AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **38** (2007), Pages 141–153

Non Phelps codes of length 15 and rank 14

Olof Heden Thomas Westerbäck

Department of Mathematics
KTH, S-100 44 Stockholm
Sweden
olohed@math.kth.se thowest@math.kth.se

Abstract

Phelps enumerated all perfect codes of length 15 and of rank 13 and 14, that can be obtained by the Phelps construction. It is known that all perfect codes of that length and of rank 13 are Phelps codes. It was an open problem to determine whether the same is true in the case of rank 14. We give an answer to that problem, as we construct perfect codes of length 15 and rank 14, that are not equivalent to any Phelps code.

1 Introduction

In this journal, Phelps [9] presented an enumeration of all extended perfect 1-error correcting binary codes of length 15, here for short perfect codes, that can be obtained by using the so-called Phelps construction [8]. They all have rank 13 or 14. Perfect codes of length 15 and of rank 11 are linear and those of rank 12 can easily be shown to be obtainable by the Vasil'ev construction [13]. It was shown in [1] that all perfect codes of length n and rank $n - \log(n+1) + 2$, i.e. if $n = 15$ then rank 13, can be obtained by using this construction of Phelps. As there is no remark in [9] whether or not there are perfect codes of length 15 and rank 14, not obtainable by the Phelps construction, and since we have not found any notice elsewhere about this fact, we think it is a good idea to present here such codes. In fact we prove the following result:

There are perfect codes of length 15 *and rank* 14 *that are not obtainable by the Phelps construction and that have kernels of dimensions* $2, 3, 4, 5$ *and* 6 *respectively.*

This result is proved below by giving five examples of such perfect codes, one code in each of these five cases.

Phelps codes are discussed in more detail in Section 2 and our constructions are given in Sections 3 and 4. We now give some elementary definitions and some necessary background needed.

A *perfect* 1*-error correcting binary code of length* n is a subset C of the direct product $Z_2^n = Z_2 \times Z_2 \times \ldots \times Z_2$, with the property that

any word $\bar{x}$ *of* Z_2^n *differs in at most one coordinate position from a unique word of* C*.*

(Certainly, this definition may be extended to the case of e-error correcting perfect q-ary codes, but here we focus on the binary case, length $n = 15$ and $e = 1$.) A perfect code must have a length equal to $n = 2^m - 1$ for some integer m, see e.g. [12]. The problem with the perfect codes is that there seem to be far too many of them for it to be possible to enumerate and classify them. Krotov [6] proved that the number of different perfect codes of length n is at least

$$2^{2^{\frac{n+1}{2}-\log_2(n+1)}} \cdot 3^{2^{\frac{n-3}{4}}} \cdot 2^{2^{\frac{n+5}{4}-\log_2(n+1)}}.$$

Thus any enumeration, like the enumeration of Phelps [9], is of great interest.

The concepts rank and kernel will be essential in this note.

The *rank* of a perfect code is the dimension of the subspace $\langle C \rangle$ of Z_2^n, spanned by the words of the code C. Since any perfect code of length n contains $2^{n-\log(n+1)}$ words, see e.g. [12], it follows that $n - \log(n+1) \leq \mathrm{rank}(C) \leq n$.

A *period* of a set A is a word $\bar{p}$ with the property that

$$\bar{p} + \bar{a} \in A \quad \text{for every word} \quad \bar{a} \in A.$$

The set of all periods of a set A is the *kernel* of A, denoted by $\ker(A)$. Trivially the kernel of any set A is a subspace of the vector space Z_2^n and further, if the all-zero word $\bar{0}$ belongs to A, then $\ker(A) \subseteq A$.

All possible triples (n, r, k), for which there exists a perfect code of length n, rank r and with a kernel of dimension k, were determined in a series of papers of which [10] and [2] perhaps are the two most important. In the case of length 15 and rank 14, the results in these papers imply that for every integer k in the interval $2 \leq k \leq 8$, there is at least one perfect code of length 15, rank 14 and with a kernel of dimension k and that no other values of k are possible for a perfect code of this length and rank.

Some further necessary concepts needed are distance, weight and orthogonality.

The *distance* between two words $\bar{c}$ and $\bar{d}$ is the number of positions in which $\bar{c}$ and $\bar{d}$ differ and the *weight* of a word $\bar{c}$ is the number of 1's in $\bar{c}$.

We will say that two words $\bar{c} = (c_1, c_2, \ldots, c_n)$ and $\bar{d} = (d_1, d_2, \ldots, d_n)$ are *orthogonal* if

$$c_1 d_1 + c_2 d_2 + \ldots + c_n d_n \equiv 0 \pmod 2.$$

A *linear* code C is a subspace of the vector space Z_2^n and the dual code $C^\perp$ of C consists of all words orthogonal to all words of C.

For other and more details and relations among perfect codes we refer to [12].

2 Phelps construction

In this section we give Phelps' construction [8] in the case of length $n = 15$ and rank $r = 14$. For these parameters n and r, Phelps' construction coincides with the construction of Solov'eva [11]. Her construction was also found independently by Phelps in [7]. So here we will call these codes *Phelps-Solov'eva codes.*

We need the concept of extended perfect codes. If C is a perfect code of length $n = 2^m - 1$, then an *extended perfect code* D is obtained from C by setting

$$D = \{(c_1, c_2, \ldots, c_n, c_1 + c_2 + \ldots + c_n) \mid (c_1, c_2, \ldots, c_n) \in C\}.$$

All words of D will have even weight and the minimum distance of D will be four. Every code D of length $n = 2^m$, with 2^{n-m} words, all of even weight, and with minimum distance four will be an extended perfect code.

Let $C_0, C_1, \ldots, C_7$ be any partition of Z_2^7 into perfect codes and let $D_0, D_1, \ldots, D_7$ be any partition of the set of even weight words of Z_2^8 into extended perfect codes. The union S of the sets

$$C_i \times D_i = \{(\bar{c}|\bar{d}) \mid \bar{c} \in C_i, \quad \bar{d} \in D_i\} \quad \text{for} \quad i = 0, 1, 2, \ldots, 7,$$

will be a perfect code of length 15. To see this we just note that:

(i) The number of words of S will be

$$|S| = 8 \cdot |C_i| \cdot |D_i| = 2^3 \cdot 2^4 \cdot 2^4 = 2^{11}, \tag{1}$$

which equals the number of words in a perfect code of length 15.

Since

$$d(\bar{c}, \bar{c}') \geq 1 \quad \text{for} \quad \bar{c} \in C_i, \ \bar{c}' \in C_j, \quad i \neq j \tag{2}$$

and

$$d(\bar{d}, \bar{d}') \geq 2 \quad \text{for} \quad \bar{d} \in D_i, \ \bar{d}' \in D_j, \quad i \neq j, \tag{3}$$

we get that

(ii) the minimum distance between any two words of S will be at least 3.

By elementary results on perfect codes, see e.g. [12], the properties *(i)* and *(ii)* together show that C is a perfect code.

The advantage with the Phelps-Solov'eva construction is, that we may choose *any* partition of Z_2^7 into perfect codes and *any* partition of the set of even weight words in Z_2^8 into extended perfect codes.

In our proofs in the following sections, we will use the following property of Phelps-Solov'eva codes.

Proposition 1. *If S is a Phelps-Solov'eva code of length* 15 *and rank* 14*, defined as above, then the only non zero word that is orthogonal to all words of S is the word* $(\bar{0}|\bar{1}) = 000000011111111$.

Proof. The dual space of S will, if the rank of S equals 14, have dimension 1. All words of the sets D_i, for $i = 0, 1, 2, \ldots, 7$, have an even weight and thus the word $(\bar{0}|\bar{1})$ belongs to the dual space of S.

Finally, as will be used in Section 4, we know that any perfect code C of length 7 containing the all zero word may be constructed by the use of a parity check matrix H,

$$C = \{\bar{c} = (c_1, c_2, \ldots, c_7) \in Z_2^7 \mid H\bar{c}^T = \bar{0}\},$$

where H is a matrix of size 3×7 in which each of the seven possible non zero columns appears exactly once. This was, in the case of length 7, the first and well known construction of a perfect 1-error correcting binary code, given by Hamming [3]. We note that the rows of the matrix H span the dual code $C^{\perp}$ of C.

3 A non Phelps code with $(n, r, k) = (15, 14, 6)$

In our first example of a non Phelps code of length 15 and of rank 14, we consider a particular Phelps-Solov'eva code, as in previous section, and cut and paste the two sets $C_i \times D_i$, $i = 0, 1$.

Let C denote the linear span

$$C = \text{span}\{1110000, 1001100, 1000011\}$$

and let $\bar{c}_1$ denote the word 0101010.

We define the code C_0 to be the set

$$C_0 = C \cup (\bar{c}_1 + C).$$

The set C_0 is a perfect code of length 7. Let

$$\bar{e}_1 = 1000000, \quad \bar{e}_2 = 0100000, \quad \bar{e}_3 = 0010000, \quad \ldots, \bar{e}_7 = 0000001.$$

If we let

$$C_i = \bar{e}_i + C_0, \quad \text{for} \quad i = 1, 2, \ldots, 7,$$

then the sets C_i, $i = 0, 1, 2, \ldots, 7$, constitute a partition of Z_2^7 into perfect codes.

Similarly, for extended perfect codes, we use the code

$$D = \text{span}\{01110001, 01001101, 11000011\}$$

and let $\bar{d}_1$ denote the word 00101011. The extended perfect code D_0 is defined to be the union of the sets D and $\bar{d}_1 + D$. We let

$$\bar{e}_1^{\star} = 10000001, \quad \bar{e}_2^{\star} = 01000001, \quad \ldots, \quad \bar{e}_7^{\star} = 00000011.$$

We denote the translates of the perfect code D_0 by

$$D_i = \bar{e}_i^\star + D_0, \quad i = 1, 2, \ldots, 7.$$

As above, these codes D_i, $i = 0, 1, 2, \ldots, 7$, constitute a partition of the set of even weight words of Z_2^8.

By using the words $\bar{c}_2 = 0101001$ and $\bar{d}_2 = 10101001$ we now cut the sets $C_0 \times D_0$ and $C_1 \times D_1$ into pieces and paste them together into four disjoint subsets. Observe that one may easily check that

$$C_0 + \bar{c}_2 = C_1 \quad \text{and} \quad D_0 + \bar{d}_2 = D_2. \tag{4}$$

The four subsets will be

$$\begin{array}{rcl} C & \times & (D \cup (D + \bar{d}_1)) \\ (C + \bar{c}_1) & \times & (D \cup (D + \bar{d}_2)) \\ (C + \bar{c}_2) & \times & ((D + \bar{d}_1) \cup (D + \bar{d}_1 + \bar{d}_2)) \\ (C + \bar{c}_1 + \bar{c}_2) & \times & ((D + \bar{d}_2) \cup (D + \bar{d}_1 + \bar{d}_2)) \end{array}$$

We will consider the code W that consists of the words in the union A of the four sets above and the words in the union B of the following six sets:

$$C_2 \times D_1, \;\; C_3 \times D_3, \;\; C_4 \times D_4, \;\; C_5 \times D_5, \;\; C_6 \times D_6, \;\; C_7 \times D_7.$$

Theorem 1. *The code W is a perfect code of length* 15 *and rank* 14*, which cannot be obtained by the Phelps-Solov'eva construction.*

Proof. The number of words of W will trivially be 2^{11}. To prove that W is perfect, it is thus sufficient to prove that the minimum distance of W equals 3.

As the the words in the set B together with the words in the sets $C_0 \times D_0$ and $C_1 \times D_2$ constitute a Phelps-Solov'eva code S we get that the minimum distance in the set B is at least 3. It follows from equation (4) that

$$A \subseteq (C_0 \cup C_1) \times (D_0 \cup D_2).$$

Again, we consider the Phelps-Solov'eva code S and conclude from the above equation that the distance between any word of A and any word of B is at least 3.

Similar arguments also show that the minimum distance of A equals 3. We have now proved that the minimum distance of W equals 3. The code W is thus perfect.

We now prove that the rank of W will be 14. We first note that

$$C_0 \times \{\bar{0}\} \subseteq W \quad \text{and} \quad \{\bar{0}\} \times D_0 \subseteq W. \tag{5}$$

It is a trivial exercise to prove that the following six words, all contained in W,

$$(\bar{e}_2|\bar{e}_1^\star), \;\; (\bar{e}_3|\bar{e}_3^\star), \;\; (\bar{e}_4|\bar{e}_4^\star), \;\; (\bar{e}_5|\bar{e}_5^\star), \;\; (\bar{e}_6|\bar{e}_6^\star), \;\; (\bar{e}_7|\bar{e}_7^\star),$$

together with the following eight words of W

$$\begin{array}{cccc} (1110000|\bar{0}), & (1001100|\bar{0}), & (1000011|\bar{0}), & (0101010|\bar{0}) \\ (\bar{0}|01110001), & (\bar{0}|01001101), & (\bar{0}|11000011), & (\bar{0}|00101011) \end{array}$$

constitute a set L of 14 linearly independent words of Z_2^{15}. Thus the rank of W is at least 14. As the word $(0000000|11111111)$ is orthogonal to all words of W, the rank of W cannot be 15. We have now proved that the rank of W equals 14.

It remains to prove that W cannot be obtained by the Phelps-Solov'eva construction. Assume that W is a Phelps-Solov'eva code. The dual code of W just consists of the all zero word and the word 000000011111111. Assume that W would be obtainable by the Phelps-Solov'eva construction. This will imply that W would be the union of the sets

$$W = \cup_{i=0}^{7}(C_i' \times D_i') \tag{6}$$

where the sets C_i' and D_i', for $i = 0, 1, 2, \ldots, 7$, are perfect codes respectively extended perfect codes, such that

$$C_i' \cap C_j' = \emptyset \quad \text{and} \quad D_i' \cap D_j' = \emptyset \quad \text{if} \quad i \neq j.$$

Now assume, that the perfect code W, that we have constructed above, is a Phelps-Solov'eva code and thus can be described as in equation (6). We note that the all zero word $\bar{0}$ belongs to W. Without any loss of any generality we may assume that $\bar{0}$ belongs to the set $C_0' \times D_0'$. This implies that $\bar{0} \in C_0'$ and $\bar{0} \in D_0'$ and that

$$C_0' = \{\bar{c} \mid (\bar{c}|\bar{0}) \in W\} \quad \text{and} \quad D_0' = \{\bar{d} \mid (\bar{0}|\bar{d}) \in W\}.$$

As $(\bar{c}_1|\bar{0}) \in W$ and $(\bar{0}|\bar{d}_1) \in W$ we get that $\bar{c}_1 \in C_0'$ and that $\bar{d}_1 \in D_0'$, still under the assumption that W is obtainable by the Phelps-Solov'eva construction. However, as easily checked, $(\bar{c}_1|\bar{d}_1) \notin W$, and consequently

$$C_0' \times D_0' \not\subseteq W. \tag{7}$$

Hence W cannot be obtained by the Phelps-Solov'eva construction.

The theorem is now proved.

We now calculate the dimension of the kernel of W.

Lemma 1. *The kernel of W is a subset of A.*

Proof. As the all zero word belongs to W, we know that the kernel of W is a subset of W. Assume that

$$(\bar{c}|\bar{d}) \in \ker(W) \setminus A.$$

Then $(\bar{c}|\bar{d}) \in C_i \times D_j$ for some couple $(i,j) \in \{(2,1),(3,3),\ldots,(7,7)\}$. The codes C_i and D_j are both translates of the linear codes C_0 respectively D_0, which both contain the all zero word. Hence, $(\bar{c}|\bar{d}) \in \ker(W)$ implies that

$$C_0 \times D_0 = (\bar{c}|\bar{d}) + C_i \times D_j \subseteq W.$$

This contradicts what we found in the proof of Theorem 1, compare equation (7). The lemma is proved.

Lemma 2. *The set $C \times D$ belongs to the kernel of W.*

Proof. All ten direct product of sets, that we used in the definition of W, are unions of translates of the set $C \times D$. As both C and D are linear spaces we immediately get that for any translate $\bar{a} + C \times D$ of $C \times D$, where $\bar{a} \in Z_2^{15}$,

$$(\bar{c}|\bar{d}) \in C \times D \quad \Rightarrow \quad (\bar{c}|\bar{d}) + (\bar{a} + C \times D) = \bar{a} + C \times D.$$

Lemma 3. *For any period $\bar{p}$ of W, and any direct product of the sets $C_i \times D_j$, $(i,j) \in R = \{(2,1),(3,3),(4,4),(5,5),(6,6),(7,7)\}$,*

$$\bar{p} + C_i \times D_j = C_{i'} \times D_{j'} \quad \textit{where} \quad (i',j') \in R.$$

Further $\bar{p} + A = A$.

Proof. Assume that $\bar{p} = (\bar{p}'|\bar{p}'')$ is a period of W. As any translate of a perfect code is a perfect code we know that

$$(i,j) \in R \quad \Rightarrow \quad \bar{p} + C_i \times D_j = C' \times D' \subseteq W, \tag{8}$$

for some perfect code $C' = \bar{p}' + C_i$ and some extended perfect code $D' = \bar{p}'' + D_j$. If $\bar{e}_x \in C'$, where $x = 2,3,\ldots,7$, then we get that

$$\{\ (\bar{e}_x|\bar{d}')\ |\ \bar{d}' \in D'\ \} \subseteq W. \tag{9}$$

From the definition of W, we know that

$$(\bar{e}_x|\bar{d}'') \in W \quad \Longleftrightarrow \quad \bar{d}'' \in D_y, \quad \text{where} \quad (x,y) \in R. \tag{10}$$

From equation (9) and (10), we thus get that $D' = D_y$. Similarly we can prove that $C' = C_x$.

If $\bar{e}_x = \bar{0}$ or $\bar{e}_x = \bar{e}_1$, then from (8) follows, as above, that either $C_0 \times D_0$ or $C_1 \times D_1$ are subsets of W. As in the proof of Theorem 1, compare equation (7), we get that this is impossible. The lemma is proved.

Proposition 2. *The kernel of W will have dimension 6 and will be equal to $C \times D$.*

Proof. By Lemma 1, the kernel of W is a subset of A and by Lemma 2, $C \times D$, which is a subset of A, belongs to the kernel of W. As

$$A \subseteq \{\bar{c}_0 = \bar{0}, \bar{c}_1, \bar{c}_2, \bar{c}_3 = \bar{c}_1 + \bar{c}_2\} \times \{\bar{d}_0 = \bar{0}, \bar{d}_1, \bar{d}_2, \bar{d}_3 = \bar{d}_1 + \bar{d}_2\} + C \times D$$

it is sufficient to check which of the words $(\bar{c}_i|\bar{d}_j)$, $i, j \in \{0, 1, 2, 3\}$, that are periods. Of these 16 words, it is only the word $\bar{p} = (\bar{c}_3|\bar{d}_3)$, that has the property that $\bar{p} + A = A$. However, as easily checked

$$(\bar{c}_1 + \bar{c}_2|\bar{d}_1 + \bar{d}_2) + C_2 \times D_1 = C_3 \times D_7.$$

This shows by Lemma 3, that $(\bar{c}_1 + \bar{c}_2|\bar{d}_1 + \bar{d}_2) \notin \ker(W)$. The proposition is now proved.

4 Non Phelps codes with $(n, r, k) = (15, 14, k)$ for $k = 2, 3, 4$ and 5

To produce perfect codes of length 15, rank 14 and with kernels of the dimensions 2, 3, 4 and 5 we will use other partitions of Z_2^7 into perfect codes, than the partitions given by translates of the code C_0, as in the previous section.

Let C be defined as in the preceding section. It will suite our purposes to find perfect codes C_i' respectively C_i'', for $i = 2, 3, \ldots, 7$, and of length 7, all containing the all zero word and satisfying

$$Z_2^7 \setminus (C_0 \cup (\bar{e}_1 + C_0)) = (\bar{e}_2 + C_2') \cup \ldots \cup (\bar{e}_7 + C_7') = (\bar{e}_2 + C_2'') \cup \ldots \cup (\bar{e}_7 + C_7'') \quad (11)$$

and such that

$$|C \cap C_2' \cap C_3' \cap \ldots \cap C_7'| = 4 \quad (12)$$

respectively

$$|C \cap C_2'' \cap C_3'' \cap \ldots \cap C_7''| = 2. \quad (13)$$

To find these partitions we made use of the following lemma, proved by Westerbäck [14].

Let $\bar{e}_i$, for $i = 1, 2, \ldots, 7$, be defined as in the preceding section.

Lemma 4. *Let C' and C'' be any two Hamming codes of length n. Then*

$$(\bar{e}_i + C') \cap (\bar{e}_j + C'') = \emptyset$$

if and only if there is a word $\bar{c}$ such that

$$\bar{c} = (c_1, c_2, \ldots, c_n) \in C'^{\perp} \cap C''^{\perp} \quad \textit{with} \quad c_i \neq c_j.$$

Further

$$C' \cap (\bar{e}_i + C'') = \emptyset$$

if and only if there is a word $\bar{c}$

$$\bar{c} = (c_1, c_2, \ldots, c_n) \in C'^{\perp} \cap C''^{\perp} \quad \textit{with} \quad c_i \neq 0.$$

For any Hamming code K of length n, the corresponding dual code $K^{\perp}$ consists of all words in K of weight $(n+1)/2$ and the zero word. We also know that the zero word and the all one word 111...11 belongs to K. This implies, by the fact that C is generated by the words 0001111, 0110011, 1111111, that

$$|C \cap K| = 2| < 0001111, 0110011 > \cap K^{\perp}|.$$

Hence, by Lemma 4 and the fact above, we get the necessary Hamming codes C_2', C_3', ..., C_7' and C_2'', C_3'', ..., C_7''.

Let C' be the Hamming code with the parity check matrix

$$H' = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

Then, with $C_2' = C_3' = C_0$ and $C_i' = C'$ for $i = 4, 5, 6, 7$, it is easily checked, that the equations (11) and (12) will be satisfied.

To get equation (13) satisfied, we have to use three distinct Hamming codes. The codes C_2'' and C_6'' equals and are Hamming codes with the parity check matrix

$$H_2'' = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Also the perfect codes C_5'' and C_7'' are equal and have the parity check matrix

$$H_5'' = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

The perfect codes C_3'' and C_4'' will both have the parity check matrix

$$H_3'' = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Again, as the rows of the matrices above span the dual codes of the perfect codes involved, we may get that the conditions (11) and (13) will be satisfied.

The extended perfect codes, needed in the Phelps-Solov'eva construction, are defined like in Section 3. More precisely, let π denote the cyclic shift of a word:

$$\pi((x_1, x_2, x_3, x_4, x_5, x_6, x_7)) = (x_7, x_1, x_2, x_3, x_4, x_5, x_6).$$

The extended perfect codes D_i', $i = 2, 3, \ldots, 7$ are defined by

$$D_i' = \{(c_1, c_2, \ldots, c_7, c_1 + c_2 + \ldots + c_7) \mid \pi^{-1}((c_1, \ldots, c_7)) \in C_i'\} \quad i = 2, 3, \ldots, 7,$$

and similarly for the extended perfect codes D_i'', $i = 2, 3, \ldots, 7$.

We now are able to define non Phelps-Solov'eva codes with the desired dimensions of their kernels. Let A, D_1, D_2, ..., D_7 be defined as in the preceding section. We remind that the codes D_1, D_2, ..., D_7 are translates of the extended perfect code D_0.

We define W_5 to be the union of the set A with the sets $(\bar{e}_2+C_2')\times D_1$, $(\bar{e}_3+C_3')\times D_3$, $(\bar{e}_4+C_4')\times D_4$, $(\bar{e}_5+C_5')\times D_5$, $(\bar{e}_6+C_6')\times D_6$ and $(\bar{e}_7+C_7')\times D_7$.

Similarly W_4 will be the union of the set A with the sets $(\bar{e}_2+C_2'')\times D_1$, $(\bar{e}_3+C_3'')\times D_3$, $(\bar{e}_4+C_4'')\times D_4$, $(\bar{e}_5+C_5'')\times D_5$, $(\bar{e}_6+C_6'')\times D_6$ and $(\bar{e}_7+C_7'')\times D_7$.

The code W_3 will be the union of the set A with the sets $(\bar{e}_2+C_2'')\times(\bar{e}_1^\star+D_7')$, $(\bar{e}_3+C_3'')\times(\bar{e}_3^\star+D_2')$, $(\bar{e}_4+C_4'')\times(\bar{e}_4^\star+D_3')$, $(\bar{e}_5+C_5'')\times(\bar{e}_5^\star+D_4')$, $(\bar{e}_6+C_6'')\times(\bar{e}_6^\star+D_5')$ and $(\bar{e}_7+C_7'')\times(\bar{e}_7^\star+D_6')$.

Finally, the code W_2 will be the union of the set A with the sets $(\bar{e}_2+C_2'')\times(\bar{e}_1^\star+D_7'')$, $(\bar{e}_3+C_3'')\times(\bar{e}_3^\star+D_2'')$, $(\bar{e}_4+C_4'')\times(\bar{e}_4^\star+D_3'')$, $(\bar{e}_5+C_5'')\times(\bar{e}_6^\star+D_5'')$, $(\bar{e}_6+C_6'')\times(\bar{e}_5^\star+D_4'')$ and $(\bar{e}_7+C_7'')\times(\bar{e}_7^\star+D_6'')$.

Theorem 2. *The codes W_2, W_3, W_4 and W_5 are perfect codes of length* 15 *and rank* 14. *They are not obtainable by the Phelps-Solov'eva construction, and further*

$$\dim(\ker(W_i)) = i \quad \textit{for} \quad i = 2,\ 3,\ 4 \quad \textit{and} \quad 5.$$

Proof. As in the proof of Theorem 1, the number of words in each of the four codes W_2, W_3, W_4 and W_5 equals 2^{11} and the minimum distance will be equal to 3. Hence these four codes are perfect.

As the set A is contained in the codes W_2, W_3, W_4 and W_5, these codes cannot be obtainable by the Phelps-Solov'eva construction, compare the proof of Theorem 1.

The word 000000011111111 is orthogonal to all words of the codes W_2, W_3, W_4 and W_5. Thus the rank of each of these codes is less then 15. The codes W_3, W_4 and W_5 contain the same set L of 14 words, which were proved to be linearly independent in the proof of Theorem 1. Hence the rank of each of these three codes will be 14.

We will below show how one can prove that the kernel of the code W_2 has dimension 2. As no perfect code of dimension 2 and length 15 can have a rank less then 14, see e.g. [10] or [2], it will then follow that also the code W_2 will have rank 14.

It remains to consider the kernels. We will here only prove that $\dim(\ker(W_3)) = 3$. The same methods apply for the codes W_2, W_4 and W_5.

Now let

$$F = \{0000000, 1111111\} \quad \text{and} \quad G = \{00000000, 11111111, 10001110, 01110001\}.$$

The set F is a subspace of each of the codes C_i'', for $i = 2, 3, \ldots, 7$ and the set G is a subspace of each of the codes D_i', for $i = 2, 3, \ldots, 7$. As these codes are linear

codes, they will all be unions of translates of F respectively G. Further as F also is a subspace of C and G also is a subspace of D we immediately get that A is a union of translates of $F \times G$. We may thus conclude that

$$F \times G \subseteq \ker(W_3). \tag{14}$$

Let $\bar{c}_1$, $\bar{c}_2$, $\bar{d}_1$ and $\bar{d}_2$ be as in Section 3. Let

$$\bar{f}_1 = 1110000, \quad \bar{f}_2 = 1001100, \quad \text{and} \quad \bar{g}_1 = 01001101.$$

These words span the set of coset representatives of F and G in respectively C and D. Thus

$$A \subseteq \operatorname{span}\{\bar{f}_1, \bar{f}_2, \bar{c}_1, \bar{c}_2\} \times \operatorname{span}\{\bar{g}_1, \bar{d}_1, \bar{d}_2\} + F \times G.$$

As in the proof of Lemma 1, we may conclude that the kernel of W_3 must be a subset of the set A. From equation (14) it thus follows that it is enough to prove which of the 128 words in $\operatorname{span}\{\bar{f}_1, \bar{f}_2, \bar{c}_1, \bar{c}_2\} \times \operatorname{span}\{\bar{g}_1, \bar{d}_1, \bar{d}_2\}$ that are periods.

We note that $\bar{f}_i$, $i = 1, 2$ and $\bar{g}_1$ belongs to C respectively D. As in the proof of Lemma 3, for a period $\bar{p}$ of W_3, we get that $\bar{p} + A = A$. Using these facts we get, compare the proof of Proposition 2, that

$$\bar{p} \in \ker(W_3) \quad \Rightarrow \quad \bar{p} \in \{\bar{0}, (\bar{c}_1 + \bar{c}_2 | \bar{d}_1 + \bar{d}_2)\} + \operatorname{span}\{\bar{f}_1, \bar{f}_2\} \times \operatorname{span}\{\bar{g}_1\}.$$

It thus remains to consider the above 16 words.

In order to make the notation short, we now let

$$A_i \times B_i = (\bar{e}_i + C_i'') \times (\bar{e}_i^\star + D_{i-1}') \quad \text{for} \quad i = 3, 4, \ldots, 7$$

and

$$A_2 \times B_2 = (\bar{e}_2 + C_2'') \times (\bar{e}_1^\star + D_7').$$

By Lemma 3, for each $i = 2, 3, 4, 5, 6, 7$,

$$\bar{p} \in \ker(W_3) \quad \Longrightarrow \quad \bar{p} + A_i \times B_i = A_j \times B_j, \tag{15}$$

for some element $j \in \{2, 3, 4, 5, 6, 7\}$. Hence the set of words in the sets $\operatorname{span}\{\bar{f}_1, \bar{f}_2, \bar{c}_1 + \bar{c}_2\}$ and $\operatorname{span}\{\bar{g}_1, \bar{d}_1 + \bar{d}_2\}$, that can contribute to be candidates for periods of W_3, give rise to sets of permutations $\mathcal{G}$ and $\mathcal{H}$ on the sets $\{A_2, A_3, \ldots, A_7\}$ respectively $\{B_2, B_3, \ldots, B_7\}$.

It is easy to see, e.g. by using the defining parity check matrix of A_2, that

$$\bar{c}_1 + \bar{c}_2 + A_2 \notin \{A_2, A_3, \ldots, A_7\}. \tag{16}$$

For the word $\bar{f}_1$ we get that

$$\bar{f}_1 + A_5 = A_7 \quad \text{and} \quad \bar{f}_1 + A_i = A_i \quad \text{for} \quad i = 3, 4, 6, 7.$$

Similar calculations for the word $\bar{f}_2$ will then give

$$\mathcal{G} = \{id., (A_5 \ \ A_7), (A_2 \ \ A_6), (A_5 \ \ A_7)(A_2 \ \ A_6)\}.$$

Since the word $\bar{d}_1 + \bar{d}_2$ can only be combined with the word $\bar{c}_1 + \bar{c}_2$, we get, from equation (16), that the only candidates for periods from the set $\text{span}\{\bar{g}_1, \bar{d}_1 + \bar{d}_2\}$ will be the words $\bar{0}$ and $\bar{g}_1$. They give rise to the group

$$\mathcal{H} = \{id., (B_2 \ \ B_5)(B_6 \ \ B_7)\}.$$

As the groups $\mathcal{G}$ and $\mathcal{H}$ only have the identity in common, we get from (15), that just the trivial coset $(\bar{0}|\bar{0}) + F \times G$ will constitute the set of periods of W_3.

We have now proved that the kernel of W_3 equals $F \times G$ and consequently $\dim(\ker(W_3)) = 3$. As mentioned above, similar methods can be used to prove that $\dim(\ker(W_i)) = i$, for $i = 2, 4, 5$. This will prove the theorem.

5 Some remarks and conclusions

It can be proved that, every perfect code of length $n = 15$, rank $r = 14$ and with a kernel of dimension $k = 8$ is equivalent to a perfect code obtainable with the Phelps construction. This can be seen e.g. by considering the classification of all such perfect codes given in [4].

At present time we have no idea whether or not there exists any perfect code of length 15, rank 14 and with a kernel of dimension 7 that is not equivalent to some perfect code obtainable by the Phelps construction.

It was proved in [10] and [2], that for every integer k in the interval

$$2^{\log(n+1)-3} \leq k \leq n - \log(n+1) - 3$$

there is at least one perfect code of length $n = 2^m - 1$, where $m \geq 4$, rank $r = n - \log(n+1) + 3$ and with a kernel of dimension k and that no other values of k are possible for a perfect code of that length and rank. As already mentioned, every perfect code of length n and rank $r = n - \log(n+1) + 2$ is equivalent with a Phelps code, see [1]. Further all perfect codes of length n and rank $n - \log(n+1) + 1$ can easily be shown to be Vasil'ev codes. The next step would be to say something general about perfect codes of length n and rank $n - \log(n+1) + 3$.

We are quite convinced that it is possible to generalize our construction to any length $n = 2^m - 1$ greater than 15 in order to get non Phelps codes of rank $n - \log(n+1) + 3$. However, we must mention that every perfect code of length $n = 15$ and with a kernel of dimension $k = n - \log(n+1) - 3$ is equivalent to a perfect code obtainable with the Phelps construction [5].

References

[1] S. V. Avgustinovich, O. Heden and F. I. Solov'eva, On the classification of some binary perfect codes, *Designs, Codes and Cryptography* 31(3) (2004), 313–318.

[2] S. V. Avgustinovich, O. Heden and F. I. Solov'eva, On perfect codes ranks and kernels problem, *Probl. Inform. Transm.* 39(4) (2003), 341–345.

[3] R. W. Hamming, Error detecting and error correcting codes, *Bell System Technical Journal* 29 (1950), 147–160.

[4] O. Heden, Perfect codes from the dual point of view I, submitted.

[5] O. Heden, Perfect codes of length n with kernels of dimension $n-\log(n+1)-3$, manuscript in preparation.

[6] D. S. Krotov, Lower bounds on the number of m-quasigroups of order 4 and the number of perfect binary codes, *Discrete Analysis and Operation Research* 1(7)2 (2000), 47–53.

[7] K. T. Phelps, A combinatorial construction of perfect codes, *SIAM J. Algebra and Discrete Methods* 4 (1983), 398–403.

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

[9] K. T. Phelps, An enumeration of 1-perfect binary codes of length 15, *Australs. J. Combin.* 21 (2000), 287–298.

[10] K. T. Phelps and M. Villanueva, On perfect codes: rank and kernel, *Designs, Codes and Cryptography* 27(3) (2002), 183–194.

[11] F. I. Solov'eva, On binary nongroup code, *Methody Discretnogo Analiza* 37 (1981), 65–76 (in Russian).

[12] F. I. Solov'eva, On Perfect Codes and Related Topics, *Com^{2}Mac Lecture Note Series* 13, Pohang 2004.

[13] Y. L. Vasil'ev, On nongroup close-packed codes, *Problems of Cybernetics* 8 (1962), 375–378.

[14] T. Westerbäck, Maximal partial packings of Z_2^n with perfect codes, *Designs, Codes and Cryptography* 42(3) (2007), 335–355.

(Received 9 Apr 2006)