On components of perfect binary codes *

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

Abstract

Special components, called i-components, of perfect binary codes are investigated. The existence of maximal cardinality nonisomorphic i-components of different perfect codes of length n for all $n = 2^k - 1, k > 3$, is proved.

1 Introduction

The principal point of our investigation is the i-component structure of single-error correcting perfect binary codes (briefly perfect codes). Investigations of i-components may be helpful for the decision of the complicated problems of the construction and enumeration of perfect codes. We prove that there exist maximal cardinality nonisomorphic i-components of different perfect codes of length n for all $n = 2^k - 1, k > 3$. The construction is given by using simultaneously the switching [1] and the concatenation [2] constructions of perfect codes.

Let C be a perfect code and M be a subset of C. Exchanging the bit in the i'th coordinate of all vectors of M with the opposite bit we obtain a new set, denoted by $M \oplus i$. We identify with i the vector having an one in the i'th coordinate and zeroes elsewhere. If $C' = (C \setminus M) \cup (M \oplus i)$ is a perfect code, we call the set M an *i-component* of the code C and say that C' is obtained from C by a *translation* of an i-component M. An i-component is *minimal* if it cannot be subdivided into smaller i-components. We omit the word minimal because we consider below only minimal i-components.

It is known [3, 4] that upper and lower bounds on the number m of i-components of an arbitrary perfect code of length n, $n = 2^k - 1$, are given by

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

Both of these bounds can be achieved, see [1, 3, 4]. The cardinality of the minimal i-components can vary from $2^{(n-1)/2}$ to $2^{n-1}/(n+1)$. According to [3] there exist nonextremal cardinality i-components of perfect codes of length n for all admissible $n > 7$. A perfect code of length $n, n > 7$, with i-components of different structures and cardinalities was presented in [5].

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

2 Definitions

A *binary code* C of length n is a subset of the vector space E^n of dimension n over $GF(2)$. The elements of C are called *codewords* or *vectors*. 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 $C' = b \oplus \pi(C) = \{b \oplus \pi(x) : x \in C\}$. *The Hamming distance* $d(x, y)$ between vectors $x, y \in C$ is the number of coordinates in which x and y differ. *The Hamming weight* of $x \in C$ is given by $wt(x) = d(x, \mathbf{0})$, where $\mathbf{0}$ is the all-zero vector. A code distance is given by $d = min\, d(x, y)$ for any different codewords $x, y \in C$. A code $C \subset E^n$ of length n is *perfect* with distance 3 if every $x \in E^n$ is within distance 1 from exactly one codeword of C. The linear perfect codes called *Hamming codes* are unique up to equivalence. There are many constructions of nonlinear perfect codes. Short summary of them is given, for example, in [6].

3 Construction

We further identify a vector $x = (x_1, \dots, x_n) \in E^n$ with its block presentation $(i_1, \dots, i_k)$ of all those positions of coordinates of vector x, which equaled to 1.

Consider the Hamming code H^n of length n given by Vasil'ev construction

$$H^n = \{(\alpha, \alpha \oplus \beta, |\alpha|) : \alpha \in E^{(n-1)/2}, \beta \in H^{(n-1)/2}\}, \tag{2}$$

where $|\alpha| = \alpha_1 + \cdots + \alpha_{(n-1)/2} \pmod 2$ for $\alpha = (\alpha_1, \dots, \alpha_{(n-1)/2})$ and $H^{(n-1)/2}$ be a Hamming code of length $(n-1)/2 = 2^k - 1, k \geq 2$.

According to Glagolev's lemma, see in [7], for any binary linear code of length n and distance d there exists a binary linear code of length n and distance d with a basis among codewords of weight d. As mentioned above Hamming codes are unique up to equivalence, therefore there exists a basis of the Hamming code among codewords of weight 3.

We construct such a basis for the Hamming code by induction. If $k = 2$ the Hamming code H^3 is generated by codeword $(1, 2, 3)$. Let $B_n = \{(i, j, k)\}$ be a basis of the Hamming code H^n, $|V_n| = n - log(n+1)$. Let $V_{2n+1} = V_n \cup \{(i, n+i, 2n+1) : i = 1, \dots, n\}$. According to (2) the vector $(i, n+i, 2n+1)$ belongs to H^{2n+1}, $i = 1, \dots, n$, and $V_n \subset H^{2n+1}$. Therefore $|V_{2n+1}| = 2n - log(n+1)$ and the set V_{2n+1} is a basis of weight 3 codewords of the Hamming code H^{2n+1}. We have then,

Proposition 1. (The Hamming code basis proposition.) *There exists a basis of weight 3 codewords of the Hamming code of length n for any $n = 2^k - 1, k \geq 2$.*

Proposition 2. *There exist Hamming codes H_1^n and H_2^n of length n, $n = 2^k - 1, k \geq 3$, with basis intersected exactly by one codeword.*

Proof. The proof is by induction on $k, k = log(n+1), k \geq 2$.

Let $k = 3$, e.g. $n = 2^k - 1 = 7$. Basis of Hamming codes H_1^7 and H_2^7 are given by

$$V_1^7 = \{(123), (147), (257), (367)\}, \tag{3}$$

$$V_2^7 = \{(123), (157), (267), (347)\}, \tag{4}$$