Constructions of perfect binary codes [*]

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

Abstract

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

Contents

1 Introduction

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

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

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

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

2 Necessary definitions

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

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

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

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

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

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

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

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

3 Short summary of constructions

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

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