Europ. J. Combinatorics (1982) **3**, 129–141

Construction of Optimal Linear Codes Using Flats and Spreads in a Finite Projective Geometry

NOBORU HAMADA AND FUMIKAZU TAMARI

In this paper, we shall consider a problem of constructing an optimal linear code whose code length n is minimum among $(*, k, d; s)$-codes for given integers k, d and s. In [5], we showed that this problem is equivalent to Problem B of a linear programming which has some geometrical structure and gave a geometrical method of constructing a solution of Problem B using a set of flats in a finite projective geometry and obtained a necessary and sufficient conditions for integers k, d and s that there exists such a geometrical solution of Problem B for given integers k, d and s. But there was no space to give the proof of the main theorem 4.2 in [5]. The purpose of this paper is to give the proof of [5, Theorem 4.2], i.e. to give a systematic method of constructing a solution of Problem B using flats and spreads in a finite projective geometry.

1. INTRODUCTION

Let $V(n; s)$ be an n-dimensional vector space 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, the number of information symbols k and the minimum distance d) if the minimum distance of the code C is equal to d (cf. [1, 2, 6]). In this paper, we shall consider the following problem.

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

In [5], we showed that Problem A is equivalent to Problem B of a linear programming which has some geometrical structure and gave a geometrical method of constructing a solution of Problem B using a set of flats in a finite projective geometry and obtained a necessary and sufficient condition (cf. [5, Theorems 4.1 and 4.2]) for integers k, d and s that there exists such a geometrical solution of Problem B for given integers k, d and s. But there was no space to give the proof of the main theorem 4.2 in [5].

The purpose of this paper is to give the proof of [5, Theorem 4.2], i.e. to give a systematic method of constructing a solution of Problem B using flats and spreads in a finite projective geometry. Using these results, we can obtain solutions of Problems A and B for many integers k, d and s even if d is not so large.

In the following, let k and d be any given integers such that $k \geq 3$ and $d \geq 1$ and let s be any given prime or prime power and let us denote by $\theta_0 + \theta_1 s + \cdots + \theta_{k-2}s^{k-2}$ and θ_{k-1} the remainder and the quotient of $d-1$, respectively, when it is divided by s^{k-1}, i.e.

$$d = 1 + \theta_0 + \theta_1 s + \theta_2 s^2 + \cdots + \theta_{k-2}s^{k-2} + \theta_{k-1}s^{k-1}, \tag{1.1}$$

where θ_is are integers such that $\theta_{k-1} \geq 0$ and $0 \leq \theta_i \leq s-1$ for $i = 0, 1, \ldots, k-2$.

2. PRELIMINARY RESULTS

Let k, d and s be given integers and let $\varepsilon_i = (s-1) - \theta_i$ for $i = 0, 1, \ldots, k-2$ and let $D = \{\mu : \varepsilon_\mu \neq 0, 0 \leq \mu \leq k-2\}$ where θ_is are integers given by (1.1). Let $\mathcal{B}$ be a set of ε_0 0-flats, ε_1 1-flats, $\ldots$, ε_{k-3} $(k-3)$-flats and ε_{k-2} $(k-2)$-flats in a finite projective geometry

0195–6698/82/020129+13 $02.00/0

$PG(k-1,s)$, i.e. let

$$\mathscr{B}=\{V_i^{(\mu)}: i=1,2,\ldots,\varepsilon_\mu, \mu\in D\}, \tag{2.1}$$

where $V_i^{(\mu)}$ $(i=1,2,\ldots,\varepsilon_\mu)$ denote (not necessarily distinct) ε_μ μ-flats in $PG(k-1,s)$ for each integer μ in D (cf. Appendix I). In the special case $(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2})=(0,0,\ldots,0)$, $\mathscr{B}$ is the empty set $\varnothing$. Let $\eta_j(\mathscr{B})$ $(j=1,2,\ldots,v_k)$ be the number of flats $V_i^{(\mu)}$ $(1\leq i\leq\varepsilon_\mu, \mu\in D)$ in $\mathscr{B}$ which contain the jth point in $PG(k-1,s)$ where $v_k=(s^k-1)/(s-1)$. Let us denote by $\mathscr{F}(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2};k,s)$, a family of all sets $\mathscr{B}$ which consist of ε_0 0-flats, ε_1 1-flats, $\ldots$, ε_{k-3} $(k-3)$-flats and ε_{k-2} $(k-2)$-flats in $PG(k-1,s)$.

In [5], we showed that Problem A is equivalent to the following Problem B (cf. [5, Theorem 2.1]) and gave a geometrical method of constructing a solution of Problem B using a set of flats in $PG(k-1,s)$ (cf. [5, Theorem 3.1]).

PROBLEM B. Find a vector $\mathbf{x}^{\mathrm{T}}=(x_1,x_2,\ldots,x_{v_k})$ of non-negative integers x_j $(j=1,2,\ldots,v_k)$ that minimizes the summation $\sum_{j=1}^{v_k}x_j$ subject to the following inequality:

$$\sum_{j=1}^{v_k}(1-n_{ij})x_j\geq d \qquad (i=1,2,\ldots,v_k) \tag{2.2}$$

for given integers k, d and s where $n_{ij}=1$ or 0 according to whether or not the jth point in $PG(k-1,s)$ is contained in the ith hyperplane in $PG(k-1,s)$.

THEOREM 2.1. *If there exists a set $\mathscr{B}$ in $\mathscr{F}(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2};k,s)$ such that* $\max\{\eta_j(\mathscr{B})-1: 1\leq j\leq v_k\}\leq\theta_{k-1}$ *for given integers k, d and s, the vector $\mathbf{x}$ whose jth component x_j $(1\leq j\leq v_k)$ is given by*

$$x_j=\theta_{k-1}-(\eta_j(\mathscr{B})-1) \tag{2.3}$$

is a solution of Problem B for given integers k, d and s where $\varepsilon_i=(s-1)-\theta_i$ for $i=0,1,\ldots,k-2$ and θ_is are integers given by (1.1).

From the actual point of view, it is desirable to obtain a solution of Problem A (i.e. Problem B) for comparatively small integers k, d and s. Since d can be expressed as (1.1) and $\theta_{k-1}\geq 0$, it is necessary that θ_{k-1} is a small integer in order that d is a small integer. Hence it is necessary to obtain a set $\mathscr{B}$ in $\mathscr{F}(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2};k,s)$ such that $\max\{\eta_j(\mathscr{B})-1: 1\leq j\leq v_k\}$ is minimum for given integers k, s and ε_j $(j=0,1,\ldots,k-2)$, that is, it is necessary to obtain a necessary and sufficient condition for integers k, s and ε_j $(j=0,1,\ldots,k-2)$ that there exists a set $\mathscr{B}$ in $\mathscr{F}(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2};k,s)$ such that

$$\max\{\eta_j(\mathscr{B})-1: 1\leq j\leq v_k\}\leq t \tag{2.4}$$

for a given non-negative integer t.

Let $E(k,s)$ be a set of ordered sets $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})$ of integers ε_i $(i=1,2,\ldots,k-2)$ such that $0\leq\varepsilon_i\leq s-1$ and let $E_t(k,s)$ $(t=0,1,2,\ldots)$ be a set of ordered sets $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})$ in $E(k,s)$ such that either (a) $\sum_{i=1}^{k-2}\varepsilon_i\leq t+1$ or (b) $\sum_{i=1}^{k-2}\varepsilon_i\geq t+2$ and $\beta_1+\beta_2+\cdots+\beta_{t+2}\leq(t+1)k-(t+2)$ for the first $t+2$ integers $\beta_1,\beta_2,\ldots,\beta_{t+2}$ (cf. Sections 3 and 4) in the following series:

$$\overbrace{k-2,k-2,\ldots,k-2}^{\varepsilon_{k-2}};\quad \overbrace{k-3,k-3,\ldots,k-3}^{\varepsilon_{k-3}};\quad \ldots;\quad \overbrace{1,1,\ldots,1}^{\varepsilon_1}. \tag{2.5}$$

The purpose of this paper is to give the proof of the following Theorem 2.3.

THEOREM 2.2. *A necessary condition for ε_j $(j=0,1,\ldots,k-2)$ that there exists a set $\mathcal{B}$ in $\mathcal{F}(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2};k,s)$ which satisfies condition* (2.4) *for given integers k, s and t is that* $0\leq\varepsilon_0\leq s-1$ *and* $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})\in E_t(k,s)$.

THEOREM 2.3. *Let k, s and* ε_j $(j=0,1,\ldots,k-2)$ *be any integers such that* $k\geq 3$ *and* $0\leq\varepsilon_j\leq s-1$. *If* $0\leq\varepsilon_0\leq s-1$ *and* $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})\in E_t(k,s)$ *for* $t=0$ *or* 1, *there exists a set* $\mathcal{B}$ *in* $\mathcal{F}(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2};k,s)$ *which satisfies condition* (2.4). (Cf. [5, Theorem 4.2].)

REMARK 2.1. It follows from [5, Corollary 3.2] that Theorem 2.3 holds for the case $k=3$. Hence it is sufficient to show that Theorem 2.3 holds for $k\geq 4$.

REMARK 2.2. It follows from [5, Lemma 4.1] that in order to show that Theorem 2.3 holds, it is sufficient to show that if $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})\in E_t(k,s)$ for $t=0$ or 1, there exists a set $\mathcal{N}$ in $\mathcal{F}(0,\varepsilon_1,\ldots,\varepsilon_{k-2};k,s)$ such that

$$\max\{\eta_j(\mathcal{N}): 1\leq j\leq v_k\}\leq t+1. \tag{2.6}$$

In the special case $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})=(0,0,\ldots,0)$, $\mathcal{N}=\varnothing$ and $\eta_j(\mathcal{N})=0$ for $j=1,2,\ldots,v_k$, i.e. $\max\{\eta_j(\mathcal{N}): 1\leq j\leq v_k\}=0$.

REMARK 2.3. In the case $\sum_{i=1}^{k-2}\varepsilon_i\leq t+1$, any set $\mathcal{N}$ in $\mathcal{F}(0,\varepsilon_1,\ldots,\varepsilon_{k-2};k,s)$ satisfies condition (2.6). In the case $\sum_{i=1}^{k-2}\varepsilon_i\geq t+2$, a set $\mathcal{N}$ in $\mathcal{F}(0,\varepsilon_1,\ldots,\varepsilon_{k-2};k,s)$ satisfies condition (2.6) if and only if $\bigcap_{i=1}^{t+2}U_i=\varnothing$ for any $t+2$ flats U_i $(i=1,2,\ldots,t+2)$ in $\mathcal{N}$.

REMARK 2.4. Let $\mathcal{N}$ be a set in $\mathcal{F}(0,\varepsilon_1,\ldots,\varepsilon_{k-2};k,s)$ and let $\mathcal{N}^*$ be a set in $\mathcal{F}(0,\varepsilon_1^*,\ldots,\varepsilon_{k-2}^*;k,s)$ such that $\mathcal{N}^*\subset\mathcal{N}$ where $0\leq\varepsilon_i^*\leq\varepsilon_i$ for $i=1,2,\ldots,k-2$. Then $\eta_j(\mathcal{N}^*)\leq\eta_j(\mathcal{N})$ for $j=1,2,\ldots,v_k$.

3. THE PROOF OF THEOREM 2.3 FOR THE CASE $t=0$

In order to show that Theorem 2.3 holds for the case $t=0$, we shall give another characterization of the set $E_0(k,s)$ where $k\geq 4$. Since $E_0(k,s)$ is a set of ordered sets $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})$ in $E(k,s)$ such that either (a) $\sum_{i=1}^{k-2}\varepsilon_i\leq 1$ or (b) $\sum_{i=1}^{k-2}\varepsilon_i\geq 2$ and $\beta_1+\beta_2\leq k-2$ for the first two integers β_1 and β_2 in the series (2.5), it follows that $\sum_{i=\omega+1}^{k-2}\varepsilon_i=0$ or 1 if $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})\in E_0(k,s)$ where $\omega=[(k-2)/2]$ and $[x]$ denotes the greatest integer not exceeding x.

Let $E_{00}(k,s)$ be a set of ordered sets $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})$ in $E(k,s)$ such that $\sum_{i=\omega+1}^{k-2}\varepsilon_i=0$ and $0\leq\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_\omega\leq s-1$ (i.e. $\beta_2\leq\beta_1\leq\omega$). Let $E_{01}(k,s)$ be a set of ordered sets $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})$ in $E(k,s)$ such that $\sum_{i=\omega+1}^{k-2}\varepsilon_i=1$ (i.e. $\varepsilon_r=1$ for some integer r such that $\omega+1\leq r\leq k-2$), $0\leq\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-r-2}\leq s-1$ and $\varepsilon_j=0$ for any integer j such that $k-r-1\leq j\leq\omega$ (i.e. $\beta_1=r$ and $\beta_2\leq k-r-2$). Then $E_{00}(k,s)\cap E_{01}(k,s)=\varnothing$ and we have the following lemma.

LEMMA 3.1. *An ordered set* $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})$ *in* $E(k,s)$ *belongs to* $E_0(k,s)$ *if and only if it belongs to either* $E_{00}(k,s)$ *or* $E_{01}(k,s)$.

LEMMA 3.2. *For any ordered set* $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})$ *in* $E_{00}(k,s)$, *there exists a set* $\mathcal{N}$ *in* $\mathcal{F}(0,\varepsilon_1,\ldots,\varepsilon_{k-2};k,s)$ *such that* $\max\{\eta_j(\mathcal{N}): 1\leq j\leq v_k\}=1$ *unless* $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})=(0,0,\ldots,0)$ *where* $k\geq 4$.

PROOF

(I) In the case $k=2m+2$ $(m\geq 1)$, it follows that $\omega=[(k-2)/2]=m$ and $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})\in E_{00}(k,s)$ if and only if $0\leq\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_m\leq s-1$ and $\varepsilon_{m+1}=\varepsilon_{m+2}=$

$\cdots=\varepsilon_{k-2}=0$. Hence it is sufficient to show that Lemma 3.2 holds for the case $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_m=s-1$ and $\varepsilon_{m+1}=\varepsilon_{m+2}=\cdots=\varepsilon_{2m}=0$ (cf. Remark 2.4).

From Theorem I.1 in Appendix I, it follows that there exists an m-spread in $PG(2m+1,s)$. Let $\{W_i: i=1,2,\ldots,s^{m+1}+1\}$ be an m-spread in $PG(2m+1,s)$ and let $V_j^{(\mu)}$ $(1\leq j\leq s-1,\ 1\leq\mu\leq m)$ be any μ-flat in $W_{(\mu-1)(s-1)+j}$ and let

$$\mathcal{N}=\{V_j^{(\mu)}: j=1,2,\ldots,s-1,\ \mu=1,2,\ldots,m\}. \tag{3.1}$$

Then $\mathcal{N}$ is a desired set since $|\mathcal{N}|=m(s-1)\leq s^{m+1}+1$ for any integer $m\geq 1$ and $U_1\cap U_2=\varnothing$ for any two flats U_1 and U_2 in $\mathcal{N}$. Note that $W_i\cap W_j=\varnothing$ for any integers i and j such that $1\leq i<j\leq s^{m+1}+1$.

(II) In the case $k=2m+1$ $(m\geq 2)$, it follows that $\omega=[(k-2)/2]=m-1$ and $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})\in E_{00}(k,s)$ if and only if $0\leq\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{m-1}\leq s-1$ and $\varepsilon_m=\varepsilon_{m+1}=\cdots=\varepsilon_{k-2}=0$. Let $\mathcal{N}$ be a set of flats in $PG(2m+1,s)$ given by (3.1) and let H be a hyperplane in $PG(2m+1,s)$ defined by

$$H=\{(\mathbf{c}): \mathbf{h}^{\mathrm{T}}\mathbf{c}=0 \text{ over } GF(s),\ \mathbf{c}\in V(2m+2;s)\} \tag{3.2}$$

for a vector $\mathbf{h}^{\mathrm{T}}=(0,0,\ldots,0,1)$ in $V(2m+2;s)$. Then H consists of v_{2m+1} points in $PG(2m+1,s)$ whose last components are all zero.

Let $U_j^{(\mu)}$ $(1\leq j\leq s-1,\ 1\leq\mu\leq m-1)$ be any μ-flat in $H\cap V_j^{(\mu+1)}$ and let $\tilde{\mathcal{N}}=\{\tilde{U}_j^{(\mu)}: j=1,2,\ldots,s-1,\ \mu=1,2,\ldots,m-1\}$ where $\tilde{U}_j^{(\mu)}$ denotes the μ-flat in $PG(2m,s)$ which is obtained from the μ-flat $U_j^{(\mu)}$ in $PG(2m+1,s)$ by deleting the last component from all points in $U_j^{(\mu)}$. Then $\tilde{\mathcal{N}}$ is a desired set for the case $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_{m-1}=s-1$ and $\varepsilon_m=\varepsilon_{m+1}=\cdots=\varepsilon_{2m-1}=0$ since the last component of any point in $U_j^{(\mu)}$ $(1\leq j\leq s-1,\ 1\leq\mu\leq m-1)$ is zero. This completes the proof.

LEMMA 3.3. *For any ordered set $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})$ in $E_{01}(k,s)$, there exists a set $\mathcal{N}$ in $\mathcal{F}(0,\varepsilon_1,\ldots,\varepsilon_{k-2};k,s)$ such that* $\max\{\eta_j(\mathcal{N}): 1\leq j\leq v_k\}=1$ *where $k\geq 4$.*

PROOF

(I) In the case $k=2m+2$ $(m\geq 1)$, it follows that $w=[(k-2)/2]=m$ and $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})\in E_{01}(k,s)$ if and only if $\varepsilon_r=1$, $0\leq\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-r-2}\leq s-1$ for some integer r such that $m+1\leq r\leq 2m$ and $\varepsilon_j=0$ for any other integer j. Hence it is sufficient to show that Lemma 3.3 holds for the case $\varepsilon_r=1$, $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_{k-r-2}=s-1$ and $\varepsilon_j=0$ for any other integer j. Let $e=r-m$. Then $1\leq e\leq m$ and $k-r-2=m-e$.

In the case $e=m$ (i.e. $\varepsilon_{2m}=1$ and $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_{2m-1}=0$), let H_1 be any hyperplane in $PG(2m+1,s)$ and let $\mathcal{N}=\{H_1\}$. Then $\mathcal{N}$ is a desired set.

In the case $1\leq e<m$ (i.e. $r=m+e$; $m+1\leq r<2m$), let $\{W_i^*: i=1,2,\ldots,s^{m+1}+1\}$ be an m-spread in $PG(2m+1,s)$ and let V_1^* be any $(m-e)$-flat in $PG(2m+1,s)$ such that $V_1^*\subset W_1^*$. Let W_i and V_1 be the dual space of W_i^* and V_1^* in $PG(2m+1,s)$, respectively (cf. Definition I.1 in Appendix I). Since $\dim(W_i^*\oplus W_j^*)=2m+1$, $W_i^*\cap W_j^*=\varnothing$ $(i\neq j)$, $V_1^*\subset W_1^*$ and $\dim(V_1^*\oplus W_l^*)=2m+1-e$ for $l=2,3,\ldots,s^{m+1}+1$, it follows from Definitions I.1 and I.2 that $\{W_i: i=1,2,\ldots,s^{m+1}+1\}$ is an m-spread in $PG(2m+1,s)$ and V_1 is an $(m+e)$-flat in $PG(2m+1,s)$ such that $W_1\subset V_1$ and $\dim(V_1\cap W_l)=e-1$ for $l=2,3,\ldots,s^{m+1}+1$ where "$\dim(W)=\mu$" means that W is a μ-flat. Hence there exists an $(m-e)$-flat R_l in W_l such that $V_1\cap R_l=\varnothing$ for $l=2,3,\ldots,s^{m+1}+1$. Let $V_j^{(\mu)}$ $(1\leq j\leq s-1,\ 1\leq\mu\leq m-e)$ be any μ-flat in $R_{(\mu-1)(s-1)+j+1}$ and let

$$\mathcal{N}=\{V_1\}+\{V_j^{(\mu)}: j=1,2,\ldots,s-1,\ \mu=1,2,\ldots,m-e\}. \tag{3.3}$$

Then $\mathcal{N}$ is a desired set since $|\mathcal{N}|=(m-e)(s-1)+1\leq s^{m+1}+1$ for any integer $m\geq 1$ and $U_1\cap U_2=\varnothing$ for any two flats U_1 and U_2 in $\mathcal{N}$.

(II) In the case $k=2m+1$ ($m\geq 2$), it follows that $\omega=[(k-2)/2]=m-1$ and $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})\in E_{01}(k,s)$ if and only if $\varepsilon_r=1$, $0\leq\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-r-2}\leq s-1$ for some integer r such that $m\leq r\leq 2m-1$ and $\varepsilon_j=0$ for any other integer j. Let $e=r-m$. Then $0\leq e\leq m-1$ and $k-r-2=m-e-1$.

In the case $1\leq e\leq m-1$, let $\mathcal{N}$ be a set of flats in $PG(2m+1,s)$ given by (3.3) and let H be the hyperplane in $PG(2m+1,s)$ defined by (3.2). Since we can assume without loss of generality that $\mathbf{h}\subset V_1^*\subset W_1^*$ in (I), it follows that $H\supset V_1\supset W_1$. Let $U_j^{(\mu)}$ ($1\leq j\leq s-1$, $1\leq\mu\leq m-e-1$) be any μ-flat in $H\cap V_j^{(\mu+1)}$ and let $\tilde{\mathcal{N}}=\{\tilde{V}_1\}+\{\tilde{U}_j^{(\mu)}: j=1,2,\ldots,s-1,\mu=1,2,\ldots,m-e-1\}$. Then $\tilde{\mathcal{N}}$ is a desired set for the case $\varepsilon_r=1$, $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_{k-r-2}=s-1$ and $\varepsilon_j=0$ for any other integer j where $r=m+e$ and $1\leq e\leq m-1$.

In the case $e=0$ (i.e. $\varepsilon_m=1$, $0\leq\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{m-1}\leq s-1$ and $\varepsilon_{m+1}=\varepsilon_{m+2}=\cdots=\varepsilon_{2m-1}=0$), let $U_j^{(\mu)}$ ($1\leq j\leq s-1$, $1\leq\mu\leq m-1$) be any μ-flat in $H\cap W_{(\mu-1)(s-1)+j+1}$ and let $\tilde{\mathcal{N}}=\{\tilde{W}_1\}+\{\tilde{U}_j^{(\mu)}: j=1,2,\ldots,s-1,\mu=1,2,\ldots,m-1\}$ where $\{W_i: i=1,2,\ldots,s^{m+1}+1\}$ is an m-spread in $PG(2m+1,s)$ such that $W_1\subset H$. Then $\mathcal{N}$ is a desired set for the case $\varepsilon_m=1$, $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_{m-1}=s-1$ and $\varepsilon_{m+1}=\varepsilon_{m+2}=\cdots=\varepsilon_{2m-1}=0$. This completes the proof.

From the above lemmas and the remarks in Section 2, it follows that Theorem 2.3 holds for the case $t=0$.

COROLLARY 3.1. *Let k, d and s be any integers such that $k\geq 3$ and $d\geq 1$. If $0\leq\theta_0\leq s-1$, $(s-1-\theta_1,s-1-\theta_2,\ldots,s-1-\theta_{k-2})\in E_0(k,s)$ and $\theta_{k-1}\geq 0$, there exists an $(n,k,d;s)$-code which attains a lower bound*

$$n\geq k+\theta_0v_1+\theta_1v_2+\cdots+\theta_{k-1}v_k, \tag{3.4}$$

where θ_is are integers given by (1.1) and $v_i=(s^i-1)/(s-1)$ for $i=1,2,\ldots,k$.

REMARK 3.1. The lower bound (3.4) for n is essentially due to G. Solomon and J. J. Stiffler [7].

REMARK 3.2. With respect to a necessary and sufficient condition for an ordered set $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})$ in $E(k,s)$ that $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{k-2})\in E_0(k,s)$, see (I) and (II) in the proofs of Lemmas 3.2 and 3.3.

EXAMPLE 3.1. Consider the case $k=8$, $d=105$ and $s=2$. Since $(\theta_0,\theta_1,\ldots,\theta_7)=(0,0,0,1,0,1,1,0)$ and $(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_6)=(1,1,1,0,1,0,0)$ in this case, it follows from Corollary 3.1 and $(1,1,0,1,0,0)\in E_0(8,2)$ (cf. (I) in the proof of Lemma 3.3) that there exists an $(n,8,105;2)$-code which attains the lower bound (3.4) (i.e. $n=213$). Using the method in [5] (cf. [5, Theorems 2.1, 3.1 and Lemma 4.1]) and the constructive method of $\mathcal{N}$ in Lemma 3.3, we can construct such an optimal linear code.

EXAMPLE 3.2. Consider the case $k=6$, $s=3$ and $(\theta_0,\theta_1,\ldots,\theta_4)=(1,0,0,2,2)$ (i.e. $(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_4)=(1,2,2,0,0)$). Since $(\theta_0,\theta_1,\ldots,\theta_4;\theta_5)=(1,0,0,2,2;0)$, $(1,0,0,2,2;1)$, $(1,0,0,2,2;2),\ldots$ according to whether $d=218$, 461, $704,\ldots$, it follows from Corollary 3.1 and $(2,2,0,0)\in E_0(6,3)$ (cf. (I) in the proof of Lemma 3.2) that there exists an $(n,6,d;3)$-code which attains the lower bound (3.4) for $d=218$, $461, 704,\ldots$.

EXAMPLE 3.3. In the case where $k=2m+2$ ($m\geq 1$), $0\leq\theta_0,\theta_1,\ldots,\theta_m\leq s-1$ and $\theta_{m+1}=\theta_{m+2}=\cdots=\theta_{2m}=s-1$, it follows from Corollary 3.1 and (I) in the proof of

Lemma 3.2 that there exists an $(n, 2m+2, d; s)$-code which attains the lower bound (3.4) for any integer $\theta_{2m+1} \geq 0$ where d is an integer given by (1.1).

4. The Proof of Theorem 2.3 for the Case $t = 1$

In the case $t = 1$, $E_t(k, s)$ is a set of ordered sets $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})$ in $E(k, s)$ such that either (a) $\sum_{i=1}^{k-2} \varepsilon_i \leq 2$ or (b) $\sum_{i=1}^{k-2} \varepsilon_i \geq 3$ and $\beta_1 + \beta_2 + \beta_3 \leq 2k - 3$ for the first three integers β_1, β_2 and β_3 in the series (2.5). Hence $\sum_{i=\tau+1}^{k-2} \varepsilon_i = 0$, 1 or 2 if $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2}) \in E_1(k, s)$ where $\tau = [(2k-3)/3]$.

Let $E_{10}(k, s)$ be a set of ordered sets $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})$ in $E(k, s) - E_0(k, s)$ such that $\sum_{i=\tau+1}^{k-2} \varepsilon_i = 0$ and $0 \leq \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\tau \leq s-1$ (i.e. $\beta_3 \leq \beta_2 \leq \beta_1 \leq \tau$). Let $E_{11}(k, s)$ be a set of ordered sets $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})$ in $E(k, s) - E_0(k, s)$ such that (i) $\sum_{i=\tau+1}^{k-2} \varepsilon_i = 1$ (i.e. $\varepsilon_r = 1$; $\beta_1 = r$) and (ii) either (a) there exists a pair of integers f and g ($f + g + r = 2k - 3$ and $f < g \leq \tau$; $\beta_2 = g$ and $\beta_3 \leq f$) such that $0 \leq \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_f \leq s-1$, $\varepsilon_g = 1$ and $\varepsilon_j = 0$ for any integer j ($f < j \leq \tau$ and $j \neq g$) or (b) there exists an integer g ($2g + r \leq 2k - 3$ and $g \leq \tau$; $\beta_2 = \beta_3 = g$) such that $0 \leq \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{g-1} \leq s-1$, $2 \leq \varepsilon_g \leq s-1$ (i.e. $s \geq 3$) and $\varepsilon_j = 0$ for any integer j ($g < j \leq \tau$). Let $E_{12}(k, s)$ be a set of ordered sets $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})$ in $E(k, s) - E_0(k, s)$ such that (i) $\sum_{i=\tau+1}^{k-2} \varepsilon_i = 2$ (i.e. $\varepsilon_r = 2$ or $\varepsilon_{r_1} = \varepsilon_{r_2} = 1$; $\beta_1 = \beta_2 = r$ or $\beta_1 = r_1$ and $\beta_2 = r_2$) and (ii) $0 \leq \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_h \leq s-1$ and $\varepsilon_{h+1} = \varepsilon_{h+2} = \cdots = \varepsilon_\tau = 0$ (i.e. $\beta_3 \leq h$) where $h = 2k - 3 - 2r$ or $2k - 3 - r_1 - r_2$ and $\tau + 1 \leq r_2 < r_1 \leq k - 2$. Then we have the following lemma.

Lemma 4.1. *An ordered set $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})$ in $E(k, s)$ belongs to $E_1(k, s) - E_0(k, s)$ if and only if it belongs to either $E_{10}(k, s)$, $E_{11}(k, s)$ or $E_{12}(k, s)$.*

Lemma 4.2. *For any integer $m \geq 1$, there exists a set of $(2m+1)$-flats Y_l ($l = 1, 2, \ldots, s^{m+1}+1$) in $PG(3m+2, s)$ such that $Y_i \cap Y_j \cap Y_k = \varnothing$ for any integers i, j and k such that $1 \leq i < j < k \leq s^{m+1}+1$.*

Proof. Let α be a primitive element of $GF(s^{3m+3})$ and let

$$W_i^* = \{(\alpha^i), (\alpha^{\theta+i}), (\alpha^{2\theta+i}), \ldots, (\alpha^{(w-1)\theta+i})\}$$

for $i = 0, 1, \ldots, \theta - 1$ where $w = (s^{m+1}-1)/(s-1)$ and $\theta = (s^{3m+3}-1)/(s^{m+1}-1)$. Then it follows from Theorem I.1 in Appendix I that $\{W_i^* : i = 0, 1, \ldots, \theta - 1\}$ is an m-spread in $PG(3m+2, s)$. Since $(\alpha^\theta)^{s^{m+1}-1} = \alpha^{s^{3m+3}-1} = 1$, $\alpha^{l\theta}$ is an element of $GF(s^{m+1})$ for $l = 0, 1, \ldots, w-1$. Hence each m-flat W_i^* ($0 \leq i < \theta$) can be regarded as a point (α^i) in $PG(2, s^{m+1})$. Since there are $q+1$ points in $PG(2, q)$ in which no three points are linearly dependent upon $GF(q)$ for any prime power q, there exist $q+1$ m-flats Y_l^* ($l = 1, 2, \ldots, q+1$) in $\{W_i^* : i = 0, 1, \ldots, \theta - 1\}$ such that no three points Y_i^*, Y_j^* and Y_k^* ($1 \leq i < j < k \leq q+1$) in $PG(2, q)$ are linearly dependent upon $GF(q)$ (i.e. $\dim(Y_i^* \oplus Y_j^* \oplus Y_k^*) = 3m+2$) where $q = s^{m+1}$. Let Y_l ($l = 1, 2, \ldots, s^{m+1}+1$) be the dual space of Y_l^* in $PG(3m+2, s)$. Then $\{Y_l : l = 1, 2, \ldots, s^{m+1}+1\}$ is a desired set.

Remark 4.1. $\dim(W_i^* \oplus W_j^* \oplus W_k^*) = 2m+1$ or $3m+2$ (i.e. $W_k^* \subset W_i^* \oplus W_j^*$ or $(W_i^* \oplus W_j^*) \cap W_k^* = \varnothing$) according as there exist two elements a and b in $PG(s^{m+1})$ such that $a\alpha^i + b\alpha^j = \alpha^k$ or not.

Remark 4.2. If $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2}) \in E(k, s) - E_0(k, s)$, it follows from Theorem 2.2 that $\max\{\eta_j(\mathcal{N}) : 1 \leq j \leq v_k\} \geq 2$ for any set $\mathcal{N}$ in $\mathcal{F}(0, \varepsilon_1, \ldots, \varepsilon_{k-2}; k, s)$.

Proposition 4.1. *For any ordered set $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})$ in $E_{10}(k, s)$, there exists a set $\mathcal{N}$ in $\mathcal{F}(0, \varepsilon_1, \ldots, \varepsilon_{k-2}; k, s)$ such that $\max\{\eta_j(\mathcal{N}) : 1 \leq j \leq v_k\} = 2$ where $k \geq 4$.*

PROOF

(I) In the case $k=3m+3$ $(m\geq 1)$, it follows that $\tau=[(2k-3)/3]=2m+1$ and $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})\in E_{10}(k,s)$ if and only if $0\leq \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{2m+1}\leq s-1$ and $\varepsilon_{2m+2}=\varepsilon_{2m+3}=\cdots=\varepsilon_{3m+1}=0$. Hence it is sufficient to show that Proposition 4.1 holds for the case $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_{2m+1}=s-1$ and $\varepsilon_{2m+2}=\varepsilon_{2m+3}=\cdots=\varepsilon_{3m+1}=0$.

Let Y_i $(i=1,2,\ldots,s^{m+1}+1)$ be $(2m+1)$-flats in $PG(3m+2,s)$ given in Lemma 4.2 and let $V_j^{(\mu)}$ $(1\leq j\leq s-1,\ 1\leq \mu\leq 2m+1)$ be any μ-flat in $Y_{(\mu-1)(s-1)+j}$ and let

$$\mathcal{N}=\{V_j^{(\mu)}: j=1,2,\ldots,s-1,\ \mu=1,2,\ldots,2m+1\}. \tag{4.1}$$

Then $\mathcal{N}$ is a desired set since $|\mathcal{N}|=(2m+1)(s-1)\leq s^{m+1}+1$ for any integer $m\geq 1$ and $U_1\cap U_2\cap U_3=\varnothing$ for any three flats U_1, U_2 and U_3 in $\mathcal{N}$.

(II) In the case $k=3m+2$ $(m\geq 1)$, it follows that $\tau=2m$ and $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})\in E_{10}(k,s)$ if and only if $0\leq \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{2m}\leq s-1$ and $\varepsilon_{2m+1}=\varepsilon_{2m+2}=\cdots=\varepsilon_{3m}=0$. Let $\mathcal{N}$ be a set of flats in $PG(3m+2,s)$ given by (4.1) and let H be a hyperplane in $PG(3m+2,s)$ given by (II.1) in Appendix II. Let $U_j^{(\mu)}$ $(1\leq j\leq s-1,\ 1\leq \mu\leq 2m)$ be any μ-flat in $H\cap V_j^{(\mu+1)}$ and let $\tilde{\mathcal{N}}=\{\tilde{U}_j^{(\mu)}: j=1,2,\ldots,s-1,\ \mu=1,2,\ldots,2m\}$. Then $\tilde{\mathcal{N}}$ is a desired set for the case $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_{2m}=s-1$ and $\varepsilon_{2m+1}=\varepsilon_{2m+2}=\cdots=\varepsilon_{3m}=0$.

(III) In the case $k=3m+1$ $(m\geq 1)$, it follows that $\tau=2m-1$ and $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})\in E_{10}(k,s)$ if and only if $0\leq \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{2m-1}\leq s-1$ and $\varepsilon_{2m}=\varepsilon_{2m+1}=\cdots=\varepsilon_{3m-1}=0$. Let $\mathcal{N}$ be a set of flats in $PG(3m+2,s)$ given by (4.1) and let G be a $3m$-flat in $PG(3m+2,s)$ given by (II.2) in Appendix II. Let $U_j^{(\mu)}$ $(1\leq j\leq s-1,\ 1\leq \mu\leq 2m-1)$ be any μ-flat in $G\cap V_j^{(\mu+2)}$ and let $\tilde{\tilde{\mathcal{N}}}=\{\tilde{\tilde{U}}_j^{(\mu)}: j=1,2,\ldots,s-1,\ \mu=1,2,\ldots,2m-1\}$ where $\tilde{\tilde{U}}_j^{(\mu)}$ denotes the μ-flat in $PG(3m,s)$ which is obtained from the μ-flat $U_j^{(\mu)}$ in $PG(3m+2,s)$ by deleting the last two components from all points in $U_j^{(\mu)}$. Then $\tilde{\tilde{\mathcal{N}}}$ is a desired set for the case $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_{2m-1}=s-1$ and $\varepsilon_{2m}=\varepsilon_{2m+1}=\cdots=\varepsilon_{3m-1}=0$. This completes the proof.

The proof of the following lemma will be given in Appendix II.

LEMMA 4.3. *For any integers e_1 and e_2 such that $1\leq e_1\leq m$ and $0\leq e_2\leq e_1/2$, there exists a set of one $(2m+1+e_1)$-flat V_1, one $(2m+1-e_2)$-flat R_2, ρ $(2m+1-e_1+e_2)$-flats R_j $(j=3,4,\ldots,\rho+2)$ and $s^{m+1}-1-\rho$ $(2m+1-e_1)$-flats T_l $(l=1,2,\ldots,s^{m+1}-1-\rho)$ in $PG(3m+2,s)$ such that the intersection of any three flats in the set is empty, where ρ is any integer such that $0\leq\rho\leq s^{\pi}$ and $\pi=[e_1/2]$.*

REMARK 4.3. In Lemma 4.3, we can assume without loss of generality that (i) $V_1=H$ in the case $e_1=m$ and (ii) $V_1\subset G\subset H$ in the case $1\leq e_1\leq m-1$ where H and G are a hyperplane and a $3m$-flat in $PG(3m+2,s)$ given by (II.1) and (II.2) in Appendix II, respectively. (Cf. the proof of Lemma II.1 in Appendix II.)

PROPOSITION 4.2. *For any ordered set $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})$ in $E_{11}(k,s)$, there exists a set $\mathcal{N}$ in $\mathcal{F}(0, \varepsilon_1, \ldots, \varepsilon_{k-2}; k, s)$ such that $\max\{\eta_j(\mathcal{N}): 1\leq j\leq v_k\}=2$ where $k\geq 4$.*

PROOF

(I) In the case $k=3m+3$, it is sufficient to show that Proposition 4.2 holds for the following two cases.

(i) In the case where $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_{2m+1-e_1+e_2}=s-1$, $\varepsilon_{2m+1-e_2}=\varepsilon_{2m+1+e_1}=1$ for some integers e_1 and e_2 $(1\leq e_1\leq m$ and $0\leq e_2<e_1/2)$ and $\varepsilon_j=0$ for any other integer j (i.e. $\beta_1=r=2m+1+e_1$, $\beta_2=g=2m+1-e_2$ and $\beta_3=f=2m+1-e_1+e_2$), let $V_j^{(\mu)}$ $(1\leq j\leq s-1,\ 2m+2-e_1\leq\mu\leq 2m+1-e_1+e_2$ and $e_2\neq 0)$ be any μ-flat in $R_{(\mu-\zeta)(s-1)+j+2}$ $(\zeta=2m+2-e_1)$ and let $V_j^{(\mu)}$ $(1\leq j\leq s-1,\ 1\leq\mu\leq 2m+1-e_1)$

be any μ-flat in $T_{(\mu-1)(s-1)+j}$ and let

$$\mathcal{N}=\{V_1, R_2\}+\{V_j^{(\mu)}: j=1,2,\dots,s-1, \mu=1,2,\dots,\xi\}$$

where V_1, R_is and T_js are flats in $PG(3m+2,s)$ given in Lemma 4.3 and $\xi=2m+1-e_1+e_2$. Then $\mathcal{N}$ is a desired set, since $\rho=e_2(s-1)\leq\pi(s-1)\leq s^\pi$ and $|\mathcal{N}|=(2m+1-e_1+e_2)(s-1)+2\leq 2m(s-1)+2\leq s^{m+1}+1$ for any integer $m\geq 1$ where $\pi=[e_1/2]$.

(ii) In the case where $s\geq 3$, $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_{2m+1-e_2}=s-1$, $\varepsilon_{2m+1+e_1}=1$ for some integers e_1 and e_2 ($1\leq e_1\leq m$ and $e_1=2e_2$) and $\varepsilon_j=0$ for any other integer j (i.e. $\beta_1=r=2m+1+e_1$ and $\beta_2=\beta_3=g=2m+1-e_2$), let $V_j^{(\mu)}$ ($1\leq j\leq s-1$, $2m+2-e_1\leq\mu\leq 2m+1-e_2$) be any μ-flat in $R_{(\mu-\zeta)(s-1)+j+1}$ ($\zeta=2m+2-e_1$) and let $V_j^{(\mu)}$ ($1\leq j\leq s-1$, $1\leq\mu\leq 2m+1-e_1$) be any μ-flat in $T_{(\mu-1)(s-1)+j}$ and let

$$\mathcal{N}=\{V_1\}+\{V_j^{(\mu)}: j=1,2,\dots,s-1, \mu=1,2,\dots,\xi\}$$

where $\xi=2m+1-e_2$. Then $\mathcal{N}$ is a desired set.

(II) In the case $k=3m+2$, let $(\varepsilon_1,\varepsilon_2,\dots,\varepsilon_{3m})$ be any ordered set in $E_{11}(3m+2,s)$ and let us denote by r the greatest integer in D where $D=\{\mu:\varepsilon_\mu\neq 0, 1\leq\mu\leq 3m\}$. Then $2m+1\leq r\leq 3m$, $\varepsilon_r=1$ and $\varepsilon_{2m+1}=\varepsilon_{2m+2}=\cdots=\varepsilon_{r-1}=\varepsilon_{r+1}=\cdots=\varepsilon_{3m}=0$. Let

$$\varepsilon_1^*=0,\qquad \varepsilon_r^*=\varepsilon_{r-1}+1,\qquad \varepsilon_{r+1}^*=0\quad\text{and}\quad \varepsilon_{i+1}^*=\varepsilon_i \tag{4.2}$$

for $i=1,2,\dots,r-2,r+1,r+2,\dots,3m$.

(a) In the case $2m+2\leq r\leq 3m$, it follows that $(\varepsilon_1^*,\varepsilon_2^*,\dots,\varepsilon_{3m+1}^*)\in E_{11}(3m+3,s)$ since $\varepsilon_r^*=1$ (i.e. $\varepsilon_{r-1}=0$). Hence there exists a set $\mathcal{N}^*$ in $\mathcal{F}(0,\varepsilon_1^*,\dots,\varepsilon_{3m+1}^*;3m+3,s)$ such that $\max\{\eta_j(\mathcal{N}^*): 1\leq j\leq v_k\}=2$.

(b) In the case $r=2m+1$, it follows that $\varepsilon_{2m+2}^*=\varepsilon_{2m+3}^*=\cdots=\varepsilon_{3m+1}^*=0$ and $\varepsilon_{2m+1}^*=s$ or $1\leq\varepsilon_{2m+1}^*\leq s-1$ according to whether or not $\varepsilon_{2m}=s-1$. Using a similar method in Proposition 4.1, we can show that there exists a set $\mathcal{N}^*$ in $\mathcal{F}(0,\varepsilon_1^*,\dots,\varepsilon_{3m+1}^*;3m+3,s)$ such that $\max\{\eta_j(\mathcal{N}^*): 1\leq j\leq v_k\}=2$ even if $\varepsilon_{2m+1}^*=s$.

Let H be the hyperplane in $PG(3m+2,s)$ given by (II.1) in Appendix II and let $U_i^{(\mu)}$ ($1\leq i\leq\varepsilon_\mu$, $\mu\in D-\{r\}$) be any μ-flat in $H\cap V_i^{(\mu+1)}$ and let $\mathcal{N}=\{\tilde{V}_1\}+\{\tilde{U}_i^{(\mu)}: i=1,2,\dots,\varepsilon_\mu, \mu\in D-\{r\}\}$ where V_1 and $V_i^{(\mu+1)}$s are an r-flat and $(\mu+1)$-flats in $\mathcal{N}^*$ of (a) or (b). Then $\mathcal{N}$ is a desired set. Note that $V_1\subset H$, i.e. the last component of any point in V_1 is zero (cf. Remark 4.3).

(III) In the case $k=3m+1$, we can construct a set $\mathcal{N}$ in $\mathcal{F}(0,\varepsilon_1,\dots,\varepsilon_{3m-1};3m+1,s)$ such that $\max\{\eta_j(\mathcal{N}): 1\leq j\leq v_k\}=2$ for any ordered set $(\varepsilon_1,\varepsilon_2,\dots,\varepsilon_{3m-1})$ in $E_{11}(3m+1,s)$ from a set of flats in $PG(3m+1,s)$ using a similar method in (II). This completes the proof.

The proof of the following lemma will be given in Appendix III.

LEMMA 4.4. *For any integers e_1 and e_2 such that $1\leq e_1, e_2\leq m$, there exists a set of one $(2m+1+e_1)$-flat V_1, one $(2m+1+e_2)$-flat V_2 and $s^{m+1}-1$ $(2m+1-e_1-e_2)$-flats K_j ($j=3,4,\dots,s^{m+1}+1$) in $PG(3m+2,s)$ such that the intersection of any three flats in the set is empty.*

PROPOSITION 4.3. *For any ordered set $(\varepsilon_1,\varepsilon_2,\dots,\varepsilon_{k-2})$ in $E_{12}(k,s)$, there exists a set $\mathcal{N}$ in $\mathcal{F}(0,\varepsilon_1,\dots,\varepsilon_{k-2};k,s)$ such that $\max\{\eta_j(\mathcal{N}): 1\leq j\leq v_k\}=2$ where $k\geq 4$.*

PROOF

(I) In the case $k=3m+3$, it is sufficient to show that Proposition 4.3 holds for the case $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_h=s-1$, $\varepsilon_{2m+1+e_1}=\varepsilon_{2m+1+e_2}=1$ $(1\leqslant e_1<e_2\leqslant m)$ or $\varepsilon_{2m+1+e_1}=2$ $(e_1=e_2)$ and $\varepsilon_i=0$ for any other integer i where $h=2m+1-e_1-e_2$.

Let $V_j^{(\mu)}$ $(1\leqslant j\leqslant s-1,\ 1\leqslant \mu\leqslant h)$ be any μ-flat in $K_{(\mu-1)(s-1)+j+2}$ and let $\mathcal{N}=\{V_1, V_2\}+\{V_j^{(\mu)}: j=1,2,\ldots,s-1,\ \mu=1,2,\ldots,h\}$ where V_1, V_2 and K_js are flats in $PG(3m+2,s)$ given in Lemma 4.4. Then $\mathcal{N}$ is a desired set.

(II) In the case $k=3m+2$, it is sufficient to show that Proposition 4.3 holds for the following two cases.

(i) In the case where $s\geqslant 3$, $\varepsilon_r=2$, $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_h=s-1$ and $\varepsilon_j=0$ for any other integer j $(h=2k-3-2r$ and $2m+1\leqslant r\leqslant 3m)$, let $\varepsilon_1^*=0$, $\varepsilon_r^*=1$, $\varepsilon_{r+1}^*=1$ and $\varepsilon_{i+1}^*=\varepsilon_i$ for $i=1,2,\ldots,r-2,r+1,r+2,\ldots,3m$. Then it is easy to see that there exists a set $\mathcal{N}^*$ in $\mathcal{F}(0,\varepsilon_1^*,\ldots,\varepsilon_{3m+1}^*; 3m+3,s)$ such that $\max\{\eta_j(\mathcal{N}^*): 1\leqslant j\leqslant v_k\}=2$. Let $V_1=V_1^{(r)}$ and $V_2=H\cap V_1^{(r+1)}$ and let $U_j^{(\mu)}$ $(1\leqslant j\leqslant s-1, 1\leqslant\mu\leqslant h)$ be any μ-flat in $H\cap V_j^{(\mu+1)}$ and let $\mathcal{N}=\{\tilde{V}_1,\tilde{V}_2\}+\{\tilde{U}_j^{(\mu)}: j=1,2,\ldots,s-1,\ \mu=1,2,\ldots,h\}$ where $V_j^{(\mu)}$s are μ-flats in $\mathcal{N}^*$. Then $\mathcal{N}$ is a desired set. Note that $\varepsilon_{r-1}=0$ in this case and $V_1^{(r)}$ is an r-flat in $\mathcal{N}^*$ such that $V_1^{(r)}\subset H$ and $H\cap V_1^{(r+1)}$ is an r-flat in H.

(ii) In the case where $\varepsilon_{r_1}=\varepsilon_{r_2}=1$, $\varepsilon_1=\varepsilon_2=\cdots=\varepsilon_h=s-1$ and $\varepsilon_j=0$ for any other integer j $(h=2k-3-r_1-r_2$ and $2m+1\leqslant r_2<r_1\leqslant 3m)$, we can construct a desired set $\mathcal{N}$ in $\mathcal{F}(0,\varepsilon_1,\ldots,\varepsilon_{3m}; 3m+2,s)$ using a similar method to that in (i).

(III) In the case $k=3m+1$, we can obtain a desired set $\mathcal{N}$ in $\mathcal{F}(0,\varepsilon_1,\ldots,\varepsilon_{3m-1}; 3m+1,s)$ using a similar method to that in (II). This completes the proof.

From the above propositions and the remarks in Section 2, it follows that Theorem 2.3 holds for the case $t=1$. We can easily generalize our results to the case $t\geqslant 2$. But it is very complicated to investigate completely whether or not Theorem 2.3 holds for each integer t $(2\leqslant t\leqslant k-2)$.

COROLLARY 4.1. *Let k, d and s be any integers such that $k\geqslant 3$ and $d\geqslant 1$. If $0\leqslant\theta_0\leqslant s-1$, $(s-1-\theta_1,\ s-1-\theta_2,\ldots,\ s-1-\theta_{k-2})\in E_1(k,s)-E_0(k,s)$ and $\theta_{k-1}\geqslant 1$, there exists an $(n,k,d;s)$-code which attains the lower bound* (3.4).

REMARK 4.4. In the case where $0\leqslant\theta_0\leqslant s-1$ and $(s-1-\theta_1,\ s-1-\theta_2,\ldots,\ s-1-\theta_{k-2})\in E_1(k,s)-E_0(k,s)$, we can construct a solution of Problem B (i.e. Problem A) using Theorem 2.1 if $\theta_{k-1}\geqslant 1$, but we can not construct a solution of Problem B using Theorem 2.1 if $\theta_{k-1}=0$. Note that $E_0(k,s)\subset E_1(k,s)\subset\cdots\subset E_{k-2}(k,s)=E(k,s)$.

EXAMPLE 4.1. In the case where $k=8$, $s=2$ and $(\theta_0,\theta_1,\ldots,\theta_6)=(0,0,0,0,1,0)$ (i.e. $(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_6)=(1,1,1,1,1,0,1)$), it follows that $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_6)\notin E_0(8,2)$ but $(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_6)\in E_1(8,2)$. Since $(\theta_0,\theta_1,\ldots,\theta_6;\theta_7)=(0,0,0,0,0,1,0;0)$, $(0,0,0,0,0,1,0;1)$, $(0,0,0,0,0,1,0;2)$, ... according to whether $d=33$, 161, 289, ..., it follows from Corollary 4.1 that there exists an $(n,8,d;2)$-code which attains the lower bound (3.4) for $d=161$, 289, ... Using the method in [5] and the constructive method of $\mathcal{N}$ in Proposition 4.2, we can construct such an optimal linear code.

EXAMPLE 4.2. In the case where $k=3m+3$ $(m\geqslant 1)$, $0\leqslant\theta_0,\theta_1,\ldots,\theta_{2m+1}\leqslant s-1$ and $\theta_{2m+2}=\theta_{2m+3}=\cdots=\theta_{3m+1}=s-1$, it follows from Corollary 4.1 and (I) in the proof of Proposition 4.1 that there exists an $(n,3m+3,d;s)$-code which attains the lower bound (3.4) for any integer $\theta_{3m+2}\geqslant 1$ where d is an integer given by (1.1). (Cf. (I), (II) and (III) in the proofs of Propositions 4.1, 4.2 and 4.3 for further details.)

APPENDIX I. A μ-FLAT AND A μ-SPREAD IN $PG(t, s)$

A finite projective geometry $PG(t, s)$ of t dimensions ($t \geq 2$) can be defined as a set of points satisfying the following conditions:

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

(b) Two points (ν_1) and (ν_2) represent the same point when and only when there exists a non-zero element σ of $GF(s)$ such that $\nu_1 = \sigma\nu_2$.

(c) A μ-flat, $0 \leq \mu \leq t$, in $PG(t, s)$ is defined as a set of points

$$\{(a_0\nu_0 + a_1\nu_1 + \cdots + a_\mu\nu_\mu): \cdots\}$$

where a_is run independently over the elements of $GF(s)$ and are not all simultaneously zero and $\nu_0, \nu_1, \ldots, \nu_\mu$ (called a generator of the μ-flat) are linearly independent elements of $GF(s^{t+1})$ over the coefficient field $GF(s)$. Hence there are $(s^{t+1} - 1)/(s-1)$ points in $PG(t, s)$ and each μ-flat consists of $(s^{\mu+1} - 1)/(s-1)$ points in $PG(t, s)$. In the special case $\mu = t-1$, a $(t-1)$-flat in $PG(t, s)$ is called a hyperplane. A t-flat in $PG(t, s)$ is a set of all points in $PG(t, s)$ and a (-1)-flat is an empty set $\emptyset$. Note that the intersection of any two flats is also a flat.

Since every non-zero element of $GF(s^{t+1})$ may be represented either as a power of the primitive element α or as a polynomial in α, of degree at most t, with coefficients from $GF(s)$ (cf. [3]), every point in $PG(t, s)$ can be expressed by using either a power of the primitive element α or a vector of $V(t+1; s)$ and a μ-flat W $(0 \leq \mu < t)$ may be defined as a set

$$W = \{(\mathbf{c}): A\mathbf{c} = \mathbf{0} \text{ over } GF(s), \mathbf{c} \in V(t+1; s)\} \tag{I.1}$$

using a $(t-\mu) \times (t+1)$ matrix A whose entries are elements of $GF(s)$ and whose rank over $GF(s)$ is equal to $t - \mu$.

DEFINITION I.1. Let W be a μ-flat $(0 \leq \mu < t)$ in $PG(t, s)$ defined by (I.1). The $(t-\mu-1)$-flat W^* generated by $t-\mu$ column vectors of A^{T} is said to be *the dual space* of W in $PG(t, s)$. In the special case $W = \emptyset$ (i.e. $\mu = -1$), the dual space of W in $PG(t, s)$ is a t-flat and the dual space of a t-flat W in $PG(t, s)$ is an empty set.

DEFINITION I.2. A set Ω of μ-flats $(0 < \mu < t)$ in $PG(t, s)$ is said to be a *μ-spread* in $PG(t, s)$ if every point in $PG(t, s)$ is contained in exactly one μ-flat of the set Ω (cf. [4]). That is, a μ-spread in $PG(t, s)$ is a partition of all points in $PG(t, s)$ by μ-flats.

DEFINITION I.3. The minimum flat which contains r flats V_i $(i = 1, 2, \cdots, r)$ in $PG(t, s)$ is denoted by $V_1 \oplus V_2 \oplus \cdots \oplus V_r$ where $r \geq 2$. In the special case where $r = 2$ and V_1 and V_2 are a μ-flat and a ν-flat in $PG(t, s)$, respectively, such that $V_1 \cap V_2 = \emptyset$, $V_1 \oplus V_2$ is a $(\mu + \nu + 1)$-flat in $PG(t, s)$.

The following theorem (cf. [4, 8]) plays an important role in constructing a set $\mathscr{B}$ which satisfies the condition in Theorem 2.3.

THEOREM I.1

(i) *There exists a μ-spread in $PG(t, s)$ if and only if $t+1$ is a multiple of $\mu + 1$.*

(ii) *Let t and μ $(1 \leq \mu < t)$ be any positive integers such that $t+1$ is a multiple of $\mu+1$ and let*

$$W_i = \{(\alpha^i), (\alpha^{\theta+i}), (\alpha^{2\theta+i}), \ldots, (\alpha^{(w-1)\theta+i})\} \tag{I.2}$$

for $i = 0, 1, \ldots, \theta - 1$ where $w = (s^{\mu+1} - 1)/(s-1)$, $\theta = (s^{t+1} - 1)/(s^{\mu+1} - 1)$ and α is a primitive element of $GF(s^{t+1})$. Then $\{W_i: i = 0, 1, \ldots, \theta - 1\}$ is a μ-spread in $PG(t, s)$.

REMARK I.1. Let $\{W_i: i=1,2,\ldots,\xi\}$ be any μ-spread in $PG(t,s)$ and let f be any linear mapping from $PG(t,s)$ onto $PG(t,s)$. Then $\{f(W_i): i=1,2,\ldots,\xi\}$ is also a μ-spread in $PG(t,s)$.

REMARK I.2. There exist a μ-flat V and a ν-flat W in $PG(t,s)$ such that $V\cap W=\emptyset$ if and only if $\mu+\nu+1\leq t$.

REMARK I.3

(i) Let W_1 and W_2 be two flats in $PG(t,s)$ and let W_i^* be the dual space of W_i in $PG(t,s)$. Then $W_1\subset W_2$ if and only if $W_1^*\supset W_2^*$.

(ii) Let V_i $(i=1,2,\ldots,r)$ be flats in $PG(t,s)$ and let V_i^* be the dual space of V_i in $PG(t,s)$ where $r\geq 2$. Then the dual space of $\bigcap_{i=1}^r V_i$ is $V_1^*\oplus V_2^*\oplus\cdots\oplus V_r^*$. Hence $\bigcap_{i=1}^r V_i=\emptyset$ if and only if $\dim(V_1^*\oplus\cdots\oplus V_r^*)=t$.

APPENDIX II. THE PROOF OF LEMMA 4.3

In order to prove Lemma 4.3, we shall prepare two lemmas. Let

$$H=\{(\mathbf{c}): \mathbf{b}_1^{\mathrm{T}}\mathbf{c}=0 \text{ over } GF(s),\ \mathbf{c}\in V(3m+3;s)\} \tag{II.1}$$

and

$$G=\{(\mathbf{c}): \mathbf{b}_1^{\mathrm{T}}\mathbf{c}=\mathbf{b}_2^{\mathrm{T}}\mathbf{c}=0 \text{ over } GF(s),\ \mathbf{c}\in V(3m+3;s)\} \tag{II.2}$$

where $\mathbf{b}_1^{\mathrm{T}}=(0,0,\ldots,0,0,1)$ and $\mathbf{b}_2^{\mathrm{T}}=(0,0,\ldots,0,1,0)$. Then H is a hyperplane in $PG(3m+2,s)$ such that the last component of any point in H is zero and G is a $3m$-flat in $PG(3m+2,s)$ such that the last two components of any point in G are zero.

LEMMA II.1. *For any integers m and e_1 such that $m\geq 1$ and $0\leq e_1\leq m$, there exist one $(2m+1+e_1)$-flat V_1 and $s^{m+1}+1$ $(2m+1)$-flats Y_i $(i=1,2,\ldots,s^{m+1}+1)$ in $PG(3m+2,s)$ such that* (a) $\dim(Y_\alpha\cap Y_\beta)=m$ *and* $Y_\alpha\cap Y_\beta\cap Y_\gamma=\emptyset$ *for any distinct integers α,β,γ $(1\leq\alpha,\beta,\gamma\leq s^{m+1}+1)$ and* (b) $\dim(V_1\cap Y_\beta)=m+e_1$ *and* $\dim(V_1\cap Y_\beta\cap Y_\gamma)=e_1-1$ *for any distinct integers β and γ $(2\leq\beta,\gamma\leq s^{m+1}+1)$ and* (c) $Y_1\subset V_1\subset H$, $\dim(H\cap Y_j)=2m$ *and* $\dim(G\cap Y_j)=2m-1$ *for $j=2,3,\ldots,s^{m+1}+1$.*

PROOF. Let Y_l^* $(l=1,2,\ldots,s^{m+1}+1)$ be m-flats in $PG(3m+2,s)$ defined in the proof of Lemma 4.2 such that $\dim(Y_i^*\oplus Y_j^*)=2m+1$ (i.e. $Y_i^*\cap Y_j^*=\emptyset$) and $\dim(Y_i^*\oplus Y_j^*\oplus Y_k^*)=3m+2$ for any distinct integers i, j and k $(1\leq i,j,k\leq s^{m+1}+1)$. We can assume without loss of generality (cf. Remark I.1) that Y_1^* contains two points $\mathbf{b}_1$ and $\mathbf{b}_2$ (i.e. $\mathbf{b}_1\oplus\mathbf{b}_2\subset Y_1^*$). Let V_1^* be any $(m-e_1)$-flat in $PG(3m+2,s)$ such that $\mathbf{b}_1\subset V_1^*\subset Y_1^*$ or $\mathbf{b}_1\oplus\mathbf{b}_2\subset V_1^*\subset Y_1^*$ according to whether $e_1=m$ or $0\leq e_1\leq m-1$ and let V_1 and Y_j $(1\leq j\leq s^{m+1}+1)$ be the dual spaces of V_1^* and Y_j^* in $PG(3m+2,s)$, respectively. Then V_1 and Y_js are a $(2m+1+e_1)$-flat and $(2m+1)$-flats in $PG(3m+2,s)$, respectively, which satisfy the three conditions (a), (b) and (c) in Lemma II.1. This completes the proof.

LEMMA II.2. *Let m, e_1 and e_2 be any integers such that $m\geq 2$, $2\leq e_1\leq m$ and $0\leq e_2\leq[e_1/2]$. Then there exists a set of one $(2m+1+e_1)$-flat V_1, one $(2m+1-e_2)$-flat R_2 and s^π $(2m+1-e_1+e_2)$-flats R_j $(j=3,4,\ldots,s^\pi+2)$ in $PG(3m+2,s)$ such that $V_1\cap R_\beta\cap R_\gamma=\emptyset$ and $R_\alpha\cap R_\beta\cap R_\gamma=\emptyset$ for any distinct integers α,β and γ $(2\leq\alpha,\beta,\gamma\leq s^\pi+2)$ where $\pi=[e_1/2]$.*

PROOF. In order to show that Lemma II.2 holds, it is sufficient to show that there exists a set of one $(m-e_1)$-flat V_1^*, one $(m+e_2)$-flat R_2^* and s^π $(m+e_1-e_2)$-flats R_j^* $(j=3,4,\ldots,s^\pi+2)$ in $PG(3m+2,s)$ such that

$$\dim(V_1^* \oplus R_\beta^* \oplus R_\gamma^*)=3m+2 \quad \text{and} \quad \dim(R_\alpha^* \oplus R_\beta^* \oplus R_\gamma^*)=3m+2 \tag{II.3}$$

for any distinct integers α, β and γ (cf. Remark I.3).

Let V_1^* and Y_l^* $(l=1,2,\ldots,s^{m+1}+1)$ be an $(m-e_1)$-flat and m-flats in $PG(3m+2,s)$ such that $V_1^* \subset Y_1^*$, $Y_i^* \cap Y_j^* = \emptyset$ and $\dim(Y_i^* \oplus Y_j^* \oplus Y_k^*)=3m+2$ for any distinct integers i, j and k.

(a) In the case $e_1=2\pi$ $(1 \le \pi \le m/2)$, there exists a $(2\pi-1)$-flat Z_1 in Y_1^* such that $Z_1 \cap V_1^* = \emptyset$ (i.e. $Z_1 \oplus V_1^* = Y_1^*$) and there exists a $(\pi-1)$-spread $\{Z_{1j}: j=2,3,\ldots,s^\pi+2\}$ in Z_1.

In the case $e_2=\pi$ (i.e. $e_2=e_1-e_2=\pi$), let $R_j^* = Y_j^* \oplus Z_{1j}$ for $j=2,3,\ldots,s^\pi+2$. Then R_j^*s are $(m+\pi)$-flats (i.e. $(m+e_1-e_2)$-flats) in $PG(3m+2,s)$ which satisfy condition (II.3) since $R_j^* \supset Y_j^*$, $V_1^* \oplus Z_{1\beta} \oplus Z_{1\gamma} = Y_1^*$ and $V_1^* \oplus R_\beta^* \oplus R_\gamma^* = Y_1^* \oplus Y_\beta^* \oplus Y_\gamma^*$.

In the case $0 \le e_2 < \pi$ (i.e. $e_1-e_2>\pi$), there exist an (e_2-1)-flat $Z_{12}(1)$ and a $(\pi-e_2-1)$-flat $Z_{12}(2)$ in the $(\pi-1)$-flat Z_{12} such that $Z_{12}(1) \cap Z_{12}(2)=\emptyset$ (i.e. $Z_{12}(1) \oplus Z_{12}(2)=Z_{12}$). Let $R_2^* = Y_2^* \oplus Z_{12}(1)$ and $R_j^* = Y_j^* \oplus Z_{1j} \oplus Z_{12}(2)$ for $j=3,4,\ldots,s^\pi+2$. Then R_2^* and R_j^*s are an $(m+e_2)$-flat and $(m+e_1-e_2)$-flats in $PG(3m+2,s)$ which satisfy condition (II.3).

(b) In the case $e_1=2\pi+1$ $(1 \le \pi \le (m-1)/2)$, there exist a $(2\pi-1)$-flat Z_1 and one point P in the m-flat Y_1^* such that $Z_1 \cap V_1^* = \emptyset$ and $V_1^* \oplus Z_1 \oplus P = Y_1^*$. Let $\{Z_{1j}: j=2,3,\ldots,s^\pi+2\}$ be a $(\pi-1)$-spread in Z_1 and let $R_2^* = Y_2^* \oplus Z_{12}(1)$ and $R_j^* = Y_j^* \oplus Z_{1j} \oplus Z_{12}(2) \oplus P$ for $j=3,4,\ldots,s^\pi+2$. Then V_1^*, R_2^* and R_j^*s are desired flats. This completes the proof.

PROOF OF LEMMA 4.3

(i) In the case $e_1=1$, it follows that $e_2=0$, $\pi=0$ and $\rho=0$ or 1. Let V_1^* and P be an $(m-1)$-flat and one point in the m-flat Y_1^* such that $P \notin V_1^*$ (i.e. $V_1^* \oplus P = Y_1^*$) and let $R_2^* = Y_2^*$.

In the case $\rho=0$, let $T_j^* = Y_{j+2}^* \oplus P$ for $j=1,2,\ldots,s^{m+1}-1$ and let V_1, R_2 and T_j $(1 \le j \le s^{m+1}-1)$ be the dual spaces of V_1^*, R_2^* and T_j^*, respectively. Then V_1, R_2 and T_js are desired flats.

In the case $\rho=1$, let $R_3^* = Y_3^* \oplus P$ and $T_j^* = Y_{j+3}^* \oplus P$ for $j=1,2,\ldots,s^{m+1}-2$ and let V_1, R_2, R_3 and T_j $(1 \le j \le s^{m+1}-2)$ be the dual spaces of V_1^*, R_2^*, R_3^* and T_j^*, respectively. Then V_1, R_2, R_3 and T_js are desired flats.

(ii) In the case $2 \le e_1 \le m$ and $0 \le e_2 \le e_1/2$, let V_1^* and Y_l^* $(l=1,2,\ldots,s^{m+1}+1)$ be an $(m-e_1)$-flat and m-flats in $PG(3m+2,s)$ such that $V_1^* \subset Y_1^*$, $Y_i^* \cap Y_j^* = \emptyset$ and $\dim(Y_i^* \oplus Y_j^* \oplus Y_k^*)=3m+2$ for any distinct integers i, j and k. Then there exists an (e_1-1)-flat Z in Y_1^* such that $Z \cap V_1^* = \emptyset$ (i.e. $Z \oplus V_1^* = Y_1^*$). Let $T_l^* = Z \oplus Y_{l+\rho+2}^*$ for $l=1,2,\ldots,s^{m+1}-1-\rho$ and let $\mathscr{C}^* = \{V_1^*\}+\{R_j^*: j=2,3,\ldots,\rho+2\}+\{T_l^*: l=1,2,\ldots,s^{m+1}-1-\rho\}$, where V_1^* and R_j^*s are flats defined in the proof of Lemma II.2. Then it is easy to see that $\dim(U_1 \oplus U_2 \oplus U_3) = 3m+2$ for any three flats U_1, U_2 and U_3 in $\mathscr{C}^*$. Hence $\mathscr{C}$ is a desired set where $\mathscr{C}$ is a set of the dual spaces of all flats in $\mathscr{C}^*$.

APPENDIX III. THE PROOF OF LEMMA 4.4

Let V_1^* and Y_j^* $(j=1,2,\ldots,s^{m+1}+1)$ be an $(m-e_1)$-flat and m-flats in $PG(3m+2,s)$, respectively, which are given in the proof of Lemma II.1 and let V_2^* be any $(m-e_2)$-flat in Y_2^*. Let Y_j and V_l ($l=1,2$) be the dual spaces of Y_j^* and V_l^* in $PG(3m+2,s)$, respectively. Since $\dim(Y_i \cap Y_j)=m$ ($i \neq j$) and $\dim(V_l \cap Y_\beta \cap Y_\gamma)=e_l-1$ for any distinct integers l, β and γ, there exist an $(m-e_2)$-flat E_j in $Y_1 \cap Y_j$ and an $(m-e_1)$-flat F_j in $Y_2 \cap Y_j$ such that

$$E_j \cap (Y_1 \cap V_2 \cap Y_j) = \varnothing \quad \text{and} \quad F_j \cap (V_1 \cap Y_2 \cap Y_j) = \varnothing$$

for $j=3,4,\ldots,s^{m+1}+1$. Let $K_j = E_j \oplus F_j$ for $j=3,4,\ldots,s^{m+1}+1$. Then K_α ($3 \leqslant \alpha \leqslant s^{m+1}+1$) is a $(2m+1-e_1-e_2)$-flat in Y_α such that

$$V_1 \cap V_2 \cap K_k = \varnothing, \qquad V_l \cap K_j \cap K_k = \varnothing \quad \text{and} \quad K_i \cap K_j \cap K_k = \varnothing$$

for any distinct integers l, i, j and k since $V_1 \cap K_k = E_k$, $E_k \cap V_2 = \varnothing$, $V_l \cap K_j \subset Y_l \cap Y_j$, $K_k \subset Y_k$ and $Y_i \cap Y_j \cap Y_k = \varnothing$. This completes the proof.

References

1. E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.
2. I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding*, Academic Press, New York, 1975.
3. R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, Dover, New York, 1956.
4. P. Dembowski, *Finite Geometries*, Springer-Verlag, Berlin, 1968.
5. N. Hamada and F. Tamari, Construction of optimal codes and optimal fractional factorial designs using linear programming, *Ann. Discrete Math.* **6** (1980), 175–188.
6. W. W. Peterson and E. J. Weldon, Jr., *Error Correcting Codes*, 2nd edn., MIT Press, Cambridge, 1972.
7. G. Solomon and J. J. Stiffler, Algebraically punctured cyclic codes, *Inform. and Control* **8** (1965), 170–179.
8. S. Yamamoto, T. Fukuda and N. Hamada, On finite geometries and cyclically generated incomplete block designs, *J. Sci. Hiroshima Univ. Ser. A—I* **30** (1966), 137–149.

Received 13 January 1981 and in revised form 19 March 1982

N. Hamada
Department of Mathematics, Faculty of Science,
Hiroshima University, Hiroshima, Japan

F. Tamari
Department of Mathematics, Fukuoka University of Education,
Akama, Munakata, Fukuoka, Japan