A proof of the nonexistence of a binary (55,7,26) code

TECHNISCHE HOGESCHOOL EINDHOVEN
NEDERLAND
ONDERAFDELING DER WISKUNDE

TECHNOLOGICAL UNIVERSITY EINDHOVEN
THE NETHERLANDS
DEPARTMENT OF MATHEMATICS

A proof of the nonexistence of a binary (55,7,26) code

by

H.C.A. van Tilborg

T.H.-Report 79-WSK-09
November 1979

I. Introduction

In the past a great number of articles have appeared on the problem of determing the smallest length $n = n(k,d)$ of a binary (n,k,d) code, where k denotes the dimension and d the minimum distance.
We quote the basic results in this field.

Theorem 1.1 (Griesmer, [6]). Let $\lceil x \rceil$ denote the smallest integer $\geq x$, then

$$n(k,d) \geq d + n(k-1,\lceil d/2 \rceil) \tag{1.1}$$

$$n(k,d) \geq g(k,d) := \sum_{i=0}^{k-1} \lceil d/2^i \rceil \tag{1.2}$$

Theorem 1.2 (Solomon and Stiffler, [9]). Let

$$s = \lceil d/2^{k-1} \rceil \text{ and } s \cdot 2^{k-1} - d = \sum_{i=1}^{p} 2^{u_i - 1} ,$$

where $k > u_1 > u_2 > \ldots > u_p > 0$. Then

$$\sum_{i=1}^{p} u_i \leq s \cdot k \Rightarrow n(k,d) = g(k,d) .$$

Theorem 1.3 (Belov, [4]). Let $s = \lceil d/2^{k-1} \rceil$ and

$$s \cdot k - d = \sum_{i=1}^{p} 2^{u_i - 1} , \text{ where } k > u_1 > \ldots > u_p > 0 .$$

If

$$\sum_{i=1}^{\min(p,s+1)} u_i \leq s \cdot k$$

or

$$u_s - u_p = p - s \text{ and } u_p \in \{1,2\}$$

then $n(k,d) = g(k,d)$.

Theorem 1.4 (Logačev, [7])

If $3 \leq d \leq 2^{k-2}-2$, then $n(k,d) \geq g(k,d) + 1$.

Theorem 1.5 (van Tilborg, [11])

If $2^{k-2}+3 \leq d \leq 2^{k-1}-2^{k-3}-4$ then $n(k,d) \geq g(k,d) + 1$.

So while Theorems 1.2 and 1.3 give sufficient conditions for equality in (1.2), we see that Theorems 1.4 and 1.5 give ranges of values of d (in terms of k), where strict inequality in (1.2) holds.
It follows from Theorem 1.4 that

$$n(7,26) \geq 55 \; . \tag{1.3}$$

In Alltop ([1]), one can find the construction of a (56,7,26) code, so

$$n(7,26) \leq 56 \; . \tag{1.4}$$

It is our aim to prove that $n(7,26) = 56$.

II. Some techniques

Definition 2.1. Let G be the generator matrix of a binary linear code C with top row $\underline{c}$. Then the residual resp. derived code of C with respect to $\underline{c}$ (abbreviated to: w.r.t $\underline{c}$) is the code generated by the restriction of G to the columns where $\underline{c}$ has a zero resp. a nonzero entry. We shall often denote these codes by C^0 resp. C^1 and similarly the corresponding parts of G by G^0 resp. G^1.

Lemma 2.1. Let C be a (n,k,d) code, $\underline{c} \in C$ of weight w, where $\lfloor \frac{w}{2} \rfloor < d$. Then the residual code C^0 of C w.r.t. $\underline{c}$ has parameters $(n-w, k-1, d^0)$, where $d^0 \geq d - \lfloor \frac{w}{2} \rfloor$.

Proof. Let $\underline{c}' \in C$, $\underline{c}' \neq \underline{0}$, $\underline{c}' \neq \underline{c}$. Then $\underline{c}'$ or $\underline{c}' + \underline{c}$ has inner product $\leq \lfloor \frac{w}{2} \rfloor$ with $\underline{c}$. So the restriction of $\underline{c}'$ to C has weight $\geq d - \lfloor \frac{w}{2} \rfloor$. □

Lemma 2.2. Let C be a (n,k,d) code with generator matrix G. If G has two repeated columns then shortening C on these two positions yields a $(n-2,k-1,d)$ code C^*.

Proof. W.l.o.g. G has the form

$$\left(\begin{array}{cc|ccc} 1 & 1 & * & * & * \\ \hline 0 & 0 & & & \\ \vdots & \vdots & & G^* & \\ 0 & 0 & & & \end{array}\right)$$

where G^* clearly generates the $(n-2,k-1,d)$ code C^* . □

Definition 2.3. (Farrell, [5]). An (m,k,δ) anticode is a k-dimensional, linear code of length m in which the maximal weight equals δ.

Lemma 2.4. (Farrell, [5]). Let G be the generator matrix of a (n,k,d) code. By punturing a set of columns of G, that generates an (m,k',δ) anticode, one obtains an $(n-m,k'',d-\delta)$ code.

On page 127 in [8] one can find the following result by MacWilliams.

Theorem 2.5. Let C be a binary, linear code. Let A_k and B_k, $0 \le k \le n$, denote the number of codewords of weight k in C, resp. in its dual code. Then

$$B_k = |C|^{-1} \sum_{i=0}^{n} A_i K_k(i) \quad , \quad 0 \le k \le n \, ,$$

where

$$K_k(i) = \sum_{\ell=0}^{k} (-1)^{\ell} \binom{n-i}{k-\ell} \binom{i}{\ell} \quad , \quad 0 \le i,\, k \le n \, .$$

Table 2.6.

$$K_0(i) = 1$$
$$K_1(i) = n - 2i \, ,$$
$$K_2(i) = \binom{n}{2} - 2ni + 2i^2,$$
$$K_3(i) = \tfrac{1}{3}\{3\binom{n}{3} - (3n^2-3n+2)i + 6ni^2 - 4i^3\} \, .$$

III. A proof that n(7,26) equals 56.

It follows from (1,3) and (1,4) that we must prove that a (55,7,26) code C cannot exist. So let us assume that C is a (55,7,26) code. Let A_w and B_w, $0 \le w \le 55$, denote the weight enumerator of C resp. the dual code of C. Let $26 \le w \le 51$ with A_w not equal to zero. Then the residual code of C w.r.t. a weight-w codeword has parameters $(55-w,6,26-\lfloor \frac{w}{2} \rfloor)$. This, however, contradicts Theorems 1.1 or 1.4 for some values of w in the range from 26 to 51. One obtains

$$A_w = 0 \quad \text{for } w \in \{27,31,33,34,35,39,41,42,43,45,46,47,49,50,51\} \tag{3.1}$$

Let C^0 be the residual code of C w.r.t. a codeword $\underline{c} \in C$ of weight 29 (resp. 37). C^0 has parameters (26,6,12) (resp. (18,6,8)) by Lemma 2.1. Let $\underline{d}^0$ be a minimum weight vector in C^0, and let it be the restriction of $\underline{d} \in C$ to C^0. Then it follows from the minimum distance of C that $\underline{d}$ or $\underline{c} + \underline{d}$ has weight 27, a contradiction with (3.1).
Hence

$$A_{29} = A_{37} = 0 \tag{3.2}$$

Since the sum of a codeword of weight 53 or 55 and a minimum weight codeword must have weight 27,29 or 31, we can conclude from (3.1) and (3.2) that

$$A_{53} = A_{55} = 0 \tag{3.3}$$

In view of (3.1) - (3.3) we do know now that C must be an evenweight code. If C has repeated columns, one has by Lemma 2.2 a code C^* with parameters (53,6,26). By the same Lemma and Theorem 1.1 C^* cannot have repeated colomns. So

$$A_0 = B_0 = 1 \, , \quad B_1 = 0 \, , \quad B_2 \in \{0,1\} \, . \tag{3.4}$$

If we now take k = 0,1,2 in theorem 2.5, we obtain after some elementary row operations the following equations

$$\begin{array}{ccccccccccccl} A_{26} & A_{28} & A_{30} & A_{32} & A_{36} & A_{38} & A_{40} & A_{44} & A_{48} & A_{52} & A_{54} & & \\ 1 & & -1 & -2 & -4 & -5 & -6 & -8 & -10 & -12 & -13 & = & 18 \\ & 1 & 2 & 3 & 5 & 6 & 7 & 9 & 11 & 13 & 14 & = & 109 \\ & & 1 & 3 & 10 & 15 & 21 & 36 & 55 & 78 & 91 & = & 117 + 8B_2 \end{array} \tag{3.5}$$

We are now going to exclude the occurence of certain weights, one after another.

$\underline{A_{54} = 0}$

Suppose the contrary i.e. $A_{54} \neq 0$.
It follows from $d = 26$ that $A_{54} = 1$ and $A_i = 0$ for $30 < i < 54$. If we now also assume that $A_{30} \neq 0$, then it follows from $d = 26$ that the residual code C^0 of C w.r.t. a weight 30 codeword (which has parameters (25,6,11)) must contain the all-one vector. The residual code of C^0 w.r.t. a weight 12 codeword would have parameters (13,5,5), contradicting Theorem 1.4. So $A_{12}{}^0 = A_{13}{}^0 = 0$ (here $A_i{}^0$ is the weight ennumerator of C^0):

$$A_0{}^0 = A_{25}{}^0 = 1 \quad , \quad A_{11}{}^0 = A_{14}{}^0 = 31 \ .$$

If one now computes the number of weight-2 codewords in the dual code of C^0 by Theorem 2.5, one obtains a non integer number.
We conclude that $A_{54} \neq 0$ implies

$$A_{54} = 1 \quad \text{and } A_i = 0 \quad \text{for} \quad 30 \le i < 54 \ .$$

From (3.5) we find the unique weight enumerator

$$A_0 = A_{54} = 1 \quad A_{26} = 31 \quad A_{28} = 95 \ .$$

However the 3rd equation in (3.5) yields a negative number for B_2, a contradiction.

$\underline{A_{52} = 0}$

Assume the contrary. Then it follows from $d = 26$ that $A_{52} = 1$ and $A_i = 0$ for $32 < i < 52$. The existence of a codeword of weight 32 leads to a residual code with parameters (23,6,10) which contains the all-one vector. In exactly the same way as above one can obtain a contradiction, so $A_{32} = 0$. In view of (3.4) and (3.5) we now have two solutions

$$A_0 = 1 \quad A_{26} = 69 \quad A_{28} = 18 \quad A_{30} = 39 \quad A_{52} = 1$$

$$A_0 = 1 \quad A_{26} = 77 \quad A_{28} = 2 \quad A_{30} = 47 \quad A_{52} = 1$$

From Theorem 2.5 one can now compute the weight enumerator of the dual code of C. One gets

$$B_0 = 1 \quad B_1 = 0 \quad B_2 = 0 \quad B_3 = 59\tfrac{1}{2} \; ,$$

resp.

$$B_0 = 1 \quad B_1 = 0 \quad B_2 = 1 \quad B_3 = 58\tfrac{1}{2} \; .$$

Since B_3 is non integer, we have obtained a contradiction

<u>$A_{48} = 0$</u>

Suppose that $\underline{c}_1 \in C$ is of weight 48. Since the residual code of C w.r.t.. $\underline{c}_1$ has parameters (7,6,2) we may assume that the generator matrix G of C has the following form:

$$\begin{array}{c|c|c} \xleftarrow{\quad 48 \quad} & \xleftarrow{\quad 6 \quad} & \leftarrow 1 \rightarrow \\ \end{array}$$

$$\left(\begin{array}{c|c|c} 1 \quad 1 \ldots\ldots\ldots\ldots 1 & 0 \ldots\ldots 0 & 0 \\ \hline & & 1 \\ & & \vdots \\ & I_6 & \vdots \\ & & 1 \end{array}\right)$$

where I_6 is a 6 x 6 identity matrix.

Because d = 26 we may conclude that the rows $\underline{c}_i$, $i \geq 2$, and the sums $\underline{c}_i + \underline{c}_j$, $2 \leq i < j \leq 7$, have intersection 24 with $\underline{c}_1$. So w.l.o.g. the restriction of $\underline{c}_2$ and $\underline{c}_3$ to the non zero coordinates of $\underline{c}_1$ looks like

$$\begin{array}{ccccc} & \leftarrow 12 \rightarrow & \leftarrow 12 \rightarrow & \leftarrow 12 \rightarrow & \leftarrow 12 \rightarrow \\ c_2 & 11..1 & 11...1 & 00..0 & 00...0 \\ c_3 & 11..1 & 00...0 & 11..1 & 00...0 \end{array}$$

Let p,q,r and s be the intersection numbers of $\underline{c}_4$ with these four 12-typles. From the arguments used above it follow that $p + q + r + s = 24$ and $p + q = p + r = 12$ i.e. $q = r = 12 - p$ and $s = p$. From $w(\underline{c}_2 + \underline{c}_3 + \underline{c}_4) \geq 26$ and $w(c_1 + c_2 + c_3 + c_4) \geq 26$ it now follows that $4p + 4 \geq 26$ and $4(12 - p) \geq 26$ i.e. $p = 6 = q = r = s$. This divide the first forty-eight coordinates in a natural way into eight 6-tuples.
In exactly the same way as above one can show that c_5 (and $\underline{c}_6$ and $\underline{c}_7$) intersects each of these 6-tuples in three positions. So w.l.o.g. we have the following picture

```
c1  111111111111111111111111111111111111111111111111        1
c2  111111111111111111111111                           1    1
c3  111111111111            111111111111                1   1
c4  111111      111111      111111      111111           1  1
c5  111   111   111   111   111   111   111   111         1 1
c6   a 3-a 3-a a 3-a a  a 3-a 3-a a  a 3-a a 3-a 3-a a     1 1
                                                            11
```

However now $w(\sum_{i=2}^{6} \underline{c}_i) \geq 26$ and $w(\sum_{i=1}^{6} \underline{c}_i) \geq 26$ yields $16.a + 6 \geq 26$ resp. $16(6 - a) + 6 \geq 26$ i.e. $1.25 \leq a \leq 1.75$, a contradiction.

$A_{44} = 0$

Suppose that C contains a codeword $\underline{c}$ of weight 44. The residual code C^0 of C w.r.t. $\underline{c}$ has parameters (11,6,4). Let A_i^0 and B_i^0, $0 \leq i \leq 11$, be the weight enumerator of C^0 resp. its dual code. We shall first try to find the weight ennumerator of C^0.
It follows from Lemma 2.1 that $A_7^0 = 0$. Since the complement of a weight-4 vector has weight 7 it follows from $A_7^0 = 0$ that $A_{11}^0 = 0$. Now assume that $A_5^0 \neq 0$. and Let $\underline{u}_1 \in C^0$ be of weight 5. Since the residual code of C^0 w.r.t. $\underline{u}_1$ has parameters (6,5,2), one has w.l.o.g. the following generator matrix for C^0 :

$$\begin{array}{l} \underline{u}_1 \\ \\ \\ \\ \\ \\ \end{array} \left[\begin{array}{ccccc|cccccc} 1&1&1&1&1&0&0&0&0&0&0 \\ \hline &&&&&1&0&0&0&0&1 \\ &&&&&0&1&0&0&0&1 \\ &&&&&0&0&1&0&0&1 \\ &&&&&0&0&0&1&0&1 \\ &&&&&0&0&0&0&1&1 \end{array}\right]$$

By adding $\underline{u}_1$ to the following rows if necessary, one has w.l.o.g. that all $\underline{u}_i$, $2 \le i \le 6$, have innerproduct 2 with $\underline{u}_1$. It now follows from the minimum distance 4 in C^0 that $\underline{u}_i$ and $\underline{u}_j$, $2 \le i < j \le 6$, must intersect in exactly one of the first five positions. So w.l.o.g. we have the following two cases

$$\left[\begin{array}{ccccc|cccccc} 1&1&1&1&1&0&0&0&0&0&0 \\ \hline 1&1&0&0&0&1&0&0&0&0&1 \\ 1&0&1&0&0&0&1&0&0&0&1 \\ 1&0&0&1&0&0&0&1&0&0&1 \\ 1&0&0&0&1&0&0&0&1&0&1 \\ &&&&&0&0&0&0&1&1 \end{array}\right] \text{ or } \left[\begin{array}{ccccc|cccccc} 1&1&1&1&1&0&0&0&0&0&0 \\ \hline 1&1&0&0&0&1&0&0&0&0&1 \\ 1&0&1&0&0&0&1&0&0&0&1 \\ 0&1&1&0&0&0&0&1&0&0&1 \\ &&&&&0&0&0&1&0&1 \\ &&&&&0&0&0&0&1&1 \end{array}\right]$$

In both cases it is impossible to finish the next row, so $A_5^{\ 0} = 0$. Since $A_9^{\ 0} \le \lfloor \frac{11}{2} \rfloor$ and the number of odd weight vectors in C^0 is either 32 or 0 it follows that $A_9^{\ 0} = 0$.
In other words C^0 must be an even weight code.
It follows from Lemma 2.2 and Theorem 1.4 that C^0 cannot have repeated columns, so

$$B_0^{\ 0} = 1 \quad , \quad B_1^{\ 0} = B_2^{\ 0} = 0 \ .$$

Since $A_{10}^{\ 0} \le 1$ one can find the following two solutions to the equations $k = 0,1$ and 2 in Theorem 2.5 .

	$A_0^{\ 0}$	$A_4^{\ 0}$	$A_6^{\ 0}$	$A_8^{\ 0}$	$A_{10}^{\ 0}$
α)	1	26	24	13	0
β)	1	25	27	10	1

Let uw now return to the original code C with a weight 44 codeword $\underline{c}$. In the following table one can find how many codewords in C have a certain intersection number with $\underline{c}$ resp. the complement of $\underline{c}$.

$\underline{c}$	←44→ 11 1	←11→ 00 .. 0	number of times
	0,44	0	1
	22,22	4	A_4^0
	20,24 22,22	6 6	x $A_6^0 - x$
	18,26 20,24 22,22	8 8 8	0, since $A_{34} = 0$ u $A_8^0 - u$
	16,28 18,26 20,24 22,22	10 10 10 10	p q 0, since $A_{34} = 0$ $A_{10}^0 - p - q$

If one now tries α) as weight enumerator for C^0 we get the following weight enumerator for C $A_0 = A_{44} = 1$, $A_{26} = 52 + x$, $A_{28} = 48 - 2x + u$, $A_{30} = 26 + x - 2u$, $A_{32} = u$.
From the 3rd equation in (3.5) one now finds

$$x + u = 55 + 8B_2$$

contradicting the fact that $x \le A_6^0 = 24$ and $u \le A_8^0 = 13$. Similary β) leads to the equation

$$x + u + 9p + 4q = 55 + 8B_2 ,$$

contradicting $x \le A_6^0 = 27$, $u \le A_8^0 = 10$ and

$$9p + 4q \le 9(p + q) \le 9\, A_{10}^0 = 9 .$$

Before we deal with A_{40}, we shall treat A_{38}

$\underline{A_{38} = 0}$

The residual code C^0 of C w.r.t. a weight 38 codeword has parameters (17,6,7), so can be extended to a (18,6,8) code $C^{0,ex}$. As before we shall first try to determine the weight enumerator $A_i^{\ 0}$, $0 \le i \le 17$, of C^0. Let $A_i^{\ 0,ex}$ and $B_i^{\ 0,ex}$, $0 \le i \le 18$, denote the weight enumerator of $C^{0,ex}$, resp. its dual code. If follows from Lemma 2.1 and Theorem 1.4 that $A_{10}^{\ 0,ex} = A_{14}^{\ 0,ex} = 0$.
Moreover since the sum of a weight 8 and weight 18 codeword in $C^{0,ex}$ would have weight 10, it follows that also $A_{18}^{\ 0,ex} = 0$.
Since $B_0^{\ 0,ex} = 1$ and $B_1^{\ 0,ex} = 1$ one can express the weight enumerator of $C^{0,ex}$ in terms of $B_2^{\ 0,ex}$ by means of Theorem 2.5:
$A_0^{\ 0,ex} = 1$, $A_8^{\ 0,ex} = 45 + B_2^{\ 0,ex} = 18 - 2B_2^{\ 0,ex}$, $A_{16}^{\ 0,ex} = B_2^{\ 0,ex}$.
We have two cases:
A : $B_2^{\ 0,ex} = 0$ i.e. $A_8^{\ 0,ex} = 45$, $A_{12}^{\ 0,ex} = 18$, $A_{16}^{\ 0,ex} = 0$.
According to a theorem by Assmus and Mattson ([2]) one has that the codewords of fixed weight in $C^{0,ex}$ form a 1-design. So the weight enumerators of C^0 and $C^{0,ex}$ are related by:

$$18A^{0}_{2i-1} = 2i\ A^{0,ex}_{2i} ,$$

$$A^{0}_{2i-1} + A^{0}_{2i} = A^{0,ex}_{2i} .$$

This uniquely determines the weight enumerator of C^0:
$A_0^{\ 0} = 1$, $A_7^{\ 0} = 20$ $A_8^{\ 0} = 25$ $A_{11}^{\ 0} = 12$ $A_{12}^{\ 0} = 6$ (3.6)
B : $B_2^{\ 0,ex} \neq 0$.
By Lemma 2.2 $C^{0,ex}$ has the following generator matrix

$$G^{0,ex} \quad \left(\begin{array}{cc|c} 1 & 1 & \underline{u} \\ \hline 0 & 0 & \\ \vdots & \vdots & G^1 \\ 0 & 0 & \end{array}\right) ,$$

where G^1 generates a (16,5,8) code C^1. This code C^1 is unique; it is the first order Reed-Muller code of length 16. Since $C^{0,ex}$ has miminum distance 8, it follows that $\underline{u}$ must be at distance at least 6 to C^1. However the covering radius of the first order RM code of length 16 equals 6, moreover it is known (see tabel IV in [10]) (and not difficult to check) that all possible choices of $\underline{u}$ are essentially equivalent. This means that w.l.o.g. $G^{0,ex}$ has the following form:

$$\begin{array}{|cc|cccccccccccccccc|l}
1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & x_1x_2 + x_3x_4 \\
\hline
0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & x_1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & x_2 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & x_3 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & x_4
\end{array}$$

It is not difficult to check that depending on whether one deletes one of the first 2 columns or one of the last 16, one obtains the following weight enumerators for C^0:

$$A_0^{\ 0} = 1 \quad A_7^{\ 0} = 16 \quad A_8^{\ 0} = 30 \quad A_{11}^{\ 0} = 16 \quad A_{12}^{\ 0} = 0 \quad A_{15}^{\ 0} = 0 \quad A_{16}^{\ 0} = 1 \qquad (3.7)$$

$$A_0^{\ 0} = 1 \quad A_7^{\ 0} = 21 \quad A_8^{\ 0} = 25 \quad A_{11}^{\ 0} = 10 \quad A_{12}^{\ 0} = 6 \quad A_{15}^{\ 0} = 1 \quad A_{16}^{\ 0} = 0 \qquad (3.8)$$

As befor we now return to our original code C (with a codeword $\underline{c}$ of weight 38). Again we make a table of all intersection numbers of codewords with $\underline{c}$ resp. the complement of $\underline{c}$.

$\underline{c}$

←— 38 —→ 11 1	←17→ 00 .. 0	number of times
0,38	0	1
19,19	7	$A_7^{\ 0}$
18,20	8	$A_8^{\ 0}$

15,23	11	0, since $A_{34} = 0$
17,21	11	p
19,19	11	$A_{11}^{0} - p$
14,24	12	q
16,22	12	0, since $A_{34} = 0$
18,20	12	$A_{12}^{0} - q$
11,27	15	0, since $A_{42} = 0$
13,25	15	r
15,23	15	s
17,21	15	$A_{15}^{0} - r - s$
19,19	15	0, since $A_{34} = 0$
10,28	16	0, since $A_{44} = 0$
12,26	16	0, since $A_{42} = 0$
14,24	16	t
16,22	16	$A_{16}^{0} - t$
18,20	16	0, since $A_{34} = 0$

This leads to the following weight enumerator for C:

$$A_0 = 1$$
$$A_{26} = 2A_7^0 + A_8^0 + q$$
$$A_{28} = A_8^0 + p + r$$
$$A_{30} = 2A_{11}^0 + A_{12}^0 - p - q + s + t$$
$$A_{32} = A_{12}^0 + A_{15}^0 + A_{16}^0 + p - q - r - s - t$$
$$A_{36} = A_{12}^0 + q - r - s$$
$$A_{38} = 1 + A_{16}^0 + s - t$$
$$A_{40} = r + t$$

We are now able to compute B_2 from the 3rd equation in (3.5):

$$15 + 2A_{11}^{\ 0} + 4A_{12}^{\ 0} + 13A_{15}^{\ 0} + 18A_{16}^{\ 0} + p + 6q + 8r + 3s + 4t = \qquad (3.9)$$

$$= 117 + 8B_2 .$$

Since $p \le A_{11}^{\ 0}$, $q \le A_{12}^{\ 0}$, $8r + 3s \le 8\ (r+s) \le 8A_{15}^{\ 0}$ and $t \le A_{16}^{\ 0}$, we find the following inequality:

$$3A_{11}^{\ 0} + 10A_{12}^{\ 0} + 21A_{15}^{\ 0} + 22A_{16}^{\ 0} \ge 102 + 8B_2 .$$

The weight enumerators in (3.6) and (3.7) do not satisfy this inequalty. For the weight enumerator of (3.8) we go back to the original equation (3.9) .

$$p + 6q + 8r + 3s + 4t = 45 + 8B_2 .$$

Now $p \le A_{11}^{\ 0} = 10$, $q \le A_{12}^{\ 0} = 6$, $r + s \le A_{15}^{\ 0} = 1$ and $t \le A_{16}^{\ 0} = 0$. Moreover we are in the case, where we did not shorten one of the repeated columns, i.e. $B_2 = 1$. So we have the equation

$$p + 6q + 8r + 3s = 53 ,$$

$p \le 10$, $q \le 6$, $r + s \le 1$.

It follows that $p = 9$, $q = 6$, $r = 1$ and $s = 0$, i.e.

$A_0 = 1$, $A_{26} = 73$, $A_{28} = 35$, $A_{30} = 2$, $A_{32} = 9$,

$A_{36} = 6$, $A_{38} = A_{40} = 1$

If one now computes the weight enumerator of the dual code of C by Theorem 2.5 one finds of course $B_0 = 1$, $B_1 = 0$, $B_2 = 1$, but also $B_3 = 139\frac{1}{2}$, an impossibility.

We now treat the case A_{40}, which we have omitted before.

$\underline{A_{40} = 0}$

Let C^0 be the residual code of C w.r.t. a weight 40 codeword $\underline{c}$ and let A_i^0 and B_i^0, $0 \le i \le 15$, be the weight enumerator of C^0 resp. its dual code. C^0 has parameters (15,6,6). It follows from Lemma 2.1 and Theorems 1.4 or 1.1 that $A_7^0 = A_{11}^0 = 0$. Suppose that C^0 contains a codeword $\underline{u}$ of weight 9. Let C^{00} be the residual code of C^0 w.r.t. $\underline{u}$. Then C^{00} has parameters (6,5,2). However any codeword in C^0 corresponding to a weight-2 codeword in C^{00} has weight 7 or its sum with $\underline{u}$ has weight 7, contradicting $A_7^0 = 0$. So $A_9^0 = 0$. Since $A_{13}^0 + A_{15}^0 \le 1$ and the total number of odd weight codewords in C^0 is 0 or 32 it follows that $A_{13}^0 = A_{15}^0 = 0$ i.e. C^0 is an even weight code. It follows from Lemma 2.2 and Theorem 1.4 that C^0 cannot have repeated columns so

$$B_0^0 = 1, \quad \underline{B_1}^0 = B_2^0 = 0 .$$

Since $A_{14}^0 \ne 0$ implies $A_{14}^0 = 1$ and $A_{12}^0 = 0$ the following weight enumerators are possible by Theorem 2.5 :

A_0^0	A_6^0	A_8^0	A_{10}^0	A_{12}^0	A_{14}^0
1	27	23	12	0	1
1	30	15	18	0	0
1	29	18	15	1	0
1	28	21	12	2	0
1	27	24	9	3	0
1	26	27	6	4	0
1	25	30	3	5	0
1	24	33	0	6	0

(3.10)

As before we make a list of possible innerproducts of codewords with the weight 40 codeword $\underline{c}$ resp. its complement.

c: ← 40 → 11 1	← 15 → 00 .. 0	number of times
0,40	0	1
20,20	6	A_6^0
18,22	8	p
20,20	8	$A_8^0 - p$
16,24	10	0, since $A_{34} = 0$
18,22	10	q
20,20	10	$A_{10}^0 - q$
14,26	12	0, since $A_{38} = 0$
16,24	12	r
18,22	12	0, since $A_{34} = 0$
20,20	12	$A_{12}^0 - r$
12,28	14	0, since $A_{42} = 0$
14,26	14	s
16,24	14	0, since $A_{38} = 0$
18,22	14	$A_{14}^0 - s$
20,20	14	0, since $A_{34} = 0$

This leads to the following weight enumerator for C:

$$\begin{aligned}
A_0 &= 1 \\
A_{26} &= 2A_6^0 + p \\
A_{28} &= 2A_8^0 - 2p + q + r + s \\
A_{30} &= 2A_{10}^0 + p - 2q \\
A_{32} &= 2A_{12}^0 + A_{14}^0 + q - 2r - s \\
A_{36} &= A_{14}^0 + r - s \\
A_{40} &= 1 + s
\end{aligned}$$

The 3rd equation in (3.5) now yields

$$21 + 2A_{10}^{0} + 6A_{12}^{0} + 13A_{14}^{0} + p + q + 4r + 8s = 117 + 8B_2 .$$

Since $p \le A_8^{0}$, $q \le A_{10}^{0}$, $r \le A_{12}^{0}$ and $s \le A_{14}^{0}$ one can deduce the following inequalty:

$$A_8^{0} + 3A_{10}^{0} + 10A_{12}^{0} + 21A_{14}^{0} \ge 96 + 8B_2 .$$

All weight enumerators in (3.10) contradict this inequalty.
We now come to our last case:

$\underline{A_{36} = 0}$

Let $\underline{c}_1 \in C$ be of weight 36. The residual code C^0 of C w.r.t. $\underline{c}_1$ has parameters (19,6,8). Let A_i^{0} and B_i^{0} , $0 \le i \le 19$, denote the weight enumerator of C^0, resp. its dual code. Let $\underline{c}_2 \in C$ correspond to a codeword $\underline{u}_2 \in C^0$ of weight 8. It follows from d = 26 that $\underline{c}_2$ has innerproduct 18 with $\underline{c}_1$.
The residual code C^{00} of C^0 w.r.t. $\underline{u}_2$ has parameters (11,5,4). Let $\underline{c}_3$ be a codeword in C, whose restriction $\underline{v}_3$ to C^{00} has weight 4. Then we have w.l.o.g. the following picture

	← a →	← 18−a →	← b →	← 18−b →	← c →	← 8−c →	← 4 →	← 7 →
$\underline{c}_1$	11...1	11...1	11...1	11...1	0..0	0..0	0..0	00..0
$\underline{c}_2$	11...1	11...1	00...0	00...0	1..1	1..1	0..0	00..0
$\underline{c}_3$	11...1	00...0	11...1	00...0	1..1	0..0	1..1	00..0

It follows from the minimum distance of C^0 that

$$c + 4 \ge 8 \quad \text{and} \quad (8-c) + 4 \ge 8 \quad \text{i.e. } c = 4$$

Since d = 26, we get from $\underline{c}_3$, $\underline{c}_1 + \underline{c}_3$, $\underline{c}_2 + \underline{c}_3$, $\underline{c}_1 + \underline{c}_2 + \underline{c}_3$ that:

$$\begin{aligned} a + b + 8 &\ge 26 \\ (18-a) + (18-b) + 8 &\ge 26 \\ (18-a) + b + 8 &\ge 26 \\ a + (18-b) + 8 &\ge 26 \end{aligned}$$

i.e. $a = b = 9$.

The residual code C^{000} of C^{00} w.r.t. $\underline{v}_3$ has parameters (7,4,2). Suppose that $\underline{c}_4 \in C$ has a restriction to C^{000} of weight 2. Let the innerproducts of $\underline{c}_4$ with the various sets of coordinates be as depicted below:

	← 9 →	← 9 →	← 9 →	← 9 →	← 4 →	← 4 →	← 4 →	← 7 →
$\underline{c}_1$	11..1	11..1	11..1	11..1	0000	0000	0000	00..0
$\underline{c}_2$	11..1	11..1	00..0	00..0	1111	1111	0000	00..0
$\underline{c}_3$	11..1	00..0	11..1	00..0	1111	0000	1111	00..0
$\underline{c}_4$	α	β	γ	δ	κ	λ	μ	2

It follows from the minimum distance of C^{00} that $\mu = 2$. Similarly by interchanging $\underline{c}_2$ and $\underline{c}_3$ one gets $\lambda = 2$. From the minimum distance of C^{0} it follows that $\kappa = 2$. By taking all linear combinations of $\underline{c}_1$, $\underline{c}_2$ and $\underline{c}_3$ with $\underline{c}_4$ one gets 8 inequlities, yielding the unique solution $\alpha = \beta = \gamma = \delta = 4\frac{1}{2}$.
We conclude that C^{000} has parameters (7,4,3) (in stead of (7,4,2)), which code is unique and generated by

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

The following property is a consequence of the observations made above:

Any two codewords of weight 4 in the (11,5,4) code C^{00} have an intersection of at most 1. (*)

We shall now show that this property implies that C^{00} is unique and equivalent to the code generated by

$$\left(\begin{array}{cccc|ccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) . \qquad (3.11)$$

We do know that C^{00} is generated by

$$G^{00} = \left[\begin{array}{cccc|ccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline & & & & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ & & & & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ & & & & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ & & & & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right] \begin{array}{c} \underline{v}_3 \\ \underline{v}_4 \\ \underline{v}_5 \\ \underline{v}_6 \\ \underline{v}_7 \end{array}$$

By adding $\underline{v}_3$ to $\underline{v}_i$, $i \geq 4$, if necessary, we can assume that the 4th coordinate of $\underline{v}_i$, $i \geq 4$, is zero.
We distinguish 2 possibilities:

A: Each of the weight 3 codewords in C^{000} corresponds to a weight 5 codeword in C^{00}. For $\underline{v}_4$, $\underline{v}_5$ and $\underline{v}_6$ we have w.l.o.g. three possibilities for the first four coordinates:

A'	A''	A'''
1 1 0 0	1 1 0 0	1 1 0 0
1 0 1 0	1 1 0 0	1 1 0 0
0 1 1 0	1 1 0 0	1 0 1 0

In case A' $\underline{v}_4 + \underline{v}_5 + \underline{v}_6$ has weight 3, contradicting the minimum distance of C^{00}. In case A" $\underline{v}_4 + \underline{v}_5$ and $\underline{v}_4 + \underline{v}_6$ are two codewords of weight 4 in C^{00} with innerproduct 2, contradicting (*). Case A''' leads to:

$$\left(\begin{array}{cccc|ccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ a & b & c & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) \begin{array}{c} \underline{v}_3 \\ \underline{v}_4 \\ \underline{v}_5 \\ \underline{v}_6 \\ \underline{v}_7 \end{array}$$

Since $\underline{v}_7 + \underline{v}_i$, $i = 5,6$, has weight 3, when restricted to C^{000} we have the following equations:

$$(1-a) + (1-b) + c = 2$$

$$(1-a) + b + (1-c) = 2$$

It follows that a = 0 and b = c. If b = c = 0 then $\underline{v}_4 + \underline{v}_5$ and $\underline{v}_7$ contradict (*), otherwise $\underline{v}_4 + \underline{v}_5$ and $\underline{v}_5 + \underline{v}_6 + \underline{v}_7$ contradict (*).

B: At least one codeword of weight 3 in C^{000} corresponds to a weight 4 (or 6 by adding $\underline{v}_3$ to it) codeword in C^{00}.
It follows from the transitive automorphism group of the (7,4,3) code, that w.l.o.g. $\underline{v}_4$ has this property, so one has

$$G^{00} = \left[\begin{array}{cccc|ccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ a & b & c & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ p & q & r & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ u & v & w & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right] \begin{array}{c} \underline{v}_3 \\ \underline{v}_4 \\ \underline{v}_5 \\ \underline{v}_6 \\ \underline{v}_7 \end{array}$$

Since the residual code of C^{00} w.r.t. $\underline{v}_4$ must also be a (7,4,3)-code, it follows that the three pairs (b,c), (q,r) and (u,w) must all be different and not equal to (0,0). By interchanging $\underline{v}_5$ and $\underline{v}_6$ and the coordinates 2 and 3, we can restrict ourselves to the following two possibilities:

B' :

$$G^{00} = \left[\begin{array}{cccc|ccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ a & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ p & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ u & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right] \begin{array}{c} \underline{v}_3 \\ \underline{v}_4 \\ \underline{v}_5 \\ \underline{v}_6 \\ \underline{v}_7 \end{array}$$

If a = 0 the residual code of $\underline{v}_5$ yields the information that p + u = 1. Both solutions are quivalent to the matrix in (3.11) (if p = 1 and u = 0, apply $\underline{v}_6 \rightarrow \underline{v}_6 + \underline{v}_4$, $\underline{v}_7 \rightarrow \underline{v}_7 + \underline{v}_4$ and a column permutation to get p = 0 and u = 1). Since $\underline{v}_5$ and $\underline{v}_6$ can be exchanged we have as other possibility that a = p = 1. If u = 0 then $\underline{v}_3 + .. + \underline{v}_6$ and $\underline{v}_5 + \underline{v}_6 + \underline{v}_7$ contradict (*), while if u = 1 we get a matrix equivalent to (3.11) by the transformation $\underline{v}_5 \rightarrow \underline{v}_5 + \underline{v}_7$, $\underline{v}_6 \rightarrow \underline{v}_6 + \underline{v}_7$.

B'' :

$$G^{00} = \left|\begin{array}{cccc|ccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ a & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ p & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ u & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right| \quad \begin{array}{c} \underline{v}_3 \\ \underline{v}_4 \\ \underline{v}_5 \\ \underline{v}_6 \\ \underline{v}_7 \end{array}$$

By comparing $\underline{v}_5 + \underline{v}_6 + \underline{v}_7$ with $\underline{v}_6 + \underline{v}_7$, $\underline{v}_3 + \underline{v}_5 + \underline{v}_7$ and $\underline{v}_4 + \underline{v}_5 + \underline{v}_6$ in the cases $a = 0, p = u$, resp. $a = p = 1$, $u = 0$ resp. $a = u = 1$, $p = 0$ one gets a contradiction with (*). So $a + p + u = 1$. From the row operations $\underline{v}_5 \to \underline{v}_5 + a\underline{v}_4$, $\underline{v}_6 \to (1-u)\underline{v}_4 + \underline{v}_5 + \underline{v}_6$, $\underline{v}_7 \to p\underline{v}_4 + \underline{v}_5 + \underline{v}_7$ one obtains a matrix equivalent to the matrix of (3.11).

We now turn back to C^0. Let $\underline{u}_4 \in C^0$ correspond to the unique weight 7 codeword in C^{000}. Let its innerproduct with $\underline{u}_2$ and $\underline{u}_3$ be as depicted below

$$\begin{array}{ccccccccccccccccccccccc l} 1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0 & \underline{u}_2 \\ 1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0&0 & \underline{u}_3 \\ &&a&&&&b&&&&c&&1&1&1&1&1&1&1 & \underline{u}_4 \end{array}$$

From (3.11) we now know that $c \in \{0,4\}$. By interchanging $\underline{u}_2$ and $\underline{u}_3$ one gets $b \in \{0,4\}$. By replacing $\underline{u}_2$ by $\underline{u}_2 + \underline{u}_3$ one obtains that $a \in \{0,4\}$. By adding $\underline{u}_2$ and/or $\underline{u}_3$ to $\underline{u}_4$ if necessary, one may assume that $b = c = 0$. If also $a = 0$ then $\underline{u}_4$ has weight 7, which is less than the miminum distance of C^0. On the other hand if $a = 4$ then $\underline{u}_3 + \underline{u}_4$ has weight 11, while the residual code of C^0 w.r.t. a weight 11 codeword has parameters (8,5,3), contradicting Theorem 1.4.

Now that we know that $A_i = 0$ for $i \geq 36$ one can reduce (3.5) to

$$\begin{aligned} A_{26} \qquad - A_{30} - 2A_{32} &= 18 \\ A_{28} + 2A_{30} + 3A_{32} &= 109 \\ A_{30} + 3A_{32} &= 117 + 8B_2 \end{aligned}$$

Subtracting the 3rd equation from the 2nd yields

$$A_{28} + A_{30} = -8 - 8B_2 \; ,$$

a clear contradiction.

References

[1] W.O. Alltop, Binary codes with improved minimum weights, IEEE Trans. Inform. Theory, vol. IT 22 (1976), 241-243.

[2] E.F. Assmus, Jr. and H.F. Mattson, New 5-designs, J. Combinetorial Theory, 6(1969), 122-151.

[3] L.O. Baumert and R.J. McEliece, A note on the Griesmer bound, IEEE Trans. Inform. Theory, vol. IT 19 (1973), 134-135.

[4] B.I. Belov, A conjecture on the Griesmer bound, Optimalization methods and their applications (All-Union Summer Sem., Khakusy, Lake Baikal, 1972) (Russian), 100-106, 182. Sibirsk. Energet. Inst. Sibirsk, Otdel, Akad. Nauk SSSR, Irkutsk, 1974.

[5] P.G. Farrell, An introduction to anticodes, CISM Summer School: Algebraic coding theory and applications, 1978.

[6] J.H. Griesmer, A bound for error-correcting codes, IBM J. Res. and Develop., 4 (1960), 532-542.

[7] V.W. Logačev, An improvement of the Griesmer bound in the case of small code distances, Optimization methods and their applications (All-Union Summer Sem., Khakusy, Lake Baikal, 1972) (Russian), 107-111, 182 Sibirsk. Energetic. Inst. Sibirsk. Otdel. Akad. Nauk SSSR, Irkutsk, 1974.

[8] F.J. MacWilliams and N.J.A. Sloane, The theory of error correcting codes, North Holland Mathematical Library, Vol. 16, North Holland, Amsterdam, 1977.

[9] G. Solomon and J.J. Stiffler, Algebraically punctured cyclic codes, Inform. and Control, 8 (1965), 170-179.

[10] H.C.A. van Tilborg, On weights in codes, Report 71-WSK-03, Department of Mathematics, Eindhoven University of Technology, The Netherlands.

[11] H.C.A. van Tilborg, On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound, to appear in Information and Control.