

Arcs and Steiner triple systems

岡山大学 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、
" $x \neq y \in S \Rightarrow \exists! z \in S$ 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、 $z = x$ かつ $\{x, y, z\} \in \beta$ 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 $\Leftrightarrow n \equiv 1$ 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、 $|K| = n$ かつ 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 であるといひ、 $S \hookrightarrow PG(2, q)$ とかく。

$S \subset \text{PG}(2, q)$ とする 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 に對して $\text{PG}(r, 2) \hookrightarrow \text{PG}(2, 2^h)$.
- (ii) $\text{AG}(r, 3) \hookrightarrow \text{PG}(2, 3^r)$.
- (iii) $X^2 - X + 1$ が F_q 上可約 $\Leftrightarrow \text{AG}(2, 3) \hookrightarrow \text{PG}(2, q)$.

例えば、 $\text{PG}(2, 4)$ の Hermitian curve $\mathcal{H}_2 = V(X_0^3 + X_1^3 + X_2^3)$ は $S(9)$ -set である。次節では $\text{PG}(2, 2^h)$ に embeddable である最大の $\text{PG}(r, 2)$ 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 $\text{PG}(3, 2)$ のみ。

$\text{PG}(r, q)$ 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 $\text{PG}(2, q)$ 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

$(S, \beta) \in S(n)$, $(S_0, \beta_0) \in S(n_0)$ ($n_0 < n$) とする. $S_0 \subset S$, $\beta_0 \subset \beta$ のとき S_0 は S の subsystem という. このとき $n \geq 2n_0 + 1$ 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 は S の k -cap という. このとき $n \geq 2k-1$ が成り立つ.

命題 2.1. $S \in S(2n+1)$, $S_0 \subset S$ 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 は $(n+1)$ -arc L を含む $S(2n+1)$ -set in $PG(2, q)$ とする.

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

これと (1.4) から次の系を得る.

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

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

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

$S \in S(n)$. $S \supset S' = \{x_1, x_2, \dots, x_m\}$ 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 $\langle x_1, x_2, \dots, x_m \rangle$ と書く.

命題 2.4. $(S, \beta) \in S(n)$ ($n \geq 7$) 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 は 4-arc in $PG(2, q)$ ($q = 2^h$ $h \geq 4$) とする. K_0 は 含み system として $K = \langle K_0 \rangle$ とする $S(15)$ -sets K の数 $= (q-2)(q-4)(q-8)$.

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

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 $PG(h-1, 2)$.

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

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

(i) $b = 2^m$ ($m < h$). $(m, h) = 1$ とすると

$$a = b \text{ or } n + m = h \iff Ka \text{ と } Kb \text{ は 射影同値}$$

(ii) $\Gamma(Ka) \simeq \mathbb{Z}_{q-1}$.

定理 2.9. $r \geq 3$ に対し

$$r \leq h-1 \iff \text{PG}(r, 2) \hookrightarrow \text{PG}(2, 2^h).$$

証明.

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

$$\Leftarrow \text{PG}(r, 2) \hookrightarrow \text{PG}(2, 2^h), r \geq 3 \text{ とすると (2.5) より } h \geq 4, \text{ かつ } 2$$

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

問題. $q = 2^h$ ($h \geq 3$) に対し $\text{PG}(2, q)$ の $S(q-1)$ -set は 全て Ka ($a = 2^n, (n, h) = 1$) と射影同値か?

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

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

quadric $\in \mathcal{L}$. $l_1, l_2 \in K \setminus X = \mathcal{L} \cap l_2$ ($\neq \emptyset$) なる H の generators, $P_i = l_i \cap C$, $\pi \in X$ を含み π の plane in $\text{PG}(3, q)$ 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 $K\alpha$ for some $\alpha = 2^n$, $(n, h) = 1$ と同値である。

同様にして, $(q+1)$ -arc in $\text{PG}(3, q)$, $q = 3^h$ 及び embedded $\text{AG}(r, 3)$ 及び得られる。 $q = 3^h$, $h \geq 2$ として D を twisted cubic in $\text{PG}(3, q)$ とする。

$D = \{(1, t, t^2, t^3) : t \in \mathbb{F}_q \cup \{\infty\}\}$ とし $P \in D$ に対し $X \in \text{PG}(3, q)$

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 $P = (1, t, t^2, t^3)$ $t \in \mathbb{F}_q$.

line PX は D の tangent line である [7]. $D \setminus \{P\}$ の X への plane

π ($\neq X$) への projection は次と同値: $D' = \{Q_t = (1, t, t^3) : t \in \mathbb{F}_q\}$.

明らかに, $s+t+u=0 \Leftrightarrow Q_s, Q_t, Q_u$ は collinear ($s, t, u \in \mathbb{F}_q$).

よって D' は embedded $\text{AG}(h, 3)$ である。また $\mathbb{F}_2$, $\mathbb{F}_q$ 上の

affine 変換群 $\{t \mapsto at+b : a, b, t \in \mathbb{F}_q, a \neq 0\} \cong \text{GA}(1, q)$ と表す。 $h \geq 2$

に対して $G(D') \cong \text{GA}(1, q)$ である。

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

本節の内容に關しては [1], [2] を参照されたい。

K を k -arc in $\text{PG}(3, q)$, q even として, $k > q - \sqrt{q} + 2$ 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 T 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 $g+1$ 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 X を通る K の tangent lines が i 本あるとき X は T_i -point と呼ばれる. T_i -points の数 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 $(g+1)$ -arc に含まれる.

補題 3.4. X を K の点 $\neq P$ T_t -point とし $l_1, l_2, \dots, l_t \in X$ を通る t tangent lines とすると他の tangent line は $l_1, l_2, \dots, l_t$ のどれか 1 本のみと交わる.

X を T_t -point とし $l_1, l_2, \dots, l_t \in X$ を通る t tangent lines とする. $P_i = l_i \cap K$ とし $\pi \in X$ 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 となることを示される。
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, $3 \nmid t-1$ 或いは h odd,
 $3 \nmid t$ 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]. $K = \{\pi_1, \pi_2, \dots, \pi_k\}$ は k -arc of planes in $PG(3, q)$.

$q = 2^h$, 各 plane π_i ($1 \leq i \leq k$) に対して、 Z_{ij} ($j \neq i$) を K の i, j 間の 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} , $j \neq i$ 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 ($1 \leq i \leq k$)。

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

定理 3.8. $K = \{\pi_1, \pi_2, \dots, \pi_k\}$ is complete k -arc of planes in $\text{PG}(3, q)$.

$q = 2^h$ 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. ϕ は hyperbolic quadric に属する.

これにより [1] と同様に (7) 次を得る.

定理 3.9. K is k -arc in $\text{PG}(3, q)$. $q = 2^h$ 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. $3 \mid r$ 或いは h odd. $3 \mid r+1$ と仮定すると

(i) $q > (r-3)^3 + r - 5 \Rightarrow \text{PG}(r, q)$ に存在しては $(q+1)$ -arc の最大の arc である.

(ii) $q > (r-2)^3 + r - 4 \Rightarrow \text{PG}(r, q)$ 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 $(q+1)_k$ -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) 39-84.

- [10] J.A. Thas. Connection between the n -dimensional affine space A_n, q , and the curve C , with equation $y = x^{\frac{q}{2}}$, of the affine plane A_2, q^n , Rend. Ist. di Matem. Univ. di Trieste. Vol II fasc. II (1970).