1, Helsinki Institute for Information Technology HIIT, Helsinki, 2008.

[33] T. P. Kirkman. On a problem in combinations. *Cambridge and Dublin Math. J.*, 2:191–204, 1847.

[34] D. E. Knuth. Dancing links. In J. Davies, B. Roscoe, and J. Woodcock, editors, *Millennial Perspectives in Computer Science*, pages 187–214. Palgrave, Houndmills, Basingstoke, Hampshire, 2000.

[35] D. S. Krotov. Combined construction of perfect binary codes. *Problemy Peredachi Informatsii*, 36(4):74–79, 2000. English translation in *Probl. Inf. Transm.*, 36:349–353, 2000.

[36] D. S. Krotov. Lower bounds for the number of m-quasigroups of order four and of the number of perfect binary codes. *Diskretn. Anal. Issled. Oper. Ser. 1*, 7:47–53, 97, 2000.

[37] C. W. H. Lam and L. Thiel. Backtrack search with isomorph rejection and consistenci check. *J. Symbolic Comput.* 7:473–485, 1989.

[38] M. LeVan and K. T. Phelps. Computing the kernel of a non-linear code. *J. Combin. Math. Combin. Comput.*, 20:237–241, 1996.

[39] B. Lindström. On group and nongroup perfect codes in q symbols. *Math. Scand.*, 25:149–158, 1970.

[40] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, 1977.

[41] S. A. Malyugin. On enumeration of the perfect binary codes of length 15. *Discrete Appl. Math.*, 135:161–181, 2004.

[42] S. A. Malyugin. On the enumeration of nonequivalent perfect binary codes of length 15 and rank 15. *Diskretn. Anal. Issled. Oper. Ser. 1*, 13:77–98, 2006.

[43] B. D. McKay. Practical graph isomorphism. *Congr. Numer.* 30:45–87, 1981.

[44] B. D. McKay. nauty user's guide (version 1.5). Technical Report TR-CS-90–02, Computer Science Department, Australian National University, Canberra, 1990.

[45] B. D. McKay. Isomorph-free exhaustive generation. *J. Algorithms*, 26:306–324, 1998.

[46] N. S. Mendelsohn and S. H. Y. Hung. On the Steiner systems $S(3, 4, 14)$ and $S(4, 5, 15)$. *Utilitas Math.*, 1:5–95, 1972.

[47] I. Yu. Mogilnykh. On weak isometries of Preparata codes. arXiv:0902.2316v3.

[48] J. C. Moreira and P. G. Farrell. *Essentials of Error-Control Coding.* Wiley, 2006.

[49] P. R. J. Östergård. Enumeration of 2-$(12, 3, 2)$ designs. *Australas. J. Combin.*, 22:227–231, 2000.

[50] P. R. J. Östergård, T. Baicheva and E. Kolev. Optimal binary one-error-correcting codes of length 10 have 72 codewords. *IEEE Trans. Inform. Theory* 45:1229–1231, 1999.

[51] K. T. Phelps. A combinatorial construction of perfect codes. *SIAM J. Algebraic Discrete Methods*, 4:398–403, 1983.

[52] K. T. Phelps. An enumeration of 1-perfect binary codes. *Australas. J. Combin.*, 21:287–298, 2000.

[53] K. T. Phelps and M. LeVan. Switching equivalence classes of perfect codes. *Des. Codes Cryptogr.*, 16:179–184, 1999.

[54] K. T. Phelps and M. Villanueva. On perfect codes: rank and kernel. *Des. Codes Cryptogr.*, 27:183–194, 2002.

[55] V. Pless. On the uniqueness of the Golay codes. *J. Combinatorial Theory*, 5:215–228, 1968.

[56] R. C. Read. Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations. *Ann. Discrete Math.*, 2:107–120, 1978.

[57] H. F. H. Reuvers. *Some Non-existence Theorems for Perfect Codes over Arbitrary Alphabets*. Ph.D. thesis, Technische Hogeschool Eindhoven, Eindhoven, 1977.

[58] J. Schönheim. On linear and nonlinear single-error-correcting q-nary perfect codes. *Information and Control*, 12:23–26, 1968.

[59] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948.

[60] H. S. Shapiro and D. L. Slotnick. On the mathematical theory of error-correcting codes. *IBM Journal of Research and Development*, 3:25–34, 1959.

[61] S. L. Snover. *The Uniqueness of the Nordstrom-Robinson and the Golay Binary Codes*. Ph.D. thesis, Dept. of Mathematics, Michigan State University, 1973.

[62] F. I. Solov′eva. Structure of i-components of perfect binary codes. *Discrete Appl. Math.*, 111:189–197, 2001.

[63] F. I. Solov′eva. On perfect binary codes. *Discrete Appl. Math.*, 156:1488–1498, 2008.

[64] F. I. Solov′eva, S. V. Avgustinovich, T. Honold, and W. Heise. On the extendability of code isometries. *J. Geom.*, 61:3–16, 1998.

[65] E. Spence. A complete classification of symmetric $(31, 10, 3)$ designs. *Des. Codes Cryptogr.*, 2:127–136, 1992.

[66] E. Spence. The complete classification of Steiner systems $S(2, 4, 25)$. *J. Combin. Des.*, 4:295–300, 1996.

[67] D. A. Spielman. Faster isomorphism testing of strongly regular graphs. In *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, pages 576–584, New York, 1996.

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

[69] A. Tietäväinen and A. Perko. There are no unknown perfect binary codes. *Ann. Univ. Turku. Ser. A I No.*, 148:6, 1971.

[70] J. H. van Lint. *Coding Theory*. Lecture Notes in Mathematics, Vol. 201. Springer-Verlag, Berlin, 1971.

[71] J. L. Vasil'ev. On nongroup close-packed codes. *Probl. Kibernet.*, 8:337–339, 1962.

[72] H. S. White, F. N. Cole, and L. D. Cummings. Complete classification of triad systems on fifteen elements. *Memoirs Nat. Acad. Sci. U.S.A.*, 14:1–89, 1919.

[73] S. K. Zaremba. Covering problems concerning Abelian groups. *J. London Math. Soc.*, 27:242–246, 1952.

[74] V. A. Zinov′ev and V. K. Leont′ev. On non-existence of perfect codes over Galois fields. *Problems of Control and Information Theory/Problemy Upravlenija i Teorii Informacii*, 2:123–132, 1973.

[75] V. A. Zinov′ev and D. V. Zinov′ev. Binary extended perfect codes of length 16 obtained by a generalized concatenated construction. *Problemy Peredachi Informatsii*, 38(4):56–84, 2002. English translation in *Probl. Inf. Transm.*, 38:296–322, 2002.

[76] V. A. Zinov′ev and D. V. Zinov′ev. Binary perfect codes of length 15 obtained by a generalized concatenated construction. *Problemy Peredachi Informatsii*, 40(1):27–39, 2004. English translation in *Probl. Inf. Transm.* 40:25–36, 2004.

[77] V. A. Zinov′ev and D. V. Zinov′ev. Binary extended perfect codes of length 16 and rank 14. *Problemy Peredachi Informatsii*, 42(2):63–80, 2006. English translation in *Probl. Inf. Transm.* 42:123–138, 2006.