数理解析研究所講究録
697巻 1989年 29-39

Arcs and Steiner triple systems

岡山大.理　丸田辰哉 (Tatsuya Maruta)

§1. 序.

n 点集合 S と S の異なる3点集合(block と呼ばれる)の集まり β が、" $x \neq y \in S \Rightarrow \exists^1 z \in S$ s.t. $\{x, y, z\} \in \beta$ " をみたすとき、(S, β) (又は単に S)を order n の Steiner triple system (又は単に $S(n)$)と呼ぶ。また、$z = xy \Leftrightarrow \{x, y, z\} \in \beta$ と定義する。次の Kirkman の定理はよく知られている。

定理 1.1 ([4]). $S(n)$ が存在する $\Longleftrightarrow n \equiv 1$ or $3 \pmod 6$.

F_q を q 個の元から成る有限体とし、$PG(r, q)$, $AG(r, q)$ をそれぞれ F_q 上の r 次元射影空間, 及び affine 空間とする。$S(7)$ と $S(9)$ は unique system であり, それぞれ $PG(2,2)$, $AG(2,3)$ である [4]。

S を $S(n)$ とする。$K \subset PG(2,q)$ が, $|K| = n$ で, K の collinear な3点を block として K が $S(n)$ をなすとき, K を $S(n)$-set in $PG(2,q)$ と呼ぶ。S に対して, system として S と同型な $S(n)$-set K in $PG(2,q)$ が存在するとき, S は $PG(2,q)$ に embeddable であるといい $S \hookrightarrow PG(2,q)$ とかく。

$S \hookrightarrow PG(2,q)$ となる F_q が存在するとき、S は embeddable であるという。明らかに、$S(7)$, $S(9)$ は embeddable である。

定理 1.2 [8], [10], [5].

(i) 十分大きな h に対して $PG(r,2) \hookrightarrow PG(2,2^h)$.

(ii) $AG(r,3) \hookrightarrow PG(2,3^r)$.

(iii) X^2-X+1 が F_q 上可約 $\Longleftrightarrow$ $AG(2,3) \hookrightarrow PG(2,q)$.

例えば、$PG(2,4)$ の Hermitian curve $\mathcal{U}_2 = V(X_0^3+X_1^3+X_2^3)$ は $S(9)$-set である。次節では $PG(2,2^h)$ に embeddable である最大の $PG(r,2)$ を arc の性質を使って求める。

定理 1.3 [8]. (i) embeddable $S(13)$ は存在しない.

(ii) embeddable $S(15)$ は $PG(3,2)$ のみ.

$PG(r,q)$ の k 点集合（又は k hyperplanes）K は、どの $r+1$ 点も 1 つの hyperplane に含まれないとき（又はどの $r+1$ hyperplanes も 1 点を共有しないとき）k-arc と呼ばれる。（$k \geq r+1$ とする）.

定理 1.4 [5]. K を k-arc in $PG(2,q)$ とする.

(i) q even, $k > q-\sqrt{q}+1 \Rightarrow K$ は unique $(q+2)$-arc に含まれる.

(ii) q odd, $k > q-\frac{\sqrt{q}}{4}+\frac{7}{4} \Rightarrow K$ は unique $(q+1)$-arc に含まれる.

arc の研究は、誤り訂正符号理論における線型 MDS 符号

(Maximum distance separable code) の研究と密接に関連している[1], [3]。§3では，$PG(3,q)$ (q even) の arc の extendability について議論する。

§2. $PG(3,q)$ の $(q+1)$-arc から得られる $S(n)$-sets

(S,β) を $S(n)$，(S_0,β_0) を $S(n_0)$ $(n_0<n)$ とする。$S_0\subset S$，$\beta_0\subset\beta$ のとき S_0 を S の subsystem という。このとき $n\geqq 2n_0+1$ が成り立つ。S の k 点部分集合 T が "$x+y\in T \Rightarrow xy\in S\setminus T$" をみたすとき，$T$ を S の k-cap という。このとき $n\geqq 2k-1$ が成り立つ。

命題 2.1. S を $S(2n+1)$，$S_0\subset S$ とすると

S_0 は S の order n の subsystem $\Leftrightarrow$ $S\setminus S_0$ は $(n+1)$-cap．

embedded k-cap in $PG(2,q)$ は k-arc である。

命題 2.2. K を $(n+1)$-arc L を含む $S(2n+1)$-set in $PG(2,q)$ とする。

L が incomplete $\Rightarrow$ $n\leqq \frac{3}{4}q$．

これと (1.4) から次の系を得る．

系 2.3. K を $S(\frac{n-1}{2})$-set を含む $S(n)$-set in $PG(2,q)$ とすると．

(i) q even，$q\geqq 2^4 \Rightarrow n\leqq 2q+1-2\sqrt{q}$

(ii) q odd，$n\neq 2q+1 \Rightarrow n\leqq 2q+\frac{5}{2}-\frac{\sqrt{q}}{2}$．

S を $S(n)$, $S \supset S' = \{x_1, x_2, \cdots, x_m\}$ とする. S' を含む S の全ての subsystems の共通部分として得られる subsystem を, S' で生成される subsystem と呼び, $\langle S' \rangle$ 或いは $\langle x_1, x_2, \cdots, x_m \rangle$ と書く.

命題 2.4. (S, β) を $S(n)$ $(n > 7)$ とする. 次は同値:

(i) S は $PG(r, 2)$ と同型 for some r.

(ii) $n = 2^{r+1} - 1$ for some r. $\exists S_0$: order $2^r - 1$ の S の subsystem.

$\exists \alpha \in S \setminus S_0$ s.t. $\langle x, y, \alpha \rangle$ は $S(7)$ for $\forall x, y \in S_0$

(iii) $\{x, y, z\} \notin \beta$ $(x, y, z \in S)$ $\Rightarrow$ $\langle x, y, z \rangle$ は $S(7)$.

(iv) 〃 〃 $\Rightarrow$ $\{xy, yz, zx\} \in \beta$.

補題 2.5. $q = 2^h$ $h \geq 4 \Leftrightarrow PG(3, 2) \hookrightarrow PG(2, q)$.

系 2.6. K_0 を 4-arc in $PG(2, q)$ $(q = 2^h, h \geq 4)$ とすると, K_0 を含み system として $K = \langle K_0 \rangle$ となる $S(15)$-sets K の数 $= (q-2)(q-4)(q-8)$.

even q $(\geq 2^3)$ に対し $K_a = \{(1, t, t^{a+1})\ ;\ t \in F_q^\times = F_q \setminus \{0\}\}$ を定義する.

命題 2.7. $q = 2^h$ $(h \geq 3)$, $a = 2^n$ に対して

$(n, h) = 1 \Leftrightarrow K_a$ は $S(q-1)$-set in $PG(2, q)$.

このとき, $S(q-1)$-set K_a は embedded $PG(h-1, 2)$.

$K \subset PG(2, q)$ を fix する $PG(2, q)$ の projectivities の群を $G(K)$ と書く.

命題2.8. $q=2^h$ $(h\geqq 3)$. $a=2^n$ $(n<h)$. $(n,h)=1$ とする.

(i) $b=2^m$ $(m<h)$. $(m,h)=1$ とすると

$a=b$ or $n+m=h$ $\Leftrightarrow$ K_a と K_b は射影同値.

(ii) $G(K_a)\simeq \mathbb{Z}_{q-1}$.

定理2.9. $r\geqq 3$ に対して.

$r\leq h-1 \Leftrightarrow PG(r,2)\hookrightarrow PG(2,2^h)$.

証明.

$\Rightarrow$) (2.7) より $PG(h-1,2)\hookrightarrow PG(2,2^h)$.

$\Leftarrow$) $PG(r,2)\hookrightarrow PG(2,2^h)$. $r\geqq 3$ とすると (2.5) より $h\geqq 4$. よって.

(2.3) より $2^r\leq q+1-\sqrt{q}<q=2^h$ i.e. $r\leq h-1$. □

問題. $q=2^h$ $(h\geqq 3)$ に対し. $PG(2,q)$ の $S(q-1)$-set は全てある K_a $(a=2^n, (n,h)=1)$ と射影同値か？

$q=16$ に対しては. (1.3)(ii). (2.6). (2.8) により $S(15)$-sets in $PG(2,16)$ は projectively unique であることが示される。

(2.7) の K_a は. 次のように $(q+1)$-arc in $PG(3,q)$ から得られる：
C を $(q+1)$-arc in $PG(3,q)$. $q=2^h$. $h\geqq 3$ とすると C は $(q+1)$-arc $\{(1,t,t^a,t^{a+1}) : t\in F_q\}\cup\{(0,0,0,1)\}$ (for some $a=2^n$. $(n,h)=1$) と射影同値 [6]. H を C の tangent lines の生成する hyperbolic

quadric とし. l_1, l_2 を $K \not\ni X = l_1 \cap l_2 \ (\neq \phi)$ なる H の generators, $P_i = l_i \cap C$, π を X を含まない plane in $PG(3,q)$ とすると容易にわかるように X から π への $C \setminus \{P_1, P_2\}$ の projection は K_a for some $a = 2^n$, $(n,h) = 1$ と同値である。

同様に. $(q+1)$-arc in $PG(3,q)$, $q = 3^h$ から embedded $AG(r,3)$ が得られる。 $q = 3^h$, $h \geq 2$ とし D を twisted cubic in $PG(3,q)$ とする。$D = \{(1,t,t^2,t^3) : t \in F_q \cup \{\infty\}\}$ としてよい。$P \in D$ に対し $X \in PG(3,q)$ を次のようにとる: $X = (0,0,1,0)$ if $P = (0,0,0,1)$,

$X = (0,1,2t,3t^2) = (0,1,-t,0)$ if $P = (1,t,t^2,t^3)$ $t \in F_q$.

line PX は D の tangent line である [7]. $D \setminus \{P\}$ の X から plane $\pi \ (\not\ni X)$ への projection は次と同値: $D' = \{Q_t = (1,t,t^3) ; t \in F_q\}$.

明らかに. $s+t+u=0 \Leftrightarrow Q_s, Q_t, Q_u$ は collinear $(s,t,u \in F_q)$. であるから D' は embedded $AG(h,3)$ である。 また. F_q 上の affine 変換群 $\{t \to at+b ; a,b,t \in F_q, a \neq 0\}$ を $GA(1,q)$ と表すと. $h > 2$ に対して $G(D') \simeq GA(1,q)$ である。

§3. $PG(3,q)$, q even の arcs の extendability について

本節の内容に関しては [1], [2] を参照されたい。

K を k-arc in $PG(3,q)$, q even とし. $k > q - \sqrt{q} + 2$ と仮定する。$t = q+3-k$ と置く。

補題3.1. (i) K の各点で t tangent lines と $\binom{t}{2}$ osculating planes が通っている.

(ii) K と 2点で交わる $PG(3,q)$ の plane は丁度 2 tangent lines を含む.

(iii) $P \in K$ における tangent line ℓ は他の tangent lines のうち $q+1$ 本と交わる (P における他の $t-1$ tangent lines と K の P 以外の $k-1$ 点における各々から1本ずつ).

補題3.2. K のどの3 tangent lines も coplanar でない.

$X \in PG(3,q) \setminus K$ に対して. X を通る K の tangent lines がきっかり i 本のとき. X は T_i-point と呼ばれる。T_i-points の数を τ_i とする.

補題3.3. (i) $\tau_i = 0$ for $t < i < k$.

(ii) $\tau_k > 0 \Rightarrow \tau_k = t-2$. K は unique $(q+1)$-arc に含まれる.

補題3.4. X を K の点又は T_t-point とし. $\ell_1, \ell_2, \dots, \ell_t$ を X を通る t tangent lines とすると 他の tangent line は $\ell_1, \ell_2, \cdots, \ell_t$ のどれか1本のみと交わる.

X を T_t-point とし. $\ell_1, \ell_2, \dots, \ell_t$ を X を通る t tangent lines とする。$P_i = \ell_i \cap K$ とし π を X を含まない plane in $PG(3,q)$ とすると (3.1)−(3.4) により $C \setminus \{P_1, P_2, \dots, P_t\}$ の X から π への

projection は π における $S(k-t)$-set となることが示される。従って、次を得る。

命題 3.5. $\tau_t > 0 \Rightarrow {}^{\exists}S(k-t)$-set in $PG(2,q)$.

$k=q+1$ に対しては、$\tau_2>0$ であり、$S(q-1)$-set を得る (§2).
(1.1) により 次を得る。

補題 3.6. $q=2^h$ に対して、h even, $3|t-1$ 或いは h odd, $3|t$ ならば $\tau_t=0$.

$PG(3,q)$ の k-arc の extendability を考える上で、次の定理が重要である。

定理 3.7. [1]. $K=\{\pi_1,\pi_2,\cdots,\pi_k\}$ を k-arc of planes in $PG(3,q)$, $q=2^h$, 各 plane π_i $(1\le i\le k)$ に対して、Z_{ij} $(j\ne i)$ を K の きっかり 2 planes 上にある $\pi_i\cap\pi_j$ の点の集合とすると、

(i) 全ての Z_{ij}, $j\ne i$ を含み、$C_i\cap\pi_j=Z_{ij}$ をみたす次数 t の代数曲線 C_i in π_i が存在する。

(ii) 代数的に C_i を含み、$V(\phi\cap\pi_i)=C_i$ をみたす次数 t の代数曲面 $\phi=\phi(K)$ が存在する $(1\le i\le k)$.

(iii) $k>q-\sqrt{q}+1$ ならば、C_i は arc of lines in π_i をなすような t lines (S-lines と呼ばれる) に分解される。

定理 3.8. $K=\{\pi_1, \pi_2, \cdots, \pi_k\}$ を complete k-arc of planes in $PG(3, q)$. $q=2^h$ とする。 $q>(t-1)^3+t-3$. $\tau_t=0$ と仮定すると、各 C_i は t S-lines に分解し、各 S-line は $\phi(K)$ に代数的に含まれるような hyperbolic quadric に属する。

これにより [1] と同様にして次を得る。

定理 3.9. K を k-arc in $PG(3, q)$. $q=2^h$ とする。 $q>(t-1)^3+t-3$, $\tau_t=0$ と仮定すると、K は K で unique に決まる $(q+1)$-arc に extend される。

従って、補題 3.6 により次の定理を得る。

定理 3.10. $q=2^h$, $h\geq 6$, $r\geq 5$ とする。 h even, $3|r$ 或いは h odd, $3|r+1$ と仮定すると

(i) $q>(r-3)^3+r-5 \Rightarrow$ $PG(r, q)$ においては $(q+1)$-arc が最大の arc である。

(ii) $q>(r-2)^3+r-4 \Rightarrow$ $PG(r, q)$ の $(q+1)$-arc は normal rational curve である。

References.

[1] A.A. Bruen, J.A. Thas and A. Blokhuis, On M.D.S. codes, arcs in $PG(n,q)$ with q even, and a solution of three fundamental problems of B. Segre, Invent. Math. 92 (1988), 441–459.

[2] L.R.A. Casse and D.G. Glynn, On the uniqueness of $(q+1)_4$-arcs of $PG(4,q)$, $q=2^h$, $h \geq 3$, Discrete Math. 48 (1984) 173–186.

[3] V.D. Goppa, Geometry and Codes, Kluwer Academic Publishers, 1988.

[4] M. Hall, Jr., Combinatorial Theory, Blaisdell, Waltham, Mass., 1967.

[5] J.W.P. Hirschfeld, Projective Geometries over Finite Fields, Oxford University Press, 1985.

[6] J.W.P. Hirschfeld, Finite Projective Spaces of Three Dimensions, Oxford University Press, 1985.

[7] H. Kaneta and T. Maruta, An elementary proof and an extension of Thas' theorem on k-arcs, to appear in Math. Proc. Cambridge Philos. Soc. 105 (1989).

[8] M. Limbos, Projective embeddings of small "Steiner triple systems", Annals of Discrete Math. 7 (1980) 151–173.

[9] L. Teirlinck, On linear spaces in which every plane is either projective or affine, Geom. Dedicata 4 (1975) 39–44.

[10] J. A. Thas. Connection between the n-dimensional affine space $A_{n,q}$, and the curve C, with equation $y = x^q$, of the affine plane A_{2,q^n}, Rend. Ist. di Matem, Univ. di Trieste. Vol II fasc. II (1970).