# 有限体上の平面曲線に関する Sziklai's conjecture について

長澤 弘明*

大阪大学大学院 理学研究科 数学専攻

前回に引き続き，城崎新人セミナーに参加させていただきありがとうございました．また，このような素晴らしい機会を設けてくださった運営委員の皆様には厚く御礼申し上げます．

## 1 序文

有限体の位数 $q$ と次数 $d$ を固定したとき, 有限体 $\mathbb{F}_q$ 上の $d$ 次射影平面曲線上にある $\mathbb{F}_q$-有理点の個数に対する上限を決定する問題の起源は, 70 年以上も前にさかのぼり, 曲線に様々な条件を課した上で現在もなお活発な研究が続けられている．また，それは代数幾何や暗号理論の発展において, 原動力のひとつであり続けている．ここでは, 射影平面曲線に対して, **$\mathbb{F}_q$-line component**<u>を持たない</u> という条件のみを課す．$\mathbb{F}_q$ 上の $d$ 次射影平面曲線 $C$ に対して $N_q(C) = {}^{\#}(C \cap \mathbb{P}^2(\mathbb{F}_q))$ とし,

$$M_q(d) = \max\{N_q(C) \mid C \text{ は } \mathbb{F}_q\text{-line component を持たない } \mathbb{F}_q \text{上の } d \text{ 次射影平面曲線 }\}$$

とおく．

2008 年に Sziklai は論文 [12] において, $\mathbb{F}_q$-line component を持たない有限体 $\mathbb{F}_q$ 上の $d$ 次射影平面曲線の $\mathbb{F}_q$-有理点の個数は, $(d-1)q+1$ を超えないことを予想した．$q+2 \le d$ のときには, 自明な不等式 $N_q(C) \le {}^{\#}\mathbb{P}^2(\mathbb{F}_q) = q^2+q+1$ より, 自動的に $M_q(d) \le q^2+q+1 \le (d-1)q+1$ が成り立つ．従って, Sziklai 予想は, $2 \le d \le q+1$ なる $d$ に対してのみ問題となる．一方, Homma-Kim [7] が指摘したように, $d = q = 4$ のときには Sziklai 予想の成立しない例が知られている ([11])．そこで, 彼らは該当する部分を次のように修正した．

**Modified Sziklai's conjecture**　$d = q = 4$ の場合を除けば $2 \le d \le q+1$ のとき

$$M_q(d) \le (d-1)q+1$$

が成り立つ．また $d = q = 4$ のときは, $N_4(C) > (4-1)\cdot 4 + 1 = 13$ なる $\mathbb{F}_4$-line component を持たない $\mathbb{F}_4$ 上の四次射影平面曲線 $C$ が存在し, 必ず

$$X^4+Y^4+Z^4+X^2Y^2+Y^2Z^2+Z^2X^2+X^2YZ+XY^2Z+XYZ^2$$

で定義される射影平面曲線と射影同値になり, $N_4(C) = (4-1)\cdot 4+2 = 14$ となる．

Hasse と Weil は $d$ 次射影平面曲線 $C$ が絶対既約な場合に $N_q(C) \le q+1+(d-1)(d-2)\sqrt{q}$ が成り立つことを証明した ([2], [3], [14], [15])．この不等式は Hasse-Weil bound と呼ばれ, のちに Serre が $N_q(C) \le q+1+(d-1)(d-2)\lfloor 2\sqrt{q}\rfloor/2$ と改良した．また Barlotti の論文 [1] の結果は, $M_q(d) \le (d-1)(q+1)+1 = (d-1)q+d$ であることと, $d \le q$ のとき $N_q(C) = (d-1)q+d$ なる $\mathbb{F}_q$-line component を持たない射影平面曲線 $C$ は, 任意の $\mathbb{F}_q$-line $l$ に対して, ${}^{\#}(C \cap l \cap \mathbb{P}^2(\mathbb{F}_q)) = 0$ または $d$ を満たすことを導いた．Segre は，論文 [10] において，

* h-nagasawa@cr.math.sci.osaka-u.jp

$M_q(d) \leq (d-1)q + \lfloor d/2 \rfloor$ を証明した．Lunelli と Sce は Barlotti の結果を改良し, 論文 [9] において, $d \nmid q$ のときに $M_q(d) \leq (d-1)q+d-3$ $(4 \leq d)$, $M_q(d) \leq (d-1)q+d-4$ $(9 \leq d)$ や $M_q(d) \leq (d-1)q+8d/13$ $(q \gg d)$ を示した．

このように, Barlotti の示した不等式はかなり評価が粗かったし, Lunelli, Sce は少し改良したものの $q, d$ に様々な条件を課さざるを得なかった．そのため, Sziklai の予想が正しければ, $q, d$ に条件を課さず, かつ, かなり精密な評価が与えられるという点で大きな進歩である．$d = q = 4$ のときに反例はあるものの, それ以外の場合に Sziklai の予想の可否を精査することは，このような意味で大変重要である．

## 2 平面曲線上の有理点の個数の上限について

平面曲線上の有理点の個数の上限について論じる前に，次のことを注意しておく必要がある．

**注意 2.1.** 平面曲線が $\mathbb{F}_q$-line component を持ってもよいとすると, $d \leq q+1$ のとき, 最大の $\mathbb{F}_q$-有理点の個数を持つ平面曲線 $C$ は, $d$ 本の $\mathbb{F}_q$-lines が同一の $\mathbb{F}_q$-有理点で交わる曲線, すなわち, $\alpha_i X + \beta_i Y$ $(1 \leq i \leq d)$ で定義される異なる $d$ 本の $\mathbb{F}_q$-lines に対し, $\sum_{i=1}^{d}(\alpha_i X + \beta_i Y)$ で与えられる曲線に射影同値であることがすでに知られている．すなわちこの場合, $\mathbb{F}_q$-有理点の個数は $dq+1$ であることが分かる．

また $d \geq q+2$ のときは, 明らかに最大の $\mathbb{F}_q$-有理点の個数は, $\mathbb{P}^2(\mathbb{F}_q) = q^2+q+1$ である．

よって興味の対象となるのは，$2 \leq d \leq q+1$ の場合であり，この条件のもとで考えることにする．

### 2.1 様々な上界

Segre は，論文 [10] において，

$$M_q(d) \leq (d-1)q + \left\lfloor \frac{d}{2} \right\rfloor \tag{2.1}$$

を証明した ([10, Teorema II])．また, Homma と Kim が

$$M_q(d) \leq (d-1)q + (q+2-d) \tag{2.2}$$

を示した ([7, Corollary.2.2])．

### 2.2 Modified Sziklai's conjecture の上限

Sziklai は論文 [12] において, 不等式

$$M_q(d) \leq (d-1)q+1$$

が成り立つことを予想した ([12, Conjecture 1])．それに対し, Homma と Kim は $q = d = 4$ のときの反例を指摘した上で，次の Modified Sziklai's conjecture を打ち立て研究を始めた．Modified Sziklai's conjecture とは次のものである．

**予想 2.2 (Modified Sziklai's conjecture).** [6] $d = q = 4$ の場合を除けば $M_q(d) \leq (d-1)q+1$ が成り立つ．また $d = q = 4$ のときは, $N_4(C) > (4-1)\cdot 4+1 = 13$ なる $\mathbb{F}_4$-line component を持たない $\mathbb{F}_4$ 上の四次平面曲線 $C$ が存在し, 必ず

$$X^4 + Y^4 + Z^4 + X^2Y^2 + Y^2Z^2 + Z^2X^2 + X^2YZ + XY^2Z + XYZ^2 \tag{2.3}$$

で定義される平面曲線と射影同値になり, $N_4(C) = (4-1)\cdot 4+2 = 14$ となる．(図 1 を参照)

また, 次のことも, Homma と Kim によって証明された．

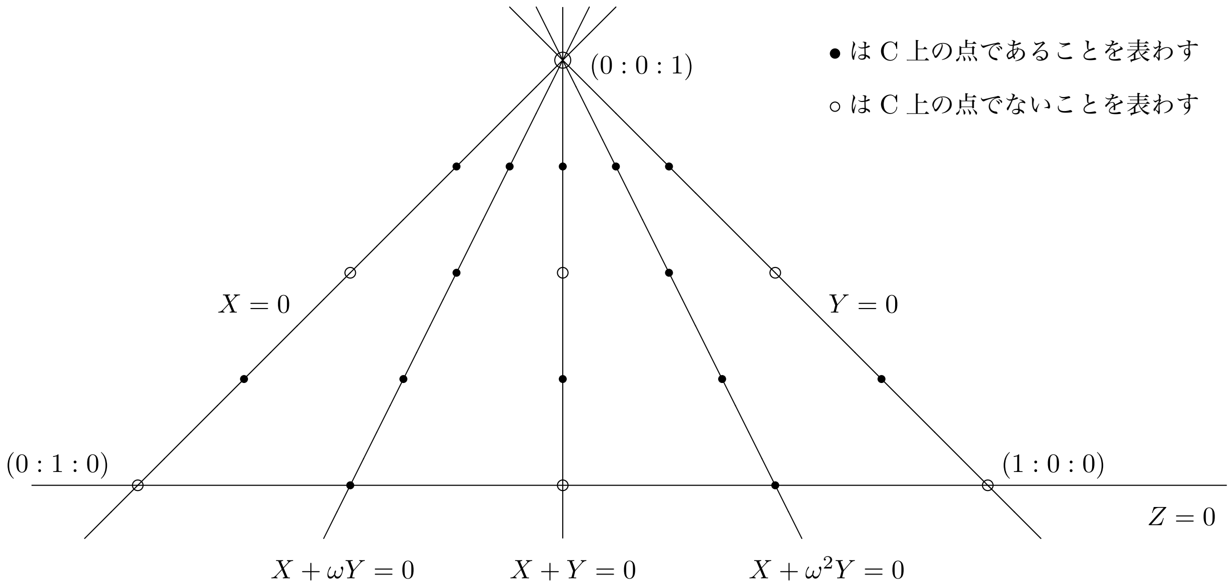



図 1

命題 **2.3.** [7, Theorem 3.3] $\mathbb{F}_4$-line component を持たない $\mathbb{F}_4$ 上の四次平面曲線 $C$ が, $N_4(C) = 14$ を満たすならば, $C$ は, 斉次多項式 (2.3) で定義される平面曲線に射影同値である.

$d = q + 1$ のとき, 不等式 (2.2) から $M_q(q + 1) \leq ((q + 1) - 1)q + 1$ が従う. このことから, $d \geq q + 1$ のとき $M_q(d) \leq (d - 1)q + 1$ が成り立つことが分かる. よって以下 $\boldsymbol{d \leq q}$ の場合のみ考えたらよい.

## 3 Homma-Kim の定理

まず $\boldsymbol{d = q}$ のとき, Modified Sziklai's conjecture が正しいことをみる. $d = q = 2, 3$ の時成り立つことはすぐ確認できるので, $d = q \geq 5$ のときに, Sziklai's conjecture が正しいことを見ていく. ここで登場するのが次の Homma-Kim の定理である.

**Homma-Kim** の定理 [6, Theorem3.3]
$d = q \geq 5$ のとき, Sziklai's conjecture が成り立つ. すなわち, $M_q(q) \leq (q - 1)q + 1$ が成り立つ.

### 3.1 必要な補題

補題 **3.1.** $\mathbb{F}_q$-point $\mathrm{P}_0 \in C(\mathbb{F}_q)$ と, $\mathrm{P}_0$ を通らない $\mathbb{F}_q$-line $l_\infty$ に対し, $\mathrm{P}_0$ を通る $t$ $(3 \leq t \leq q)$ 本の $\mathbb{F}_q$-lines $l_1, \ldots, l_t$ が存在し, 任意の $i$ $(1 \leq i \leq t)$ に対し, $l_i \setminus l_\infty$ における $q$ 個すべての $\mathbb{F}_q$-points は $C$ 上にあるとする. このとき, $l_1, \ldots, l_t$ 以外の $\mathrm{P}_0$ を通る $\mathbb{F}_q$-line $l$ があって, $^{\#}((l \setminus l_\infty) \cap C(\mathbb{F}_q)) \geq q - t + 2$ を満たすならば, $l \setminus l_\infty$ 上の $q$ 個すべての $\mathbb{F}_q$-points は $C$ 上にある. (図 2)

補題 **3.2.** $\mathbb{F}_q$-point $\mathrm{Q}_0 \in \mathbb{P}^2(\mathbb{F}_q) \setminus C(\mathbb{F}_q)$ に対し, $\mathrm{Q}_0$ を通る $t$ $(2 \leq t \leq q - 1)$ 本の $\mathbb{F}_q$-lines $l_1, \ldots, l_t$ が存在し, 任意の $i$ $(1 \leq i \leq t)$ に対し, $l_i \setminus \{Q_0\}$ における $q$ 個すべての $\mathbb{F}_q$-points は $C$ 上にあるとする. このとき, $\mathrm{Q}_0$ を通る $l_1, \ldots, l_t$ 以外の $\mathbb{F}_q$-line $l$ があって, $^{\#}((l \setminus \{\mathrm{Q}_0\}) \cap C(\mathbb{F}_q)) \geq q - t + 1$ を満たすならば, $l \setminus \{\mathrm{Q}_0\}$ 上の $q$ 個すべての $\mathbb{F}_q$-points は $C$ 上にある. (図 3)

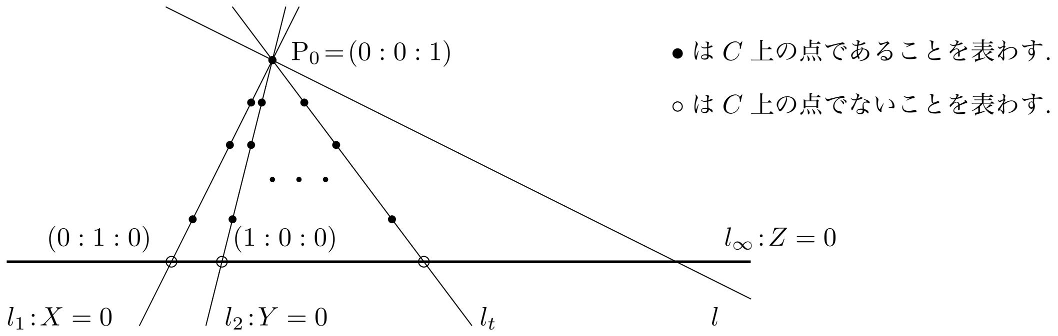



図 2

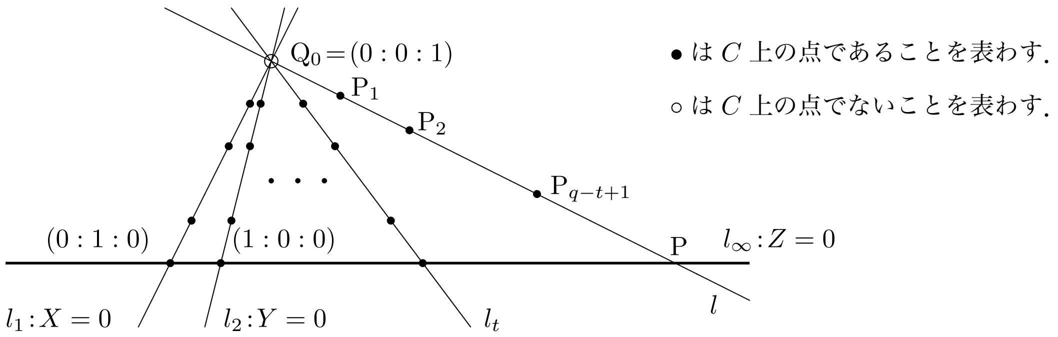



図 3

**補題 3.3.** $\mathbb{F}_q$-有理点を特異点に持たない平面曲線 $C$ の $i$-secants の本数を $a_i$ で表わしたとき, 次の四つが成り立つ.

(1) $\displaystyle\sum_{i=0}^{q} a_i = q^2 + q + 1$

(2) $\displaystyle\sum_{i=1}^{q} ia_i = (q+1)N_q(C)$

(3) $\displaystyle\sum_{i=2}^{q} i(i-1)a_i = N_q(C)\cdot(N_q(C)-1)$

(4) $\displaystyle\sum_{i=1}^{\lfloor\frac{q}{2}\rfloor} ia_i + \sum_{j=1}^{\lfloor\frac{q-1}{2}\rfloor} ja_{q-j} \geq N_q(C)$

**補題 3.4.** 平面曲線 $C$ が $\mathbb{F}_q$-有理点 $\mathrm{P}_0$ を特異点に持つとき, $N_q(C) < q(q-1)$ が成り立つ.

## 3.2 Homma-Kim の定理の証明

**定理 3.5** (**Homma-Kim の定理**)**.** $C$ を $\mathbb{F}_q$-line component を持たない $q$ 次平面曲線とする. このとき, $d = q \geq 5$ ならば Sziklai's conjecture が成り立つ. すなわち, $M_q(q) \leq (q-1)q+1$ が成り立つ.

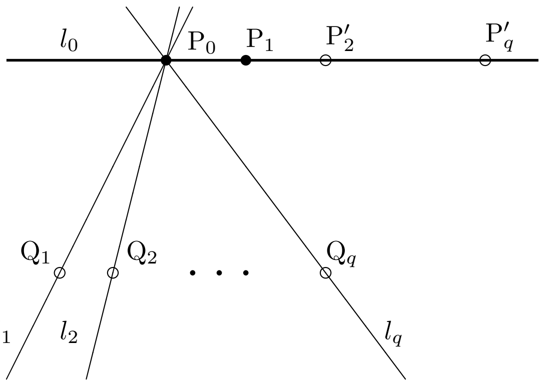
**Homma-Kim の定理の証明.**
$N_q(C) = (q-1)q+2 = q^2-q+2$ を満たす $q$ 次平面曲線 $C$ があると仮定する. このとき補題 3.4 により $C$ は $\mathbb{F}_q$-有理点を特異点に持たないとしてよい. 補題 3.3 と同様に, $C$ の $i$-secants の本数を $a_i$ で表わすことにする.

**主張 3.6.** $a_0 = a_1 = a_2 = 0$ が成り立つ.

証明. 補題 3.3 (1), (3), (4) と $q \geq 5$ より,

$$
\begin{aligned}
qa_0 + (q-2)a_1 + (q-4)a_2 &\leq \sum_{i=0}^{\lfloor \frac{q}{2} \rfloor} (q-2i)\, a_i \\
&= \sum_{i=0}^{\lfloor \frac{q}{2} \rfloor} (q-i)a_i - \sum_{i=1}^{\lfloor \frac{q}{2} \rfloor} ia_i \\
&= \sum_{i=0}^{q} (q-i)a_i - \sum_{i=\lfloor \frac{q}{2} \rfloor +1}^{q} (q-i)a_i - \sum_{i=1}^{\lfloor \frac{q}{2} \rfloor} ia_i \\
&= q\sum_{i=0}^{q} a_i - \sum_{i=0}^{q} ia_i - \sum_{i=1}^{\lfloor \frac{q-1}{2} \rfloor} ia_{q-i} - \sum_{i=1}^{\lfloor \frac{q}{2} \rfloor} ia_i \\
&\leq q(q^2+q+1) - (q+1)(q^2-q+2) - (q^2-q+2) \\
&= q-4
\end{aligned}
$$

が成り立つ. $a_0, a_1, a_2$ は非負整数より $a_0 = a_1 = 0$ かつ $a_2 = 0, 1$ がいえる.
そこで $a_2 = 1$ と仮定し, 唯一の bisecant line を $l_0$ とする. $l_0$ 上の $q+1$ 個の $\mathbb{F}_q$-有理点のうち, $C$ 上にある二点を $\mathrm{P}_0, \mathrm{P}_1$ とし, $C$ 上にない $q-1$ 点を $\mathrm{P}'_2, \mathrm{P}'_3, \ldots, \mathrm{P}'_q$ とする. $\mathrm{P}_0$ を通る $q+1$ 本の $\mathbb{F}_q$-lines を $l_0, l_1, \ldots, l_q$ とする. また $q$ 次平面曲線 $C$ が $\mathbb{F}_q$-line component を持たないことから, 任意の $i$ $(1 \leq i \leq q)$ に対し, $C$ 上にない $\mathbb{F}_q$-line $l_i$ 上の $\mathbb{F}_q$-有理点 $\mathrm{Q}_i$ が必ず存在する.



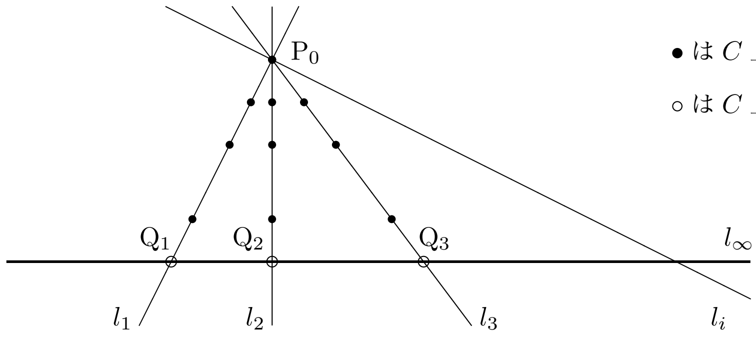

● は $C$ 上の点であることを表わす.

○ は $C$ 上の点でないことを表わす.

ここで $N_q(C) = q^2 - q + 2$ より, $^{\#}(\mathbb{P}^2(\mathbb{F}_q) \setminus C(\mathbb{F}_q)) = (q^2+q+1) - (q^2-q+2) = 2q-1$ であるから, $\mathbb{P}^2(\mathbb{F}_q) \setminus C(\mathbb{F}_q) = \left\{\mathrm{P}'_2, \ldots, \mathrm{P}'_q, \mathrm{Q}_1, \ldots, \mathrm{Q}_q\right\}$ と分かる. すなわち, $\mathrm{Q}_i$ が $C$ 上にない唯一の $l_i$ 上の $\mathbb{F}_q$-有理点である. 特に, 任意の $i, j$ $(1 \leq i < j \leq q)$ に対し, 三点 $\mathrm{P}_0, \mathrm{Q}_i, \mathrm{Q}_j$ は同一の $\mathbb{F}_q$-line 上にないことが分かる. また, $\mathrm{P}_0$ のかわりに $\mathrm{P}_1$ を考えることにより, 任意の $i, j$ $(1 \leq i < j \leq q)$ に対し, 三点 $\mathrm{P}_1, \mathrm{Q}_i, \mathrm{Q}_j$ が同一の $\mathbb{F}_q$-line 上にないことがいえる.

次に, 三点 $\mathrm{Q}_1, \mathrm{Q}_2, \mathrm{Q}_3$ が同一の $\mathbb{F}_q$-line $l_\infty$ 上にあるとする. このとき任意の $\mathbb{F}_q$-line $l_i$ $(4 \leq i \leq q)$ に対し, $^{\#}((l_i \setminus l_\infty) \cap C(\mathbb{F}_q)) \geq q-1 = q-3+1$ (ただし, 等号成立は $l_i \cap l_\infty \neq \{\mathrm{Q}_i\}$ のとき) が成り立つから, 補題 3.1 を適用することによって, $l_i \cap l_\infty = \{\mathrm{Q}_i\}$ であることが分かる.
すなわち, 点 $\mathrm{Q}_i$ $(1 \leq i \leq q)$ は $l_\infty$ 上にあることになり, $l_\infty \cap \{\mathrm{P}_0, \mathrm{P}_1\} = \emptyset$ であることから, $a_0 = 0$ に矛盾である. ここから, $\mathrm{Q}_i$ $(1 \leq i \leq q)$ の任意の異なる三点は, 同一の $\mathbb{F}_q$-line 上にないことが分かる. ゆえに, $\mathcal{K} := \{\mathrm{P}_0, \mathrm{P}_1, \mathrm{Q}_1, \ldots, \mathrm{Q}_q\}$ は $(q+2)$-arc となる. すなわち, $q$ は偶数で $\mathcal{K}$ は oval であると分かる. 今 $q \geq 5$ であるから, $q \geq 8$ がいえる.

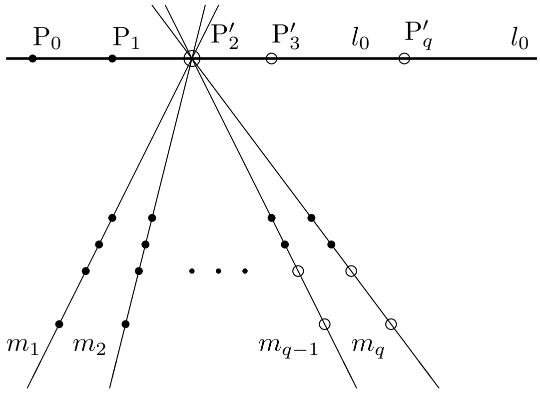
次に, $\mathrm{P}'_2$ を通る $l_0$ 以外の $q$ 本の $\mathbb{F}_q$-lines $m_1, \ldots, m_q$ について考える. $(q+2)$-arc $\mathcal{K}$ は unisecant を持




● は $C$ 上の点であることを表わす.

○ は $C$ 上の点でないことを表わす.

たないので, bisecant しか持たないことが分かる. よって, 半分の $m_1, \ldots, m_{\frac{q}{2}}$ が $\mathcal{K}$ を通らず, もう半分の $m_{\frac{q}{2}+1}, \ldots, m_q$ はそれぞれ, $\mathcal{K}$ のちょうど二点を通るとしてよい.




● は $C$ 上の点であることを表わす.

○ は $C$ 上の点でないことを表わす.

ところが, $q \geq 8$ なので, $m_j(\mathbb{F}_q) \setminus \{\mathrm{P}'_2\} \subset C$ $(j = 1, 2, 3)$ かつ ${}^{\#}((m_q \setminus \{\mathrm{P}'_2\}) \cap C(\mathbb{F}_q)) = (q+1) - 3 \geq q - 3 + 1$ であるから, 補題 3.2 を $\mathrm{P}'_2, m_1, m_2, m_3, m_q$ に対して適用できるが, このとき $m_q(\mathbb{F}_q) \setminus \{\mathrm{P}'_2\} \subset C$ となり矛盾する. 以上により, $a_0, a_1, a_2 = 0$ が示された. □

**主張 3.7.** $3 \leq \min\{i \mid a_i \neq 0\} \leq q - 3$ が成り立つ.

証明. $k := \min\{i \mid a_i \neq 0\}$ とおく. $q - 2 \leq k$ と仮定する.

このとき, $a_0 = a_1 = \cdots = a_{q-3} = 0$ であるから, 補題 3.3 (1), (2), (3) より次が成り立つ.

$$\begin{aligned}
&a_{q-2} + a_{q-1} + a_q &&= q^2 + q + 1 \\
&(q-2)a_{q-2} + (q-1)a_{q-1} + qa_q &&= (q+1)(q^2 - q + 2) \\
&(q-2)(q-3)a_{q-2} + (q-1)(q-2)a_{q-1} + q(q-1)a_q &&= (q^2 - q + 2)(q^2 - q + 1)
\end{aligned}$$

$a_q, a_{q-2}$ を消去することにより, $a_{q-1} = (q-2)(4-q)$ を得る. ところが今 $q \geq 5$ であるから, $a_{q-1} < 0$ となり矛盾である. ゆえに, $k \leq q - 3$ がいえる. □

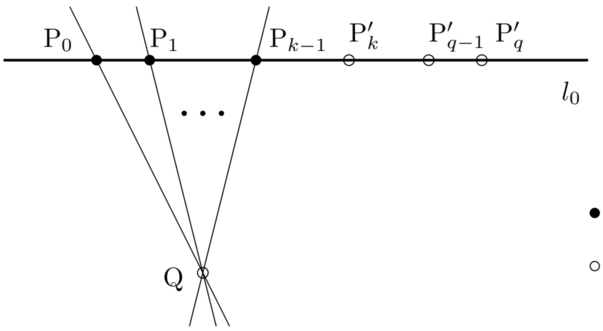
そこで, その $k$-secant を $l_0$ とする. また, $l_0 \cap C(\mathbb{F}_q) = \{\mathrm{P}_0, \ldots, \mathrm{P}_{k-1}\}, l_0 \setminus C(\mathbb{F}_q) = \left\{\mathrm{P}'_k, \ldots, \mathrm{P}'_q\right\}$ とする.

さて, $l_0$ 上にも $C$ 上にもない $\mathbb{F}_q$-points 全体からなる集合 $S = \mathbb{P}^2(\mathbb{F}_q) \setminus (l_0 \cup C)$ を考えると,

$$\begin{aligned}
{}^{\#}S &= {}^{\#}\mathbb{P}^2(\mathbb{F}_q) - (q - k + 1) - N_q(C) \\
&= (q^2 + q + 1) - (q - k + 1) - (q(q-1) + 2) \\
&= q + k - 2 \ (\geq q + 1)
\end{aligned}$$

である. このとき次が成り立つ.

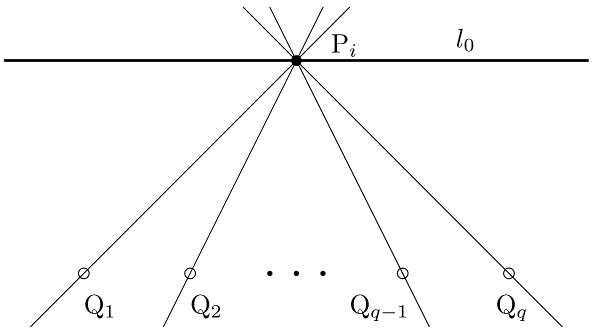
**主張 3.8.** ある点 $\mathrm{Q} \in S$ があり, ${}^{\#}\{\mathrm{P}_i \mid 0 \leq i \leq k-1, \mathrm{P}_i\mathrm{Q}$ は $q$-secant$\} \geq 3$ が成り立つ




● は $C$ 上の点であることを表わす.

○ は $C$ 上の点でないことを表わす.

証明. $i \in \{0, \dots, k-1\}$ を一つ固定する. ここで, $q$ 次平面曲線 $C$ が $\mathbb{F}_q$-line component を持たないことから, $\mathrm{P}_i$ を通る $l_0$ 以外の $q$ 本の $\mathbb{F}_q$-lines は, すべて $S$ の点を必ず通る. そこで, $S = \{\mathrm{Q}_1, \mathrm{Q}_2, \dots, \mathrm{Q}_{q+k-2}\}$ とし, $q$ 本の $\mathbb{F}_q$-lines を $\mathrm{P}_i\mathrm{Q}_1, \mathrm{P}_i\mathrm{Q}_2, \dots \mathrm{P}_i\mathrm{Q}_q$ としてよい.




● は C 上の点であることを表わす

○ は C 上の点でないことを表わす

この下で, 任意の $j$ $(1 \le j \le q)$ に対し, $\mathrm{P}_i\mathrm{Q}_j$ が $C$ の $q$-secant であることと, $\mathrm{P}_i\mathrm{Q}_j \cap \{\mathrm{Q}_{q+1}, \dots, \mathrm{Q}_{q+k-2}\} = \emptyset$ であることは同値であるから,

$$
{}^{\#}\{\mathrm{P}_i \mid 1 \le j \le q, \mathrm{P}_i\mathrm{Q}_j \text{は } C \text{ の } q\text{-secant}\} \ge q - (k-2)
$$

(ただし, 等号成立は $\mathrm{Q}_{q+1}, \dots, \mathrm{Q}_{q+k-2}$がすべて異なる $\mathbb{F}_q$-line 上にあるとき.)

がいえる. これがすべての $i \in \{0, \dots, k-1\}$ でいえるので,

$$
{}^{\#}\{(\mathrm{P}_i, \mathrm{Q}) \mid 0 \le i \le k-1, \mathrm{Q} \in S, \mathrm{P}_i\mathrm{Q} \text{ は } q\text{-secant}\} \ge k(q-k+2) \tag{3.1}
$$

が成り立つ.

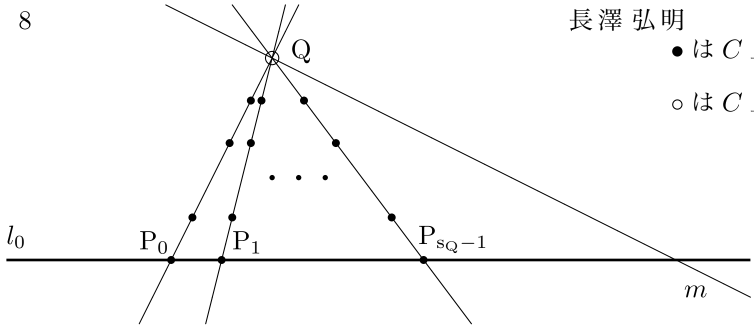
また, 任意の点 $\mathrm{Q} \in S$ に対して, ${}^{\#}\{\mathrm{P}_i \mid 0 \le i \le k-1, \mathrm{P}_i\mathrm{Q} \text{ は } q\text{-secant}\} \le 2$ と仮定すると, (不等式 (3.1) の左辺) $\le 2\,{}^{\#}S = 2(q+k-2)$ がいえる. ゆえに, $2(q+k-2) - k(q-k+2) = (2-k)(q-k-2) \ge 0$ が成り立つ. ところが, これは主張 3.7 に矛盾である. ゆえに題意は示された. □

そこで, $s_{\mathrm{Q}} := {}^{\#}\{\mathrm{P}_i \mid 0 \le i \le k-1, \mathrm{P}_i\mathrm{Q} \text{ は } q\text{-secant}\} \ge 3$ なる $\mathrm{Q} \in S$ をとる. ここで, $\mathrm{P}_0\mathrm{Q}, \dots, \mathrm{P}_{s_{\mathrm{Q}}-1}\mathrm{Q}$ $(3 \le s_{\mathrm{Q}} \le k)$ は $q$-secant としてよい. 点 Q を通る他の $\mathbb{F}_q$-lines $\mathrm{P}_{s_{\mathrm{Q}}}\mathrm{Q}, \dots, \mathrm{P}_{k-1}\mathrm{Q}, \mathrm{P}'_k\mathrm{Q}, \dots, \mathrm{P}'_q\mathrm{Q}$ は $q$-secant でなく, そのうちの一本を $m$ とすると, 補題 3.2 より, ${}^{\#}(m \cap C(\mathbb{F}_q)) \le q - s_{\mathrm{Q}}$ がいえる.

ゆえに,

$$
{}^{\#}(m \cap (S \setminus \{\mathrm{Q}\})) \ge \begin{cases} s_{\mathrm{Q}} & (m \text{ として}, \mathrm{P}_i\mathrm{Q}\ (s_{\mathrm{Q}} \le i \le k-1) \text{ をとったとき.}) \\ s_{\mathrm{Q}-1} & (m \text{ として}, \mathrm{P}'_j\mathrm{Q}\ (k \le j \le q) \text{ をとったとき.}) \end{cases}
$$

となる. 従って, ${}^{\#}(S \setminus \{\mathrm{Q}\}) \ge s_{\mathrm{Q}}(k - s_{\mathrm{Q}}) + (s_{\mathrm{Q}} - 1)(q - k + 1)$ がいえる.




● は $C$ 上の点であることを表わす.

○ は $C$ 上の点でないことを表わす.

一方, ${}^{\#}S = q + k - 2$ かつ $3 \leq s_{\mathrm{Q}} \leq k \leq q - 3$ であるから,

$$\begin{aligned}
&{}^{\#}(S \setminus \{\mathrm{Q}\}) - s_{\mathrm{Q}}(k - s_{\mathrm{Q}}) - (s_{\mathrm{Q}} - 1)(q - k + 1) \\
&\qquad = q + k - 3 + s_{\mathrm{Q}}(s_{\mathrm{Q}} - q - 1) + (q - k + 1) \\
&\qquad = {s_{\mathrm{Q}}}^2 - (q + 1)s_{\mathrm{Q}} + 2(q - 1) \\
&\qquad = (s_{\mathrm{Q}} - 2)(s_{\mathrm{Q}} - (q - 1)) < 0
\end{aligned}$$

なのでこれは矛盾である.

以上により, Homma-Kim の定理が証明された. □

## 4 $d \leq q - 1$ の場合の Sziklai's conjecture

Homma と Kim はプレプリント [6] において, $d \leq q - 1$ の場合の Modified Sziklai's conjecture についても言及している.

**命題 4.1.** [6, Theorem 4.1, Remark 4.2] 平面曲線 $C$ が, 特異点としてカスプを持たない既約曲線であれば, $d \leq q - 1$ のとき $N_q(C) \leq (d - 1)q + 1$ が成り立つ.

また不等式 (2.1) によって次が示される.

**命題 4.2.** 平面曲線 $C$ が, $\mathbb{F}_q$-line component を持たない $q + 1$ 次以下の可約曲線であれば, $N_q(C) < (d - 1)q$ が成り立つ.

以上をもって次のことが証明されたことになる.

**定理 4.3.** $C$ を $\mathbb{F}_q$-line component をもたない可約曲線, または特異点としてカスプを持たない既約曲線とする. このとき, 任意の $q, d$ $(2 \leq d \leq q + 1)$ に関して, $C$ が斉次多項式 (2.3) で定義される平面曲線に射影同値でなければ $N_q(C) \leq (d - 1)q + 1$ が成り立つ.

## 5 終わりに

以上が, 城崎新人セミナーに対する報告です. その後, 2010 年 3 月に本間正明教授から $d \leq q - 1$ の場合も Sziklai's conjecture が正しいことが, 証明できたとのメールをいただきました. (詳しくは, プレプリント Sziklai's conjecture on the number of a plane curve over a finite field III をご覧ください. )

## 参考文献

[1] A. Barlotti. *Sui k,n-archi di un piano lineare finito*, Boll. Unione Mat. Ital. **11** (1956) 553–556

[2] H. Hasse, *Abstrakte Begründung der Komplexen Multiplication und Riemannsche Vermutung in Funktionenkörpern*, Abh. Math. Sem. Univ. Hamburg **10** (1934), 325–348

[3] H. Hasse, *Punti razionali sopra curve algebriche a congruenze*, Reale Accademia d'Italia, Fondazione Allessandro Volta, Atti dei Convegni, v. 9 (1939), pp. 85–140 publisher, unknown, Rome, 1943.

[4] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford Univ. Press (1979)

[5] J. W. P. Hirschfeld, G. Korchmaros, F. Torres, *Algebraic Curves Over a Finite Field*, Princeton Univ. Press (2008)

[6] M. Homma, S. J. Kim, *Sziklai's conjecture on the number of a plane curve over a finite field II*, arXiv:0907.1325 (2009)

[7] M. Homma, S. J. Kim, *Around Sziklai's conjecture on the number of points of a plane curve over a finite field*, Finite Fields Appl. **15** (2009), 468–474

[8] M. Homma, S. J. Kim, *Nonsingular plane filling curves of minimum degree over a finite field and their automorphism groups: Supplements to a work of Tallini*, arXiv:0903.1918 (2009)

[9] L. Lunelli, M. Sce, *Considerazioni arithmetiche e risultati sperimentali sui* $\{K;n\}_q$*-archi*, Ist. Lombardo Accad. Sci. Rend. A **98** (1964) 3–52

[10] B. Segre, *Le geometrie di Galois*, Ann. Mat. Pura Appl. (4) **48** (1959), 1–96

[11] J. P. Serre, *Nombres de points des courbes algébriques sur* $\mathbb{F}_q$, Sem. de Théorie des Nombres de Bordeaux 1982–1983, exp. 22; Oeuvres III, No. 129, 664–668

[12] P. Sziklai, *A bound on the number of points of a plane curve*, Finite Fields Appl. **14** (2008), 41–43

[13] G. Tallini, *Le ipersuperficie irriducibili d'ordine minimo che invadono uno spazio di Galois*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat, Vol. 8, No. 30 (1961) pp. 706–712

[14] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Publ. Inst. Math. Univ. Strasbourg **7**(1945). Hermann et Cie., Paris, 1948. iv+85 pp.

[15] A. Weil, *Variétés abéliennes et courbes algébriques*, Publ. Inst. Math. Univ. Strasbourg **8** (1946). Hermann & Cie., Paris, 1948. 165 pp.