数理解析研究所講究録
第 311 巻 1977 年 1-10

有限射影幾何における spread を用いた maximal t-linearly independent set の構成法

広島大 理　浜田 昇
福岡教育大　玉利 文和

§1. はじめに

$V(r;s)$ をガロア体 $GF(s)$（s は素数または素数巾）上の r 次元ベクトル空間とする．$V(r;s)$ の m 個のベクトル $\underline{a}_1$, $\underline{a}_2, \cdots, \underline{a}_m$ からなる集合を L とするとき，L のどの t 個（$3 \leqq t \leqq r$）のベクトルも $GF(s)$ 上で一次独立であるならば，L を "t-linearly independent set" または "長さ m の $L_t(r,s)$-set" という．$L_t(r,s)$-set のうちで，長さのもっとも大きいものを "maximal t-linearly independent set" または "maximal $L_t(r,s)$-set" という．以下，maximal $L_t(r,s)$-set の長さを $M_t(r,s)$ で表わす．

maximal $L_t(r,s)$-set を求める問題は線型符号理論（情報理論）や線型一部実施要因計画（実験計画法）に関連する重要な問題（[1], [2] 参照）であるが，いまだ，部分的な結果しか得られていない．

最近，我々は maximal t-linearly independent set を求める問題はある特殊な線形計画法（linear programming）の問題を解くこと，すなわち，$t \geqq n \geqq 3$ の場合には，与えられた整数 r, n と素数または素数巾 s に対して，

<u>（条件A）</u> $$N\underline{x} \leqq (r-1)\underline{J}_{v_n} + \underline{w}_{v_n}$$

のもとで，$\sum_{j=1}^{v_n} x_j$ の値を最大にする非負の整数 x_j からなるベクトル $\underline{x}^T = (x_1, x_2, \cdots, x_{v_n})$ を求めることと同値であることを示し，一部の解を与えた。（文献[4]，[5]，[8] 参照）

ここに，$N = \| n_{ij} \|$ $(i, j = 1, 2, \cdots, v_n)$ は有限射影幾何 $PG(n-1, s)$ における $v_n = (s^n - 1)/(s-1)$ 個の点 $\{\underline{c}_i\}$（座標表現）と v_n 個の hyperplane $\{H_j\}$ との結合行列，i.e.,

$$n_{ij} = \begin{cases} 1, & \underline{c}_i \in H_j \text{ のとき}, \\ 0, & \text{その他}, \end{cases}$$

$\underline{J}_m$ はすべての元が 1 である m 次元列ベクトル，$\underline{w}_{v_n}^T = (w(\underline{c}_1), w(\underline{c}_2), \cdots, w(\underline{c}_{v_n}))$，$w(\underline{c}_i)$ はガロア体 $GF(s)$ 上の n 次元ベクトル $\underline{c}_i$ の non-zero 元の個数を表わす。

今回はこの線形計画法の問題に対する $\sum x_j$ の upper bound を与え，この upper bound を attain する解を有限射影幾何における flat や spread を用いて構成する方法を与える。（詳細は，文献[6]，[7] を参照）

§2. $\sum x_j$ に対する upper bound

(定理 2.1) 与えられた正の整数 r を $v_{n-1} = (s^{n-1}-1)/(s-1)$ で割ったときの商を r_1, 余りを $v_{n-1} - r_0$ で表わす. すなわち, $r = (r_1+1)v_{n-1} - r_0$ とおくと, 条件Aをみたすどんな非負の整数 $\{x_j\}$ に対しても, 次のことが成り立つ。

(i) $1 \leqq r_0 \leqq n-1$ の場合には,

$$\sum x_j \leqq (r_1+1)v_n - (r_0+1)$$

(ii) r_0 が下の(注)の(a)の型で表わせる場合には,

$$\sum x_j \leqq (r_1+1)v_n - n - \sum_{i=1}^{n-2} \varepsilon_i v_{i+1}$$

(iii) r_0 が下の(注)の(b)の型で表わせる場合には,

$$\sum x_j \leqq (r_1+1)v_n - (n-\delta_k) - \sum_{i=k}^{n-2} \varepsilon_i^* v_{i+1}$$

(注) $n-1 < r_0 \leqq v_{n-1}$ なるどんな整数も, 次のうちのいずれかで一意的に表わせる.

(a) $r_0 = n-1 + \varepsilon_1 v_1 + \varepsilon_2 v_2 + \cdots + \varepsilon_{n-2} v_{n-2}$

(b) $r_0 = n-1 + (\varepsilon_k^* v_k - \delta_k) + \sum_{i=k+1}^{n-2} \varepsilon_i^* v_i$

ここに, k, δ_k は $3 \leqq k \leqq n-2$, $1 \leqq \delta_k \leqq k-2$ をみたす整

数，$\varepsilon_1, \cdots, \varepsilon_{n-2}$ は $0 \leqq \varepsilon_1 \leqq s$, $0 \leqq \varepsilon_i \leqq s-1$, $(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{n-2}) \neq (s, s-1, \cdots, s-1)$ をみたす整数，$\varepsilon_k^*, \cdots, \varepsilon_{n-2}^*$ は $1 \leqq \varepsilon_k^* \leqq s-1$, $0 \leqq \varepsilon_j^* \leqq s-1$ $(k+1 \leqq j \leqq n-2)$ をみたす整数である．

定理 2.1 を証明するために，次の記号と補題を用意する．

$K = \{P_1, P_2, \cdots, P_k\}$ を $PG(t, s)$ $(t \geqq 2)$ の k 個の点からなる集合，$W = (w_1, w_2, \cdots, w_k)$ を $\sum_{j=1}^{k} w_j = k^*$ をみたす正の整数《非負の整数》w_j からなる *ordered set* とし，$PG(t, s)$ の i 番目の *hyperplane* H_i $(i = 1, 2, \cdots, v_n)$ に含まれる K の点を $P_{l_{ij}}$ $(j = 1, 2, \cdots, \pi_i)$ で表わす．このとき，

$$\min_i \sum_{j=1}^{\pi_i} w_{l_{ij}} = m \qquad 《\ \max_i \sum_{j=1}^{\pi_i} w_{l_{ij}} = m\ 》$$

ならば，(K, W) を *weight* $W = (w_1, w_2, \cdots, w_k)$ をもつ $\{k^*, m; t, s\}$*-min・hyper*《$\{k^*, m; t, s\}$*-max・hyper*》という．ただし，ある i に対して $\pi_i = 0$ ならば，$\min_i \sum_j w_{l_{ij}} = 0$ とする．

(補題 2.1)　ε を任意の正の整数，δ を $0 \leqq \delta \leqq t-1$ をみたす任意の整数とすると，$PG(t, s)$ におけるどんな $\{k^*, \varepsilon v_t + \delta; t, s\}$*-max・hyper* に対しても，$k^* \leqq \varepsilon v_{t+1} + \delta$ が成り立つ．

(補題 2.2)　ε_i $(i = 1, 2, \cdots, t)$ を $0 \leqq \varepsilon_1 \leqq s$, $0 \leqq \varepsilon_i \leqq s-1$ $(2 \leqq i \leqq t-1)$, $\varepsilon_t \geqq 0$ をみたす任意の整数とし，$m = \sum_{i=1}^{t} \varepsilon_i v_i$ とおくと，$PG(t, s)$ のどんな $\{k^*, m; t, s\}$−

min·hyper に対しても，$k^* \geqq \sum_{i=1}^{t} \varepsilon_i v_{i+1}$ が成り立つ．

（補題 2.3）　β を任意の非負の整数とし，

$$m = \varepsilon_k^* v_k - \delta_k + \sum_{i=k+1}^{n-2} \varepsilon_i^* v_i + \beta v_{n-1}$$

とおくと，PG$(n-1,s)$ におけるどんな $\{k^*, m; n-1, s\}$-min·hyper に対しても，

$$k^* \geqq \varepsilon_k^* v_{k+1} - \delta_k + \sum_{i=k+1}^{n-2} \varepsilon_i^* v_{i+1} + \beta v_n$$

が成り立つ．　（補題の証明は文献[6]参照）

（定理 2.1 の証明）　(i)　条件Aをみたし，かつ，

$$\sum_{j=1}^{v_n} x_j = (\gamma_1+1)v_n - (\gamma_0+1) + \nu \qquad (\nu > 0)$$

をみたす非負の整数 $\{x_j\}$ が存在したと仮定する．

$$y_j = \begin{cases} 1, & 1 \leqq j \leqq n, \\ 0, & n < j \leqq v_n \end{cases}$$

とし，$z_j = x_j + y_j \; (j = 1, 2, \cdots, v_n)$ とおくと，

$$\sum_{j=1}^{v_n} z_j = (\gamma_1+1)v_n + (n-1-\gamma_0) + \nu$$

$$\sum_{j=1}^{v_n} n_{ij} z_j \leqq (\gamma_1+1)v_{n-1} + (n-1-\gamma_0)$$

($i=1,2,\cdots,v_n$)が成り立つ．$\{z_j^*\}$ を $z_j^* \geqq z_j$ ($j=1,2,\cdots,v_n$)かつ $\max_i \sum_j n_{ij} z_j^* = (r_1+1)v_{n-1}+n-1-r_0$ をみたす任意の整数とし，

$$K=\{h_1, h_2, \cdots, h_{v_n}\}, \quad W=(z_1^*, z_2^*, \cdots, z_{v_n}^*),$$
$$k^*=\sum_j z_j^*, \quad m=\max_i \sum_j n_{ij} z_j^* = (r_1+1)v_{n-1}+n-1-r_0$$

とおくと，(K, W) は $PG(n-1,s)$ における $\{k^*, m; n-1, s\}$-max・hyper である．従って，$\varepsilon = r_1+1$，$\delta = n-1-r_0$ とおくと，補題2.1より，

$$\sum_{j=1}^{v_n} z_j^* \leqq (r_1+1)v_n+(n-1-r_0)$$

が成り立つ．一方，$\sum_j z_j = (r_1+1)v_n+(n-1-r_0)+\nu$，かつ，$\sum_j z_j \leqq \sum_j z_j^*$ であるから，$\nu \leqq 0$ をうる．これは $\nu > 0$ に矛盾する．従って，$\sum_j x_j \leqq (r_1+1)v_n-(r_0+1)$ が成り立つ．(ii), (iii) の証明には，それぞれ補題2.2，補題2.3を用いる．証明は省略する．（詳細は文献[6]参照）

§3．定理2.1の upper bound を attain する解の構成

$V(n;s)$ を $GF(s)$ の元を係数にもつ n 次元ベクトル空間，h_j ($j=1,2,\cdots,v_n$)をどの2つも $GF(s)$ 上で一次独立な $V(n;s)$ の v_n 個のベクトルとし，$H_j=\{c_i : c_i^T h_j = 0$ over $GF(s)$，

$1 \leqq i \leqq v_n\}$ とおくと，H_j は $\{\underline{c}_i\}$ を v_n 個の点とする有限射影幾何 $PG(n-1, s)$ の hyperplane である．以下，$\underline{h}_i^T = (\overset{1}{0}, \cdots, 0, \overset{i}{1}, 0, \cdots, \overset{n}{0})$ $(1 \leqq i \leqq n)$ とし，$\{\underline{h}_j\}$ を v_n 個の点とする有限射影幾何を $\overline{PG}(n-1, s)$ で表わし，$\{\underline{c}_i\}$ を v_n 個の点とする $PG(n-1, s)$ と区別することにする．

$(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{n-2})$ を $0 \leqq \varepsilon_1 \leqq s$，$0 \leqq \varepsilon_j \leqq s-1$ $(2 \leqq j \leqq n-2)$，$(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{n-2}) \neq (s, s-1, \cdots, s-1)$，$\sum \varepsilon_j \geqq 1$ をみたす任意の整数の組とし，

$F(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{n-2}; n, s) = \{ V_i^{(d)} : i = 1, 2, \cdots, \varepsilon_d, d \in S \}$ とおく．ここに，$V_i^{(d)}$ は $\overline{PG}(n-1, s)$ の d-flat で，$S = \{d : \varepsilon_d \neq 0, 1 \leqq d \leqq n-2\}$ である．

$\eta_j(F)$ $(j = 1, 2, \cdots, v_n)$ を $\overline{PG}(n-1, s)$ の点 $\underline{h}_j$ を cover する $F(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{n-2}; n, s)$ の中の flat の数とし，

$$a(F) = \max\{\eta_j(F) : 1 \leqq j \leqq n\}, \quad b(F) = \max\{\eta_j(F) - 1 : n < j \leqq v_n\}$$

とおくと，次のことが成り立つ．

(<u>定理 3.1</u>) 次の式によって与えられる $\{x_j\}$ は条件 A をみたし，かつ，定理 2.1 の upper bound を attain する解である．

(i) $1 \leqq r_0 \leqq n-1$ の場合，$(r_1 \geqq 0)$

$$x_j = \begin{cases} r_1, & 1 \leqq j \leqq r_0+1 \text{ のとき}, \\ r_1+1, & \text{その他}, \end{cases}$$

(ii) $r_0 = n-1+\sum_{i=1}^{n-2} \varepsilon_i v_i$ の場合, $r_1 \geqq \max\{a(F), b(F)\}$ ならば,

$$x_j = \begin{cases} r_1 - \eta_j(F), & 1 \leqq j \leqq n \text{ のとき}, \\ r_1+1-\eta_j(F), & \text{その他}, \end{cases}$$

(iii) $r_0 = n-1+(\varepsilon_k^* v_k - \delta_k)+\sum_{i=k+1}^{n-2} \varepsilon_i^* v_i$ の場合,

$$x_j = \begin{cases} x_j^*+1, & 1 \leqq j \leqq \delta_k \text{ のとき}, \\ x_j^*, & \text{その他}, \end{cases}$$

ここに, $\{x_j^*\}$ は $r_0^* = n-1+\sum_{i=k}^{n-2} \varepsilon_i^* v_i$ の場合の upper bound をattainする解を表わす.(証明は省略, 詳細は文献[7]参照)

(注) 上の定理は, 次のことを意味する.

(イ) $1 \leqq r_0 \leqq n-1$ の場合には, $r_1 \geqq 0$ なるどんな整数 r_1 に対しても, 定理2.1の upper bound を attain する解がある.

(ロ) (iii)の場合には, (ii)の場合に帰着される.

(ハ) (ii)の場合には, $r_1 \geqq \max\{a(F), b(F)\}$ をみたすどんな整数 r_0, r_1 (i.e., 整数 r) に対しても定理2.1の upper bound をattainする解がある. 従って, 与えられた整数 r_0 (i.e., $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{n-2}$, と n) に対して, $\max\{a(F), b(F)\}$ の値が出来るだけ小さくなるように flat の集り $F(\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{n-2}; n, s)$ を作ることが望ましい。特に, $\max\{a(F), b(F)\} = 0$

(i.e., $a(F)=b(F)=0$) となる $F(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-2};n,s)$ が存在するための r_0 に対する必要十分条件，および，そのような flat の構成方法を求めることが必要である．

(定理 3.2)　$n \geqq 4$ の場合には，$a(F)=b(F)=0$ となる $F(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-2};n,s)$ が存在するための整数 r_0，すなわち，$(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-2})$ に対する必要十分条件は，$\varepsilon_{\theta+1}=\varepsilon_{\theta+2}=\cdots=\varepsilon_{n-2}=0$ であるか，または，ある整数 k ($\theta+1 \leqq k \leqq n-2$) に対して，$\varepsilon_k=1$，$\varepsilon_{n-k-1}=\varepsilon_{n-k}=\cdots=\varepsilon_{k-1}=\varepsilon_{k+1}=\cdots=\varepsilon_{n-2}=0$ となることである．ここに，$\theta=[(n-2)/2]$ である．

(注)　$a(F)=b(F)=0$ をみたす flat の集り $F(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-2};n,s)$ を構成する際に，spread が用いられる．(詳細は，文献[7]参照)　文献[7]では，さらに，$\max\{a(F),b(F)\}=0$ となる $F(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-2};n,s)$ が存在しない場合に，$\max\{a(F),b(F)\}=1$ となる $F(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-2};n,s)$ が存在するための r_0 (i.e., $\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-2}$) に対する必要十分条件，およびそのような flat の集り $F(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-2};n,s)$ を spread を用いて構成する方法を与えている．(証明は非常に長いので省略する．)

参 考 文 献

[1] R. C. Bose (1947), Mathematical theory of the symmetrical factorial design, Sankhyā 8, 107-166.

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

[3] B. R. Gulati and E. G. Kounias (1973), Maximal sets of points in finite projective space, no t-linearly dependent, J. Combinatorial Theory (A) 15, 54-65.

[4] N. Hamada and F. Tamari (1976), Construction of maximal t-linearly independent sets, Essays in Probability and Statistics 41-55, which is presented in honor of Prof. J. Ogawa on his 60th birthday.

[5] N. Hamada and F. Tamari (1977), On a geometrical method of construction of maximal t-linearly independent sets, To appear in J. Combinatorial Theory.

[6] N. Hamada and F. Tamari (1976), Construction of maximal t-linearly independent sets using spreads in a finite projective geometry (I), Submitted to Discrete Mathematics.

[7] N. Hamada and F. Tamari (1977), Construction of maximal t-linearly independent sets using spreads in a finite projective geometry (II), Submitted to Discrete Mathematics.

[8] 浜田昇, 玉利文和 (1976), maximal t-linearly independent set の幾何学的構成法, 京大数理解析研究所講究録 285「デザインの構成法および不存在性」