Bulletin of Fukuoka University of Education, Vol. 33, Part III, 9-16 (1983)

Generalization of a Griesmer's Result with Respect to Construction of Optimal Linear Codes

Noboru HAMADA and Fumikazu TAMARI
Department of Mathematics, Osaka Women's University
and
Department of Mathematics, Fukuoka University of Education
(Received August 31, 1983)

Abstract

Griesmer [6] gave two methods (cf. (i) and (ii) of Theorem 5 in his paper) of constructing $(n, k, d; 2)$-codes which achieve the Griesmer's lower bound for some given integers k and d. Theorem 5-(ii) due to Griesmer [6] was generalized by many authors. The purpose of this note is to generalize Theorem 5-(i) for binary codes to s-ary codes using a flat in a finite projective geometry and a t-linearly independent set where s is a prime or prime power.

1. Introduction

Let $V(n; s)$ be an n-dimensional vector space (consisting of column vectors) over a Galois field $GF(s)$ of order s where n is a positive integer and s is a prime or prime power. A k-dimensional subspace C of $V(n; s)$ is said to be an $(n, k, d; s)$-code (or an s-ary linear code with code length n, k information symbols and the minimum distance (Hamming distance) d if the minimum distance of the code C is equal to d. In this paper, we shall consider the following problem:

PROBLEM A. Find a liner code C whose code length n is minimum among $(n, k, d; s)$-codes for given integers k, d and s.

A lower bound for the code length n of Problem A was given by Griesmer [6] for the case $s=2$ and by Solomon and Stiffler [17] for the general case. Hence in order to obtain a solution of Problem A for given integers k, d and s, it is sufficient to obtain an $(n, k, d; s)$-code which achieves the Griesmer's lower bound (in the case $s=2$) or the Solomon-Stiffler's lower bound (in the general case) for given integers k, d and s in the case where there exists such a code.

Griesmer [6] gave two methods (cf. (i) and (ii) of Theorem 5 in his paper) of constructing $(n, k, d; 2)$-codes which achieved the Griesmer's lower bound for some given integers k and d. Theorem 5-(ii) due to Griesmer [6] was generalized by many authors (cf. Solomon and Stiffler [17], Baumert and McEliece [1], Belov [2], Hamada and Tamari [10-12] and so on). The purpose of this note is to generalize Theorem 5-(i) for binary codes to s-ary codes.

2. Preliminary results

It is well known (cf. Appendix) that there are v_k points and v_k hyperplanes in a finite projective geometry $PG(k-1, s)$ of $k-1$ dimensions where $k \geqq 3$ and $v_k=(s^k-1)/(s-1)$. After numbering v_k points and v_k hyperplanes in $PG(k-1, s)$, respectively, in some way, we shall denote v_k points and v_k hyperplanes in $PG(k-1, s)$ by Q_j $(j=1, 2,..., v_k)$ and H_i $(i=1, 2,..., v_k)$, respectively. Let

$$N=\|n_{ij}\| \qquad (i=1, 2,..., v_k, j=1, 2,..., v_k)$$

be the incidence matrix of v_k hyperplanes H_i $(i=1, 2,..., v_k)$ in $PG(k-1, s)$ and v_k points Q_j $(j=1, 2,..., v_k)$ in $PG(k-1, s)$ where

$$n_{ij}=\begin{cases} 1, & \text{if the } i\text{th hyperplane } H_i \text{ contains the } j\text{th point } Q_j, \\ 0, & \text{otherwise.} \end{cases}$$

Hamada and Tamari [11] have shown that Problem A is equivalent to the following linear programming, that is, there is a one-to-one correspondence between solutions (i.e., linear codes) of Problem A and solutions (i.e., vectors) of Problem B (cf. McCluskey [14] and Griesmer [6] for the case $s=2$).

PROBLEM B. Find a vector $\boldsymbol{x}^T=(x_1, x_2,..., x_{v_k})$ of nonnegative integers x_j $(j=1, 2,..., v_k)$ that minimizes $n=\sum_{j=1}^{v_k} x_j$ subject to the following inequality:

$$\sum_{j=1}^{v_k} (1-n_{ij})x_j \geqq d \qquad (i=1, 2,..., v_k) \tag{2.1}$$

for given integers k, d and s.

Any positive integer d can be expressed uniquely as follows:

$$d=1+\theta_0+\theta_1 s+\theta_2 s^2+\cdots+\theta_{k-1}s^{k-1}, \tag{2.2}$$

using given integers k and s where θ_i's are integers such that $0 \leqq \theta_i \leqq s-1$ for $i=0, 1,..., k-2$ and $\theta_{k-1} \geqq 0$. Using integers θ_i's in (2.2), the lower bound for the code length n obtained by Griesmer [6] and Solomon and Stiffler [17] can be also expressed as follows (cf. Hamada and Tamari [11]).

THEOREM 2.1. *If d is expressed by* (2.2), *then*

$$\sum_{j=1}^{v_k} x_j \geqq k+\theta_0 v_1+\theta_1 v_2+\cdots+\theta_{k-1}v_k \tag{2.3}$$

for any vector $\boldsymbol{x}$ of nonnegative integers x_j $(j=1, 2,..., v_k)$ which satisfy condition (2.1) *where $v_i=(s^i-1)/(s-1)$ for $i=1, 2,..., k$ and $n=\sum_{j=1}^{v_k} x_j$.*

Hence in order to obtain a solution of Problem A for given integers k, d and s, it is sufficient to obtain a vector $\boldsymbol{x}$ of nonnegative integers x_j $(j=1, 2,..., v_k)$ which satisfy condition (2.1) and achieves the lower bound (2.3) in the case where there exists such a vector $\boldsymbol{x}$.

3. Generalization of Theorem 5-(i) due to Griesmer

Let k be any given integer such that $k\geqq 3$ and let s be any given prime or prime power. In this section, we shall denote v_k points in $PG(k-1, s)$ by $\boldsymbol{c}_j$ $(j=1, 2,..., v_k)$ instead of Q_j $(j=1, 2,..., v_k)$ in Section 2 where $\{\boldsymbol{c}_1, \boldsymbol{c}_2,..., \boldsymbol{c}_{v_k}\}(\equiv C(k, s))$ is a set of v_k nonzero vectors in $V(k; s)$ given by (A.1) in Appendix. Let

$$W_r=\{\boldsymbol{c}: B_r\boldsymbol{c}=\boldsymbol{0} \text{ over } GF(s),\ \boldsymbol{c}\in C(k, s)\} \tag{3.1}$$

for $r=2, 3,..., k-1$ and let $W_k=C(k, s)$ where $B_r=[O_{k-r,r}: I_{k-r}]$, $O_{m,r}$ is an $m\times r$ zero matrix and I_m is an $m\times m$ unit matrix. Then W_r is a $(r-1)$-flat in $PG(k-1, s)$ consisting of v_r vectors $\boldsymbol{c}$, $\boldsymbol{c}^T=(c_1, c_2,..., c_k)$, in $C(k, s)$ such that $c_{r+1}=c_{r+2}=\cdots=c_k=0$.

A collection, $S=\{\boldsymbol{d}_1, \boldsymbol{d}_2,..., \boldsymbol{d}_m\}$, of m vectors in $V(r; s)$ is said to be a t-linearly independent set or an $L_t(r, s)$-set with length m if no t vectors of them are linearly dependent over $GF(s)$, where $2\leqq t\leqq \min\{r, m\}$. An $L_t(r, s)$-set with length m is maximal if there exists no other $L_t(r, s)$-set with length $m'>m$. The length m of the maximal $L_t(r, s)$-set is denoted by $M_t(r, s)$. (cf. Hamada and Tamari [9]).

It is well known that in the special case $t=r$, $r+1\leqq M_r(r, s)\leqq r+s-1$ for any integers r and s. Hence there exists an $L_r(r, s)$-set with length m if $r+1\leqq m\leqq M_r(r, s)$. Let r and m be any integers such that $2\leqq r\leqq k$ and $r+1\leqq m\leqq M_r(r, s)$ and let $S=\{\boldsymbol{d}_1, \boldsymbol{d}_2,..., \boldsymbol{d}_m\}$ be an $L_r(r, s)$-set with length m. Then there exists a unique vector $\boldsymbol{e}_i$, $\boldsymbol{e}_i^T=(e_{i1}, e_{i2},..., e_{ik})$, in $C(k, s)$ for each integer i such that (a) $e_{i,r+1}=e_{i,r+2}=\cdots=e_{ik}=0$ and (b) $\boldsymbol{e}_i^T\sim(\boldsymbol{d}_i^T, 0, 0,..., 0)$ where $\boldsymbol{a}\sim\boldsymbol{b}$ means that there exists some nonzero element σ in $GF(s)$ such that $\boldsymbol{a}=\sigma\boldsymbol{b}$. Let

$$E_{r,m}=\{\boldsymbol{e}_1, \boldsymbol{e}_2,..., \boldsymbol{e}_m\} \tag{3.2}$$

for given integers r and m. Then $E_{r,m}\subset W_r$. The following theorem is a generalization of the Griesmer's result in the case $s=2$ (cf. Theorem 5-(i) in his paper).

THEOREM 3.1. *Let k be any integer such that $k\geqq 3$ and let s be any prime or prime power. If d is an integer which can be expressed as follows*:

$$d=1+\theta_0+\sum_{l=r-1}^{k-2}(s-1)s^l+\theta_{k-1}s^{k-1} \tag{3.3}$$

using some integers r, θ_0 and θ_{k-1} such that

$$2\leqq r\leqq k,\ 0\leqq\theta_0\leqq M_r(r, s)-r \quad \textit{and} \quad \theta_{k-1}\geqq 0, \tag{3.4}$$

then the vector $\boldsymbol{x}$ *whose jth component* $(1 \leqq j \leqq v_k)$ *is given by*

$$x_j = \begin{cases} \theta_{k-1}, & \text{if } \boldsymbol{c}_j \in W_r - E_{r,r+\theta_0}, \\ \theta_{k-1}+1, & \text{otherwise} \end{cases} \tag{3.5}$$

is a solution of Problem B for given integers k, d and s, where W_r *and* $E_{r,m}$ *are sets given by* (3.1) *and* (3.2), *respectively.*

REMARK. In the special case $r=k$, (3.3) means that

$$d = 1+\theta_0+\theta_{k-1}s^{k-1} \tag{3.3'}$$

and W_k is a set of all vectors in $C(k, s)$.

PROOF. Since $|W_r - E_{r,r+\theta_0}| = v_r-(r+\theta_0)$, it follows from (3.5) and $v_i=(s^i-1)/(s-1)$ for $i=1, 2,\ldots, k$ that

$$\begin{aligned} \sum_{j=1}^{v_k} x_j &= v_k(\theta_{k-1}+1)-\{v_r-(r+\theta_0)\} \\ &= k+\theta_0 v_1+\sum_{i=r}^{k-1}(s-1)v_i+\theta_{k-1}v_k, \end{aligned} \tag{3.6}$$

which shows that the x_j's given by (3.5) achieve the lower bound (2.3). Since the x_j's given by (3.5) are nonnegative integers, it is sufficient to show that those integers satisfy condition (2.1).

Let H_i $(i=1, 2,\ldots, v_k)$ be v_k hyperplanes in $PG(k-1, s)$ given by (A.3) in Appendix and let us denote $\boldsymbol{h}_i$ by

$$\boldsymbol{h}_i^T = (h_{i1}, h_{i2},\ldots, h_{ik}) \tag{3.7}$$

for $i=1, 2,\ldots, v_k$.

(i) In the case where i is an integer such that $(h_{i1}, h_{i2},\ldots, h_{ir})=(0, 0,\ldots, 0)$, it follows from (3.1) that $\boldsymbol{h}_i^T\boldsymbol{c}_j=0$ over $GF(s)$ (i.e., $n_{ij}=1$) for any vector $\boldsymbol{c}_j$ in W_r. Hence we have

$$\sum_{j=1}^{v_k}(1-n_{ij})x_j = \sum_{j=1}^{v_k}(1-n_{ij})(\theta_{k-1}+1) = s^{k-1}+\theta_{k-1}s^{k-1} \geqq d$$

because

$$\sum_{j=1}^{v_k}(1-n_{ij}) = v_k - v_{k-1} = s^{k-1}. \tag{3.8}$$

Hence condition (2.1) holds in this case.

(ii) In the case where i is an integer such that $(h_{i1}, h_{i2},\ldots, h_{ir}) \neq (0, 0,\ldots, 0)$, there are (v_k-v_{k-1}) vectors $\boldsymbol{c}_j$ in $C(k, s)$ such that $\boldsymbol{h}_i^T\boldsymbol{c}_j \neq 0$ over $GF(s)$ (*i.e.*, $n_{ij}=0$) and there are (v_r-v_{r-1}) vectors $\boldsymbol{c}_j$ in W_r such that $\boldsymbol{h}_i^T\boldsymbol{c}_j \neq 0$ over $GF(s)$. Hence there are $(s^{k-1}-s^{r-1})$ vectors $\boldsymbol{c}_j$ in $C(k, s)-W_r$ such that $\boldsymbol{h}_i^T\boldsymbol{c}_j \neq 0$ over $GF(s)$. Since

$$\sum_{l=r-1}^{k-2}(s-1)s^l=s^{k-1}-s^{r-1},$$

it follows from (3.5) and (3.8) that

$$\sum_{j=1}^{v_k}(1-n_{ij})x_j=\theta_{k-1}s^{k-1}+\{z_i+\sum_{l=r-1}^{k-2}(s-1)s^l\} \tag{3.9}$$

where z_i denotes the number of vectors $\boldsymbol{c}$ in $E_{r,r+\theta_0}$ such that $\boldsymbol{h}_i^T\boldsymbol{c}\neq 0$ over $GF(s)$. Hence it is sufficient to show that $z_i\geqq\theta_0+1$ in order to show that condition (2.1) holds.

Since any r vectors in $E_{r,r+\theta_0}$ are linearly independent over $GF(s)$, there are at most $r-1$ vectors $\boldsymbol{c}$ in $E_{r,r+\theta_0}$ such that $\boldsymbol{h}_i^T\boldsymbol{c}=0$ over $GF(s)$. This implies that $z_i\geqq(r+\theta_0)-(r-1)=\theta_0+1$. This completes the proof.

From Theorem 2.1 due to Hamada and Tamari [11], we have

THEOREM 3.2. *For any integers k, d and s which satisfy conditions in Theorem* 3.1, *there exists an $(n, k, d; s)$-code which achieves the Solomon-Stiffler's lower bound.*

Since $M_r(r, s)\geqq r+1$ for any integers r and s, we have

COROLLARY 3.3. *In the case $\theta_0=0$ or* 1, *there exists an $(n, k, d; s)$-code which achieves the Solomon-Stiffler's lower bound if d can be expressed as* (3.3) *using some integers r, k, s and θ_{k-1} such that $2\leqq r\leqq k$ and $\theta_{k-1}\geqq 0$.*

In the special case $s=2$, Corollary 3.3 coincides with Theorem 5-(i) due to Griesmer [6]. (cf. Theorem 7.1 of Hamada and Tamari [10])

EXAMPLE 3.1. In the special case $r=2$, it follows that $M_2(2, s)=s+1$. Hence condition (3.4) can be expressed as follows:

$$r=2,\quad 0\leqq\theta_0\leqq s-1\quad\text{and}\quad\theta_{k-1}\geqq 0.$$

This implies that there is no restriction with respect to θ_0 and θ_{k-1} in the case $r=2$.

EXAMPLE 3.2. In the case $r=3$, it is well known (cf. Bose [3]) that $M_3(3, s)=s+2$ or $s+1$ according as s is a power of 2 (i.e., $s=2^m$ for some integer $m\geqq 1$) or not. Hence condition (3.4) means that

$$r=3,\quad 0\leqq\theta_0\leqq s-1\quad\text{and}\quad\theta_{k-1}\geqq 0$$

or

$$r=3,\quad 0\leqq\theta_0\leqq s-2\quad\text{and}\quad\theta_{k-1}\geqq 0$$

according as s is a power of 2 or not.

EXAMPLE 3.3. In the case $r=4$ and $k\geqq 4$, it is well known (cf. Segre [15, 16] and Gulati and Kounias [7]) that $M_4(4, 2)=M_4(4, 3)=5$ and $M_4(4, s)=s+1$ for any prime power $s\geqq 4$. Hence condition (3.4) implies that

$$r=4,\quad 0\leqq\theta_0\leqq s-1 \quad\text{and}\quad \theta_{k-1}\geqq 0,$$
$$r=4,\quad 0\leqq\theta_0\leqq s-2 \quad\text{and}\quad \theta_{k-1}\geqq 0,\quad\text{or}$$
$$r=4,\quad 0\leqq\theta_0\leqq s-3 \quad\text{and}\quad \theta_{k-1}\geqq 0$$

according as $s=2$, 3 or $s\geqq 4$.

EXAMPLE 3.4. Consider the case $k=5$, $r=4$ and $s=5$. In this case, $M_4(4, 5)=6$ and $0\leqq\theta_0\leqq 2$. Let $C(5, 5)$ be a set of $(5^5-1)/(5-1)$ nonzero vectors in $V(5; 5)$ such that the first component of each vector is equal to 1 (cf. Example A.1 in Appendix) and let $W_4=\{\boldsymbol{c}: B_4\boldsymbol{c}=0 \text{ over } GF(5), \boldsymbol{c}\in C(5, 5)\}$ where $B_4=(0, 0, 0, 0, 1)$.

In the case $\theta_0=2$ and $\theta_{k-1}=0$ (i.e., $d=503$), let $E_{4,6}=\{\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3, \boldsymbol{e}_4, \boldsymbol{e}_5, \boldsymbol{e}_6\}$ where $\boldsymbol{e}_1^T=(1, 0, 0, 0, 0)$, $\boldsymbol{e}_2^T=(0, 1, 0, 0, 0)$, $\boldsymbol{e}_3^T=(0, 0, 1, 0, 0)$, $\boldsymbol{e}_4^T=(0, 0, 0, 1, 0)$, $\boldsymbol{e}_5^T=(1, 1, 1, 1, 0)$, $\boldsymbol{e}_6^T=(1, 2, 3, 4, 0)$. Then we can obtain a (631, 5, 503; 5)-code from Theorems 3.1 and 3.2 which achieve the Solomon-Stiffler's lower bound.

Appendix

With the help of the Galois field $GF(s)$, we can define a finite projective geometry $PG(t, s)$ of t ($\geqq 2$) dimensions as a set of points satisfying the following conditions:

(a) A point in $PG(t, s)$ is represented by (v) where v is a nonzero element of $GF(s^{t+1})$.

(b) Two points (v_1) and (v_2) represent the same point when and only when there exists a nonzero element σ of $GF(s)$ such that $v_1=\sigma v_2$.

(c) A μ-flat, $0\leqq\mu\leqq t-1$, in $PG(t, s)$ is defined as a set of $(s^{\mu+1}-1)/(s-1)$ points $(a_0v_0+a_1v_1+\cdots+a_\mu v_\mu)$ where a_i's run independently over the elements of $GF(s)$ and are not all simultaneously zero and $v_0, v_1,\ldots, v_\mu$ are linearly independent elements of $GF(s^{t+1})$ over the coefficient field $GF(s)$. In the special case $\mu=t-1$, a $(t-1)$-flat is also called a hyperplane.

It is well known that there is a one-to-one correspondence between $s^{t+1}-1$ nonzero elements in $GF(s^{t+1})$ and $s^{t+1}-1$ nonzero vectors in $V(t+1; s)$ (cf. Carmichael [5]). Hence any point in $PG(t, s)$ can be expressed as $(\boldsymbol{c})$ using some nonzero vector $\boldsymbol{c}$ in $V(t+1; s)$ where two points $(\boldsymbol{c}_1)$ and $(\boldsymbol{c}_2)$ represent the same point if and only if two vectors $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ are linearly dependent over $GF(s)$, i.e., there exists a nonzero element σ of $GF(s)$ such that $\boldsymbol{c}_1=\sigma\boldsymbol{c}_2$. Since there are $s-1$ nonzero elements in $GF(s)$, there are $(s^{t+1}-1)/(s-1)$ points in $PG(t, s)$.

Let k be any given integer such that $k\geqq 3$. Then there exist v_k nonzero vectors

in $V(k; s)$ such that the first nonzero component of each vector is equal to 1 where $v_k=(s^k-1)/(s-1)$ (cf. Example A.1). After numbering those v_k vectors in some way, we shall denote v_k vectors by $\boldsymbol{c}_j$ $(j=1, 2,..., v_k)$ and let

$$C(k, s)=\{\boldsymbol{c}_1, \boldsymbol{c}_2,..., \boldsymbol{c}_{v_k}\}. \tag{A.1}$$

It is easy to see that (a) any two vectors in $C(k, s)$ are linearly independent over $GF(s)$ and (b) for any nonzero vector $\boldsymbol{c}$ in $V(k; s)$, there exists a unique vector $\boldsymbol{c}_j$ in $C(k, s)$ such that $\boldsymbol{c}=\sigma\boldsymbol{c}_j$ for some nonzero element σ of $GF(s)$. This implies that there is a one-to-one correspondence between v_k points in $PG(k-1, s)$ and v_k vectors in $C(k, s)$. Hence in Section 3, we shall denote v_k points in $PG(k-1, s)$ by $\boldsymbol{c}_j$ $(j=1, 2,..., v_k)$ instead of $(\boldsymbol{c}_j)$ or Q_j in Section 2.

EXAMPLE A.1. In the special case $k=3$ and $s=3$, $C(3,3)$ is a set of 13 vectors in $V(3; 3)$ as follows:

$\boldsymbol{c}_1$	$\boldsymbol{c}_2$	$\boldsymbol{c}_3$	$\boldsymbol{c}_4$	$\boldsymbol{c}_5$	$\boldsymbol{c}_6$	$\boldsymbol{c}_7$
1	0	0	1	1	1	1
0	1	0	1	2	0	0
0	0	1	0	0	1	2

$\boldsymbol{c}_8$	$\boldsymbol{c}_9$	$\boldsymbol{c}_{10}$	$\boldsymbol{c}_{11}$	$\boldsymbol{c}_{12}$	$\boldsymbol{c}_{13}$
0	0	1	1	1	1
1	1	1	1	2	2
1	2	1	2	1	2

Let $\boldsymbol{c}^T=(2, 1, 2)$. Then $\boldsymbol{c}=2\boldsymbol{c}_{12}$. Hence two points $(\boldsymbol{c})$ and $(\boldsymbol{c}_{12})$ represent the same point in $PG(2, 3)$.

A μ-flat, $0\leqq\mu\leqq k-2$, in $PG(k-1, s)$ may be defined as a set

$$W=\{\boldsymbol{c}: B\boldsymbol{c}=\boldsymbol{0} \text{ over } GF(s),\ \boldsymbol{c}\in C(k, s)\} \tag{A.2}$$

using some $(k-1-\mu)\times k$ matrix B whose entries are elements of $GF(s)$ and whose rank over $GF(s)$ is equal to $k-1-\mu$. In the special case $\mu=k-2$, there are v_k hyperplanes in $PG(k-1, s)$ and those v_k hyperplanes in $PG(k-1, s)$ can be expressed as follows:

$$H_i=\{\boldsymbol{c}: \boldsymbol{h}_i^T\boldsymbol{c}=0 \text{ over } GF(s),\ \boldsymbol{c}\in C(k, s)\} \tag{A.3}$$

using some vectors $\boldsymbol{h}_i$ $(i=1, 2,..., v_k)$ in $V(k; s)$ where $\{\boldsymbol{h}_1, \boldsymbol{h}_2,..., \boldsymbol{h}_{v_k}\}$ $(\equiv H(k, s))$ is a set of v_k nonzero vectors in $V(k; s)$ such that any two vectors in $H(k, s)$ are linearly independent over $GF(s)$.

EXAMPLE A.2. In the case $k=3$ and $s=3$, let $\boldsymbol{h}_i=\boldsymbol{c}_i$ and $H_i=\{\boldsymbol{c}: \boldsymbol{h}_i^T\boldsymbol{c}=0$ over $GF(3),\ \boldsymbol{c}\in C(3, 3)\}$ for $i=1, 2,..., 13$ where $\boldsymbol{c}_i$'s are vectors given in Example A.1.

Then H_i $(i=1, 2,..., 13)$ are 13 hyperplanes in $PG(2, 3)$. For example, $H_1=\{c_2, c_3, c_8, c_9\}$ and $H_4=\{c_3, c_5, c_{12}, c_{13}\}$.

References

[1] L. D. Baumert and R. J. McEliece, A note on the Griesmer bound, IEEE Trans. Information Theory **IT-19** (1973), 134–135.

[2] B. I. Belov, A conjecture on the Griesmer bound in "Optimization Methods and Their Applications (All-Union Summer Sem., Khakusy, Lake Baikal, 1972)" (Russian), pp. 100–106, 182, Sibirsk. Energet. Inst. Sibirsk. Otdel. Akad. Nauk SSSR, Irkutsk. 1974.

[3] R. C. Bose, Mathematical theory of the symmetrical factorial design, Sankhya **8** (1947), 107–166.

[4] R. C. Bose, On some connections between design of experiments and information theory, Bull. Inst. Int. Statist. **38** (1961), 257–271.

[5] R. D. Carmichael, Introduction to the theory of groups of finite order, Ginn and Company, Boston, 1937.

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

[7] B. R. Gulati and E. G. Kounias, On bounds useful in the theory of symmetrical factorial designs, J. Roy. Statist. Soc. Ser. B **32**, No. 1 (1970), 123–133.

[8] N. Hamada and F. Tamari, Construction of maximal t-linearly independent sets, in "Essays in Probability and Statistics", (presented in honor of Prof. Junjiro Ogawa on his 60th birthday), (S. Ikeda et al., Eds.), Keibundo Matsumoto Printing Co. Inc., Japan (1978), 14–28.

[9] N. Hamada and F. Tamari, On a geometrical method of construction of maximal t-linearly independent sets, J. Combinatorial Theory Ser. A, **25** (1978), 14–28.

[10] N. Hamada and F. Tamari, Construction of optimal linear codes and optimal fractional factorial designs using flats and spreads in a finite projective geometry, Tech. Rep. **No. 6**, Statistical Research Group, Hiroshima University, Hiroshima, Japan, 1979.

[11] N. Hamada and F. Tamari, Construction of optimal codes and optimal fractional factorial designs using linear programming, Annals of Discrete Mathematics **6** (1980), 175–188.

[12] N. Hamada and F. Tamari, Construction of optimal linear codes using flats and spreads in a finite projective geometry, European Journal of Combinatorics **3** (1982), 129–141.

[13] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error Correcting Codes", North-Holland Mathematical Library, **Vol. 16**, North-Holland, Amsterdam, 1977.

[14] E. J. McCluskey, Error-correcting codes — A linear programming approach, Bell System Tech. J. **38** (1959), 1485–1512.

[15] B. Segre, Curve razionale e k-archi negli spazi finiti, Ann. Mat. Pura Appl. (4) **39** (1955), 357–379.

[16] B. Segre, "Lectures on Modern Geometry", Cremonese, Roma, 1961.

[17] G. Solomon and J. J. Stiffler, Algebraically punctured cyclic codes, Information and Control **8** (1965), 170–179.