Bulletin of Fukuoka University of Education, Vol. 37, Part III, 39–48 (1988)

L Intersectional Empty Sets (or ℓ-*IE* Sets) and Linear Codes

Fumikazu TAMARI

Department of Mathematics, Fukuoka University of Education

(Received August 31, 1987)

Abstract

In this paper, we shall construct optimal linear codes using ℓ intersectional empty set (or ℓ-*IE* set) where ℓ is a positive integer such that $\ell \geqq 2$. Furthermore, we shall study 4-*IE* sets in detail.

1. Introduction and summary

Let $\mathscr{A}$ be a family of flats in a t-dimensional finite projective geometry $PG(t, s)$. Let ℓ be a positive integer such that $\ell \geqq 2$. Then, a family $\mathscr{A}$ is said to be an ℓ intersectional empty set (or ℓ-*IE* set) if the intersection of any ℓ flats $A_1, A_2, \ldots, A_\ell$ in $\mathscr{A}$, is empty but the intersection of some $(\ell-1)$ flats $B_1, B_2, \ldots, B_{\ell-1}$ in $\mathscr{A}$, is not empty. $\mathscr{A}$ is also said to be a regular ℓ-*IE* set if all flats in $\mathscr{A}$ have the same dimension, i.e., $\dim(A)=v$ for all A in $\mathscr{A}$. Furthermore, $\mathscr{A}_0$ is said to be a maximal (regular) ℓ-*IE* set if $|\mathscr{A}_0| \geqq |\mathscr{A}|$ for all (regular) ℓ-*IE* sets $\mathscr{A}$ in $PG(t, s)$ where $|\mathscr{A}|$ denotes the cardinality of $\mathscr{A}$.

REMARK. Let $\{Q_i\}$ $(i=1, 2, \ldots, \pi)$ be a 3-independent set in $PG(2, s)$ and let L_i be the dual space of Q_i for $i=1, 2, \ldots, \pi$ where $\pi=s+1$ or $s+2$ according as s is odd or not. Then, the set $\{L_i\}$ $(1 \leqq i \leqq \pi)$ is a maximal regular 3-*IE* set.

Let $V(n; s)$ denote an n-dimensional vector space over a Galois field $GF(s)$ where s is a prime or prime power. A k-dimensional subspace C of $V(n; s)$ is called an s-ary linear code with code length n, k information symbols and the minimum distance d if the minimum distance (Hamming distance) of the code C is equal to d, and is denote by $(n, k, d; s)$-code.

We now consider the following problem.

PROBLEM. *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 this paper, we shall construct optimal linear codes using ℓ-*IE* sets

2. Preliminaly results

Let W be a μ-flat in $PG(n, s)$ and let $\boldsymbol{b}_i$ $(i=1, 2, \ldots, \mu+1)$ be a basis of the μ-flat W. The $(n-\mu-1)$-flat W which is defined by $W^*=\{\boldsymbol{h} \in PG(n, s)\colon \boldsymbol{h}\boldsymbol{b}_i^T=0$ over $GF(s)$

$(i=1,2,\dots,\mu+1)\}$ is called the dual space of the μ-flat W where $\boldsymbol{a}^T$ denotes the transpose of $\boldsymbol{a}$. Especially the empty set will be defined as the dual space of the whole space and vice versa. Then we can easily prove the following:

PROPOSITION 1. *Let V and W be any flats in $PG(n, s)$ and let V^* and W^* be the dual space of V and W, respectively. Then*

(i) *$V \subset W$ if and only if $V^* \supset W^*$*

(ii) *$V^* \cap W^* = (V \oplus W)^*$ and $(V \cap W)^* = V^* \oplus W^*$*

where $V \oplus W$ denotes the flats generated by V and W.

A family of t-flats $\{V_i\}$ in $PG(n, s)$ is called a t-spread if every point in $PG(n, s)$ belong to one and only one t-flat of $\{V_i\}$.

Let α be a primitive element of $GF(s^{n+1})$. Then every point in $PG(n, s)$ is represented by the power α^i of α for some $i=0, 1,\dots, v_{n+1}-1$ where $v_{n+1}=(s_{n+1}-1)/(s-1)$. If $t+1$ divides $n+1$, then a family of cyclically generated t-flats in $PG(n, s)$, represented by

$$V_i=\{\alpha^{0+i}, \alpha^{\theta+i},\dots, \alpha^{(w-1)c+i}\} \quad (i=0, 1,\dots, \theta-1)$$

is a t-spread in $PG(n, s)$ where $w=(s^{t+1}-1)/(s-1)$ and $\theta=(s^{n+1}-1)/(s^{t+1}-1)$. Since α is a primitive element of $GF(q)$, $q=s^{t+1}$, every nonzero element of $GF(q)$ may be represented by $\alpha^{j\theta}$ $(j=0, 1,\dots, q-2)$. Moreover, the set of points α^i $(i=0, 1,\dots, \theta-1)$ may be regarded as that of $PG(k, q)$ where $k+1=(n+1)/(t+1)$. This implies that $\{V_i\}$ defined above can also be regarded as the set of all points of $PG(k, q)$. Thus we have

PROPOSITION 2 (*cf.* [1], [6]). *There exists a t-spread in $PG(n, s)$ if and only if $t+1$ divides $n+1$. Furthermore, there exists a t-spread $\{V_i\}$ which can be regarded as the set of all points of $PG(k, q)$ where $k+1=(n+1)/(t+1)$.*

A set L of vectors $\boldsymbol{a}_1, \boldsymbol{a}_2,\dots, \boldsymbol{a}_m$ in $V(r; s)$ such that no t vectors of L are linearly dependent, is called a t-linearly independent set and a t-linearly independent set L_0 is said to be maximal if there exists no t-linearly indenpendent set such that $|L|>|L_0|$. The cardinality of a maximal t-linearly independent set L_0 in $V(r; s)$ is denoted by $M_t(r, s)$.

Attempts of obtaining $M_t(r, s)$ have been made by many research workers. But, unfortunately, $M_t(r, s)$ are partially obtained for some t, r and s but not yet completely.

PROPOSITION 3. *Let m be a nonnegative integer. Then, there exists a set of m-flats Y_k^* $(k=1, 2,\dots, \pi)$ in $PG(\ell(m+1)-1, s)$ such that* $\dim(Y_{i_1}^* \oplus Y_{i_2}^* \oplus \cdots \oplus Y_{i_\ell}^*) = \ell m+\ell-1$ *for any flats $Y_{i_j}^*$ $(j=1, 2,\dots, \ell)$ in $\{Y_k^*\}$ $(1 \leqq k \leqq \pi)$ where $\pi=M_\ell(\ell, s^{m+1})$.*

PROOF. It follows from Proposition 2 that there exists an m-spread $\{W_n^*\}$ $(n=1, 2,\dots,\zeta)$ in $PG(\ell(m+1)-1, s)$ where $\zeta=(s^{\ell(m+1)}-1)/(s^{m+1}-1)$. Since each m-flat W_n^* can be regarded as a point in $PG(\ell-1, s^{m+1})$, there exists a maximal ℓ-linearly independent set $\{Y_k^*\}$ $(k=1, 2,\dots,\pi)$ in $\{W_n^*\}$, i.e., $\dim(Y_{i_1}^*\oplus Y_{i_2}^*\oplus\cdots\oplus Y_{i_\ell}^*)=\ell m+\ell-1$ for any flats $\{Y_{i_j}^*\}$ $(j=1, 2,\dots,\ell)$ in $\{Y_k^*\}$. $\{Y_k^*\}$ $(k=1, 2,\dots,\pi)$ is a reguired set. This completes the proof.

COROLLARY. *Let Y_k be the dual space of Y_k^* $(1\leqq k\leqq\pi)$ which was obtained in Proposition* 3. *Then, the set $\{Y_k\}$ $(1\leqq k\leqq\pi)$ is a regular ℓ-IE set with cardinality π in $PG(\ell(m+1)-1, s)$.*

PROPOSITION 4. *A necessary condition for $\mu_1, \mu_2,\dots,\mu_\ell$ that there exists μ_i-flats W_i $(i=1, 2,\dots,\ell)$ in $PG(k-1, s)$ such that $W_1\cap W_2\cap\cdots\cap W_\ell=\phi$, is that $\mu_1, \mu_2,\dots,\mu_\ell$ satisfy the following condition*:

$$\mu_1+\mu_2+\cdots+\mu_\ell\leqq(\ell-1)k-\ell.$$

PROOF. Let W_i^* $(i=1, 2,\dots,\ell)$ be the dual space of W_i in $PG(k-1, s)$. Then, it is easily shown that $\sum_{i=1}^{\ell}\{\dim(W_i^*)+1\}\geqq k$. Since $\dim(W_i^*)=k-2-\mu_i$ for $i=1, 2,\dots,\ell$, we have the required result.

Let d be a positive integer. 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.,

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

where θ_i's are integers satisfying $0\leqq\theta_i\leqq s-1$ for $i=0, 1,\dots,k-2$ and $\theta_{k-1}\geqq 0$.

PROPOTION 5 (*cf.* [2]). *For any $(n, k, d; s)$-code,*

$$n\geqq k+\theta_0 v_1+\theta_1 v_2+\cdots+\theta_{k-1}v_k \tag{2}$$

if d is expressed by (1) *where $v_i=(s^i-1)/(s-1)$ for $i=1, 2,\dots,k$.*

The lower bound (2) on n is called the Solomon-Stiffier bound.

3. *ℓ-IE* sets and linear codes

Put $\varepsilon_i=s-1-\theta_i$ for $i=0, 1,\dots,k-2$ where θ_i's are integers given in (1). Let $\mathscr{B}$ be a set which consists of ε_μ μ-flats V_i^μ $(0\leqq\mu\leqq k-2,\ i=0, 1,\dots,\varepsilon_\mu)$ where V_i^μ's are not necessarily distinct. Given ε_i $(i=0, 1,\dots,k-2)$, let us denote by $\mathscr{T}(\varepsilon_0, \varepsilon_1,\dots,\varepsilon_{k-2})$ the family of all such that $\mathscr{B}$'s

Note that if there exists an ℓ-*IE* set in $\mathscr{T}(0, \varepsilon_1,\dots, \varepsilon_{k-2})$, then there exists an ℓ-*IE* set in $\mathscr{T}(\varepsilon_0, \varepsilon_1,\dots, \varepsilon_{k-2})$ for all ε_0 (cf. Lemma 4.1 in [2]). On the other hand, it is known (cf. [3], [4]) that in order to obtain linear codes attaining the lower bound (2), it is sufficient to obtain ℓ-*IE* sets ($\ell \geqq 2$) in $PG(t, s)$. Therefore, in this paper, we shall study ℓ-*IE* sets in $\mathscr{T}(0, \varepsilon_1,\dots, \varepsilon_{k-2})$ for some ε_i ($1 \leqq i \leqq k-2$) satisfying a certain condition.

Let $E(k, s)$ be a collection of ordered sets $(\varepsilon_1, \varepsilon_2,\dots, \varepsilon_{k-2})$ of integers ε_i such that $0 \leqq \varepsilon_i \leqq s-1$ for $i=1, 2,\dots, k-2$. Consider a subset $E_t(k, s)$ of $E(k, s)$ for some $t=0, 1,\dots, k-2$ satisfying the following condition:

$$\text{(a)} \quad \sum_{i=1}^{k-2} \varepsilon_i \leqq t+1$$

or (3)

$$\text{(b)} \quad \sum_{i=1}^{k-2} \varepsilon_i \geqq t+2, \ \beta_1+\beta_2+\cdots+\beta_{t+2} \leqq (t+1)(k-1)-1$$

where β_i's ($i=1, 2,\dots, t+2$) are the first $t+2$ integers in the following series:

$$\overbrace{k-2, k-2,\dots, k-2}^{\varepsilon_{k-2}}; \ \overbrace{k-3, k-3,\dots, k-3}^{\varepsilon_{k-3}};\dots; \overbrace{1, 1,\dots, 1}^{\varepsilon_1}.$$

It is easy to see that

$$E_0(k, s) \subset E_1(k, s) \subset E_2(k, s) \subset \cdots$$

and

$$E_j(k, s) = E(k, s) \qquad \text{for} \quad j \geqq k-2.$$

So we shall study ℓ-*IE* sets in $\mathscr{T}(0, \varepsilon_1,\dots, \varepsilon_{k-2})$ such that $2 \leqq \ell \leqq k-2$.

PROPOSITION 6 (*cf.* [2]). *There exists an ℓ-IE set in $\mathscr{T}(0, \varepsilon_1,\dots, \varepsilon_{k-2})$, then $(\varepsilon_1, \varepsilon_2,\dots, \varepsilon_{k-2}) \in E_{\ell-2}(k, s) - E_{\ell-3}(k, s)$ where $E_{-1}(k, s) = \phi$.*

Put $k = \ell(m+1) - q$ ($m \geqq 0$, $0 \leqq q \leqq \ell - 1$) and let $(\varepsilon_1, \varepsilon_2,\dots, \varepsilon_{k-2})$ be an element in $E_{\ell-2}(k, s) - E_{\ell-3}(k, s)$. Then it follows from (3) that $(\varepsilon_1, \varepsilon_2,\dots, \varepsilon_{k-2})$ must be an ordered set such that $0 \leqq \sum_{i=\delta+1}^{k-2} \varepsilon_i \leqq \ell - 1$ where $\delta = [(\ell k - k - 1)/\ell] = (\ell - 1)m + \ell - 2 - q$ and $[x]$ denotes the greatest integer not exceeding x.

THEOREM 1. *Let $(\varepsilon_1, \varepsilon_2,\dots, \varepsilon_{k-2})$ be an element in $E_{\ell-2}(k, s) - E_{\ell-3}(k, s)$ such that $\sum_{i=\delta+1}^{k-2} \varepsilon_i = 0$. If $(\varepsilon_1, \varepsilon_2,\dots, \varepsilon_{k-2})$ satisfies the following condition:*

$$\sum_{j=z}^{\delta-2} \varepsilon_j^* + \varepsilon_{\delta-1} + \varepsilon_\delta \leqq M_\ell(\ell, s^{m+1}), \tag{4}$$

where $z = [\delta/2]$, $\varepsilon_i^* = \max\{\varepsilon_i, \varepsilon_{\delta-1-i}\}$ ($i = z, z+1,\dots, \delta-2$) and $\varepsilon_z^* = \varepsilon_z$ if δ is odd, then there exists an ℓ-IE set in $\mathscr{T}(0, \varepsilon_1,\dots, \varepsilon_{k-2})$.

PROOF. Two cases must be considered, i.e., $q=0$ and $1\leqq q\leqq \ell-1$ where $k=\ell(m+1)-q$.

Case (I) when $q=0$ (i.e., $k=\ell(m+1)$). Let Y_i $(i=1, 2,\dots, \pi)$ be $\{(\ell-1)m+\ell-2\}$-flats obtained in Corollary.

We prove this theorem about only the case when δ is even, because the proof in other case is similar to the case when δ is even.

First, choose μ-flats V_j^μ $(\mu=\delta-1, \delta; j=1, 2,\dots, \varepsilon_\mu)$ in Y_k $(k=1, 2,\dots, t)$ where $t=\varepsilon_\delta+\varepsilon_{\delta-1}$. In the case $\varepsilon_i<\varepsilon_{\delta-1-i}$ $(z\leqq i\leqq \delta-2)$, let V_j^i and $V_j^{\delta-1-i}$ be an i-flat and a $(\delta-1-i)$-flat in Y_n such that $V_j^i\cap V_j^{\delta-1-i}=\phi$ for $j=1, 2,\dots, \varepsilon_i$. Let $V_j^{\delta-1-i}$ be a $(\delta-1-i)$-flat in Y_t for $j=\varepsilon_i+1, \varepsilon_i+2,\dots, \varepsilon_{\delta-1-i}$. In the case $\varepsilon_i\geqq\varepsilon_{\delta-1-i}$, we can also choose flats V_j^μ $(1\leqq\mu\leqq\delta; j=1, 2,\dots, \varepsilon_\mu)$ which are elements of an ℓ-IE set. The inequality (4) implies that there exists an ℓ-IE sets in $\mathscr{T}(0, \varepsilon_1,\dots, \varepsilon_{k-2})$.

Case (II) when $1\leqq q\leqq \ell-1$ (i.e., $k=\ell(m+1)-q$). Let G be an $\{\ell(m+1)-q-1\}$-flats in $PG(\ell(m+1)-1, s)$. Choose $(\mu+q)$-flats $V_j^{\mu+q}$ $(1\leqq\mu\leqq k-2, j=1, 2,\dots, \varepsilon_\mu)$ contained in $PG(\ell(m+1)-1, s)$ which were obtained in Case (I). Put $U_j^\mu=G\cap V_j^{\mu+q}$ for all μ and j. Then, $\mathscr{B}=\{U_j^\mu\}$ $(1\leqq\mu\leqq k-2; j=1, 2,\dots, \varepsilon_\mu)$ is a required set, because G can be identified with $PG(\ell(m+1)-q-1, s)$. This completes the proof.

Put $k=\ell(m+1)-q$ $(m\geqq 0, 0\leqq q\leqq \ell-1)$ and $\delta=[(\ell k-k-\ell)/\ell]=(\ell-1)m+\ell-2-q$. In the case $\sum_{i=\delta+1}^{k-2}\varepsilon_i=p$ $(\geqq 1)$, let us denote by $\delta+e_i$ $(i=1, 2,\dots, p)$ p integers such that

$$\overbrace{\delta+1, \delta+1,\dots, \delta+1}^{\varepsilon_{\delta+1}};\ \overbrace{\delta+2, \delta+2,\dots, \delta+2}^{\varepsilon_{\delta+2}};\dots;\ \overbrace{k-2, k-2,\dots, k-2}^{\varepsilon_{k-2}}$$

where $1\leqq e_1\leqq e_2\leqq\cdots\leqq e_p\leqq k-2$.

Put $e_1+e_2+\cdots+e_p=e$. Then, we have

THEOREM 2. *Let $(\varepsilon_1, \varepsilon_2,\dots, \varepsilon_{k-2})$ be an element in $E_{\ell-2}(k, s)-E_{\ell-3}(k, s)$ such that $1\leqq \sum_{i=\delta+1}^{k-2}\varepsilon_i(=p)\leqq \ell-2$. If $\ell-p\geqq 2$, $\tau=[e/(\ell-p)]\geqq 1$ and $(\varepsilon_1, \varepsilon_2,\dots, \varepsilon_{k-2})$ satisfies the following condition:*

$$\sum_{i=z}^{\delta-e-2}\varepsilon_i^* + \sum_{i=\delta-e-1}^{\delta}\varepsilon_i+p\leqq M_\ell(\ell, s^{m+1}) \tag{5}$$

and

$$\sum_{i=\delta-e+1}^{\delta}\varepsilon_i\leqq M_{\ell-p}(\ell-p, s^\tau) \tag{6}$$

where $z=[(\delta-e)2]$, $\varepsilon_i^*=\max\{\varepsilon_i, \varepsilon_{\delta-e-1-i}\}$ $(i=z, z+1,\dots, \delta-e-2)$ and $\varepsilon_z^*=\varepsilon_z$ if $\delta-e$ is odd, then there exists an ℓ-IE set in $\mathscr{T}(0, \varepsilon_1,\dots, \varepsilon_{k-2})$.

THEOREM 3. *Let $(\varepsilon_1, \varepsilon_2,\dots, \varepsilon_{k-2})$ be an element in $E_{\ell-2}(k, s)-E_{\ell-3}(k, s)$ such* *that* $\sum_{i=\delta+1}^{k-2} \varepsilon_i = \ell - 1$. *If* $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})$ *satisfies the following condition*:

$$\sum_{j=z}^{v-2} \varepsilon_j^* + \varepsilon_{v-1} + \varepsilon_v + \ell - 1 \leqq M_\ell(\ell, s^{m+1}), \tag{7}$$

where $v = \delta - e_\ell$, $z = [v/2]$ *and* $\varepsilon_i^* = \max\{\varepsilon_i, \varepsilon_{v-1-i}\}$ $(i = z, z+1, \ldots, v-2)$ *and* $\varepsilon_z^* = \varepsilon_z$ *if* v *is odd, then there exists an* ℓ*-IE set in* $\mathscr{T}(0, \varepsilon_1, \ldots, \varepsilon_{k-2})$.

In order to Theorems 2 and 3, we prepare a lemma. Let V_i $(i=1, 2, \ldots, p)$ and V_j $(j=p+1, p+2, \ldots, \ell)$ are $\{(\ell-1)m+\ell-2+e_i)\}$-flats and $\{(\ell-1)m+\ell-2-e_j\}$-flats in PG $(\ell(m+1)-1, s)$, respectively, such that $V_1 \cap V_2 \cap \cdots \cap V_p \cap V_{p+1} \cap \cdots \cap V_\ell = \phi$. Then it follows from Proposition 4 that e_i $(i=1, 2, \ldots, \ell)$ must be integers satisfying the following condition:

$$e_1 + e_2 + \cdots + e_p \leqq e_{p+1} + e_{p+2} + \cdots + e_\ell. \tag{8}$$

Let e_i $(i=1, 2, \ldots, \ell-1)$ be integers such that $1 \leqq e_1 \leqq e_2 \leqq \cdots \leqq e_p \leqq m$ and $0 \leqq e_{p+1} \leqq e_{p+2} \leqq \cdots \leqq e_{\ell-1}$. Put $e_\ell = \max\{(e_1+e_2+\cdots+e_p) - (e_{p+1}+e_{p+2}+\cdots+e_{\ell-1}), e_{\ell-1}\}$. Then, it is easy to see that $e_1, e_2, \ldots, e_\ell$ are integers which satisfy the inequality (8) and $e_{p+1} \leqq e_{p+2} \leqq \cdots \leqq e_{\ell-1} \leqq e_\ell$. Put $e_1+e_2+\cdots+e_p = e$ and $[e/(\ell-p)] = \tau$. Then we have

LEMMA. *If* $\tau \geqq 1$ *and* $\ell - p \geqq 2$, *then there exists an* ℓ*-IE set consists of* $\{(\ell-1)m+\ell-2+e_i\}$*-flats* V_i $(i=1, 2, \ldots, p)$, $\{(\ell-1)m+\ell-2-e_i\}$*-flats* Q_j $(j=p+1, p+2, \ldots, \ell-1)$, $\{(\ell-1)m+\ell-2-e_\ell\}$*-flats* R_k $(k=\ell, \ell+1, \ldots, \lambda+p)$ *and* $\{(\ell-1)m+\ell-2-e\}$*-flats* T_n $(n=\lambda+p+1, \lambda+p+2, \ldots, \pi)$ *in* $PG(\ell(m+1)-1, s)$ *where* $e_\ell \leqq e$, $\lambda = M_{\ell-p}(\ell-p, s^\tau)$, $\pi = M_\ell(\ell, s^{m+1})$ *and* $\lambda + p \leqq \pi$.

PROOF. Let Y_t^* $(t=1, 2, \ldots, \pi)$ be m-flats given in the proof of Proposition 3. Let U_i and V_i^* be an (e_i-1)-flat and an $(m-e_i)$-flat in Y_i^*, respectively, such that $U_i \cap V_i^* = \phi$ for $i=1, 2, \ldots, p$. Let W be the flat generated by $U_1, U_2, \ldots, U_p$, i.e., $W = U_1 \oplus U_2 \oplus \cdots \oplus U_p$. Then, it is easy to see that W is an $(e-1)$-flat where $e = e_1+e_2+\cdots+e_p$, because $\dim(Y_{i_1}^* \oplus Y_{i_2}^* \oplus \cdots \oplus Y_{i_\ell}^*) = \ell m + \ell - 1$ for any flats $Y_{i_j}^*$ $(j=1, 2, \ldots, \ell)$ in $\{Y_k^*\}$. Let $e = (\ell-p)\tau + f$ $(0 \leqq f < \ell - p)$. Then we can choose an $(e-f-1)$-flat W_1 and a $(f-1)$-flat W_2 in W such that $W_1 \cap W_2 = \phi$. Then we can obtain a set of $(\tau-1)$-flats D_i $(i=p+1, p+2, \ldots, \lambda+p)$ in W_1 such that $\dim(D_{i_1} \oplus D_{i_2} \oplus \cdots \oplus D_{i_{\ell-p}}) = e-f-1 = (\ell-p)\tau - 1$ for any flats $D_{i_1}, D_{i_2}, \ldots, D_{i_{\ell-p}}$ in $\{D_k\}$ $(i=p+1, p+2, \ldots, \lambda+p)$ where $\lambda = M_{\ell-p}(\ell-p, s^\tau)$.

We now prove this lemma by separating two cases.

Case (I) $e - (e_{p+1}+e_{p+2}+\cdots+e_{\ell-1}) > e_{\ell-1}$ (i.e., $e_\ell = e - (e_{p+1}+e_{p+2}+\cdots+e_{\ell-1})$.

Put $g - p = |\{j\colon 0 \leqq e_j \leqq \tau - 1\}|$ and $r - g = |\{j\colon e_j = \tau\}|$.

(i) Case $0 \leqq e_j \leqq \tau - 1$ $(p+1 \leqq j \leqq g)$. Let B_j and F_j be an $(e_j - 1)$-flat and a $(\tau - 1 - e_j)$-flat in D_j, respectively, such that $B_j \cap F_j = \phi$ and put $Q_j^* = B_j \oplus Y_j^*$ for $j = p+1, p+2, \ldots, g$.

(ii) Case $e_j = \tau$ $(g+1 \leqq j \leqq r)$. Put $Q_j^* = D_j \oplus Y_j^*$ for $j = g+1, g+2, \ldots, r$.

(iii) Case $\tau + 1 \leqq e_j \leqq u$ $(r+1 \leqq j \leqq \ell)$. Let F_j be a $(\tau - 1 - e_j)$-flat obtained in (i) and let $\boldsymbol{a}_{(\sigma_j + n)}$ $(n = 1, 2, \ldots, \tau - e_j)$ be a basis of F_j for $j = p+1, p+2, \ldots, g$ where $\sigma_{p+1} = 0$ and $\sigma_j = \sum_{i=p+1}^{j-1} (\tau - e_i)$ $(p+2 \leqq j \leqq g)$. Since $e_\ell = e - (e_{p+1} + e_{p+2} + \cdots + e_{\ell-1}) = (\ell - p)\tau + f - (e_{p+1} + e_{p+2} + \cdots + e_{\ell-1})$ i.e., $(\ell - p)\tau = e_\ell - f + e_{p+1} + \cdots + e_{\ell-1}$ and $e_j = \tau$ $(j = g+1, g+2, \ldots, r)$, it follows that $(\tau - e_{p+1}) + \cdots + (\tau - e_g) + (\tau - e_{g+1}) + \cdots + (\tau - e_r) + (\tau - e_{r+1}) + \cdots + (\tau - e_{\ell-1}) + (\tau - e_{\ell-1}) + (\tau - e_\ell) = (\ell - p)\tau - (e_{p+1} + e_{p+2} + \cdots + e_{\ell-1}) - e_\ell$ implies

$$\sum_{i=p+1}^{g} (\tau - e_i) = (e_\ell - f - \tau) + \sum_{i=r+1}^{\ell-1} (e_i - \tau).$$

Put $K_i = \boldsymbol{a}_{(\sigma_i+1)} \oplus \boldsymbol{a}_{(\sigma_i+2)} \oplus \cdots \oplus \boldsymbol{a}_{(\sigma_i+e_i-\tau)}$ for $i = r+1, r+2, \ldots, \ell-1$ and put $K_\ell = \boldsymbol{a}_{(\sigma_\ell+1)} \oplus \boldsymbol{a}_{(\sigma_\ell+2)} \oplus \cdots \oplus \boldsymbol{a}_{(\sigma_\ell+e_\ell-f-\tau)}$ where $\sigma_{r+1} = 0$ and $\sigma_j = \sum_{i=r+1}^{j-1} (e_i - \tau)$ $(r+2 \leqq j \leqq \ell - 1)$.

Let $Q_j^* = D_j \oplus K_j \oplus Y_j^*$ for $j = r+1, r+2, \ldots, \ell-1$ and let $R_k^* = D_k \oplus K_\ell + W_2 \oplus Y_k^*$ for $k = \ell, \ell+1, \ldots, \lambda+p$ and let $T_n^* = Y_n^* \oplus W$ for $n = \lambda+p+1, \lambda+p+2, \ldots, \pi$. It is easily to see that Q_j^* $(j = p+1, p+2, \ldots, \ell-1)$ is an $(m+e_j)$-flat and R_k^* is an $(m+e_\ell)$-flat. Let V_i, Q_j, R_k and T_n be the dual space of V_i^*, Q_j^*, R_k^* and T_n^*, respectively, for each i, j, k and n. Let $\mathscr{B} = \{V_i\} \cup \{Q_j\} \cup \{R_k\} \cup \{T_n\}$. Then $\mathscr{B}$ is a required set.

Case (II) $e - (e_{p+1} + e_{p+2} + \cdots + e_{\ell-1}) \leqq e_{\ell-1}$ (i.e., $e_\ell = e_{\ell-1}$).

Similary, it can be shown that Lemma also holds in this case. This completes the proof.

[PROOFS OF THEOREMS 2 and 3]. From lemma, we can easily prove Theorems 2 and 3 similary to Theorem 1. So we omit the proofs of Theorems 2 and 3.

As an application of Theorems 1, 2 and 3, we shall study 4-IE sets in $\mathscr{T}(0, \varepsilon_1, \ldots, \varepsilon_{k-2})$ where $(\varepsilon_1, \ldots, \varepsilon_{k-2}) \in E_2(k, s) - E_1(k, s)$. Let K_p be a set of $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})$ in $E_2(k, s) - E_1(k, s)$ such that $\sum_{i=\delta+1}^{k-2} \varepsilon_i = p$. Then we know that $0 \leqq p \leqq 3$.

PROPOSITION 7. *For each ordered set* $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})$ *in* K_0 *or* K_3, *there exists a* 4-IE *set in* $\mathscr{T}(0, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-2})$.

PROOF. We prove this theorem for only K_0, because the proof for K_3 is similar to that for K_0.

Case (I) when $q = 0$ (i.e., $k = 4(m+1)$). It is sufficient to show that there exists a 4-IE set in $\mathscr{T}(0, \varepsilon_1, \ldots, \varepsilon_{k-2})$ for the case $\varepsilon_1 = s-1$, $\varepsilon_2 = s-1, \ldots, \varepsilon_{3m+2} = s-1$ and $\varepsilon_i = 0$

$(i=3m+3,\dots, 4m+2)$.

By computing the left hand in (4), we have

$$\sum_{j=z}^{\delta} \varepsilon_j = \sum_{j=z}^{3m+2} (s-1) = ((3m+4)/2)(s-1) \quad \text{or} \quad ((3m+5)/2)(s-1)$$

according as m is even or not, because $z=(3m+2)/2$ or $z=(3m+1)/2$ according as m is even or not.

Since $M_4(4, s^{m+1})=s^{m+1}+1$, $m\geqq 1$ and $s\geqq 2$, we have $((3m+5)/2)(s-1)\leqq s^{m+1}+1$. It follows from Theorem 1 that there exists a 4-*IE* set in $\mathscr{T}(0, \varepsilon_1,\dots, \varepsilon_{k-2})$ for the case $\varepsilon_1=s-1$, $\varepsilon_2=s-1,\dots, \varepsilon_{3m+2}=s-1$ and $\varepsilon_i=0$ $(i=3m+3,\dots, 4m+2)$.

Case (II) when $1\leqq q\leqq 3$. The proof in this case is similar to that in Case (II) in Theorem 1. Thus we have the required results. This completes the proof.

PROPOSITION 8. *Let* $(\varepsilon_1, \varepsilon_2,\dots, \varepsilon_{k-2})$ *be an element in* K_1. *If* $\tau\geqq 2$, *then there exists a* 4-*IE set in* $\mathscr{T}(0, \varepsilon_1,\dots, \varepsilon_{k-2})$ *where* $\tau=[e/3]$.

PROOF. We prove this proposition about only the case when $q=0$, because the proof in another case is similar to that in the case (II) in Theorem 1.

In this case, we now prove this proposition by separating two cases $e-(e_2+e_3)>e_3$ or $e-(e_2+e_3)\leqq e_3$ (i.e., $e_4=e-(e_2+e_3)$) or $e_3=e_4$).

(i) The case $e-(e_2+e_3)>e_3$ (i.e., $e_4=e-(e_2+e_3)$).

It is sufficient to show that there exists a 4-*IE* set in $\mathscr{T}(0, \varepsilon_1, \varepsilon_2,\dots, \varepsilon_{k-2})$ for $\varepsilon_1=s-1,\dots, \varepsilon_{3m+2-e_4}=s-1$, $\varepsilon_{3m+2-e_3}=1$, $e_{3m+2-e_2}=1$, $\varepsilon_{3m+2+e_1}=1$ and $\varepsilon_i=0$ for any other integer i where $1\leqq i\leqq k-2$. Since $\tau\geqq 2$, we have $6\leqq e\leqq m$. This implies that the left hand of (5) is less than or equall to M_4 $(4, s^{m+1})$. By computing left hand in (6), it follows that

$$\sum_{i=\delta-e+1}^{\delta} \varepsilon_i = (e_2+e_3)(s-1)+2 \leqq 2\tau(s-1)+2 \leqq M_3(3, s^{\tau})$$

because $M_3(3, s^{\tau})=s^{\tau}+2$ or $s^{\tau}+1$ according as s is even or not.

PROPOSITION 9. *Let* $(\varepsilon_1, \varepsilon_2,\dots, \varepsilon_{k-2})$ *be an element in* K_1. *For* $\tau=0$, *there exists a* 4-*IE set in* $\mathscr{T}(0, \varepsilon_1,\dots, \varepsilon_{k-2})$ *where* $\tau=[e/3]$.

PROOF. (I) The case $e=1$. If $e-(e_2+e_3)>e_3$, we have $e_2=0$, $e_3=0$ and $e_4=1$ since $0\leqq e_2\leqq e_3\leqq e_4$. Therefore, it is sufficient to show that there exists 4-*IE* set in $\mathscr{T}(0, \varepsilon_1,\dots, \varepsilon_{k-2})$ for the case $\varepsilon_{3m+3}=1$, $\varepsilon_{3m+2}=2$, $\varepsilon_{3m+1}=s-1,\dots, \varepsilon_1=s-1$. It is noticed that this case occurs for $s\geqq 3$. Since $3+2(s-1)+[(3m-1+1)/2](s-1)\leqq s^{m+1}+1$, we can get the required set by similar arguments mentioned in the proof of Lemma. If $e-(e_2+e_3)\leqq e_3$, we have $e_3\geqq e/3$, i.e., $e_3\geqq 1$. In this case, it is sufficient to prove this proposition for the case $e_2=0$ and $e_3=1$ (or $e_2=1$ and $e_3=1$). Similarly to the above case, we can get the required set.

(II) The case $e=2$. The proof of this case is similar to that in the case $e=1$ except the case $e_2=0$, $e_3=1$ and $e_4=1$ $(s\geqq 3)$.

In the case case $e_2=0$, $e_3=1$ and $e_4=1$, it is sufficient to show that there exists 4-*IE* set in $\mathscr{T}(0, \varepsilon_1,..., \varepsilon_{k-2})$ for the case $\varepsilon_{3m+4}=1$, $\varepsilon_{3m+2}=1$, $\varepsilon_{3m+1}=s-1,..., \varepsilon_1=s-1$. Let $\{Y_i^*\}$ be flats given in Proposition 3. Let V_1^* and W^* be an $(m-2)$-flat and a 1-flat in Y_1^* such that $V_1^*\cap W^*=\phi$. Let us denote all the points of W^* by Q_i $(i=1, 2,..., s+1)$. Let $V_1^{(3m+4)}$ and $V_2^{(3m+2)}$ be the dual spaces of V_1^* and Y_2^*, respectively. Let $V_i^{(3m+1}$ $(i=1, 2,..., s-1)$ be the dual space of $Y_{i+2}^*\oplus Q_i$. We can choose other flats $V_j^{(3m+2-i)}$ $(i=2,..., 3m+1, j=1,..., s-1)$ in Y_j^* $(j=s+2, s+3,...)$ so that $\{V_j^\mu\}$ $(1\leqq\mu\leqq 3m+4,$ $\mu\neq 3m+3,$ $j=1, 2,..., \varepsilon_\mu)$ is a 4-*IE* set since $2+2(s-1)+[(3m-1)/2]\leqq s^{m+1}+1$. This completes the proof.

PROPOSITION 10. *Let* $(\varepsilon_1, \varepsilon_2,..., \varepsilon_{k-2})$ *be an element in* K_1. *For* $\tau=1$, *there exists a 4-IE set in* $\mathscr{T}(0, \varepsilon_1,..., \varepsilon_{k-2})$ *where* $\tau=[e/3]$.

PROOF. Two cases must be considered (i.e., $q=0$ and $1\leqq q\leqq \ell-1$)

We prove this proposition about only the case $q=0$.

(I) The case $e=3$. If $e-(e_2+e_3)>e_3$, then since $0\leqq e_2\leqq e_3$, it is sufficient to consider the following two cases, that is,

(a) $e_2=0$, $e_3=0$ and $e_4=3$

(b) $e_2=0$, $e_3=1$ and $e_4=2$

Case (a). Since $e=3$, we get $m\geqq 3$. This shows that $3+2(s-1)+[(3m-2)/2]\cdot(s-1)\leqq s^{m+1}+1$. By similar arguments in the proof of lemma we can show that there exists a 4-*IE* set in $\mathscr{T}(0, \varepsilon_1,..., \varepsilon_{k-2})$ for all $(\varepsilon_1,..., \varepsilon_{k-2})$ in K_1.

Case (b). The proof of this case is similar to that of the case $e=2$ in Proposition 9. So we omit it.

If $e-(e_2+e_3)\leqq e_3$, then we have $e_3\geqq 1$ since $0\leqq e_2\leqq e_3$. On the other hand, it is sufficient to consider the case $e_3\leqq 2$. This case is separated as follows:

(a) $e_2=1$ and $e_3=1$, (*b*) $e_2=0$ and $e_3=2$,

(c) $e_2=1$ and $e_3=2$, (d) $e_2=2$ and $e_3=2$.

Case (a). It is sufficient to show that there exists a 4-*IE* set in $\mathscr{T}(0, \varepsilon_1,..., \varepsilon_{k-2})$ for the case $\varepsilon_1=s-1$, $\varepsilon_2=s-2,..., \varepsilon_{3m+1}=s-1$, $\varepsilon_{3m+5}=1$.

Let Y_i^* $(i=1, 2,..., \pi)$ be an m-flat given in Proposition 3. Let V_1^* and W^* be an $(m-3)$-flat and a 2-flat in Y_1^* such that $V_1^*\cap W^*=\phi$. Let $\{Q_i\}$ $(i=1, 2,..., s)$ be a 3-independent set W^* and let L_i $(i=1, 2,..., s-1)$ be points passing through the point Q_s. Put $R_i^*=Y_{i+1}^*\oplus Q_i$, $T_i^*=Y_{s+i}^*\oplus L_i$ for $i=1, 2,..., s-1$ and put $U_j^*=Y_{(2s-1+j)}^*\oplus W^*$ for $j=1, 2,..., \pi-2s+1$. Let V_1, R_i, T_i and U_j be the dual space of V_1^*, R_i^*, T_i^* and U_j^*, respectively for all i and j. Put $V_1^{(3m+5)}=V_1$, $V_i^{(3m+1)}=R_i$ and $V_i^{3m}=T_i$. Let V_j^{3m-r}

$(r=1, 2; j=1, 2,\ldots, s-1)$ be a $(3m-r)$-flat in U_n $(n=1, 2,\ldots, 2s-2)$. If $3m-3$ is even, then for $d=1, 2,\ldots, z$ and $j=1, 2,\ldots, s-1$, let $V_j^{(3m-2-d)}$ and V_j^d be a $(3m-2-d)$-flat and a d-flat in U_k $(k=2s-1, 2s,\ldots, z(s-1)+2(s-1))$ such that $V_j^{(3m-2-d)} \cap V_j^d=\phi$ where $z=(3m-3)/2$. Since $1+4(s-1)+z(s-1)\leqq s^{m+1}+1$, we have the required set. We can also easily get the required set when $3m-3$ is odd.

In the case (b), (c) or (d), the proof is similar to that in the above cases in this proposition. So it is omitted here.

(II) The case $e=4$. If $e-(e_2+e_3)\geqq e_3$, then it is sufficient to consider the following four cases, that is,

(a) $e_2=0$, $e_3=0$ and $e_4=4$, (*b*) $e_2=0$, $e_3=1$ and $e_4=3$.

(c) $e_2=0$, $e_3=2$ and $e_4=2$, (d) $e_2=1$, $e_3=1$ and $e_4=2$.

The proof of Case (a) or (b) is similar to that of case (a) or (b) in the case $e=3$. So we omit them.

Case (c). Let Y_i^* $(i=1, 2,\ldots, \pi)$ be an m-flat given in Proposition 3 and let W_1^* be a 3-flat in Y_1^*. Let W^* be a 2-flat contained in W_1^* and let X be a point in W_1^* but not contained in W^*. Let $\{Q_i\}$ $(i=1, 2,\ldots, s)$ be a 3-independent set in W^* and let L_i $(i=1, 2,\ldots, s-1)$ be points passing through the point Q_s. Put $R_i^*=Y_{i+1}^*\oplus Q_i\oplus X$, $T_i^*=Y_{s+i}^*\oplus L_i\oplus X$ for $i=1, 2,\ldots, s-1$. Then, similarly to the proof of Case (a) in (I), we can get the required 4-*IE* set which contains R_i and T_i for $i=1, 2,\ldots, s-1$ where R_i and T_i denotes the dual space of R_i^* and T_i^*, respectively.

In the case (d), we can get the required 4-*IE* set similarly to the case (a) in the case $e=4$.

(III) The case $e=5$. The proof of this case is omitted, because it is also similar to the cases $e=3$ and $e=4$.

References

[1] P. Dembowski, Finite geometries, Springer-Verlag, Berlin, Heidelberg, New York, 1968.
[2] 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.
[3] N. Hamada and F. Tamari, Construction of optimal codes using flats and spreads in a finite projective geometry, European Journal of Combinatorics **3**, (1982), 129–141.
[4] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-correcting codes, North-Holland Mathematical Library, **Vol. 16**, Amsterdam, 1977.
[5] G. Solomon and J. J. Stiffler, Algebraically punctured cyclic codes, Information and Control **8** (1965), 170–179.
[6] 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.