ON THE SYMMETRY GROUP OF EXTENDED PERFECT
BINARY CODES OF LENGTH $n + 1$ AND RANK $n - \log(n + 1) + 2$

OLOF HEDEN
Department of Mathematics, KTH
S-100 44 Stockholm, Sweden

FABIO PASTICCI
Dipartimento di Matematica e Informatica
Università degli Studi di Perugia
Via Vanvitelli, 1, I-06123 Perugia, Italy

THOMAS WESTERBÄCK
Department of Mathematics, KTH
S-100 44 Stockholm, Sweden

(Communicated by Patrick Solé)

Abstract. It is proved that for every integer $n = 2^k - 1$, with $k \geq 5$, there exists a perfect code $C$ of length $n$, of rank $r = n - \log(n + 1) + 2$ and with a trivial symmetry group. This result extends an earlier result by the authors that says that for any length $n = 2^k - 1$, with $k \geq 5$, and any rank $r$, with $n - \log(n + 1) + 3 \leq r \leq n - 1$ there exist perfect codes with a trivial symmetry group.

1. Introduction

A perfect 1-error correcting binary code of length $n$, or for short a perfect code, is a subset $C$, of the direct product $Z_2^n$ of $n$ copies of the finite field $Z_2$, with the property that every word $\bar{x} \in Z_2^n$ differs in at most one coordinate position from a unique word $\bar{c}$ of $C$.

We may consider $Z_2^n$ as a vector space over the finite field $Z_2$. The rank of a perfect code is the dimension of the subspace $\langle C \rangle$ spanned by the words of $C$. The length of a perfect code is always equal to $n = 2^k - 1$ for some integer $k$ and the size of a perfect code of length $n$ is equal to $|C| = 2^{n - \log(n + 1)}$. Henceforth, we will always assume that the all zero word belongs to the perfect codes we consider. Perfect codes of rank $r$ and of length $n = 2^k - 1$, where $k \geq 4$, are known to exist for every integer $r$ in the interval $n - \log(n + 1) \leq r \leq n$, see [4].

The symmetry group of $C$, $\text{Sym}(C)$, consists of the set of permutations $\pi$ of the coordinate positions that maps the code $C$ into itself, or more precisely, if we let $\pi(C)$ denote the following set

$$\pi(C) = \{ (c_{\pi^{-1}(1)}, c_{\pi^{-1}(2)}, \ldots, c_{\pi^{-1}(n)}) \mid (c_1, c_2, \ldots, c_n) \in C \}$$

2000 Mathematics Subject Classification: Primary: 94B25.

Key words and phrases: Perfect codes, symmetry group.

Third author supported by grant KAW 2005.0098 from the Knut and Alice Wallenberg Foundation.
then
\[ \text{Sym}(C) = \{ \pi \in S_n \mid \pi(C) = C \}, \]
where \( S_n \) denotes the group of all permutations of a set with \( n \) elements.

The aim of this note is to prove the following theorem:

**Theorem 1.** For every integer \( n = 2^k - 1 \), with \( k \geq 5 \), there exists a perfect code \( C \) of length \( n \), of rank \( r = n - \log(n+1) + 2 \) and with a trivial symmetry group.

This result extends a previous result proved by us:

**Theorem 2** ([5]). For any length \( n = 2^k - 1 \), with \( k \geq 5 \), and any rank \( r \), with \( n - \log(n+1) + 3 \leq r \leq n - 1 \) there exists a perfect code with a trivial symmetry group.

As well known, see e.g [8], every linear perfect code of length \( n \), i.e., of rank \( n - \log(n+1) \), has a symmetry group which is isomorphic to the general linear group \( \text{GL}(n, 2) \), and hence never trivial. By a result of Avgustinovich, Heden and Solov’eva [2] no perfect codes of length \( n \) and rank \( r = n - \log(n+1) + 1 \) has a trivial symmetry group. Using a computer search, Phelps, Pottonen and Östergård [7] described all perfect codes of length \( n = 15 \). Several of these codes have a trivial symmetry group. As far as we can judge, the ranks of these codes are not described there, but could probably easily be found by a computer search. In [5] we found one perfect code of length 15, rank 14 and with a trivial symmetry group. In [11] there is an enumeration of all perfect codes of length 15, rank 13, and it was shown there that none of these codes has a trivial symmetry group. Hence we think that it is now, with this note, and with the exception of just full rank perfect codes, clarified exactly for which ranks and lengths there exist perfect codes with a trivial symmetry group.

The proof of our theorem is very similar to our proof of Theorem 2 in [5]. We will use a rather general construction of perfect codes described by Phelps in 1984 [6]. In the case of a rank less or equal to \( n - \log(n+1) + 2 \), a variant of Phelps construction for the case \( d = 4 \) was published by Zinoviev already in 1975, see [10] or [9]. Both of their constructions are concatenating constructions, with MDS-codes as fundamental ingredients. However, we will here make advantage of the possibility, that the Phelps construction gives, to use non equivalent MDS-codes of length \((n+1)/4\) over an alphabet with four letters. In Section 2 the construction is described in detail for the perfect codes we consider when we prove Theorem 1.

We get an extended perfect code \( C^* \) from a perfect code \( C \) by including an extra parity-check bit:
\[ C^* = \{ (c_1, c_2, \ldots, c_n, \sum_{i=1}^{n} c_i) \mid (c_1, c_2, \ldots, c_n) \in C \}. \]

As in [5] we will prove our results for extended perfect codes. In fact, we will prove the following theorem:

**Theorem 3.** There are extended perfect codes \( C \) of every length \( n+1 = 2^k \), where \( k \geq 5 \), and with a trivial symmetry group, if and only if for the rank \( r \) of \( C \),
\[ n - \log(n+1) + 2 \leq r \leq n - 1. \]

Trivially, the ranks of \( C \) and \( C^* \) are equal. The symmetry group of \( C \) is isomorphic to a subgroup of the symmetry group of \( C^* \). Hence, Theorem 1 and Theorem 2 are immediate consequences of Theorem 3.
For basic definitions and for an historical background to this problem, see [5]. For a good introduction to perfect codes in general we recommend [8].

2. Phelps construction and MDS-codes

In our constructions we will use MDS-codes $D$ of length $m = (n + 1)/4$ over an alphabet $\mathcal{A}$ with four letters, the elements of the finite field $\text{GF}(4) = \{0, \alpha_1, \alpha_2, \alpha_3\}$. The minimum distance of the MDS-codes will be 2 and the size of the MDS-codes alphabet subspace, of $\text{GF}(4)$.

$\alpha$ denotes the element kernel of a MDS-code in $\text{GF}(4)$ inequivalent by calculating the size of the kernel of each of them. Note that the fact that some MDS-codes are inequivalent and we will show that they are evidently equivalent codes will have kernels of the same size. We will make use of the fact that some MDS-codes are inequivalent and we will show that they are inequivalent by calculating the size of the kernel of each of them. Note that the kernel of a MDS-code in $\text{GF}(4)^m$ is an additive subgroup, and not necessarily a subspace, of $\text{GF}(4)^m$.

To simplify notation, we will denote the elements of $\text{GF}(4)$ by 0, 1, 2, 3, where $i$ denotes the element $\alpha_i$, for $i = 1, 2, 3$.

The first basic MDS-code is

$$D_0 = \{ (x_1, x_2, x_3, x_1 + x_2 + x_3) \mid (x_1, x_2, x_3) \in \text{GF}(4)^3 \},$$

which is linear and thus has a kernel of size $|D_0| = 4^3$. The second one, denoted $D_1$, has a kernel of size 8 and consists of the union of the following sets of words:

$$A_0 = \{0000, 1100, 2200, 3300\} + \{0000, 0011, 0022, 0033\},$$
$$A_1 = \{0300, 1200, 2100, 3000\} + \{0003, 0021, 0012, 0030\},$$
$$A_2 = \{1000, 2300\} + \{0010, 0023, 0001, 0032\},$$
$$A_3 = \{2000, 1300\} + \{0020, 0013, 0002, 0031\},$$
$$A_4 = \{0100, 3200\} + \{0001, 0032, 0013, 0020\},$$
$$A_5 = \{0200, 3100\} + \{0002, 0031, 0023, 0010\}.$$

The third MDS-code we will use is denoted by $D_2$ and has a kernel of size 16. The code $D_2$ consists of the words in the union of the set $A_0$ and the sets

$$B_1 = \{3000, 0100, 1200, 2300\} + \{0003, 0021, 0012, 0030\},$$
$$B_2 = \{1000, 2100, 3200, 0300\} + \{0010, 0023, 0001, 0032\},$$
$$B_3 = \{2000, 3100, 0200, 1300\} + \{0020, 0013, 0002, 0031\}.$$

The fourth MDS-code has a kernel of size 4 and consists, besides the set of words in the sets $A_0$ and $B_1$, of the words in the union of the following sets

$$C_2 = \{1000, 2100, 3200, 0300\} + \{0020, 0001, 0032, 0013\},$$
$$C_3 = \{2000, 3100, 0200, 1300\} + \{0010, 0031, 0002, 0023\}.$$

This MDS-code will be denoted $D_3$.

We will also need a fifth MDS-code $D_1'$, equivalent to $D_1$ and obtained from $D_1$ by the permutation $\varphi = (0)(1)(2\ 3)$ in each coordinate position, an example of a permutation that here will be called a coordinate fixing permutation. More exactly

$$D_1' = \{ (\varphi_1(d_1), \varphi_2(d_2), \varphi_3(d_3), \varphi_4(d_4)) \mid (d_1, d_2, d_3, d_4) \in D_1 \},$$

where $\varphi_i = \varphi$, for $i = 1, 2, 3, 4$.

The important clue in the proof of our main theorem is the following proposition.
Proposition 1. The set of coordinate fixing permutations that maps $D_1$ into itself is the following group $G$ of size 8

$$G = \langle ((0 \ 3)(1 \ 2), \text{id.}, \text{id.}), \text{id.}, (0 \ 3)(1 \ 2), (0 \ 3)(1 \ 2)), ((0 \ 3)(1 \ 2), \text{id.}, (0 \ 3)(1 \ 2), \text{id.}) \rangle,$$

and the set of coordinate fixing permutations that maps $D'_1$ into itself is the following group $G'$ of size 8

$$G' = \langle ((0 \ 2)(1 \ 3), \text{id.}, \text{id.}), \text{id.}, (0 \ 2)(1 \ 3), (0 \ 2)(1 \ 3)), ((0 \ 2)(1 \ 3), \text{id.}, (0 \ 2)(1 \ 3), \text{id.}) \rangle.$$

Proof. We proved this proposition by an exhaustive search for all coordinate fixing permutations.

We will need to concatenate MDS-codes, and, as the verification of the validity of the concatenation procedure we are to describe is a complete triviality, this concatenation procedure should be well known.

Let $E$ and $F$ be any two MDS-codes of lengths $s$ and $t$, respectively, over the alphabet GF(4) and of minimum distance 2. Denote by $D(E,F)$ the following set

$\{(e_1, \ldots, e_{s-1}, e_s + \alpha, f_1, \ldots, f_{t-1}, f_t + \alpha) \mid (e_1, \ldots, e_s) \in E, (f_1, \ldots, f_t) \in F, \alpha \in \text{GF}(4)\}$.

We omit the proof of the following lemma.

Lemma 1. For any two MDS-codes $E$ and $F$ of length $s$ and $t$, respectively, $D(E,F)$ is a MDS-code of length $s + t$. Furthermore,

$$|\ker(D(E,F))| = 4 \cdot |\ker(E)| \cdot |\ker(F)|.$$

Let $E_1, E_2, \ldots, E_k$ be MDS-codes. To simplify notation in what follows, we will write $E_1E_2 \ldots E_k$ instead of $D(E_1,D(E_2,D(E_3,...)))$, and for example, instead of $E_1E_1E_2E_2$ we will write $E_1^3E_2$.

We now describe Phelps construction to obtain extended perfect codes of length $n + 1$ and of rank at most equal to $n - \log(n + 1) + 2$. In [6] the construction is given for a more general situation. The codes we construct will here be called Phelps codes.

The construction of Phelps uses a partition of the set of coordinate position into subsets of size 4:

$$\{1, 2, \ldots, n + 1\} = \bigcup_{i=1}^{(n+1)/4} I_i,$$

where $I_i = \{4i - 3, 4i - 2, 4i - 1, 4i\}$, for $i = 1, 2, \ldots, (n + 1)/4$. We will also need a partition of the set $\mathbb{Z}_4^4$ into cosets of the extended perfect code \{0000, 1111\} of length 4. We denote these cosets by

(1) $C_0^{(0)} = \{0000, 1111\}, \quad C_1^{(0)} = \{1100, 0011\},$

$C_2^{(0)} = \{1010, 0101\}, \quad C_3^{(0)} = \{1001, 0110\}.$

*This notation will in this context be very convenient to use. To avoid any confusion we would like to emphasize that for example, and with $D_0$ defined as above, the code $D_0^2$ is an MDS-code of length 8.
Perfect codes of rank \( n - \log(n+1) + 2 \) with trivial symmetry group

One further ingredient in Phelps construction is an extended Hamming code \( H \) of length \( (n+1)/4 \). Here we will let \( H \) be the null space of the following matrix

\[
H = \begin{bmatrix}
1 & 1 & 1 & 1 & \ldots & 1 \\
0 & 0 & 0 & 0 & \ldots & 1 \\
\vdots \\
0 & 0 & 0 & 1 & \ldots & 1 \\
0 & 0 & 1 & 1 & 0 & \ldots & 1 \\
0 & 1 & 0 & 1 & 0 & \ldots & 1
\end{bmatrix}
\]

(It is not important which of all possible such parity check matrices we choose.) The code \( H \) will be called the outer code of the Phelps code \( C \).

To every word \( \tilde{h} \) of \( H \) we associate a Phelps component \( P_{\tilde{h}} \) which will consist of binary words of length \( n+1 \) given by the choice of \( \tilde{h} \) and the choice of a MDS-code \( D_{\tilde{h}} \). More precisely, the Phelps component \( P_{\tilde{h}} \) will consist of the following set of words

\[
P_{\tilde{h}} = \bigcup_{d \in D_{\tilde{h}}} C_{d_1}^{(h_1)} \times C_{d_2}^{(h_2)} \times \cdots \times C_{d_{(n+1)/4}}^{(h_{(n+1)/4})}.
\]

The Phelps code \( C \) is defined to be the union of all such Phelps components

\[
C = \bigcup_{\tilde{h} \in H} P_{\tilde{h}}.
\]

It was proved by Phelps that for any choice of MDS-codes \( D_{\tilde{h}} \), for \( \tilde{h} \in H \), the code \( C \) is an extended perfect code of length \( n+1 \), see [6].

The dimension of the dual code \( C^\perp \) of the Phelps code \( C \) constructed by the receipt above, is at least equal to the dimension of the dual space of \( H \), i.e., the dimension of the row space of the matrix \( H \). This proves the next lemma.

**Lemma 2.** The rank \( r \) of the code \( C \) is at most equal to \( n - \log(n+1) + 2 \).

As in [5] we can prove the following lemma.

**Lemma 3.** If the rank of \( C \) equals \( n - \log(n+1) + 2 \) then for every \( \varphi \in \text{Sym}(C) \) and every \( i = 1, 2, \ldots, (n+1)/4 \),

\[
\varphi(I_i) = I_j,
\]

for some \( j \in \{1, 2, \ldots, (n+1)/4\} \), and furthermore, to every \( \tilde{h} \in H \) there is a word \( \tilde{h}' \in H \) such that

\[
\varphi(P_{\tilde{h}}) = P_{\tilde{h}'}.
\]

As the words of a Phelps component \( P_{\tilde{h}} \) are completely defined by just the MDS-code \( D_{\tilde{h}} \), and the word \( \tilde{h} \) of \( H \), the kernel of \( P_{\tilde{h}} \) will just depend on the size of the kernel of \( D_{\tilde{h}} \), as described in the next proposition.

**Proposition 2.** For every \( \tilde{h} \in H \) and every MDS-code \( D_{\tilde{h}} \) used in the Phelps component \( P_{\tilde{h}} \)

\[
|\ker(P_{\tilde{h}})| = 2^{(n+1)/4} \cdot |\ker(D_{\tilde{h}})|.
\]
Proof. It is enough to prove the proposition in the case $h = \bar{0}$, as, for any subset $D$ of $Z_2^n$ and any word $\bar{p}$, it is true that
\[ \ker(\bar{p} + D) = \ker(D). \]

Let $e_I$, for $j = 1, 2, \ldots, (n + 1)/4$, denote the word with a support equal to the set $I_j$. From the definition of the Phelps component $P_{\bar{0}}$ and from Equation (1) follows that each such word will belong to the kernel of $P_{\bar{0}}$. As these words are linearly independent, they span a subspace $L$ of the kernel of $P_{\bar{0}}$ of dimension $(n + 1)/4$.

Let $\psi$ denote the map from $GF(4)$ to $Z_4^2$ defined by
\[
\psi(0) = \bar{0}000, \quad \psi(\alpha_1) = 1100, \quad \psi(\alpha_2) = 1010, \quad \psi(\alpha_3) = 1001.
\]

We extend this map to a map $\Psi$ from $GF(4)^{(n+1)/4}$ to $Z_4^{n+1}$ by
\[
\Psi(x_1, x_2, \ldots, x_{(n+1)/4}) = (\psi(x_1), \psi(x_2), \ldots, \psi(x_{(n+1)/4})),
\]
and observe that
\[
(2) \quad P_{\bar{0}} = \Psi(D_{\bar{0}}) + L = \{ \Psi(\bar{d}) + \bar{l} \mid \bar{d} \in D_{\bar{0}}, \bar{l} \in L \}.
\]
As $\Psi$ is injective and
\[ \dim(\Psi(D_{\bar{0}}) \cap L) = 0, \]
it suffices to verify that
\[ \ker(P_{\bar{0}}) = \Psi(\ker(D_{\bar{0}})) + L. \]
However, this is an immediate consequence of Equation (2), and the fact that for any two distinct non zero elements $\alpha_i$ and $\alpha_j$ of $GF(4)$, it is true that
\[ \psi(\alpha_i) + \psi(\alpha_j) = \psi(\alpha_i + \alpha_j) + e_I, \]
where $e_I$ denotes the word 1111.

We have now made enough preparations to be able to prove our theorem. Please, for the necessary definitions of inner product, orthogonality and dual code, see [5].

3. Proof of Theorem 3

From [5] we know that there are extended perfect codes of any length $n + 1 = 2^k$, where $k \geq 5$, and for any possible rank $n - \log(n + 1) + 2 < r \leq n - 1$ and with a trivial symmetry group. From [2] we know that there are no extended perfect codes of rank $r < n - \log(n + 1) + 2$ with a trivial symmetry group. So in order to prove Theorem 3, it remains to consider the case of rank $r = n - \log(n + 1) + 2$.

We will use the Phelps construction, as described in the previous section, in order to find an extended perfect code $C$ of rank $r = n - \log(n + 1) + 2$ and with a trivial symmetry group.

We first choose two of the Phelps components in a way such that the Phelps code $C$ we are to construct will have rank $n - \log(n + 1) + 2$. For that purpose we choose the MDS-code $D_{\bar{0}}^{(n+1)/16}$ for the Phelps component $P_{\bar{0}}$, and for the Phelps component $P_{\bar{h}}$, where $\bar{h} = 11110000 \ldots 0000$, we choose the MDS-code $D_{\bar{h}}^{(n+1)/16}$. It is elementary to check that these choices of MDS-codes imply that the rank of the Phelps code $C$ will be $n - \log(n + 1) + 2$.

Now we know that we can apply Lemma 3.
The next step is to choose MDS-codes for some of the Phelps components of $C$ such that the following implication will be true:

\[(3) \quad \varphi \in \text{Sym}(C) \implies \varphi(I_j) = I_j, \quad j = 1, 2, \ldots, (n + 1)/4.\]

Let $\bar{h}_i$ denote row number $i$ of the matrix $H$, defined in the previous section. As the intersection of the supports of any two of the rows $h_i$, for $i = 2, 3, \ldots, k + 1 = \log(n + 1) + 1$, will be of size $(n + 1)/16$, which is an even number, we may conclude that all these rows will belong to the null space of $H$ and thus to the outer code $H$.

We will choose the MDS-code $D_2^{2-i+16}D_0^{2-i(n+1)/16}$ for the Phelps component $P_{\bar{h}_i}$ for $i = 2, 3, \ldots, k + 1$. For all other Phelps components, except the component $P_0$, we will later and below declare how we either choose the MDS-code $D_4^{(n+1)/16}$ or choose the MDS-code $D_4^{(n+1)/16}$.

From Lemma 1 and Proposition 2, we get that for any $i$ and $j$, with $2 \leq i < j \leq k + 1$,

\[
\frac{|\ker(P_{\bar{h}_i})|}{|\ker(P_{\bar{h}_j})|} = \frac{|\ker(D_2)|^{n-i} \cdot |\ker(D_2)|^{2-i(n+1)/16}}{|\ker(D_2)|^{n-j} \cdot |\ker(D_2)|^{2-j(n+1)/16}} = \left(\frac{|\ker(D_2)|}{|\ker(D_0)|}\right)^{n-j} = 4^{j-i}.
\]

Thus, the sizes of the kernels of the Phelps components $P_{\bar{h}_i}$, for $i = 2, 3, \ldots, k + 1$, are of mutually distinct sizes. Similarly, we get that the kernels of these Phelps components are of sizes distinct to the sizes of the kernels of all other Phelps components $P_{\bar{h}_i}$, such that $\text{wt}(\bar{h}) = (n + 1)/8$.

Trivially, no member of $\text{Sym}(C)$ can map Phelps components, with kernels of different sizes, to each other. Hence, and as we have proved that the rank of $C$ equals $n - \log(n + 1) + 2$, we can apply Lemma 3, and so we may conclude that

\[
\varphi \in \text{Sym}(C) \implies \varphi(P_{\bar{h}_i}) = P_{\bar{h}_i}, \quad i = 2, 3, \ldots, k + 1.
\]

Again as in [5], this implies that Equation (3) will hold.

From Equation (3) follows that every member $\varphi$ of $\text{Sym}(C)$ can be described as an $(n + 1)/4$-tuple

\[
\varphi = (\varphi_1, \varphi_2, \ldots, \varphi_{(n+1)/4}),
\]

where $\varphi_j(I_j) = I_j$ for $j = 1, 2, \ldots, (n + 1)/4$. Moreover, it follows from (3) that

\[(4) \quad \varphi \in \text{Sym}(C) \implies \varphi(P_{\bar{h}_i}) = P_{\bar{h}_i},
\]

for every $\bar{h} \in H$.

It remains to prove that $\varphi_j = \text{id}$, for $j = 1, 2, \ldots, (n + 1)/4$. For that purpose we now specify the choices of MDS-codes for the remaining Phelps components.

We first consider the case $n + 1 = 2^k$, where $k \geq 6$. The following set $K$ of words of weight 4 is a subset of the code $H$:

\[
K = \{11110000, 0000, 000011110000, 00000000, 0000001111\}.
\]

To the Phelps components $P_{\bar{h}_i}$ for $\bar{h} \in K$, we choose the MDS-code $D_4^{(n+1)/16}$ and for all other Phelps components, for which we have not already chosen an MDS-code, we choose the MDS-code $D_4^{(n+1)/16}$.

We now consider the Phelps component $P = P_{\bar{h}}$ where $\bar{h} = 11110000$. Let $R$ denote the set of words $\bar{c}$ of $P$ satisfying

\[
|\text{supp}(\bar{c}) \cap I_i| = \begin{cases} 1, & \text{if } i = 1, 2, 3, 4; \\ 0, & \text{else.} \end{cases}
\]
Again, we will now use the special notation for the elements of GF(4) introduced in Section 2, i.e., the integer $i$ denotes the element $\alpha^i$ of GF(4). Then we get, from the construction of Phelps, that $\bar{c}$ belongs to $R$ if and only if
$$\text{supp}(\bar{c}) = \{1 + d_1, 5 + d_2, 9 + d_3, 13 + d_4\}^\dagger,$$
for some word $(d_1, d_2, \ldots, d_{(n+1)/4})$ of $D_h$.

From Equation (3) follows that for every $\bar{c} \in P_h$ and every $\varphi \in \text{Sym}(C)$
$$|\text{supp}(\varphi(\bar{c})) \cap I_i| = |\text{supp}(\bar{c}) \cap I_i|,$$
for $i = 1, 2, 3, 4$. Hence from the definition of the set $R$ and Equation (4) follows that for any member $\varphi$ of $\text{Sym}(C)$, we have that $\varphi(R) = R$. Consequently, we may derive from Proposition 1 that
$$(5) \quad \varphi_i \in \{\text{id.}, \ (1 \ 4)(2 \ 3) \},$$
for $i = 1, 2, 3, 4$. As the supports of the words in the set $K$ cover all coordinate positions, we may similarly deduce that Equation (5) must hold for every $i = 1, 2, \ldots, (n+1)/4$.

It is now enough to consider the Phelps components $P_h$ where $\bar{h}$ belongs to the following subset $L$ of words of $H$:
$$L = \{110011000000 \ldots 0000, 001100110000 \ldots 0000, \ldots, 0000 \ldots 0000110011 \}.$$

As we for the Phelps components $P_h$, with $\bar{h} \in L$, have chosen the MDS-codes $D_1^{(n+1)/16}$ we now get, as above, from Proposition 1 that
$$(6) \quad \varphi_i \in \{\text{id.}, \ (1 \ 3)(2 \ 4) \},$$
for $i = 1, 2, \ldots, (n+1)/4$. So, simply, Equation (5) and Equation (6) together implies that $\varphi_i = \text{id.}$, for $i = 1, 2, \ldots, (n+1)/4$.

In the case $n+1 = 32$ we cannot use the sets $K$ and $L$ defined as above. However, all arguments above apply to the sets
$$K' = \{11000011, 00111100 \},$$
and
$$L' = \{10101010, 01011010 \}.$$

4. Remarks

There are many possibilities to prove our theorem. One is to first prove the theorem for the case of length $n+1 = 32$ and then show, by recursion, how our result, for all other lengths, follows from this basic case. However, our proof shows that there indeed are very many possibilities to construct extended perfect codes of length $n+1 = 2^k$ and rank $n - \log(n + 1) + 2$ with a trivial symmetry group. In fact, there are very many choices of MDS-codes that will give us this result, and as follows from the construction, the bigger length, the more codes with the desired parameters there are.

It is easy to verify, by a direct proof, the result of Zinoviev and Zinoviev [11], mentioned in the introduction, that no extended perfect code of length 16 and rank 13 has a trivial symmetry group. This result was an immediate consequence of their computer search for all extended perfect codes of length 16 and rank 13.

\[\dagger\text{The addition is here the addition as it is defined in the ring of integers. Further, the coordinate positions are enumerated from the left to the right, so e.g. the support of the word 0100...0 is the set }\{2\}.\]
First of all it was proved by Avgustinovich, Heden and Solov’eva [1] that every extended perfect code of length \( n + 1 = 2^k \) and rank \( n - \log(n + 1) + 2 \) is a Phelps code. Furthermore, there are just a few MDS-codes of length 4 over an alphabet with four letters, and they are easy to enumerate. This was done by the first author in 1987 in an unpublished manuscript [3], and also by other authors. From these investigations follows, by inspection, that the symmetry group of every such code contains a symmetry of the type

\[
\varphi = (\text{id.}, \text{id.}, \pi, \pi),
\]

where \( \pi \) is one of the elements distinct from \( \text{id.} \) in the 4-group of Klein, i.e.,

\[\pi \in \{ (0 \, 3)(1 \, 2), (0 \, 2)(1 \, 3), (0 \, 1)(2 \, 3) \}.\]

It is easy to observe that for every permutation \( \pi \) in the 4-group of Klein

\[
\pi(C_i^{(0)}) = C_i^{(0)}, \quad i = 1, 2, 3, 4,
\]

where the sets \( C_i^{(0)} \) are defined as in Equation (1). Finally, using the fact that every Phelps code \( C \) of length 16 can be regarded as a union of the Phelps components \( P_{0000} \) and \( P_{1111} \), it is more or less obvious that any permutation \( \varphi \), as described in Equation (7), will belong to the symmetry group of \( C \).

**Acknowledgments**

We are grateful to the anonymous referee who draw our attention to the references [10] and [9], and pointed out to us that in fact we use an easily found improvement of the special case of Phelps construction that was described there by Zinoviev already in 1975.

The anonymous referee also encouraged us to make our presentation more clear, in particular he suggested that we should include a proof of Proposition 2.

We are grateful also to Victor Zinoviev, Moscow, Russia. If he had not shown and discussed his construction with the first author of this paper, at University of Linköping in 1985, this research would never have come to the start.

**References**

[1] S. V. Avgustinovich, O. Heden and F. I. Solov’eva, *The classification of some perfect codes*, Des. Codes Cryptogr., 31 (2004), 313–318.

[2] S. V. Avgustinovich, O. Heden and F. I. Solov’eva, *On the structure of symmetry groups of Vasilev codes*, Probl. Inform. Transm., 41 (2005), 105–112.

[3] O. Heden, *On the kernel of binary perfect 1-error correcting codes of length 15*, manuscript, 33 pp., 1987.

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

[5] O. Heden, F. Pasticci and T. Westerbäck, *On the existence of extended perfect binary codes with trivial symmetry group*, Adv. Math. Commun., 3 (2009), 295–309.

[6] K. T. Phelps, *A general product construction for error correcting Codes*, SIAM J. Algebra Discrete Methods, 5 (1984), 224–228.

[7] K. T. Phelps, O. Pottonen and P. R. J. Östergård, *The perfect binary one-error-correcting codes of length 15: Part II properties*, IEEE Trans. Inform. Theory, 56 (2010), 2571–2582.

[8] F. I. Solov’eva, “On Perfect Codes and Related Topics,” Pohang, 2004.

[9] V. A. Zinoviev, *On generalized concatenated codes*, in “Colloquia Math. Societ. Janos Bolyai, 16, Topics in Inform. Theory,” Keszthely, Hungary, (1975), 587–592.

[10] V. A. Zinoviev, *Generalized cascade codes*, Probl. Inform. Transm., 12 (1976), 5–15.
[11] V. A. Zinoviev and D. A. Zinoviev, *Binary perfect and extended perfect codes of length 15 and 16 with ranks 13 and 14* (in Russian), Problemy Peredachi Informatsii, 46 (2010), 20–24.

Received January 2011; revised August 2011.

*E-mail address:* olohed@math.kth.se

*E-mail address:* pasticci@dipmat.unipg.it

*E-mail address:* thowest@math.kth.se