数理解析研究所講究録
第607巻 1987年 39-51

Linear codes and t-spreads

Fumikazu Tamari

Department of Mathematics
Fukuoka University of Education
Munakata, Fukuoka 811-41
Japan

1. Introduction

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

Let V(n;s) denote an n-dimensional vector space over a Galois field GF(s). 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 (Hammming distance) of the code C is equal to d, and is denoted by (n,k,d;s)-code.

We now consider the following problem.

Problem A. Find a linear codes 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

We shall give some properties of flats in PG(n,s) in this section.

Let W be a μ-flat in PG(n,s) and let $\underline{b}_i$ $(i = 1,2,\ldots,\mu+1)$ be a basis of the μ-flat W. The $(n - \mu - 1)$-flat W defined by $W^* = \{\underline{h} \in PG(n,s) : \underline{h}\underline{b}_i^T = 0$ over GF(s) $(i = 1,2,\ldots,\mu+1)$ is called the dual space of the μ-flat W where $\underline{a}^T$ denotes the transpose of $\underline{a}$. 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 $\{V_i\}$.

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 $i = 0,1,\ldots,v_{n+1} - 1$ 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

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

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 of element of GF(q) may be represented by $\alpha^{j\theta}$ $(j = 0,1,\ldots,q - 2)$. Morever, the set of points α^i $(i = 0,1,\ldots,\theta - 1)$ 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.[2]). There exists a t-spread in PG(n,s) if and only if $t + 1$ divides $n + 1$. Furthermore, there exists a t-spread $\{V_i\}$ such that $\{V_i\}$ 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 $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_m$ 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-lineary independent set such that $|L| > |L_0|$. The cardinality of a maximal t-lineary independent set L_0 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 patially 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 $\{(\ell - 1)m + (\ell - 2)\}$-flats Y_i $(i = 1,2,\ldots,\pi)$ in $PG(\ell(m+1)-1,s)$ such that $\dim(Y_{i_1} \cap Y_{i_2} \cap \cdots \cap Y_{i_r}) = (\ell - r)m + (\ell - r - 1)$ for any flats Y_{i_j} $(j = 1, 2,\ldots,r)$ in $\{Y_k\}$ $(1 \leqq k \leqq \pi)$ where $1 \leqq r \leqq \ell$ and $\pi = M_\ell(\ell,s^{m+1})$.

Proof. It follows from Proposition 2 that there exists an m-spread $\{W_i^*\}$ $(i = 1,2,\ldots,\zeta)$ in $PG(\ell(m+1)-1,s)$ where $\zeta = (s^{\ell(m+1)} - 1)/(s^{m+1} - 1)$. Since each m-flat W_i^* can be regarded as a point in $PG(\ell-1,s^{m+1})$, there exists a maximal ℓ-linearly independent set $\{Y_k^*\}$ $(k = 1,2,\ldots,\pi)$ in $\{W_i^*\}$, i.e., $\dim(Y_{i_1}^* \oplus Y_{i_2}^* \oplus \cdots \oplus Y_{i_r}^*) = rm + r - 1$ for any flats $\{Y_{i_j}^*\}$ $(j = 1,2,\ldots,r)$ in $\{Y_k^*\}$. Let Y_k be the dual space of Y_k^* in $PG(\ell(m+1)-1,s)$ for $k = 1,2,\ldots,\pi$. Then, it follows from Proposition 1 that $\{Y_k\}$ $(k = 1,2,\ldots,\pi)$ is a required set. This completes the proof.

Corollary. There exists a regular ℓ-IE set with the cardinality π in $PG(\ell(m + 1) - 1,s)$ where π is an integer given in Proposition 3.

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

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

Proof. Let W_i^* $(i = 1,2,\ldots,\ell)$ 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 $i = 1,2,\ldots,\ell$, we have required result.

3. Linear codes and linear programmings

Let $N = \|n_{ij}\|$ $(i = 1,2,\ldots,v_k,\ j = 1,2,\ldots,v_k)$ be the incidence matrix of v_k hyperplanes H_i $(i = 1,2,\ldots,v_k)$ and v_k points Q_j $(j = 1,2,\ldots,v_k)$ in $PG(k-1,s)$ defined by

$$n_{ij} = \begin{cases} 1, & \text{if the ith hyperplane } H_i \text{ contains the jth point } Q_j, \\ 0, & \text{otherwise,} \end{cases}$$

where $v_k = (s^k - 1)/(s - 1)$.

It is known that Problem A is equivalent to the following Problem B (cf. Theorem 2.2 in [3]).

Problem B. Find a set $\{x_j\}$ $(1 \leqq j \leqq v_k)$ of nonnegative integers $\{x_j\}$ that minimizes $\sum_{j=1}^{v_k} x_j$ subject to the inequalities:

$$\sum_{j=1}^{v_k} (1 - n_{ij})x_j \geqq d \quad (i = 1,2,\ldots,v_k) \tag{3.1}$$

for given integers k, d and s.

Let d be a positive integer. It is easy to see that d can be expressed uniquely by

$$d = 1 + \theta_0 + \theta_1 s + \ldots + \theta_{k-2}s^{k-2} + \theta_{k-1}s^{k-1} \tag{3.2}$$

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

Proposition 5 (cf. Theorem 2.2 in [3]). If $\{X_j\}$ $(j = 1,2,\ldots,v_k)$ is a set of nonnegative integers satisfying the inequalities (3.1) and d is expressed as (3.2), then

$$\sum_{j=1}^{v_k} x_j \geqq k + \theta_0 v_1 + \theta_1 v_2 + \cdot \cdot \cdot + \theta_{k-1} v_k \qquad (3.3)$$

where $v_i = (s^i - 1)/(s - 1)$ for $i = 1,2,\ldots,k$.

We now give a general construction of a solution of Problem B, that is, a set of nonnegative integers satisfying the inequalities (3.1) and attaining the lower bound (3.3).

Let $\varepsilon_i = s - 1 - \theta_i$ for $i = 0,1,\ldots, k - 2$ and let $\mathcal{B}$ be a set which consists of ε_μ μ-flats V_i^μ $(0 \leqq \mu \leqq k - 2,\ i = 1,2,\ldots,\varepsilon_\mu)$ where V_i^μ's are not necessarily distinct. Given ε_i $(i = 0,1,\ldots,k - 2)$, let $\mathfrak{F}(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2})$ be the family of all such $\mathcal{B}$'s and let $\zeta_j(\mathcal{B})$ denote the number of flats in $\mathcal{B}$ which contain the point Q_j in PG(k-1,s).

Proposition 6 (cf. Theorem 3.1 in [3]). Let d be an integer given by (3.2). If there exists a set $\mathcal{B}$ in $\mathfrak{F}(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2})$ such that $\max\{\zeta_j(\mathcal{B}) : 1 \leqq j \leqq v_k\} \leqq \theta_{k-1} + 1$, then a set $\{x_j\}$ of nonnegative integers which is given by

$$\{x_j = \theta_{k-1} + 1 - \zeta_j(\mathcal{B}) \ : \ j = 1,2,\ldots,v_k\}$$

is a solution of Problem B.

Note that there exists a set $\mathcal{B}$ in $\mathfrak{F}(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2})$ such that $\max\{\zeta_j(\mathcal{B}) : 1 \leqq j \leqq v_k\} = \ell - 1$ if and only if there exists an ℓ-IE set $\mathcal{B}$ in $\mathfrak{F}(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2})$. It is known in [3] that if there exists an ℓ-IE set $\mathcal{B}$ in $\mathfrak{F}(0,\varepsilon_1,\ldots,\varepsilon_{k-2})$, then there exists an ℓ-IE set $\mathcal{B}$ in $\mathfrak{F}(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_{k-2})$ (cf. Lemma 4.1 in [3]). Therefore, in this paper we shall investigate about ℓ-IE sets of $\mathfrak{F}(0,\varepsilon_1,\ldots,\varepsilon_{k-2})$ in details.

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

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

or $$(3.4)$$

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

where β_i $(i = 1,2,\dots,t+2)$ are the first $t+2$ integers in the following series:

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

Proposition 7. A necessary condition for ε_j $(j = 1,2,\dots,k-2)$ that there exists an ℓ-IE set $\mathcal{B}$ in $\mathfrak{F}(\theta,\varepsilon_1,\dots,\varepsilon_{k-2})$ for a given positive integer ℓ $(\geqq 2)$ is that $(\varepsilon_1,\varepsilon_2,\dots,\varepsilon_{k-2}) \in E_{\ell-2}(k,s) - E_{\ell-3}(k,s)$ where $E_{-1}(k,s) = \phi$.

Proof. See Theorem 4.1 in [3].

In the following, let ℓ be an integer such that $2 \leqq \ell \leqq k-2$. Let $(\varepsilon_1, \varepsilon_2,\dots,\varepsilon_{k-2})$ be any element in $E_{\ell-2}$ where $k = \ell(m+1) - q$ $(m \geqq 0,\ 0 \leqq q \leqq \ell - 1)$. Then it follows from (3.4) that $(\varepsilon_1,\varepsilon_2,\dots,\varepsilon_{k-2})$ must be an ordered set satisfying the condition:

$$0 \leqq \sum_{i=\delta+1}^{k-2} \varepsilon_i \leqq \ell - 1 \qquad (3.5)$$

where $\delta = [(\ell k - k - \ell)/\ell] = (\ell-1)m + \ell - 2 - q$ and $[x]$ denotes the greatest integer not exceeding x.

Now, we shall describe main theorems in this paper.

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

$$\sum_{i=1}^{k-2} \varepsilon_i \leqq M_\ell(\ell,s^{m+1}),$$

then there exists an ℓ-IE set $\mathcal{B}$ in $\mathfrak{F}(0,\varepsilon_1,\ldots,\varepsilon_{k-2})$.

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

Case (I) when $q = 0$ (i.e., $k = \ell(m + 1)$). Let Y_i $(i = 1,2,\ldots,\pi)$ be $\{(\ell - 1)m + \ell - 2\}$-flats obtained in Proposition 3. Consider a μ-flat V_j^μ $(1 \leqq \mu \leqq k-2,\ j = 1,2,\ldots,\varepsilon_\mu)$ in Y_{t+j} where $t = \sum_{i=0}^{\mu-1} \varepsilon_i$ and $\varepsilon_0 = 0$. Then $\mathcal{B} = \{V_j^\mu\}$ $(1 \leqq \mu \leqq k-2,\ j = 1,2,\ldots,\varepsilon_\mu)$ is a required set.

Case (II) when $1 \leqq q \leqq \ell - 1$ (i.e., $k = \ell(m + 1) - q$). Let G be any $\{\ell(m + 1) - q - 1\}$-flat in $PG(\ell(m+1)-1,s)$. Let $V_j^{\mu+q}$ $(1 \leqq \mu \leqq k - 2,\ j = 1,2,\ldots,\varepsilon_{\mu+q})$ be a set of $(\mu + q)$-flats in $PG(\ell(m+1)-1,s)$ which were obtained in Case (I) of this theorem. Since $\dim(G \cap V_j^{\mu+q}) \geqq \mu$, we can obtain μ-flats U_j^μ $(1 \leqq \mu \leqq k - 2,\ j = 1,2,\ldots,\varepsilon_\mu)$ contained in $G \cap V_j^{\mu+q}$. Let $\mathcal{B} = \{U_j^\mu\}$. Then, $\mathcal{B}$ is required set, because G can be identified with $PG(\ell(m+1)-q-1,s)$. This completes the proof.

In the case $\sum_{i=\delta+1}^{k-2} \varepsilon_i = p \geqq 1$, let us denote by $\delta + e_i$ $(i = 1,2,\ldots,p)$ p integers such that

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

where $1 \leqq e_1 \leqq e_2 \leqq \cdots \leqq e_p \leqq k - 2$. Put $e_1 + e_2 + \cdots + e_p = e$.

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

$$\sum_{i=1}^{k-2} \varepsilon_i \leqq M_\ell(\ell,s^{m+1})$$

and

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

where $\sum_{i=\delta+1}^{k-2} \varepsilon_i = p$ and $\tau = [e/(\ell - p)](\geqq 1)$, then there exists an ℓ-IE set $\mathcal{B}$ in $\mathfrak{F}(0,\varepsilon_1,\dots,\varepsilon_{k-2})$.

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

$$\sum_{i=1}^{k-2} \varepsilon_i \leqq M_\ell(\ell,s^{m+1}) ,$$

then there exists an ℓ-IE set $\mathcal{B}$ in $\mathfrak{F}(0,\varepsilon_1,\dots,\varepsilon_{k-2})$

In order to prove Theorems 2 and 3, we prepare two lemmas.

For simplicity, Put $(\ell - 1)m + \ell - 2 = u$. Let V_i $(i = 1,2,\dots,p)$ and V_j $(j = p + 1,p + 2,\dots,\ell)$ are $(u + e_i)$-flats and $(u - e_j)$-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 condition:

$$e_1 + e_2 + \cdots + e_p \leqq e_{p+1} + e_{p+2} + \cdots + e_\ell . \tag{3.6}$$

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

Proof. Let Y_j^* ($j = 1,2,\ldots,\pi$) 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 an $(f - 1)$-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 ($i = p + 1,p + 2,\ldots,\xi + p$) 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 $\{D_i\}$ ($i = 1,2,\ldots,\xi$) where $\xi = M_{\ell-p}(\ell-p,s^\tau)$

We now prove this lemma by separating two cases.

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

(i) Case $0 \leqq e_j \leqq \tau - 1$ for $j = p + 1, p + 2, \dots, g$ where $p + 1 \leqq g \leqq \ell - 1$. 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 $j = p + 1, p + 2, \dots, g$.

(ii) Case $e_j = \tau$ for $j = g + 1, g + 2, \dots, r$ where $g + 1 \leqq r \leqq \ell - 1$. Let $Q_j^* = D_j \oplus Y_j^*$ for $j = g + 1, g + 2, \dots, r$.

(iii) Case $\tau + 1 \leqq e_j \leqq u$ for $j = r + 1, r + 2, \dots, \ell$.

Let F_j be a $(\tau - 1 - e_j)$-flat obtained in (i) and let $\underline{a}_{(\sigma_j+n)}$ $(n = 1, 2, \dots, \tau - e_j)$ be a basis of F_j for $j = p + 1, p + 2, \dots, g$ where $\sigma_{p+1} = 0$ and $\sigma_j = \sum_{i=p+1}^{j-1} (\tau - e_j)$ $(p + 2 \leqq j \leqq g)$. Since $e_\ell = e - (e_{p+1} + e_{p+2} + \dots + e_{\ell-1}) = (\ell - p)\tau + f - (e_{p+1} + e_{p+2} + \dots + e_{\ell-1})$ and $e_j = \tau$ $(j = g + 1, g + 2, \dots, r)$,

$(\tau - e_{p+1}) + \dots + (\tau - e_g) + (\tau - e_{g+1}) + \dots + (\tau - e_r) + (\tau - e_{r+1}) + \dots + (\tau - e_{\ell-1}) + (\tau - e_\ell) = (\ell - p)\tau - (e_{p+1} + e_{p+2} + \dots + e_{\ell-1}) - e_\ell$

implies

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

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

Let $Q_j^* = D_j \oplus K_j \oplus Y_j^*$ for $j = r + 1, r + 2, \ldots, \ell - 1$ and let $R_k^* = D_k \oplus K_\ell \oplus W_2 \oplus Y_k^*$ for $k = \ell, \ell + 1, \ldots, \lambda + p$ and let $T_n^* = Y_n^* \oplus W$ for $n = \lambda + p + 1, \lambda + p + 2, \ldots, \pi$.

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 $\beta = \{V_i\} \cup \{Q_j\} \cup \{R_k\} \cup \{T_n\}$. Then β is a required set.

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

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

Lemma 2. There exists an ℓ-IE set β consists of $(u + e_i)$-flats V_i $(i = 1, 2, \ldots, \ell - 1)$, $(u - e_j)$-flats Q_j $(j = \ell, \ell + 1, \ldots, \pi)$ in $PG(\ell(m+1)-1, s)$ where π is an integer which is given in Lemma 1.

Proof of this lemma is similar to that of lemma 1 and hence we omit the proof of this lemma.

[Proof of Theorem 2]. Similary to the proof of Theorem 1, we shall prove that of this theorem by separating two cases.

Case (I) when $q = 0$. From Lemma 1, we can obtain $(\delta + e_i)$-flats V_i $(i = 1, 2, \ldots, p)$ and μ-flats V_j^μ $(1 \leqq \mu \leqq \delta,\ j = 1, 2, \ldots, \varepsilon_\mu)$ such that

$$V_1 \cap V_2 \cap \cdots \cap V_p \cap U_{p+2} \cap \cdots \cap U_\ell = \phi$$

for any flats $U_{p+1}, U_{p+2}, \ldots, U_\ell$ in $\{V_j^\mu\}$. Let $\beta = \{V_j^\mu\} \cup \{V_i\}$. Then it is easy to see that β is a required set.

Case (II) when $1 \leqq q \leqq \ell - 1$. Similary to case (II) in the proof of Theorem 1, we can easily prove this theorem. This completes the proof.

[Proof of Theorem 3]. Similary to the proof of Theorem 2, we can easily prove this theorem and hence the proof of this theorem is omitted.

References

[1] B. I. Belov. V. N. Logachev. and V. P. Sadimirov, Construction of a class of linear binary codes achieving the Varshamov-Griesmer bound, Problems of Info. Transmission, 10 (3) (1974), 211-217.

[2] P. Dembowski, Finite Geometries (Springer-Verlag, Berlin, Heidelberg, New York, 1968).

[3] 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.

[4] 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.

[5] G. Solomon and J. J. Stiffler, Algebraically puctured cyclic codes, 170-179.