ISSN 0333–3590

How to find a [33,8,14] code

Tor Helleseth and Øyvind Ytrehus

REPORT NO. 41 NOVEMBER 1989

Abstract — We characterize up to equivalence all codes with parameters [30,6,14] and [29,5,14]. There is a strong relation between these codes and a [33,8,14] code. A computer search based on some of the [29,5,14] codes actually found a [33,8,14] code, which beats the world record [1, 2].

Dept. of Informatics, Thormøhlensgt. 55, N-5008 Bergen, Norway.

This research was sponsored by

the Norwegian Research Council for Science and the Humanities (NAVF).

Introduction

In this report, an $[n, k, d]$ code is a binary linear block code with block length n, dimension k, and minimum Hamming distance d. Define

$$n(k, d) \stackrel{\triangle}{=} min\{n | \text{an } [n, k, d] \text{ code exists}\}$$

A strongly related quantity is

$$d(n, k) \stackrel{\triangle}{=} max\{d | \text{an } [n, k, d] \text{ code exists}\}$$

Although general lower and upper bounds on $n(k, d)$ exist, it can sometimes be hard to determine $n(k, d)$ exactly. [1] gives a table of bounds on $d(n, k)$ for $1 \leq k \leq n \leq 127$. For $k \leq 7$, $n(k, d)$ is completely determined for any d. However, for $d \leq 80$, $n(8, d)$ remains undetermined for a number of values of d [3]. In particular, the smallest unsolved case [4] is $n(8, 14)$ where it is known [1] that

$$33 \leq n(8, 14) \leq 34.$$

The question to be considered in the following is:

Is there a [33,8,14] code?

Preliminaries

Assume that $\mathcal{C}$ is an $[n, k, d]$ code containing a codeword $\mathbf{c}$ of weight w. Then the *residual code* $\mathcal{C}_1 = Res(\mathcal{C}, \mathbf{c})$ is obtained from $\mathcal{C}$ by deleting the coordinates where $\mathbf{c}$ is nonzero. If only the weight w of $\mathbf{c}$ is important, $\mathcal{C}_1$ is denoted by $Res(\mathcal{C}, w)$. It is easy to see that

Lemma 1. *If $w < 2d$, then $Res(\mathcal{C}, w)$ is an $[n - w, k - 1, d_1]$ code where $d_1 \geq d - \lfloor w/2 \rfloor$.*

Definition. *Let $W(\mathcal{C}) = \{w(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\}\}$, where $w(\mathbf{c})$ is the Hamming weight of* $\mathbf{c}$.

Lemma 1 can be generalized to

Lemma 2. *For every $w \in W(\mathcal{C})$ such that $d \leq w < 2d$,*

a)

$$W(Res(\mathcal{C}, w)) \subseteq$$
$$\{v_0 \mid \exists v_1 : 0 \leq v_1 \leq w, \text{ and } \{v_0 + v_1, v_0 + w - v_1\} \subseteq W(\mathcal{C}).\}$$

b)

$$W(\mathcal{C}) \subseteq \{w\} \cup \{v_0 + v_1 \mid 0 \leq v_1 \leq w \text{ and}$$
$$v_0 \in W(Res(\mathcal{C}, w) \text{ and } \{v_0 + v_1, v_0 + w - v_1\} \subseteq W(\mathcal{C})\}.)$$

Lemma 3 (The MacWilliams identities, [5], ch.5, eq. (13)). *Let $\mathcal{C}$ be an $[n, k]$ code, and let $\mathcal{C}^\perp$ be the dual code of $\mathcal{C}$. Also, in the rest of this correspondence, let $\{A_i\}$ and $\{B_i\}$ be the weight enumerators of $\mathcal{C}$ and $\mathcal{C}^\perp$, respectively. Then*

$$B_j = \frac{1}{2^k} \sum_{i=0}^{n} A_i \cdot P_j(n, i), \qquad \forall j : 0 \leq j \leq n,$$

where

$$P_j(n, i) = \sum_{l=0}^{j} (-1)^l \binom{i}{l} \binom{n-i}{j-l}$$

is a Krawtchouk polynomial.

Assume that a [33,8,14] code $\mathcal{C}$ exists. Then $W(\mathcal{C}) \subset \{14, 16, 18, 20, 22, 24, 26, 28, 30\}$ and the minimum distance of the dual code is at least 3 and at most 4.

The code contains no codeword of weight 32, for if there were such a codeword, it would be contained in some [32,7,14] code. However, this contradicts the MacWilliams identities.

We shall consider two cases: $B_3 > 0$ and $B_3 = 0$, $B_4 > 0$.

The [30,6,14] code.

If $B_3 > 0$, then $\mathcal{C}$ can be generated by a matrix on the form

Figure 1. $B_3 > 0$

[3,2,2]	$\mathbf{r}_1$ $\mathbf{r}_2$
0	[30,6,14]

Lemma 4. *There is, up to isomorphism, only one [30,6,14] code, $\mathcal{C}_0^*$. Its weight distribution is*

$$A_0 = 1, A_{14} = A_{16} = 31, A_{30} = 1, B_2 = 1.$$

Proof. Let $\mathcal{C}^*$ be the [30,6,14] code. By the residual construction, $\mathcal{C}^*$ contains no codewords of weights 18, 22, or 26. The MacWilliams identities for $\mathcal{C}^*$ yield

$$A_{14} + A_{16} + A_{20} + A_{24} + A_{28} + A_{30} = 63$$
$$A_{16} + 3A_{20} + 5A_{24} + 7A_{28} + 8A_{30} = 39$$
$$3A_{20} + 10A_{24} + 21A_{28} + 28A_{30} = 24 + 4B_2$$

- If $A_{30} = 1$, this gives the weight distribution

  $$A_0 = 1, A_{14} = A_{16} = 31, A_{30} = 1, B_2 = 1.$$

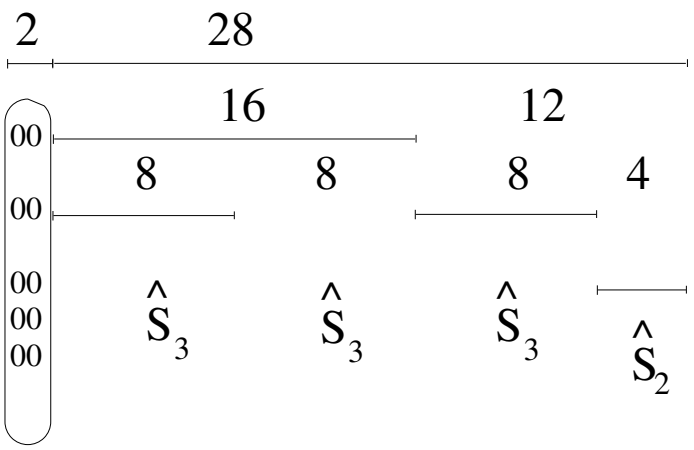
  Thus the code coordinates can be permuted to fit the form

Figure 2. A [30,6,14] code

1 1	**x**
0	[28,5,14]

A [28,5,14] code meets the Griesmer bound. It is unique, and can be constructed as $S_5 \setminus S_2$. The only weights occurring are 14 and 16, so **x** can be assumed to be the all-one vector, and $\mathcal{C}^*$ can be constructed as shown in Figure 3:

Figure 3. A [30,6,14] code in more detail. $\hat{S}_i$ denotes the set of all i—dimensional column vectors. Runs of ones and zeros of the indicated lengths are shown as lines and no-lines, respectively. For instance, the second row below consists of two zeros followed by sixteen ones and then twelve zeros.



- If $A_{28} = 1$, then the only other weights that occur are 14 and 16. This contradicts the MacWilliams identities.
- If $A_{24} = 1$, then the only other weights that occur are 14,16, and 20. $Res(\mathcal{C}^*, 24)$ is a [6,5,2] code $\mathcal{C}^{*,24}$. Every codeword of weight 20 in $\mathcal{C}^*$ must have weight 6 when restricted to $\mathcal{C}^{*,24}$. Hence $A_{20} = 1$. However, this contradicts the MacWilliams identities ("$4B_2 = 11$").
- If $A_{20} > 0, A_i = 0$ for $i > 20$, then $W(\mathcal{C})^* \subset$ {14,16,20}. From the MacWilliams identities, $A_{20} \geq 8$. $Res(\mathcal{C}^*, 20)$ is a [10,5,4] code $\mathcal{C}^{*,20}$. For each codeword of weight 8 (resp. 10) in $\mathcal{C}^{*,20}$, there is one (resp. 2) codeword of weight 20 in $\mathcal{C}^*$. $\mathcal{C}^{*,20}$ contains at most 5 codewords of weight 8 *or* 1 codeword of weight 10. Hence, in $\mathcal{C}^*$, $A_{20} \leq 6$, a contradiction.

□

Theorem 5. *In a [33,8,14] code $\mathcal{C}$, $B_3 = 0$.*

Proof. If $B_3 > 0$, then $\mathcal{C}_0^*$ is contained in $\mathcal{C}$ as depicted in Figure 1, and $30 \in W(\mathcal{C}) \Rightarrow W(\mathcal{C}) \subset \{14, 16, 18, 20\}$ (since the inner product between vectors of weight 22 and 30 is at least 20). Without loss of generality, we can assume

that $\mathcal{C}$ is generated by $\mathbf{G} =$

Block I		Block II															Block III											Block IV		
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0
0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0
0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	0	0
0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0
<															**x**													>	1	1	0
<															**y**													>	1	0	1

where the first six rows of Blocks I, II, and III generate $\mathcal{C}_0^*$. In $\mathcal{C}$, $B_3 = 2$, since the only way to find three linearly dependent columns is to take the three columns in Block IV, or to take the two columns in Block I together with the appropriate column of Block IV — this is possible since the columns of Block I are distinct, since $B_2 = 0$. Hence, the weight distribution for $\mathcal{C}$ would be

$$A_0 = 1, A_{14} = 107, A_{16} = 51, A_{18} = 20, A_{20} = 76, A_{30} = 1, B_3 = 2.$$

Note that Block II essentially contains a first-order Reed-Muller code of length 16, $\mathcal{R}(1,4)$.

The following information on the cosets of $\mathcal{R}(1,4)$ can be found in Fig. 14.6, p.418 of [5]:

Coset class number	Weights in coset	Remarks
0	0,8,16	The code itself
1	1,7,9,15	
2	2,6,8,10,14	
3	3,5,7,9,11,13	
4	4,6,8,10,12	
5	4,8,12	
6	5,7,9,11	
7	6,10	Bent functions

By considering the residual code with respect to the second row of **G**, which is a [17,7,6] code exactly located in Blocks I, III, and IV, and relating this to the cosets of $\mathcal{R}(1,4)$, we get the table (explained below):

Possible coset classes	Truly possible coset classes	Weight in the restriction of the codeword of weight 16		Weight in Res.Code	Weights in code	
0,2,4,5	none	8	8	6	14	14
1,3,6	6	7	9	7	14	16
2,4,7	7	6	10	8	14	18
0,2,4,5	none	8	8	8	16	16
3,6	6	5	11	9	14	20
1,3,6	6	7	9	9	16	18
2,4,7	7	6	10	10	16	20
0,2,4,5	none	8	8	10	18	18
1,3,6	6	7	9	11	18	20
0,2,4,5	none	8	8	12	20	20
0	0	0	16	14	14	30

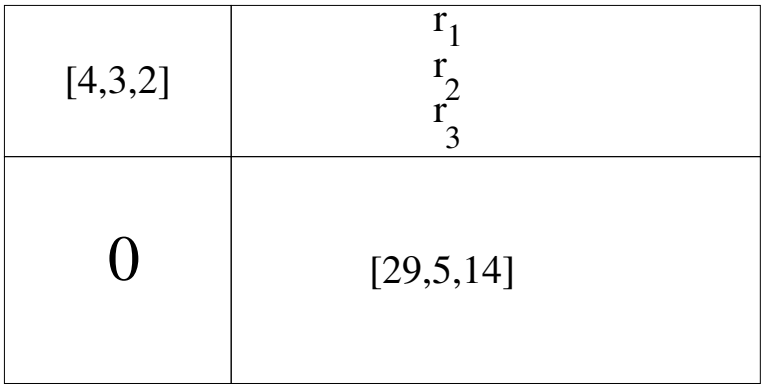
We can see that the weight of **x** must be at least 5 when restricted to Block II (, unless the weight of **x** in the residual code is 14. But there is only one such codeword in the residual code; the first row). The "truly possible coset classes" are those that contain no weights less than 5. By interchanging **x** and **y** or adding **y** if necessary, we can assume that the weight of **x** is even in the residual code; that is, the weight of **x** must be 6 or 8 when restricted to Blocks I and III. Hence, the first six rows of **G** generate a code that contains a [14,6,6] code in Blocks I and III. This is not possible.

So $B_3 = 0$ in any [33,8,14] code. □

The [29,5,14] codes

From Theorem 5 and the fact that $n(25, 5) > 33$ [1], it follows that $B_4 > 0$ and $\mathcal{C}$ can be generated by a matrix on the form

Figure 4. $B_4 > 0$



where it is assumed that the [4,3,2] code is generated by codewords of weight 2.

Lemma 6. *There are, up to isomorphism, seven [29,5,14] codes, denoted* $\mathcal{C}_1^*, \ldots, \mathcal{C}_7^*$. *Their weight distributions are*

	A_0	A_{14}	A_{16}	A_{18}	A_{20}	A_{22}	$\ldots$	B_1	B_2	$\ldots$
$\mathcal{C}_1^*$:	1	22	7			2		0	7	
$\mathcal{C}_2^*$:	1	20	9		2			0	4	
$\mathcal{C}_3^*$:	1	21	6	3	1			0	4	
$\mathcal{C}_4^*$:	1	18	11	2				0	2	
$\mathcal{C}_5^*$:	1	20	7	4				0	3	
$\mathcal{C}_6^*$:	1	16	15					0	1	
$\mathcal{C}_7^*$:	1	24	7					1	0	

Proof. Let $\mathcal{C}^*$ be the [29,5,14] code. By the residual construction, $\mathcal{C}^*$ contains no codewords of weight 26. The MacWilliams identities for $\mathcal{C}^*$ yield

$$A_{14} + A_{16} + A_{18} + A_{20} + A_{22} + A_{24} + A_{28} = 31$$
$$A_{16} + 2A_{18} + 3A_{20} + 4A_{22} + 5A_{24} + 7A_{28} = 15 - 8B_1$$
$$A_{18} + 3A_{20} + 6A_{22} + 10A_{24} + 21A_{28} = -2 + 2B_1 + 2B_2$$

If $B_1 > 0$, then the code is determined uniquely. We shall consider also that possibility eventually; but if $\mathcal{C}^*$ contains a codeword of weight > 16 it is easy to show that $B_1 = 0$.

- If $A_{28} = 1$, the third MacWilliams identity is contradicted.

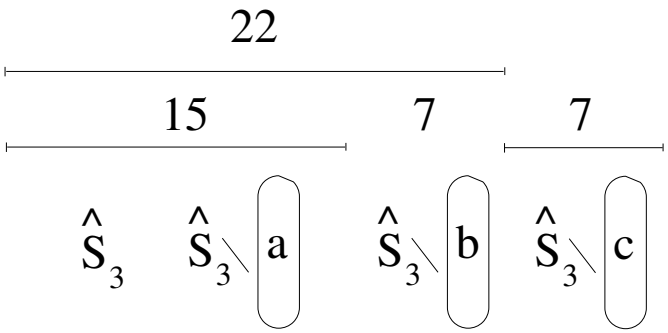
- If $A_{24} = 1$, then $Res(\mathcal{C}^*, 24)$ is a [5,4,2] code $\mathcal{C}^{*,24}$, with 5 codewords of weight 4 and 10 codewords of weight 2. This implies that all other weights < 20. $Res(\mathcal{C}^*, 18)$ is a [11,4,5] code $\mathcal{C}^{*,18}$. This code meets the Griesmer bound and is unique — in particular, it has no codewords of weight more than 8. But this contradicts the fact that $A_{24} = 1$, so the only other weights that occur in $\mathcal{C}^*$ are 14 and 16. This gives the weight distribution

  $$A_0 = 1, A_{14} = 20, A_{16} = 10, A_{24} = 1, B_2 = 6.$$

  But consider the 24 columns corresponding to the codeword of weight 24. There can be at most 16 distinct columns among these, so $B_2 \geq 8$, a contradiction.
- If $A_{22} > 0$, then $Res(\mathcal{C}^*, 22)$ is a [7,4,3] code $\mathcal{C}^{*,22}$, which of course is unique. Since another codeword of weight 22 must have weight 7 when restricted to $\mathcal{C}^{*,22}$, $A_{22} \leq 2$.
  - If $A_{22} = 2$, then, by considering the weights of $\mathcal{C}^{*,22}$, the only other weights in $\mathcal{C}^*$ are 14 and 16 and its weight distribution is

    $$A_0 = 1, A_{14} = 22, A_{16} = 7, A_{22} = 2, B_2 = 7.$$

    Now $\mathcal{C}^*$ can be uniquely constructed by



    where the columns a, b, and c generate a [3,2,2] code, for instance

$$\begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&1&1&1&1&1&1&1\\
1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&1&1&1&1&0&0&0&1&1&1&1&0&0&0\\
1&1&0&0&1&1&0&0&1&1&0&0&1&0&0&1&1&0&0&1&0&0&1&1&0&0&1&1&0\\
1&0&1&0&1&0&1&0&1&0&1&0&0&1&0&1&0&1&0&1&1&0&1&0&1&0&1&0&0
\end{pmatrix}$$

We call this construction $\mathcal{C}_1^*$.

- If $A_{22} = 1$, then, by considering the weights of $\mathcal{C}^{*,22}$, there are two "possible" weight distributions of $\mathcal{C}^*$,

$$A_0 = 1, A_{14} = 21, A_{16} = 8, A_{20} = 1, A_{22} = 1, B_2 = 11/2,$$

which is sick, and

$$A_0 = 1, A_{14} = 21, A_{16} = 7, A_{18} = 2, A_{22} = 1, B_2 = 5,$$

which is also impossible since by arguments similar to above $B_2 \geq (22 - 16)$.

- If $A_{20} > 0, A_i = 0$ for $i > 20$, then $W(\mathcal{C})^* \subset$ {14,16,18,20}. $Res(\mathcal{C}^*, 20)$ is a [9,4,4] code $\mathcal{C}^{*,20}$. Comparing the weights in $\mathcal{C}^{*,20}$ with those in $\mathcal{C}^*$, we get

Type	Weight in the restriction of the codeword of weight 20		Weight in Res.Code	Weights in code	
A	10	10	4	14	14
B	9	11	5	14	16
C	8	12	6	14	18
D	10	10	6	16	16
E	8	12	8	16	20
F	10	10	8	18	18
G	9	11	9	18	20

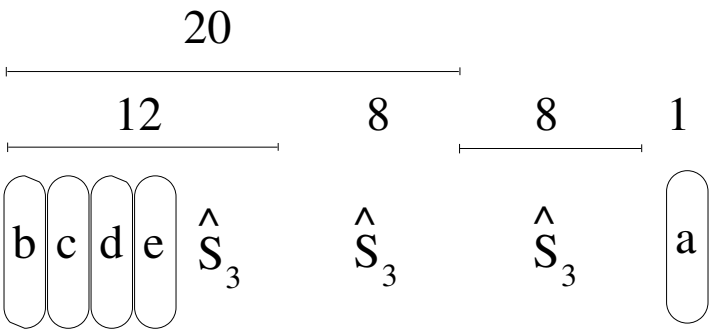
- If $\mathcal{C}^{*,20}$ contains a codeword of weight 9, then, in $\mathcal{C}^*$, $A_{18} = 1, A_{20} = 2$, contradicting the first three MacWilliams identities.
- If $\mathcal{C}^{*,20}$ contains a codeword of weight 8, then this codeword must be of one of the types E or F. In any case, there are two possible weight distributions of $\mathcal{C}^{*,20}$:

$$\text{(I) } A_0 = 1, A_4 = 6, A_5 = 8, A_8 = 1, B_2 = 0,$$
$$\text{(II) } A_0 = 1, A_4 = 10, A_6 = 4, A_8 = 1, B_2 = 1.$$

- Type E, weight distribution (I): Then, in $\mathcal{C}^*$, the weight distribution is

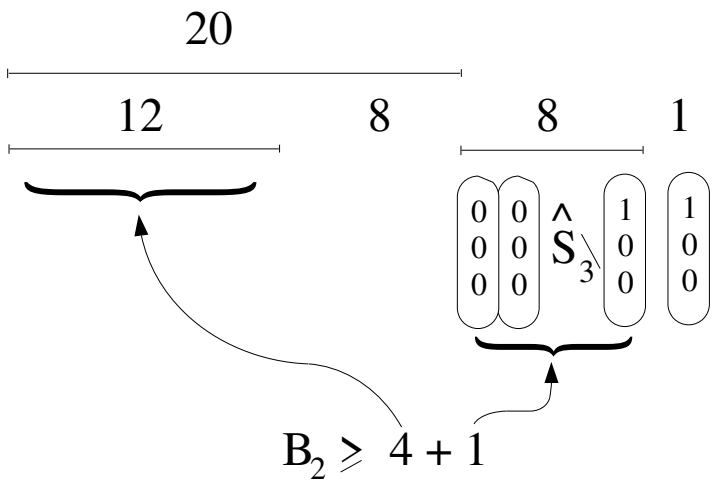
$$A_0 = 1, A_{14} = 20, A_{16} = 9, A_{20} = 2, B_2 = 4,$$

and the code can be constructed as follows:



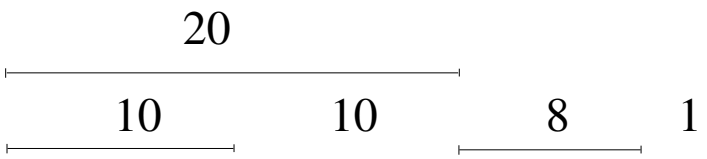
where the columns a,b,c,d, and e constitute a [5,4,2] code. We call this construction $\mathcal{C}_2^*$.

- Type F, weight distribution (I): Then, in $\mathcal{C}^*$, $A_{18} = 2, A_{20} = 3$, contradicting the first three MacWilliams identities.
- Type E, weight distribution (II): Then, in $\mathcal{C}^*$, from $2B_2 - 2 = A_{18} + 3A_{20}$ and the figure



it follows that $A_{18} \geq 2$. But in $Res(\mathcal{C}^*, 18)$, only *one* codeword (of weight 8) can be extended to *one* codeword of weight 20 in $\mathcal{C}^*$.

- Type F, weight distribution (II): Then, from the figure

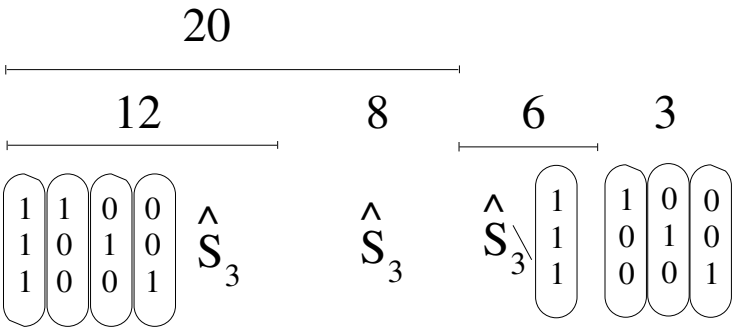


it follows that $Res(\mathcal{C}^*, 18)$, which is an [11,4,5] code, contains a codeword of weight 10. This is not possible.

- If $\mathcal{C}^{*,20}$ contains some codeword of weight 6, but no codewords of weight > 6, then the weight distribution of $\mathcal{C}^{*,20}$ is

$$A_0 = 1, A_4 = 9, A_6 = 6, B_2 = 0, B_3 = 6.$$

In $\mathcal{C}^*$, $2B_2 - 2 = A_{18} + 3A_{20}$, implying that A_{18} is either 3 or 5, corresponding to B_2=4 or 5, respectively, in $\mathcal{C}^*$. But from $Res(\mathcal{C}^*, 18)$, $A_{18} \leq 3$. So, since $B_2 = 4$, $\mathcal{C}^*$ looks like



We call this construction $\mathcal{C}_3^*$. Its weight distribution is

$$A_0 = 1, A_{14} = 21, A_{16} = 6, A_{18} = 3, A_{20} = 1, B_2 = 4.$$

- If $A_{18} > 0, A_i = 0$ for $i > 18$, then $W(\mathcal{C})^*$ = {14,16,18}. $Res(\mathcal{C}^*, 18)$ is a [11,4,5] code $\mathcal{C}^{*,18}$ with weight distribution

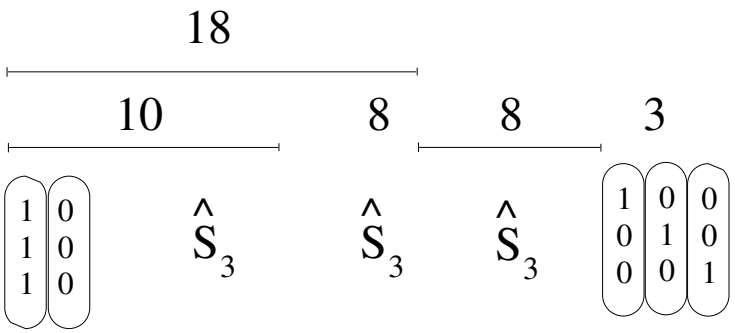
$$A_0 = 1, A_5 = 6, A_6 = 6, A_7 = 2, A_8 = 1, B_2 = 0, B_3 = 12.$$

Comparing the weights in $\mathcal{C}^{*,18}$ with those in $\mathcal{C}^*$, we get

Weight in the restriction of the codeword of weight 18		Weight in Res.Code	Weights in code	
9	9	5	14	14
8	10	6	14	16
7	11	7	14	18
9	9	7	16	16
8	10	8	16	18

There are two cases to consider:

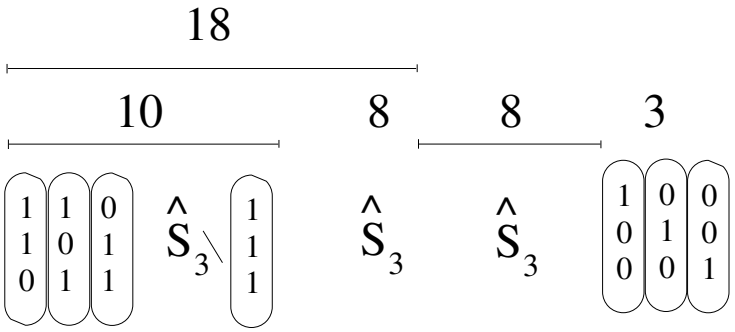
- If $B_2 = 2$ in $\mathcal{C}^*$, then the code looks like



We call this construction $\mathcal{C}_4^*$. Its weight distribution is

$$A_0 = 1, A_{14} = 18, A_{16} = 11, A_{18} = 2.$$

- If $B_2 = 3$ in $\mathcal{C}^*$, then the code looks like



We call this construction $\mathcal{C}_5^*$. Its weight distribution is

$$A_0 = 1, A_{14} = 20, A_{16} = 7, A_{18} = 4.$$

- If $\mathcal{C}^*$ only contains codewords of weight 14 and 16, then it can be *lengthened* ([5], p. 30) by adding the all-one vector of length 30. In other words, all[29,5,14] code with weights only 14 and 16 can be obtained by taking a *cross-section* (deleting a code coordinate and those codewords that have a one in this coordinate) of the unique even-weight [30,6,14] code. Two non-equivalent classes of codes arise from this construction:
  - Deleting one of the last twenty-eight coordinates (corresponding to the distinct columns) and the first row in the [30,6,14] code, we get a [29,5,14] code $\mathcal{C}_6^*$ with weight distribution

    $$A_0 = 1, A_{14} = 16, A_{16} = 15, B_1 = 0, B_2 = 1.$$

  - Deleting one of the first two coordinates (corresponding to the two equal columns) and the first row in the [30,6,14] code, we get a [29,5,14] code $\mathcal{C}_7^*$ with weight distribution

    $$A_0 = 1, A_{14} = 24, A_{16} = 7, B_1 = 1, B_2 = 0.$$

This concludes the proof of Lemma 6. □

Computer search

Theorem 7. *There is a [33,8,14] code with weight distribution*

$$A_0 = 1, A_{14} = 96, A_{16} = 69, A_{18} = 40, A_{20} = 24, A_{22} = 24, A_{24} = 2,$$
$$B_3 = 0, B_4 = 153.$$

Proof. This is achieved by the code generated by

$$\begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0\\
1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0\\
1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&0&0&0&0\\
1&0&1&0&1&0&1&0&1&0&1&0&1&0&0&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&0&0\\
1&0&0&1&0&1&0&0&1&0&0&0&1&0&1&0&1&1&1&1&1&0&0&0&0&0&1&0&0&1&1&0\\
0&1&0&1&0&0&1&0&1&1&0&1&0&1&1&0&1&1&0&0&0&0&0&1&1&0&0&0&0&1&0&1\\
1&0&0&1&1&1&1&1&0&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&1&0&1&0&0&1&0&0&1
\end{pmatrix}$$

□

The code above was found by a computer program (like the one in [4]), which tried to add three rows to each of the seven [29,5,14] codes described in the previous section. In the case of $\mathcal{C}_7^*$, it is not possible in any way to complete the generator matrix. However, *all the other* [29,5,14] codes allow three rows to be added. The computer search was in these cases not exhaustive, but all the [33,8,14] codes *found* have the same weight distribution. We have not investigated whether these [33,8,14] codes are equivalent.

References

[1] T. Verhoeff, "An updated table of minimum-distance bounds for binary linear codes," *IEEE Transactions on Information Theory*, vol. IT-33, pp. 665–680, Sept 1987.

[2] T. Verhoeff, "An updated table of minimum-distance bounds for binary linear codes." Jan, 1989.

[3] S. M. Dodunekov, T. Helleseth, N. Manev, and Ø. Ytrehus, "New bounds on binary linear codes of dimension eight," *IEEE Transactions on Information Theory*, vol. IT-33, pp. 917–919, Nov 1987.

[4] T. Helleseth and Ø. Ytrehus, "There is no [25,8,10] code," *IEEE Transactions on Information Theory*, pp. 695–696, May 1990.

[5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1977.