PLISKA
STUDIA MATHEMATICA BULGARICA

ПЛИСКА
БЪЛГАРСКИ МАТЕМАТИЧЕСКИ СТУДИИ

ON THE UNIQUENESS OF CERTAIN CODES MEETING THE GRIESMER BOUND

NICOLAI L. MANEV

A uniqueness (up to isomorphism) of the codes with minimum distance $d=2^{k-1}-2^{a-1}-2^{b-1}$, dimension k and which meets the Griesmer bound is proved. The integers a and b satisfy the conditions $k\geqq a+b$, $a>b>0$ and if $b=2$ then $a\geqq 4$.

1. Introduction. Linear codes over $GF(2)$ are considered. Let $n(k, d)$ denote the smallest integer n for which a binary $[n, k, d]$ code (i. e. a binary linear code with dimension k, block length n and minimum distance d) exists. Griesmer [1] proved, that

(1.1) $$n(k, d)\geqq g(k, d),$$

where

$$g(k, d)=\sum_{j=0}^{k-1} \lceil d/2^j \rceil$$

($\lceil x \rceil$ denotes the smallest integer $\geqq x$).

The $[n, k, d]$ codes with $n=g(k, d)$ will be referred to as Griesmer codes. For example, the simplex $[2^k-1, k, 2^{k-1}]$ code with generator matrix S_k (the columns of it are all distinct, nonzero binary k-types) and the Mac-Donald codes $C_{k,u}$: $[2^k-2^u, k, 2^{k-1}-2^{u-1}]$, $1\leqq u\leqq k-1$, with generator matrix

$$G_{k,u}=S_k\diagdown\left(\frac{0}{S_u}\right)$$

are Griesmer codes. (Let $A=B|C)$ be a partitioning of a matrix A. Then we shall denote C by $A\diagdown B$)

By deleting columns of S_k (or several copies of S_k) form themselves subspaces large classes of codes meeting the Griesmer bound are obtained (see Solomon and Stifler [2], Belov et al. [3], Belov [4], Helleseth and van Tilborg [5]). The most general result from the preceding ones is that of Belov:

Theorem 1.1 [4]. *Let* $s=\lceil d/2^{k-1}\rceil$ *and* $s2^{k-1}-d=\sum_{i=1}^{p} 2^{u_i-1}$, *where* $k>u_1>u_2>\dots>u_p>0$. *If*

(1.2) $$\sum_{i=1}^{\min(s+1,p)} u_i\leqq s.k$$

or

(1.3) $$u_{i+1}=u_i-1,\ i=s, s+1,\dots,p-1 \text{ and } u_p\in\{1, 2\}$$

then there exists a binary linear $[g(k, d), k, d]$ *code.*

Two codes $\mathcal{A}$ and $\mathcal{B}$ are called isomorphic (equivalent) if they differ only in the order of symbols of codewords, or more formally if there is a permutation the coordinates of vectors $\sigma: \mathcal{A} \to \mathcal{B}$.

In [6] van Tilborg proved the uniqueness of Mac-Donald codes, or more exactly:

Theorem 1.2 [6]. *Let C be a linear* $[2^k-2^u,\ k,\ 2^{k-1}-2^{u-1}]$ *code,* $1 \leq u \leq k-1$. *Then C is isomorphic to* $C_{k,u}$.

Let $\{A_i\}_{i=1}^n$ be a weight distribution of the code $\mathscr{C}$, i. e. A_i denotes the number of the codewords of weight i in $\mathscr{C}$.

Theorem 1.3 [7]. *For any* $2 \leq i \leq k-4$ *every* $[2^k-2^{k-i}-3,\ k,\ 2^{k-1}-2^{k-i-1}-2]$ *code is isomorphic the code* $\mathscr{D}_{k,k-i}$ *with a generator matrix*

$$G_{k,k-i} = S_k \setminus \left(\frac{0'}{s_{k-i}} \setminus \left(\frac{s_2}{0''}\right)\right),$$

where $2 \leq i \leq k-1$, $0'$ *and* $0''$ *are* $i \times (2^{k-i}-1)$ *and* $(k-2) \times 3$ *matrixes of noughts. The weight distribution of* $\mathscr{D}_{k,k-i}$ *is*

$$A_0 = 1,\ A_{2^{k-1}-2^{k-i-1}-2} = 3(2^{k-2}-2^{i-2}), \quad A_{2^{k-1}-2} = 3.2^{i-2},$$

$$A_{2^{k-1}-2^{k-i-1}} = 2^{k-2}-2^{i-2}, \qquad A_{2^{k-1}} = 2^{i-2}-1.$$

Theorem 1.4 [7]. *Let* $\mathscr{C}$ *be a linear* $[2^k-11,\ k,\ 2^{k-1}-6]$ *code,* $k \geq 5$. *Then* $\mathscr{C}$ *is isomorphic to* $\mathscr{D}_{k,3}$ *or to* $N_k^{(k-3)}$, *which has generator matrix*

$$G_k^{(k-3)} = \left|\begin{array}{c|c|c} 0 & \begin{matrix}0\\ \vdots\\ 0\end{matrix} & \\ \cline{1-2} \begin{matrix}1&&&\\&1&&\\&&1&\\&&&1\end{matrix} & \begin{matrix}1\\1\\1\\1\end{matrix} & S_k \setminus S_4 \end{array}\right|$$

and weight distribution $A_0 = 1;\ A_{2^{k-1}-6} = 10.2^{k-4},\ A_{2^{k-1}-4} = 5.2^{k-4};\ A_{2^{k-1}} = 2^{k-4}-1.$

The connection between weight distributions of code $\mathscr{C}$ and its dual code $\mathscr{C}^{\perp}$ denoted by $\{A_i\}_{i=1}^n$ and $\{B_i\}_{i=1}^n$, is given by the Mac-William equations [8, p. 129]. The following equations, which are equivalent to Mac-William ones will be used in the article:

$$\sum_{i=0}^{n} \binom{i-d}{m} A_i = 2^{k-m} \sum_{i=0}^{m} (-1)^i L_m(i) B_i, \tag{1.4}$$

where $L_m(x) = \sum_{\nu=0}^{m-x} (-2)^{\nu} \binom{n-x}{m-x-\nu} \binom{d+\nu-1}{\nu}$.

Definition (after van Tilborg). *Let* $\mathscr{C}$ *be a binary linear code with generator matrix G, the top row of which is c. Then the residual code of* $\mathscr{C}$ *with respect to c is the code generated by the restriction of G to the columns where c has a zero entry. We shall often denote this by* res $(\mathscr{C}; c)$, *or if only the weight w of c is relevant then by* res $(\mathscr{C}; w)$.

Lemma 1.5 [9]. *Let* $\mathscr{C}$ *be an* $[n, k, d]$ *code and* $c \in \mathscr{C}$ *with weight* $wt(c) < 2d$. *Then* res $(\mathscr{C}; c)$ *is an* $[n-wt(c),\ k-1,\ d_0]$ *code, where* $d_0 \geq d - \lfloor wt(c)/2 \rfloor$ ($\lfloor x \rfloor$ *denotes the greatest integer* $\leq x$).

Lemma 1.6 [10]. *If the code $\mathscr{C}$ achieves the Griesmer bound and it has minimum distance $d=2^m s$, where $s>0$ is an integer, then 2^m divides the weights of all codewords.*

2. A uniqueness of Griesmer code of minimum distance $d=2^{k-1}-2^{a-1}-2^{b-1}$, $k\geqq a+b$.

Lemma 2.1. *The $[2^k-2^a-2^b+1,\ k,\ 2^{k-1}-2^{a-1}-2^{b-1}]$ code $SM_k(a, b)$ with generator matrix*

$$(2.1)\qquad G_k(a, b)=S_k\diagdown\left(\frac{0'}{S_a}\right)\diagdown\left(\frac{S_b}{0''}\right),$$

where a, b are integers, $a>b>0$, $k\geqq a+b$ but $0'$ and $0''$ are matrixes of noughts, has a weight distribution:

$$(2.2)\quad A_0=1,\ A_{2^{k-1}-2^{a-1}-2^{b-1}}=2^{k-a-b}(2^a-1)(2^b-1),\ A_{2^{k-1}-2^{b-1}}=2^{k-a-b}(2^b-1),$$
$$A_{2^{k-1}-2^{a-1}}=2^{k-a-b}(2^a-1),\qquad A_{2^{k-1}}=2^{k-a-b}-1.$$

The proof of Lemma 2.1 is not difficult and we omit it (see Lemma 1 in [7]).

Theorem 2.2. *For $k\geqq a+b$ and $b\neq 2$ or $b=2$, but $a>3$ any $[2^k-2^a-2^b+1,\ k,\ 2^{k-1}-2^{a-1}-2^{b-1}]$ code is isomorphic to $SM_k(a, b)$.*

Remark. The case $b=2$, $a=3$ is the Theorem 1.4.

Proof. We argue by induction on b, the case $b=2$ being proved by Theorem 1.3 ($a=k-i$). The case $b=1$ can be proved easily basing oneself on Theorem 1.2.

Let $b>2$ and $\mathscr{C}$ be an $[2^k-2^a-2^b+1,\ k,\ 2^{k-1}-2^{a-1}-2^{b-1}]$ code. Since $\mathscr{C}$ has no repeated columns as Griesmer code then $A_j=0$ for $j>2^{k-1}$ (according to [8, Th. 28, p. 553]). Using Lemma 1.6 we obtain that any codeword has weight multiple of 2^{b-1}. We consider two cases.

1) Let $a>b+1$. Applaying the Griesmer bound to the res $(\mathscr{C};2^{k-1}-2^{a-1}+2^{b-1})$ with parametrs $[2^{k-1}-2^{a-1}-3.2^{b-1}+1,\ k-1,\ 2^{k-2}-2^{a-2}-3.2^{b-2}]$ leads up to a contradiction, because $g(k-1,\ 2^{k-2}-2^{a-2}-3.2^{b-2})=2^{k-1}-2^{a-1}-3.2^{b-1}+2>2^{k-1}-2^{a-1}-3.2^{b-1}+1$. It follows $A_{2^{k-1}-2^{a-1}+2^{b-1}}=0$. Then in the case $a=b+2$ the weight of any nonzero codeword of $\mathscr{C}$ is some of

$$(2.3)\qquad 2^{k-1}-2^{a-1}-2^{b-1};\ 2^{k-1}-2^{a-1};\ 2^{k-1}-2^b;\ 2^{k-1}-2^{b-1};\ 2^{k-1}.$$

We shall show that the preceding is held in the case $a>b+2$, too. Let v be codeword of $wt(v)=2^{k-1}-2^{b-1}x$, $3\leqq x\leqq 2^{a-b-1}+1$. Then res $(\mathscr{C};wt(v))$ is an $[2^{k-1}-2^a+2^{b-1}.\ \delta+1,\ k-1,\ 2^{k-2}-2^{a-1}+2^{b-2}.\ \delta]$ code, where $\delta=x-2$, $1\leqq\delta\leqq 2^{a-b-1}-1$. From

$$g(k-1,\ 2^{k-2}-2^{a-1}+2^{b-2}.\ \delta)=\sum_{j=0}^{a-1}\lceil(2^{k-2}-2^{a-1}+2^{b-2}\ \delta)/2^j\rceil$$
$$+\sum_{j=a}^{k-2}\lceil 2^{k-2-j}-(2^{a-1}-2^{b-2}.\ \delta)/2^j\rceil=2^{k-1}-2^a+2^{b-1}\ \delta+2-\delta$$
$$+\sum_{\nu=1}^{a-b-1}\lceil\delta/2^\nu\rceil\geqq 2^{k-1}-2^a+2^{b-1}.\ \delta+2-\delta/2^{a-b-1}$$

and since $g(k-1,\ 2^{k-2}-2^{a-1}+2^{b-2}\ \delta)$ is integer and $0<\delta/2^{a-b-1}<1$, it follows

$$g(k-1,\ 2^{k-2}-2^{a-1}+2^{b-2}\ \delta)\geqq 2^{k-1}-2^a+2^{b-1}\ \delta+2.$$

But it contradicts to (1.1). Therefore

(2.4) $$A_{2^{k-1}-2^{b-1}x}=0 \text{ for } 3\leqq x\leqq 2^{a-b-1}+1.$$

Let us consider the residual code $\mathscr{C}^0(x)=\text{res}(\mathscr{C};2^{k-1}-2^{a-1}-2^{b-1})$. It is a $[2^{k-1}-2^{a-1}-2^{b-1}+1, k-1, 2^{k-2}-2^{a-2}-2^{b-2}]$ code. Since $k-1>(a-1)+(b-1)$ and $a-1>(b-1)+1\geqq 3$ the code $\mathscr{C}^0$ satisfies the theoremś condition, but for $b:=b-1$. We can apply the induction hypothesis and then $\mathscr{C}^0\cong SM_{k-1}(a-1, b-1)$. Therefore, if $\{A_i^0\}$ is the weight distribution of $\mathscr{C}^0$, then

(2.5) $$A_0^0=1,\quad A^0_{2^{k-2}-2^{a-2}-2^{b-2}}=2^{k-a-b+1}(2^{a-1}-1)(2^{b-1}-1),\quad A^0_{2^{k-2}-2^{b-2}}$$
$$=2^{k-a-b+1}(2^{b-1}-1),\ A^0_{2^{k-2}-2^{a-2}}=2^{k-a-b+1}(2^{a-1}-1),\ A^0_{2^{k-2}}=2^{k-a-b+1}-1.$$

Without loss of generality the codewords of $\mathscr{C}$ form the following matrix (up to isomorphic)

$\leftarrow wt(u)\rightarrow$	
$u: 111\ldots 11$	$000\ldots 00$
$v:\ \ v^1$	v^0
— — — — — —	— $\mathscr{C}^0$ — —
$w:\ \ w^1$	w^0

where $wt(u)=2^{k-1}-2^{a-1}-2^{b-1}$ is a minimum weight of $\mathscr{C}$ codewords $v=(v^1\,|\,v^0)$ with $wt(v^0)=\{2^{k-2}-2^{a-2}-2^{b-2};\ 2^{k-2}-2^{b-2}\}$; codewords $w=(w^1|\,w^0)$ with $wt(w)=\{2^{k-2}-2^{b-2};\ 2^{k-2}\}$.

Evidently, for any vector $v^0\in\mathscr{C}^0$ there are exactly two codewords of $\mathscr{C}$ ($v=(v^1\,|\,v^0)$ and $u+v$), which restrictions on $\mathscr{C}^0$ are v^0. Also

(2.6) $$wt(u)\leqq wt(v)\leqq 2wt(v^0),$$
$$wt(u+v)=wt(u)-wt(v)+2wt(v^0),$$

since $wt(u+v)=wt(u)-wt(v^1)+wt(v^0)$.

Therefore,

for $wt(v^0)=2^{k-2}-2^{a-2}-2^{b-2}$ it is held $wt(v)=wt(u+v)=2^{k-1}-2^{a-1}-2^{b-1}$;

for $wt(v^0)=2^{k-2}-2^{a-2}$ it is held $wt(v)=2^{k-1}-2^{a-1}-2^{b-1}$, $wt(u+v)=2^{k-1}-2^{a-1}$

for $wt(w^0)=2^{k-2}-2^{b-2}$ it is held $wt(w)=2^{k-1}-2^{b-1}x$, $wt(u+v)=2^{k-1}-2^{b-1}(2^{a-b}-x+2)$;

for $wt(w^0)=2^{k-2}$ it is held $wt(w)=2^{k-1}-2^{b-1}x$, $wt(u+v)=2^{k-1}-2^{b-1}(2^{a-b}-x+1)$.

Then using (2.4) we obtain $A_{2^{k-1}-2^{b-1}x}=0$, for $2^{a-b-1}+2\leqq x\leqq 2^{a-b}-2$. Therefore

(2.7) $$A_{2^{k-1}-2^{b-1}x}=0 \text{ for } 3\leqq x\leqq 2^{a-b}-2,$$

i. e. (2.3) gives the possible nonzero weights of $\mathscr{C}$ for $a>b+2$, too,

Let $wt(w)=\{2^{k-1}-2^b;\ 2^{k-1}-2^{b-1};\ 2^{k-1}\}$. Then $wt(w^0)=\{2^{k-2}-2^{b-2}$, or $2^{k-2}\}$ by (2.6). Hence

(2.8) $$A_{2^{k-1}-2^b}+A_{2^{k-1}-2^{b-1}}+A_{2^{k-1}}=A^0_{2^{k-2}-2^{b-2}}+A^0_{2^{k-2}}=2^{k-a}-1.$$

Also, if A_1 and A_2 denote the number of codewords $w \in \mathscr{C}$ of weight $2^{k-1}-2^{a-1}-2^{b-1}$ and respectively $2^{k-1}-2^{a-1}$ with $wt(w^0)=\{0;\ 2^{k-1}-2^{b-2}$ or $2^{k-2}\}$ then

$$(2.9)\qquad \begin{aligned} A_1 &= A_{2^{k-1}-2^{a-1}-2^{b-1}} - 2A^0_{2^{k-2}-2^{a-2}-2^{b-2}} + 1 = A_{2^{k-1}-2^{a-1}-2^{b-1}} \\ &\quad -2^{k-a-b+1}(2^{a-1}-1)(2^b-1)+1, \\ A_2 &= A_{2^{k-1}-2^{a-1}} - A^0_{2^{k-2}-2^{a-2}} = A_{2^{k-1}-2^{a-1}} - 2^{k-a-b+1}(2^{a-1}-1). \end{aligned}$$

Let $u*v$ denote the intersection of binary vectors u and v, i. e. vector $u*v=(u_1 v_1, \ldots, u_n v_n)$ which has 1's only where both u and v do. One can easily prove the following

$$(2.10)\qquad wt(u*v)=[wt(u)+wt(v)-wt(u+v)]/2 \geqq wt(u)+wt(v)-n,$$

where n is the code's block length. The code $\mathscr{C}$ as Griesmer code has no repeated columns and thus $wt(u*v) \leqq 2^{k-2}$, for any $u, v \in \mathscr{C}$. Then for $wt(u)=wt(v)=2^{k-1}$ the equalities $wt(u*v)=2^{k-2}$, $wt(u+v)=2^{k-1}$ are held, i. e. the codewords of weight 2^{k-1} form a subspace. Thus

$$(2.11)\qquad A_{2^{k-1}}=2^{\beta}-1, \quad \text{where } \beta \geqq 0 \text{ is integer.}$$

Also, if $wt(u)=wt(v)=2^{k-1}-2^{b-1}$ and $wt(u+v)<2^{k-1}-2^b$, then $wt(u*v)>2^{k-2}$ by (2.10). But it is impossible. If $wt(u+v)=2^{k-1}-2^b$, then $wt(u*v)=2^{k-2}$ and res $(\mathscr{C};u)$ with parameters $[2^{k-1}-2^a-2^{b-1}+1,\ k-1,\ 2^{k-2}-2^{a-1}-2^{b-2}]$ has codeword of weight $2^{k-2}-2^{b-1}$, which is impossible by induction hypothesis, too. Therefore $wt(u+v)=\{2^{k-1}-2^{b-1}$ or $2^{k-1}\}$, for $wt(u)=wt(v)=2^{k-1}-2^{b-1}$. Similarly, if $wt(u)=2^{k-1}$ and $wt(v)=2^{k-1}-2^{b-1}$, then $wt(u+v)=\{2^{k-1}-2^{b-1}$ or $2^{k-1}\}$. So, we obtain the codewords of weights 2^{k-1} and $2^{k-1}-2^{b-1}$ form a subspace, i. e.

$$(2.12)\qquad A_{2^{k-1}-2^{b-1}}+A_{2^{k-1}}=2^{\alpha}-1, \quad \text{where } k-a \geqq \alpha \geqq \beta \geqq 0.$$

Since code $\mathscr{C}$ meets the Griesmer bound, then $B_1=B_2=0$ (by [8, Th. 28, p. 553]) and the equations (1.4) gives

$$\begin{aligned} &A_{2^{k-1}-2^{a-1}-2^{b-1}}+A_{2^{k-1}-2^{a-1}}+A_{2^{k-1}-2^b}+A_{2^{k-1}-2^{b-1}}+A_{2^{k-1}}=2^k-1, \\ &A_{2^{k-1}-2^{a-1}}+(2^{a-b}-1)A_{2^{k-1}-2^b}+2^{a-b}A_{2^{k-1}-2^{b-1}}+(2^{a-b}+1)A_{2^{k-1}} \\ &\qquad =2^{k-b+1}-2^{a-b}-1, \\ &(2^{2a-2b-1}-3.2^{a-b-1}+1)A_{2^{k-1}-2^b}+(2^{2a-2b-1}-2^{a-b-1})A_{2^{k-1}-2^{b-1}} \\ &\quad +(2^{2a-2b-1}+2^{a-b-1})A_{2^{k-1}}=2^{a-b-1}(2^{k-b}-2^{a-b}-2^{k-a}+2^{k-a-b+1}-1). \end{aligned}$$

Using (2.8) and (2.9), we obtain

$$(2.13)\qquad \begin{aligned} &A_{2^{k-1}-2^b}+A_{2^{k-1}-2^{b-1}}+A_{2^{k-1}}=2^{k-a}-1, \\ &A_1+A_2=2^{k-a}, \\ &A_2-A_{2^{k-1}-2^b}+A_{2^{k-1}}=2^{k-a-b+1}, \\ &(1/2^{a-b}-1)A_{2^{k-1}-2^b}+A_{2^{k-1}}=2^{k-a-b}-1. \end{aligned}$$

Suppose $A_{2^{k-1}-2^b} \neq 0$. Then $A_{2^{k-1}-2^b} = 2^{k-a} - 2^\alpha$ and $k-a-1 \geq \alpha \geq \beta \geq k-a-b+1$ by third equation of (2.13) and (2.12). Also, the preceding equation gives

$$2^{k-2b}(2^{\beta-k+a+b}-1) = 2^\alpha(2^{a-b}-1)(2^{k-a-\alpha}-1).$$

Hence, $\alpha = k-2b$ and $2^{\beta-k+a+b}-1 = (2^{a-b}-1)(2^{k-a-\alpha}-1)$. But $(2^{a-b}-1)(2^{k-a-\alpha}-1) \equiv 1 \pmod 2$ and the preceding equality is possible if and only if $\beta - k+a+b = 1$, i. e. $2^{a-b}-1 = 1$. But then $a = b+1$, which contradicts to $a > b+1$. Therefore, $A_{2^{k-1}-2^b} = 0$. Then the equations (2.13) lead up to the weight distribution (2.2).

2) Let $a = b+1$. Then $\mathscr{C}$ is an $[2^k-3,\ 2^b+1,\ k,\ 2^{k-1}-3.2^{b-1}]$ code and has exactly four nonzero weights (by Lemma 1.6): $2^{k-1}-2^b-2^{b-1}$; $2^{k-1}-2^b$; $2^{k-1}-2^{b-1}$; 2^{k-1}. Using (1.4), we obtain

$$
\begin{aligned}
&A_{2^{k-1}-3.2^{b-1}} + A_{2^{k-1}-2^b} + A_{2^{k-1}-2^{b-1}} + A_{2^{k-1}} - 2^k - 1,\\
(2.14)\qquad &A_{2^{k-1}-2^b} + 2A_{2^{k-1}-2^{b-1}} + 3A_{2^{k-1}} = 2^{k-a} - 3,\\
&A_{2^{k-1}-2^{b-1}} + 3A_{2^{k-1}} = 2^{k-2b}(2^{b-1}+1) - 3.
\end{aligned}
$$

As in the case 1), we prove that the codewords of weight 2^{k-1} and respectively 2^{k-1} and $2^{k-1}-2^{b-1}$ form themselves a subspace, i. e.

$$A_{2^{k-1}} = 2^\beta - 1,\quad A_{2^{k-1}} + A_{2^{k-1}-2^{b-1}} = 2^\alpha - 1,\quad k \geq \alpha \geq \beta.$$

Then the third equation of (2.14) leads up to

$$2^\alpha + 2^{\beta+1} = 2^{k-b-1} + 2^{k-2b}.$$

There are two cases:

The first, $\alpha = k-2b$ and $\beta = k-b-2$. Then $k-2b \geq k-b-2$, i. e. $b \leq 2$. It contradicts to assumption $b > 2$.

The second, $\alpha = k-b-1$, $\beta = k-2b-1$. Then

$$A_0 = 1,\quad A_{2^{k-1}} = 2^{k-a-b}-1,\quad A_{2^{k-1}-2^b} = 2^{k-a-b}(2^a-1),$$

$$A_{2^{k-1}-2^{b-1}} = 2^{k-a-b}(2^b-1),\quad A_{2^{k-1}-3.2^{b-1}} = 2^{k-a-b}(2^b-1)(2^a-1),$$

which is exactly equality (2.2).

Therefore we have already showed that every $[2^k-2^a-2^b+1,\ k,\ 2^{k-1}-2^{a-1}-2^{b-1}]$ code $\mathscr{C}$ has a weight distribution (2.2). Now we shall prove that $G_k(a;b)$ is generator matrix of $\mathscr{C}$.

Let $u \in \mathscr{C}$, $wt(u) = 2^{k-1}-2^{b-1}$. By induction hypothesis the res $(\mathscr{C}; u)$ has generator matrix

$$G_{k-1}(a;b-1) = S_{k-1} \diagdown \begin{pmatrix} O' \\ S_a \end{pmatrix} \diagdown \begin{pmatrix} S_{b-1} \\ O'' \end{pmatrix} = \begin{pmatrix} wt = 2^{k-2}-2^{b-2} \\ \hline wt = 2^{k-2} \\ \hline wt = 2^{k-2}-2^{a-1} \end{pmatrix} \begin{matrix} \}\ b-1 \text{ rows} \\ \}\ k-a-b \text{ rows} \\ \}\ a \text{ rows} \end{matrix}$$

Then without loss of generality $\mathscr{C}$ has generator matrix

$$G=\left(\begin{array}{c|c}
\longleftarrow 2^{k-1}-2^{b-1}\longrightarrow & \\
1\ 1\ 1 \ldots 1\ 1 & 0\ 0\ 0 \ldots 0\ 0 \\
\hline
wt(v^1)=2^{k-2}-2^{b-2} & wt(v^0)=2^{k-2}-2^{b-2} \\
\hdashline
wt(v^1)=2^{k-2} & wt(v^0)=2^{k-2} \\
\cdashline{2-2}
 & wt(v^0)=2^{k-2}-2^{a-1}
\end{array}\right)
\begin{array}{l} \\ \\ \}\ b-1 \text{ rows} \\ \\ \}\ a \quad \text{rows} \end{array}$$

Since $\mathscr{C}$ has no repeated columns then $wt\ (v^1)=2^{k-2}-x$, where $v=(v^1\,|\,v^0)\in\mathscr{C}$ and x is integer ≥ 0. The weight distribution of $\mathscr{C}$ shows that $wt\,(v^1)=2^{k-2}-2^{b-2}$, for $wt\,(v^0)=2^{k-2}-2^{b-2}$ and $wt\ (v^1)=2^{k-2}$ (after adding u to v, if $wt\,(v^1)=2^{k-2}-2^{b-1}$), for $wt\,(v^0)=\{2^{k-2}$ or $2^{k-2}-2^{a-1}\}$.

Let $v, w\in\mathscr{C}$. Using (2.10), we obtain that if $wt\,(v^1)=wt\,(w^1)=2^{k-2}$ then $wt\,(v^1+w^1)=2^{k-2}$, and if $wt\,(v^1)=2^{k-2}$, $wt\,(w^1)=2^{k-2}-2^{b-2}$, then $wt\,(v^1+w^1)=2^{k-2}-2^{b-2}$. Therefore, the matrix A (formed by first $2^{k-1}-2^{b-1}$ columns and the last $k-1$ rows) generate a $[2^{k-1}-2^{b-1},\ k-1,\ 2^{k-2}-2^{b-2}]$ Mac-Donald code, i. e., according Theorem 1.2, we can regard the matrix A as $S_k\diagdown\left(\frac{S_{b-1}}{0}\right)$ (after permuting the colomns). But then

$$G\equiv S_k\diagdown\left(\frac{S_b}{0'}\right)\diagdown\left(\frac{0''}{S_a}\right)\equiv G_k(a\,;b).$$

The theorem is proved.

Acknowledgements are due to S. M. Dodunekov for setting the problem and for his encouragement throughout this work.

REFERENCES

1. J. H. Griesmer. A bound for error-correcting codes. *IBM J. Res. Develop.*, **4**. 1960, 532—542.
2. G. Solomon, J. Stiffler. Algebraically punctured cyclic codes. *Inf. and Control*, **8**, 1965, 170—179.
3. B. Belov, V. Logachev, V. Sandimirov. Constructing class linear binary codes, which meet the Griesmer bound. *Problems Inform. Transmission*, **10**, 1974, No 3, 36—44.
4. B. Belov. A conjecture on the Griesmer bound. Optimization methods their applications. *All-Union Summer Sem.*, 1974, 100—106.
5. T. Helleseth, H. C. A. van Tilborg. A new class of codes meeting the Griesmer bound. *IEEE Trans. Inf. Theory*. IT-27, 1981, No 5, 548—555.
6. H. C. A. van Tilborg. On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound. *Inf. and Control*, **44**, 1980, No 1, 16—35.
7. S. Dodunekov, N. Manev. A characterization of two classes of codes meeting the Griesmer bonud. *Problems Inform. Transmission*, **19**, 1983, No 4, 3—10.
8. F. J. Mac Williams, N. J. A. Sloane. The Theory of Error-Correcting Codes. *North Holland Math. Library*, **16**, 1977, Amsterdam.
9. H. C. A. van Tilborg. The smallest length of binary 7-dimensional linear codes with prescribed minimum distance. *Discrete Math.*, **33**, 1981, No 2, 197—207.
10. S. Dodunekov, N. Manev. Minimal possible block length of a linear binary code for some minimum distances. *Problems Inform. Transmission*, **20**, 1984, No 1, 12—18.

Centre for Mathematics and Mechanics
1090 Sofia P. O. Box 373

Received 5. 8. 1982