

Perfect codes and related topics

(Introduction lecture)

Faina I. Solov'eva

Sobolev Institute of Mathematics,
Novosibirsk State University,
Novosibirsk, Russia
Email: sol@math.nsc.ru

The topic of perfect codes is one of the most important topics in the theory of error-correcting codes. The class of perfect codes is very complicated, large (double exponential) and intensively studied by many researches. The investigation of nontrivial properties of perfect codes is significant both from coding point of view (for the solution of the classification problem for such codes) and for combinatorics, graph theory, group theory, geometry, cryptography. Many constructions and properties for perfect binary codes can be applied for codes with other parameters (lengths, sizes, distances) or for nonbinary cases. In this talk an introduction to the theory of perfect codes is presented. Some links with related subjects are outlined and some open problems are given.

Classification of the Perfect Binary One-Error-Correcting Codes of Length 15

Patric R. J. Östergård

Department of Communications and Networking
Helsinki University of Technology TKK
Helsinki, Finland

Joint work with Olli Pottonen

Email: pat@cc.hut.fi

After the solution of the existence problem for perfect codes over prime power alphabets by Tietäväinen and others in the 1970s, much effort has been put on getting a thorough understanding of the structure of such codes. A complete classification up to equivalence of codes with short length is of great help in the investigation of the structure and properties of codes. As for computer-aided classification of perfect binary one-error-correcting codes, the cases of length at most 7 are trivial, whereas the next admissible case, length 15, is already challenging (and length 31 out of reach).

A computer-aided classification of the perfect binary one-error-correcting codes of length 15 is here obtained. There are, up to equivalence, 5983 such perfect codes and 2165 extended codes of length 16. The recent classification of Steiner quadruple systems of order 16 plays a central role in this classification. Utilizing a result of Blackmore, the optimal binary one-error-correcting codes of length 14 can also be classified; there are, up to equivalence, 38408 such codes. These computational results have been validated through double counting arguments.

As for the classification of short optimal binary one-error-correcting codes, after the current work there is a gap for the cases of length 12 and 13.

Properties of the Perfect One-Error-Correcting Codes of Length 15

Olli Potttonen

Finnish Defence Forces Technical Research Centre,
Riihimäki, Finland

Joint work with Patric Östergård and Kevin Phelps
E-mail: olli.potttonen@iki.fi

A complete classification of the perfect binary one-error-correcting codes of length 15 as well as their extensions of length 16 was recently carried out in [P. R. J. Östergård and O. Potttonen, “The perfect binary one-error-correcting codes of length 15: Part I—Classification,” *IEEE Trans. Inform. Theory* vol. 55, pp. 4657–4660, 2009.] In this work, the classified codes are studied in detail.

The shortened and double-shortened perfect codes are classified. It is known that the former set contains all optimal one-error-correcting codes of length 14, but it turns out that the same does not hold for length 13.

Exactly 33 of the 80 Steiner triple systems of order 15 occur in the perfect codes. The codes divide into 9 switching classes, none of which contains only full-rank codes. Other topics studied include (non)systematic codes, embedded one-error-correcting codes, and defining sets of codes. A classification of certain mixed perfect codes is also obtained.

On perfect 2-colorings of Johnson graphs

Ivan Yu. Mogilnykh

Sobolev Institute of Mathematics,

Novosibirsk State University,

Novosibirsk, Russia

Email: ivmog84@gmail.com

Perfect m -coloring of a graph G with the matrix $A = \{a_{ij}\}_{i,j=1,\dots,m}$ is a coloring of the vertices of G into the set of colors $\{1, \dots, m\}$ such that the number of vertices of the color j adjacent with the fixed vertex x of the color i does not depend on a choice of the vertex x and equals to a_{ij} . In this talk we study perfect 2-colorings of Johnson graphs. Such combinatorial structures like 1-perfect constant weight codes, Steiner triple and quadruple systems can be defined in terms of perfect 2-colorings of Johnson graphs. We consider several approaches for proving the nonexistence of perfect 2-colorings of Johnson graphs; we give a survey on known constructions.

Equitable partitions as a generalization of perfect codes

Svetlana A. Puzynina

Sobolev Institute of Mathematics,

Novosibirsk, Russia

University of Turku, Finland

Email: puzynina@math.nsc.ru

This note is a survey of results on a generalization of perfect codes called equitable partitions, emphasizing relations with coding theory. A partition of vertices of a graph is called equitable, if for every vertex the number of adjacent vertices from each partition class is determined by the partition class of the vertex. Parameters of equitable partition are given by a square matrix. A perfect code is a particular case of an equitable partition with two partition classes, codevertices and non-codevertices. The notion of equitable partition can be used for obtaining results on codes in general form. Besides equitable partitions, some other related generalizations of perfect codes are considered.

On the binary codes with parameters of doubly-shortened 1-perfect codes

Denis S. Krotov

Sobolev Institute of Mathematics,

Novosibirsk, Russia

Email: krotov@math.nsc.ru

We show that any binary $(n = 2^k - 3, 2^{n-k}, 3)$ code C_1 is a cell of an equitable partition (perfect coloring) (C_1, C_2, C_3, C_4) of the n -cube with the quotient matrix

$$\begin{pmatrix} 0 & 1 & n-1 & 0 \\ 1 & 0 & n-1 & 0 \\ 1 & 1 & n-4 & 2 \\ 0 & 0 & n-1 & 1 \end{pmatrix}.$$

Now the possibility to lengthen the code C_1 to a 1-perfect code of length $n+2$ is equivalent to the possibility to split the cell C_4 into two distance-3 codes or, equivalently, to the biparticity of the graph of distances 1 and 2 of C_4 . In any case, C_1 is uniquely embeddable in a twofold 1-perfect code of length $n+2$ with some structural restrictions, where by a twofold 1-perfect code we mean that any vertex of the space is within radius 1 from exactly two codewords. By one example, we briefly discuss $2-(v, 3, 2)$ multidesigns with similar restrictions.

We also show a connection of the problem with the problem of completing latin hypercuboids of order 4 to latin hypercubes.

Keywords: 1-perfect code; doubly-shortened 1-perfect code; equitable partition; perfect coloring; weight distribution; distance distribution.

On the existence of extended perfect binary codes with trivial symmetry group

Thomas Westerbäck

Department of Mathematics, KTH,
Stockholm, Sweden

Joint work with Olof Heden and Fabio Pasticci

Email: thowest@kth.se

The set of permutations of the coordinate set that maps a code C into itself is called the symmetry group of C and is denoted by $\text{Sym}(C)$.

In this talk we will discuss the existence of perfect and extended perfect codes of different length and rank with a trivial symmetry group. More precisely it will be shown that for all integers $m = 4, 5, 6, \dots$, and for any r , where $2^m - m + 2 \leq r \leq 2^m - 2$, there are extended perfect codes C of length 2^m and rank r with $\text{Sym}(C) = \{\text{id}\}$. Consequently the same result is also true for perfect codes of length $2^m - 1$.

Preparata codes over $GF(4)$

Thomas Ericson

Linköping, Sweden

Email: annette.och.thomas@telia.com

The binary Preparata codes are sometimes referred to as nearly perfect. The reason, of course, is that although non-perfect they are remarkably close to perfect. The codes are inherently non-linear and better than any comparable linear code.

The original construction, published already 1968, is rather complicated. A number of alternative and usually simpler constructions have been suggested resulting in closely related codes with the same parameters. Of particular interest is the relatively recent construction obtained by applying the so called Gray map to certain codes over the quaternary ring \mathbb{Z}_4 .

In the present talk we present still another construction, using the quaternary field $GF(4)$ rather than the ring \mathbb{Z}_4 . Our approach is based on a binary construction originally suggested by Van Lint et al.

An enumeration of Kerdock codes of length 64

Kevin T. Phelps

Mathematics & Statistics Dept.,

Auburn University,

Auburn, AL, USA

Email: phelpkt@auburn.edu

Interest in Kerdock codes, was greatly stimulated by the discovery that they can be represented as linear codes over \mathbb{Z}_4 (Hammons, Kumar, Calderbank, Sloane, Sole). This spurred investigations into \mathbb{Z}_4 -linear Kerdock codes and \mathbb{Z}_4 -linear codes in general (e. g. Calderbank et al.; Kantor and Williams; Borges, Phelps, Rifa, Zinoviev, etc.). In particular, a lower bound on the number of \mathbb{Z}_4 -linear Kerdock codes of length 2^{2n} was established (Kantor and Williams). Previously, it had been established that the asymptotic number of *generalized* Kerdock codes was exponential (Kantor). There is only one Kerdock code of length 16. It would be interesting to find the exact number and the combinatorial structures of Kerdock codes of moderate length as this could provide further insight into various combinatorial, geometric and algebraic structures. This talk presents an investigation and enumeration of Kerdock codes of length 64 as a first step towards this goal.

$\mathbb{Z}_2\mathbb{Z}_4$ -additive (extended) perfect codes: intersection problem

Mercè Villanueva

Department of Information and Communications Engineering,
Universitat Autònoma de Barcelona,
Barcelona, Spain

Joint work with Josep Rifà and Faina I. Solov'eva

Email: merce.villanueva@autonoma.edu

The intersection problem for $\mathbb{Z}_2\mathbb{Z}_4$ -additive perfect codes, i.e. which are the possibilities for the number of codewords in the intersection of two $\mathbb{Z}_2\mathbb{Z}_4$ -additive codes \mathcal{C}_1 and \mathcal{C}_2 of the same length, is shown. Lower and upper bounds for the intersection number are computed and, for any value between these bounds, codes which have this given intersection value can be constructed.

For all these $\mathbb{Z}_2\mathbb{Z}_4$ -additive codes \mathcal{C}_1 and \mathcal{C}_2 , the abelian group structure of the intersection codes $\mathcal{C}_1 \cap \mathcal{C}_2$ is characterized. The parameters of this abelian group structure corresponding to the intersection codes are computed and lower and upper bounds for these parameters are established. Finally, for all possible parameters between these bounds, constructions of codes with these parameters for their intersections are given.

Similar results for $\mathbb{Z}_2\mathbb{Z}_4$ -additive extended perfect codes and $\mathbb{Z}_2\mathbb{Z}_4$ -additive Hadamard codes can be described.

On linear equivalence and Phelps codes

Martin Hessler

Department of Mathematics, Linköping University,

Linköping, Sweden

Joint work with Olof Heden

Email: mahes@mai.liu.se

We define the class of full rank Hamming perfect codes (for short FRH -code). Further, we show that each FRH -code can be mapped onto a Phelps-code of the same length using a bijective linear map. We established that the class of FRH -codes contains perfect codes that are not equivalent to any Phelps code.

Families of Quasi-Perfect Codes

Danyo Danev

Department of Electrical Engineering,

Linköping University,

Linköping, Sweden

Email: danyo@isy.liu.se

Quasi-perfect codes have the property that their covering radius is one more than their packing radius. The classification of the parameters for which quasi-perfect codes exist seems to be an extremely difficult one. In this talk we shall briefly give an account of the known families of quasi-perfect codes. Some cyclic and constacyclic ternary codes have been recently shown to be quasi-perfect. These are among few examples of such families of non-binary linear quasi-perfect codes. We shall present an algebraic proof of their quasi-perfectness. Some interesting open problems concerning quasi-perfect codes will be stated and shortly discussed during the talk.

Quasi-perfect linear codes with distance 4

Fabio Pasticci

Dipartimento di Matematica e Informatica,
Università degli Studi di Perugia,
Perugia, Italy

Joint work with Massimo Giulietti

Email: pasticci@dmf.unipg.it

Some new infinite families of short quasi-perfect linear codes are described. Such codes provide improvements on the currently known upper bounds on the minimal length of a quasi-perfect $[n, n - m, 4]_q$ -code when either (a) $q = 16$, $m \geq 5$, m odd, or (b) $q = 2^i$, $7 \leq i \leq 15$, $m \geq 4$, or (c) $q = 2^{2^\ell}$, $\ell \geq 8$, $m \geq 5$, m odd. As quasi-perfect $[n, n - m, 4]_q$ -codes and complete n -caps in projective spaces $PG(m - 1, q)$ are equivalent objects, new upper bounds on the size of the smallest complete cap in $PG(m - 1, q)$ are obtained.

Partitions of F_q^n into perfect codes

Faina I. Solov'eva

Sobolev Institute of Mathematics,
Novosibirsk State University, Russia

Email: sol@math.nsc.ru

The problem of the enumeration and the classification of all partitions of the set \mathbb{F}_q^n of all q -ary ($q \geq 2$) vectors of length n into perfect codes is closely linked to the classical problem of classifying all perfect codes. Partitions of \mathbb{F}_2^n are closely related to the important vertex-coloring problem of \mathbb{F}_2^n into codes with prescribed distance. Each partition can generate a coloring, concerning the study of scalability of optical networks, or a perfect coloring, called also a partition design or equitable partition. Several methods to construct partitions of the set \mathbb{F}_q^n into perfect binary codes are considered in the talk. The lower bounds on the number of different such partitions of \mathbb{F}_q^n into perfect codes (of \mathbb{F}_2^n into extended perfect binary codes), the lower bounds on the number of nonequivalent transitive, vertex-transitive and 2-transitive partitions into perfect binary codes, and also the lower bound on the number of different partitions of \mathbb{F}_2^n into nonparallel Hamming codes are given.

On Preparata-like codes and 2-resolvable Steiner quadruple systems

Victor A. Zinoviev

Institute for Problems of Information Transmission,
Moscow, Russia

Joint talk with Dimitrii Zinoviev

Email: zinov@iitp.ru

It is known that any Preparata-like code P is a subcode of some extended Hamming-like code H of the same length. For all constructed Preparata-like codes the code H is partitioned into translates of the code P . This induces a partition of Steiner quadruple system $S(n, 4, 3)$ (formed by codewords of H of weight 4) into disjoint Steiner systems $S(n, 4, 2)$, i.e. the Steiner system $S(n, 4, 3)$ is 2-resolvable.

In this paper we show that any Preparata-like code P of length n induces a 2-resolvable Steiner quadruple system $S(n, 4, 3)$. We prove also that any 2-resolvable Steiner quadruple system $S(n, 4, 3)$, which satisfies certain conditions, defines uniquely a 3- $(n, 6, \lambda)$ design with $\lambda = 10(n - 4)/3$.