On the symmetry group of perfect 1-error correcting binary codes

Olof Heden

January 24, 2003

Abstract

It is shown that for any rank r with $n-\log(n+1)+4 \leq r \leq n-4$ and any length n, where $n = 2^k - 1$ and $k \geq 8$, there is a perfect code with these parameters and with a trivial group of symmetries.

1 Introduction

We consider the direct product Z_2^n of n copies of the ring Z_2. The elements of Z_2^n will be called *words*. The *distance*, $d(c, v)$, between two words c and v is the number of positions in which they differ. A *perfect 1-error correcting binary code* is a subset C of Z_2^n, satisfying the following condition:

to any word v of Z_2^n there is a unique word c of C such that $d(c, v) \leq 1$.

Below we will write *perfect code* instead of perfect 1-error correcting binary code.

Perfect codes of length n exist if and only if $n = 2^k - 1$ where $k \geq 2$ is an integer. If $n = 3$ or $n = 7$ they are unique and linear subspaces of the vector space Z_2^n. In case $n \geq 15$ there are both linear and non linear perfect codes. There are now many different constructions of non linear perfect codes, see [11]. Many constructions are given by switching processes, see [1], and many by concatenations, see [10].

Let the *rank*, $r(C)$, of a code C be the dimension of the linear span, $< C >$, of the words of C. The linear perfect code H of length n has rank $n - \log(n + 1)$ and is unique. (If $n = 2^k$ then $\log(n) = k$.) This code will be called the *Hamming code* of length n.

Let the *symmetry group* of C, $\text{Sym}(C)$, be defined as the set of permutations π of the coordinate set that fixes C, that is for any $c \in C$, $\pi(c) \in C$. The purpose of this note is to show the following theorem:

JCMCC 52 (2005), pp. 109-115

Theorem 1 *For any possible length $n = 2^k - 1$, where $k \geq 8$, and rank r with*

$$n - \log(n+1) + 4 \leq r \leq n - 4,$$

there is a perfect code with these parameters and with a trivial symmetry group.

It is well known that the number of different perfect codes of length n is extremely large, more than $2^{2^{n/2-\log(n+1)}}$. So there is a need for some kind of classification or a tool to distinguish perfect codes.

Beside the rank and symmetry group mentioned above, the *kernel* of a perfect code has also been studied and seems to be of great importance for the classification of perfect codes.

A word p is a *period* of the code D if

$$p + D = \{p + d \mid d \in D\} = D.$$

The set of periods of a code D will be called the *kernel* of D, $ker(D)$. We note that the kernel is a linear subspace of Z_2^n.

All possible pairs (r, k), for which there is a perfect code of length n, rank r and with a kernel of dimension k have been determined, see e.g. [5]. Theorem 1 above is perhaps a little step on the way to see which the possibilities are for the symmetry group of a perfect code. It has already been proved that there are perfect codes with a trivial symmetry group. Phelps [9] proved that any finite group is the symmetry group of some perfect code. Avgustinovich and Solov'eva [2] showed that for any length ≥ 255 there is a perfect code of rank n, with a trivial symmetry group and a trivial kernel. This result was extended to perfect codes of length ≥ 31 by Malyugin [7] and of length 15, also by Malyugin [8], by using a computer search. Theorem 1 shows that this is true for any length n and any rank r as stated in the theorem.

2 Preliminaries

We will let N denote the set $\{1, 2, \ldots, n\}$.

The *weight* of a word c, $w(c)$, is the number of non zero positions of c. We denote by e_i the word of weight one with the only one in the position i. We denote by e_I the word $\sum_{i \in I} e_i$.

In [3] we showed that to any perfect code of rank r with

$$n - \log(n+1) + 2 \leq r \leq n - 1$$

there is a partition of the set N:

$$I_0 \cup I_1 \cup I_2 \cup \ldots \cup I_t = N,$$

where $t = 2^{n-r} - 1$, $I_i \cap I_j = \emptyset$ for $i \neq j$ and $|I_0| + 1 = |I_1| = |I_2| = ... = |I_t| = (n+1)/(t+1)$, such that each of the words e_{I_i}, $i = 0, 1, 2, \ldots, t$, are periods. This partition is called *the fundamental partition of N associated with C.*

With the *support* of a word $c = (c_1, ..., c_n)$ we mean the set

$$supp(c) = \{i \mid c_i \neq 0\}.$$

The set of vectors v of Z_2^n satisfying $supp(v) \subseteq I_i$ is a subspace of the vector space Z_2^n that we denote by $Z_2^{I_i}$.

For words c of Z_2^n, we sometimes write $c = (c_0|c_1|\ldots|c_t)$, where c_i, for $i = 0, 1, 2, \ldots, t$, is the projection of c on the subspace $Z_2^{I_i}$.

If c is a word of Z_2^{s+1} then c^* denotes the word of Z_2^s obtained from c by deleting the last coordinate of c. If $c = (c_1, c_2, \ldots, c_s)$, then we denote by c^e the word $(c_1, c_2, \ldots, c_s, c_1 + c_2 + \ldots + c_s)$ of Z_2^{s+1}. For any code D we denote by D^e the set $\{c^e \mid c \in D\}$.

If π is a permutation of the coordinate set of Z_2^n then π induces in the most natural way a map on the subsets of Z_2^n. If under this map a set D is mapped on a set D' we denote D' by $\pi(D)$.

We denote by **1** and **0** the words $(1, 1, \ldots, 1)$ respectively $(0, 0, \ldots, 0)$.

Let, for $x \in (Z_2^s)^t$, $\sigma_i(x) = \sum_{j=1}^{s} x_{ij}$ and $\sigma'_j(x) = \sum_{i=1}^{t} x_{ij}$. Let $\sigma(x) = (\sigma_1(x), \ldots, \sigma_t(x))$ and $\sigma'(x) = (\sigma'_1(x), \ldots, \sigma'_s(x))$.

3 Proof of the Theorem 1

We consider Z_2^n where $n = (s+1)(t+1) - 1$. The words of Z_2^n are denoted by

$$(x_{01}, \ldots, x_{0s}|x_{11}, \ldots, x_{1,s+1}|x_{21}, \ldots, x_{2,s+1}| \ldots |x_{t1}, \ldots, x_{t,s+1})$$

where $x_{ij} \in Z_2$.

Let H be a Hamming code of length t. We define τ to be the following map from H to Z_2^n:

$$\tau((h_1, h_2, \ldots, h_t)) = (0|0\ldots 0h_1|0\ldots 0h_2|\ldots|0\ldots 0h_t).$$

We will use a construction similar to the Krotov construction [6] to define a perfect code $C_{H,\mathcal{F}}$ of length $(s+1)(t+1) - 1$, where $s \geq 15$ and $t \geq 15$, with the desired properties. The code $C_{H,\mathcal{F}}$ will be the disjoint union of codes C_h, $h \in H$.

Let C_0 be a perfect code of length s and with $Sym(C_0) = \{id\}$ and such that $\mathbf{0} \in C_0$. For the existence of such codes, see the introduction. For $h = \mathbf{0} \in \mathbf{H}$ we let

$$C_0 = \{(c_1^* + \ldots + c_t^* + C_0|c_1|c_2|\ldots|c_t) \mid c_1, c_2, \ldots, c_t \in Z_2^{s+1}\}.$$

Let C_1 be a perfect code of length s with a trivial kernel, see [4], and containing the zero word $\mathbf{0}$. Trivially $h = \mathbf{1} \in H$ and we define $C_{\mathbf{1}}$ to be the code

$$\tau((1,1,\ldots,1)) + \{(c_1^* + \ldots + c_t^* + C_1|c_1|c_2|\ldots|c_t) \mid c_1, c_2, \ldots, c_t \in Z_2^{s+1}\}.$$

To describe the codes C_h, for $h \in H \setminus \{\mathbf{0}, \mathbf{1}\}$ we need a notation: For any integer $i = 1, 2, \ldots t$, f_{i0} denotes the zero word $(0|0|\ldots|0)$ and f_{ik}, for $i = 1, 2, \ldots, t$ and $k = 1, 2, \ldots, s$, the word $e_{i,k} + e_{i,s+1}$.

Denote the dimension of the dual space of H by p. Let $\{d_1, d_2, \ldots, d_p\}$ be a set of base vectors for the dual code of H. Let G be a non linear perfect code of length s. Below we will use the extended codes H^e and G^e.

Define, for $h = (h_1 \ldots, h_t) \in H \setminus \{\mathbf{0}, \mathbf{1}\}$, C_h to be the code

$$(\cup_{(k_1,\ldots,k_t) \in S^t} (\sigma(f_{1k_1} + \ldots + f_{tk_t}) + C_{h,0}|f_{1k_1} + C_{h,1}|\ldots|f_{tk_t} + C_{h,t})) + \tau(h)$$

where $S = \{0, 1, 2, \ldots, s\}$ and $C_{h,l}$, for $l = 1, 2, \ldots, t$, are extended perfect codes that we will describe below.

The weight spectrum of the Hamming code H of length $n \geq 15$ contains $n-3$ integers. Thus we may define $C_{h,l}$, for $h \in H$, with $3 \leq w(h) \leq p+2$, to be

$$C_{h,l} = \begin{cases} H^e & \text{if} \quad l \in supp(d_{w(h)-2}); \\ G^e & \text{if} \quad l \notin supp(d_{w(h)-2}); \end{cases}$$

and for $p+2 < w(h) < t-2$, $C_{h,l}$, $l = 1, 2, \ldots, t$ to be any extended perfect code of length s.

By considering the minimum distance and the number of elements of $C_{H,\mathcal{F}}$ we get that $C_{H,\mathcal{F}}$ is a perfect code, see also [6].

We first note that if π belongs to $Sym(C)$ then π maps the fundamental partition of N associated to the perfect code C to the same fundamental partition of N. As C_1 has a trivial kernel, we may conclude from Corollary 1 of [4], that $r(C) = n - \log(t+1)$, and as a consequence, that the sets $I_0 = \{(0,1), (0,2), \ldots (0,s)\}$, $I_1 = \{(1,1), (1,2), \ldots, (1, s+1)\}$, ..., $I_t = \{(t,1), (t,2), \ldots, (t, s+1)\}$ in fact form the fundamental partition of the set N. Hence:

if $i_1, i_2 \in I_k$ *then there is* k' *such that* $\pi(i_1), \pi(i_2) \in I_{k'}$.

As I_0 is the only set with s elements in the fundamental partition, we get that $\pi(I_0) = I_0$. We now prove that $\pi(I_k) = I_k$, for $k = 1, 2, \ldots, t$.

Assume that $\pi \in Sym(C)$, and that $\pi(I_k) = I_{k'}$, $k \neq k'$. As the minimum distance in H is three, we deduce that there must be a base vector d_q, $q \in \{1, 2, \ldots, p\}$, of the dual code of H such that $|\{k, k'\} \cap supp(d_q)| = 1$. Assume that $k \in supp(d_q)$ and $k' \notin supp(d_q)$. Let $h \in H$ be such that

$q = w(h) - 2$ and consider the code C_h. The symmetry π maps C_h to another code $C_{h'}$ with $w(h) = w(h')$. The code C_h contains words

$$(c_0|c_1|\dots|c_t) + \tau(h) \qquad \text{where} \qquad c_i \in \begin{cases} \{0\} \text{ if } i \neq k \\ H^* \text{ if } i = k \end{cases} \qquad i = 0, 1, \dots, t$$

and $C_{h'}$ contains words

$$(c_0|c_1|\dots|c_t) + \tau(h') \qquad \text{where} \qquad c_i \in \begin{cases} \{0\} \text{ if } i \neq k' \\ G^* \text{ if } i = k' \end{cases} \qquad i = 0, 1, \dots, t.$$

If $\pi(I_k)$ were equal to $I_{k'}$, then, as $\pi(C) = C$, we get that $\pi(H^e) = G^e$. As an extended non linear perfect code never can be equivalent to an extended Hamming code, this is not true and hence we get a contradiction and $\pi(I_k)$ must be equal to I_k, for $k = 1, 2, \dots t$.

We observe that if $\pi \in Sym(C)$ then, as

$$(C_0|0|\dots|0) \subseteq C_{H,\mathcal{F}}$$

is mapped to $\pi(C_0|0|\dots|0)$ and as $Sym(C_0) = \{id\}$, the restriction of π to the set I_0 must be the identity.

We now show that if $\pi \in Sym(C)$ then, for $(k,i) \in I_k$, $k = 1, 2, \dots t$, $\pi((k,i)) = (k,i)$.

Assume that $\pi(i_1) = j_1$ (where i_1 and j_1 are contained in the same set I_k) and let $i_2 = \pi^{-1}(i_1)$. From the definition of C and from the observation above we deduce that C contains the words $c = (\sigma^*(e_{i_1} + e_{i_2})|0|\dots|0|e_{i_1} + e_{i_2}|0|\dots|0)$, $c' = (\sigma^*(e_{i_1} + e_{j_1})|0|\dots|0|e_{i_1} + e_{j_1}|0|\dots|0)$ and $\pi(c) = (\sigma^*(e_{i_1} + e_{i_2})|0|\dots|0|e_{j_1} + e_{i_1}|0|\dots|0)$.

We note that

$$d(\sigma^*(e_{i_1} + e_{j_1}), \sigma^*(e_{i_1} + e_{i_2})) = \begin{cases} 0 & \text{if} \quad j_1 = i_2; \\ 2 & \text{else.} \end{cases}$$

As $d(c', \pi(c)) \geq 3$, we may conclude that $\pi(i_1) = j_1 = i_2$ and hence that π must be a product of disjoint 2-cycles.

Without loss of generality we may thus assume that if $\pi \in Sym(C)$ then

$$\pi(2b-1) = 2b \qquad \text{and} \qquad \pi(2b) = 2b - 1 \qquad \text{for} \qquad b = 1, 2 \dots, s/2.$$

We now show that this implies that C_1 has a non trivial kernel.

If $a = (a_1, a_2, \dots, a_{s-1}) \in C_1$ then:

$$\overline{a} = (a + a|(a_1, \dots, a_{s-1}, \sigma(a))|0|\dots|0) + (0|0\dots01|\dots|0\dots01|) \in C.$$

As $\pi \in Sym(C)$ we get that $\pi(\overline{a}) \in C$ and that $\pi(\overline{a})$ equals

$$(0|(a_2, a_1, a_4, a_3, \dots, \sigma(a), a_{s-1})|0|\dots|0) + (0|0\dots01|\dots|0\dots01|) \in C$$

and hence, for any $z = 1, 2, \ldots, (s-2)/2$,

$$\overline{a}' = (e_{2z}|(a_2, a_1, a_4, a_3, \ldots, \sigma(a), a_{s-1}+1) + e_{2z}|0|\ldots|0)+$$
$$(0|0\ldots01|\ldots|0\ldots01|)$$

belongs to C. This implies that also the word

$$\pi(\overline{a}') = (e_{2z}|(a_1, a_2, a_3, a_4, \ldots, a_{s-1}+1, \sigma(a)) + e_{2z-1}|0|\ldots|0)+$$
$$(0|0\ldots01|\ldots|0\ldots01|)$$

as well as the word

$$(a + e_{2z-1} + e_{s-1}|(a_1, a_2, a_3, a_4, \ldots, a_{s-1}+1, \sigma(a)) + e_{2z-1}|0|\ldots|0)+$$
$$(0|0\ldots01|\ldots|0\ldots01|)$$

belongs to C and hence that

$$a + e_{2z-1} + e_{s-1} \in e_{2z} + C_1.$$

As $a \in C_1$ was chosen arbitrarily and as $a + e_{2z-1} + e_{s-1} + e_{2z} \in C_1$, we get that the word $e_{2z-1} + e_{s-1} + e_{2z}$ is a period of C_1. As C_1 is assumed to have a trivial kernel we get a contradiction.

The theorem is proved.

Acknowledgement I am grateful to Faina I. Solov'eva for her support on this search and for her comments on a previous version of this text.

References

[1] *Avgustinovich S. V., Solov'eva F. I.,* Construction of perfect binary codes by sequential translations of an $\tilde{\alpha}$-components, Problems of Information Transmission 33 (3) (1997) 202-207.

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

[3] *Avgustinovich S. V., Heden O., Solov'eva F. I.,* The classification of some perfect codes, submitted.

[4] *Avgustinovich S. V., Heden O., Solov'eva F. I.,* On ranks and kernels of perfect codes, submitted.

[5] *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.

[6] *Krotov D. S.,* Combining construction of perfect binary codesProblems of Information Transmission36(2000)349-353.

[7] *Malyugin S. A.,* Perfect codes with trivial automorphism group, Proc. Second Int. Workshop on Optimal Codes and Related Topics. Sozopol, Bulgaria. June. 1998. P. 163–167.

[8] *Malyugin S. A.,* Private comunication with Faina I. Solov'eva.

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

[10] *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.

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

O. Heden, Department of Mathematics, KTH, S-100 44 Stockholm, Sweden. (olohed@math.kth.se)