The maximum number of rational points on plane curves over a finite field
(arXiv:0907.1325)

Seon Jeong Kim
Gyeongsang National University, Korea

(Joint work with Masaaki Homma)

Fq9
UCD, July 13-17, 2009
Notations

\( \mathbb{F}_q \), a finite field with \( q \) elements

\( \mathbb{P}^2 \), the projective plane over \( \overline{\mathbb{F}}_q \), the algebraic closure of \( \mathbb{F}_q \)

\( C \), the curve defined by a homogeneous equation \( f(x, y, z) = 0 \)
with coefficients in \( \mathbb{F}_q \)

\[ \mathbb{P}^2(\mathbb{F}_q) := \{ (\alpha, \beta, \gamma) \in \mathbb{P}^2 \mid \alpha, \beta, \gamma \in \mathbb{F}_q \} \]

\[ C(\mathbb{F}_q) := \{ (\alpha, \beta, \gamma) \in \mathbb{P}^2(\mathbb{F}_q) \mid f(\alpha, \beta, \gamma) = 0 \} \],
the set of \( \mathbb{F}_q \)-rational points of \( C \)

\( N_q(C) \), the cardinality of the set \( C(\mathbb{F}_q) \).
We suppose that $C$ has no $\mathbb{F}_q$-line as a component.

$M_q(d) := \max\{N_q(C) \mid C \in \mathcal{C}_d(\mathbb{F}_q)\},$

where $\mathcal{C}_d(\mathbb{F}_q)$ is the set of all plane curves over $\mathbb{F}_q$ of degree $d$ without an $\mathbb{F}_q$-linear component.

$M_q(d) \leq \#\mathbb{P}^2(\mathbb{F}_q) = q^2 + q + 1$ for any $d \geq 1$

For $d \geq q + 2$, $M_q(d) = q^2 + q + 1$. (Homma and Kim)

In particular, for $d = q + 2$, G. Tallini proved there are irreducible curves $C$ with $N_q(C) = q^2 + q + 1$. Homma and I proved there are even nonsingular curves $C$ with $N_q(C) = q^2 + q + 1$. 
\[ M_q(d) \leq (d - 1)q + 1 \text{ (Sziklai Conjecture)} \]

For \( d = q + 2 \), \( M_q(q + 1) = q^2 + q + 1 \). (Tallini)

For \( d = q + 1 \), \( M_q(q + 1) = q^2 + 1 \). (Homma and Kim)

For \( d = \sqrt{q} + 1 \), when \( q \) is a square, \( M_q(d) = (d - 1)q + 1 \) is attained for a Hermitian curve. (well-known)

For \( d = 3 \), \( M_q(3) = 2q + 1 \) if and only if \( q = 2 \) or \( 3 \) or \( 4 \). (Schoof)

For \( d = 2 \), \( M_q(2) = q + 1 \). (well-known)
Some bounds and a conjecture

\[ M_q(d) \leq (d - 1)q + \left\lfloor \frac{d}{2} \right\rfloor \] (B. Segre)

\[ M_q(d) \leq (d - 1)q + (q + 2 - d) \] (Homma and Kim)

This bound is better than Segre’s in the range \( \frac{2}{3}q + \frac{5}{3} < d \leq q + 1 \) and implies that the Sziklai conjecture is true for \( d = q + 1 \).

For \( d = q = 4 \), the Sziklai’s conjecture is false since \( M_4(4) = 14(> (4 - 1)4 + 1) \). Indeed, \( N_4(C) = 14 \) for the nonsingular curve \( C \) defined by the equation

\[ X^4 + Y^4 + Z^4 + X^2 Y^2 + Y^2 Z^2 + Z^2 X^2 + X^2 YZ + XY^2 Z + XYZ^2 = 0. \]
Modified Sziklai’s conjecture

Unless $C$ is a curve defined over $\mathbb{F}_4$ which is projectively equivalent to

$$X^4 + Y^4 + Z^4 + X^2Y^2 + Y^2Z^2 + Z^2X^2 + X^2YZ + XY^2Z + XYZ^2 = 0$$  \hspace{1cm} (1)

over $\mathbb{F}_4$, we might have

$$N_q(C) \leq (d - 1)q + 1.$$  \hspace{1cm} (2)
The Main Theorems

**Theorem 1**

For $d = q$, the modified Sziklai’s conjecture is true, and for each $q$ there exists a nonsingular curve of degree $q$ over $\mathbb{F}_q$ with $(q-1)q+1$ rational points.

Now the case $d \leq q - 1$ is remained.

**Theorem 2**

The modified Sziklai’s conjecture is true for nonsingular curves of degree $d \leq q - 1$. Moreover there is an example of a nonsingular curve for which equality holds in (2) if $d = q + 2, q + 1, q, q - 1, \sqrt{q} + 1$ (when $q$ is square), or 2.
In this talk, we concentrate on a proof of Theorem 1.

For $q = 2$, we have $M_2(2) = 3$, since $M_q(2) = q + 1$ for arbitrary $q$.

For $q = 3$, $M_3(3) = 7$ (Segre’s bound and an example).

For $q = 4$, $M_4(4) = 14$ (Segre’s bound and an example), and we already proved that any plane curve attaining this bound is projectively equivalent to the curve defined by (1) over $\mathbb{F}_4$.

Thus it remains to prove the theorem for $q \geq 5$. 
**Lemma 1** (Homma and Kim)

If $2 \leq d \leq q + 1$, then

$$M_q(d) \leq (d - 1)q + (q + 2 - d).$$

In particular, we have $M_q(q) \leq (q - 1)q + 2$.

**Lemma 2**

Let $C$ be the plane curve defined by the equation $x^q - xz^{q-1} + y^{q-1}z - z^q$ over $\mathbb{F}_q$ where $q \geq 2$. Then $C$ is nonsingular and $\# C(\mathbb{F}_q) = (q - 1)q + 1$. 
To prove Theorem 1

Thus, to prove $M_q(q) \leq (q - 1)q + 1$ it suffices to prove that there is no irreducible curve $C$ of degree $q$ with $N_q(q) = (q - 1)q + 2$.

Indeed, note that if the curve $C$ of degree $q$ is reducible and decomposed into two curves of degree $d_1$ and $d_2$ with $2 \leq d_1, d_2 \leq q - 2$ as $C = C_1 \cup C_2$, then

$$N_q(C) \leq N_q(C_1) + N_q(C_2)$$
$$\leq ((d_1 - 1)q + \lfloor \frac{d_1}{2} \rfloor) + ((d_2 - 1)q + \lfloor \frac{d_2}{2} \rfloor)$$
$$\leq (q - 1)q + \lfloor \frac{q}{2} \rfloor - q \leq (q - 1)q.$$
More notations

Let $f$ be a homogeneous polynomial in $\mathbb{F}_q[x, y, z]$.

$$Z(f) := \{(\alpha, \beta, \gamma) \in \mathbb{P}^2(\mathbb{F}_q) \mid f(\alpha, \beta, \gamma) = 0\}, \text{ the zero set of } f$$

We use the following notation:

- $(\alpha, \beta, \gamma)$ denotes a point.
- $[\alpha, \beta, \gamma]$ denotes the line with equation $\alpha x + \beta y + \gamma z = 0$.

Note that the lines through the origin $(0, 0, 1)$ have the equation of the form $\alpha x + \beta y = 0$, i.e., are expressed as $[\alpha, \beta, 0]$. 
Lemma 3

Let \( f \) be an irreducible homogeneous polynomial of degree \( d = q \geq 5 \) in \( \mathbb{F}_q[x, y, z] \). Let \([-\gamma_i, \beta_i, 0]\), \(i = 1, \ldots, k + 1\) with \(3 \leq k \leq q\) be \(k + 1\) distinct lines through the origin \((0, 0, 1)\). Suppose that \(Z(f) \supseteq [-\gamma_i, \beta_i, 0] - \{(\beta_i, \gamma_i, 0)\}\) for \(i = 1, \ldots, k\). If \(Z(f)\) contains \(q+2-k\) points in the deleted line \([-\gamma_{k+1}, \beta_{k+1}, 0] - \{(\beta_{k+1}, \gamma_{k+1}, 0)\}\), then \(Z(f)\) contains all of them.
Lemma 4

Let $f$ be an irreducible homogeneous polynomial of degree $d = q \geq 5$ in $\mathbb{F}_q[x, y, z]$. Let $[-\gamma_i, \beta_i, 0]$, $i = 1, \ldots, k+1$ with $2 \leq k \leq q-1$ be $k + 1$ distinct lines through the origin $(0, 0, 1)$. Suppose that $Z(f) \supseteq [-\gamma_i, \beta_i, 0] - \{(0, 0, 1)\}$ for $i = 1, \ldots, k$.

If $Z(f)$ contains $q+1-k$ points in the deleted line $[-\gamma_{k+1}, \beta_{k+1}, 0] - \{(0, 0, 1)\}$, then $Z(f)$ contains all of them.
Proof of Theorem 1

Suppose that there exists an irreducible curve $C$ of degree $q$ with $N_q(C) = (q - 1)q + 2$. If $C$ is singular at some $\mathbb{F}_q$-rational point $P$, then each line through $P$ meets $C$ at most $q - 1$ points. Then $N_q(C) \leq (q - 2) \cdot (q + 1) + 1 = q^2 - q - 1$. Thus we may assume that $C$ is nonsingular at every $\mathbb{F}_q$-rational point of $C$. Let $a_i$ $(0 \leq i \leq q)$ be the number of lines ($i$-point lines) $\ell$ in the projective plane such that $\# \ell \cap C(\mathbb{F}_q) = i$. Then we obtain the following;
(1) $\sum_{i=0}^{q} a_i = q^2 + q + 1$ (the number of all lines on the plane).

(2) $\sum_{i=0}^{q} ia_i = (q^2 - q + 2) \cdot (q + 1)$ (the sum of \(\# \ell \cap C(\mathbb{F}_q)\) for all lines on the plane).

(3) If $q$ is even [resp. odd], then

$$\sum_{i=1}^{q} ia_i + \sum_{i=\frac{q}{2}}^{q} (q - i)a_i \geq q^2 - q + 2$$

[resp. $\sum_{i=1}^{\frac{q-1}{2}} ia_i + \sum_{i=\frac{q+1}{2}}^{q} (q - i)a_i \geq q^2 - q + 2$].

(the number of tangent lines at $\mathbb{F}_q$-rational points to $C$).

(4) $\sum_{i=2}^{q} \binom{i}{2} a_i = \binom{q^2 - q + 2}{2}$ (counting the number of elements in the set $\{(\{P, Q\}, \langle P, Q \rangle) \mid P, Q \in C(\mathbb{F}_q) \text{ and } P \neq Q\}$ in two ways).
From above equations (1), (2), (3) and (4), we obtain
\[ qa_0 + (q - 2)a_1 + (q - 4)a_2 + \cdots \leq q - 4, \]
which implies \( a_0 = 0 \) and \( a_1 = 0 \) since \( a_i \)'s are nonnegative integers.

Now we need the following lemma.

**Lemma 5**

At least one among \( \{ a_i \mid 2 \leq i \leq q - 3 \} \) is non-zero.

**Proof of Lemma 5.** Suppose that all of them are zero. Then the equations become

1. \( a_{q-2} + a_{q-1} + a_q = q^2 + q + 1 \)
2. \( (q - 2)a_{q-2} + (q - 1)a_{q-1} + qa_q = (q^2 - q + 2) \cdot (q + 1) \)
3. \( \binom{q-2}{2} a_{q-2} + \binom{q-1}{2} a_{q-1} + \binom{q}{2} a_q = (q^2 - q + 2) \cdot \binom{q+2}{2} \)

Using the elimination method, we have \( a_{q-1} = -(q - 3)^2 + 1 \),
which is smaller than zero for \( q \geq 5 \), and hence it is contradiction.
Now let $k$ be the smallest positive integer such that $a_k > 0$. By Lemma 5, we have $2 \leq k \leq q - 3$. Let $\ell_0$ be a fixed $k$-point line. Let $\ell_0 \cap \mathbb{P}^2(F_q) = \{P_0, P_1, \ldots, P_q\}$, and $\ell_0 \cap C(F_q) = \{P_0, P_1, \ldots, P_{k-1}\}$. Let $S := \mathbb{P}^2(F_q) - \ell_0 - C(F_q)$ then $\# S = q + k - 2$. For each $P_i$ with $0 \leq i \leq k - 1$, let $\mathcal{S}(P_i)$ be the set of points $Q \in S$ such that the line $\langle P_i, Q \rangle$ is a $q$-point line. Then $\# \mathcal{S}(P_i) \geq q - k + 2$ since the union of $q$ lines except $\ell_0$ through $P_i$ contains $S$. 
<table>
<thead>
<tr>
<th>Introduction</th>
<th>Main Results</th>
<th>Proof of Theorem 1</th>
<th>A proof of Theorem 2</th>
<th>References</th>
</tr>
</thead>
</table>

\[ P_0, P_1, \ldots, P_{k-1}, P_k, \ldots, P_8 \]

\[ \exists \mathcal{Q} \cap S \quad 9+k-2 \text{ points} \]
Now we consider the case \( k \geq 3 \) at first. Since we have

\[
\sum_{i=0}^{k-1} \# \mathcal{I}(P_i) \geq k(q - k + 2) > 2(q + k - 2) = 2 \cdot \# S
\]

for \( 3 \leq k \leq q - 3 \) by simple computation, there exists a point \( Q \in S \) such that \( Q \in \mathcal{I}(P_{i_1}) \cap \mathcal{I}(P_{i_2}) \cap \mathcal{I}(P_{i_3}) \) for some distinct \( i_1, i_2, i_3 \in \{0, 1, \ldots, k - 1\} \). Then we have a contradiction by the following lemma which can be proved using Lemma 4.
Lemma 6

Let \( Q \in \mathbb{P}^2(\mathbb{F}_q) - C(\mathbb{F}_q) \). If there are at least two \( q \)-point lines containing \( Q \), then the pencil of lines through \( Q \) consists of two \( q \)-point lines and \( q - 1 \) \((q - 2)\)-point lines.

Proof. Suppose that there are exactly \( r \) (\( \geq 2 \)) \( q \)-point lines through \( Q \). Then by Lemma 4, each of the other lines through \( Q \) contains at most \( q - r \) rational points of \( C \). Note that \( r \leq q - 1 \) since \( a_0 = a_1 = 0 \). The total number of rational points on \( C \) is equal to \( \sum_{Q \in \ell} \#(\ell \cap C(\mathbb{F}_q)) \). Thus

\[
q^2 - q + 2 = \sum_{Q \in \ell} \#(\ell \cap C(\mathbb{F}_q)) \leq rq + (q - r + 1)(q - r),
\]

which is equivalent to \((r - 2)q \leq (r - 2)(r + 1)\). Since \( 2 \leq r \leq q - 1 \), that inequality implies \( r = 2 \) or \( r = q - 1 \). If \( r = q - 1 \), at least one of the remaining two lines is 0-point line or 1-point line which contradicts the fact \( a_0 = a_1 = 0 \). Thus we have \( r = 2 \) and the other \( q - 1 \) lines are exactly \((q - 2)\)-point ones.
The case $a_2 = 1$
Now only the case \( a_2 > 0 \) is remained. In fact, the computation above Lemma 5 implies \( a_2 = 1 \). As in the part of proof above Lemma 6, we use the same notation. The line \( \ell_0 \) is the unique 2-point line and \( \ell_0 \cap C(\mathbb{F}_7) = \{P_0, P_1\} \), 
\( \ell_0 \cap (\mathbb{P}^2(\mathbb{F}_q) - C(\mathbb{F}_q)) = \{P_i \mid 2 \leq i \leq q\} \). Then every line through \( P_0 \) or \( P_1 \) except \( \ell_0 \) is a \( q \)-point line.

Let \( \ell_1, \ldots, \ell_q \) be the \( q \) lines through \( P_0 \) except \( \ell_0 \).

Let \( \ell_i \cap (\mathbb{P}^2(\mathbb{F}_q) - C(\mathbb{F}_q)) = \{Q_i\} \) for \( i = 1, \ldots, q \), then \( S = \{Q_1, Q_2, \ldots, Q_q\} \).

By Lemma 3, no three points of \( S \) are collinear. Thus the set \( S \cup \{P_0, P_1\} = \{P_0, P_1, Q_1, Q_2, \ldots, Q_q\} \) becomes a \((q + 2)\)-arc, i.e., no three points in that set are collinear. For odd \( q \), this is contradiction since \( \mathbb{P}^2(\mathbb{F}_q) \) can not contain \( r \)-arcs for \( r \geq q + 2 \). Thus we may assume \( q \) is even.
The case $a_2 = 1$ and $q$ even

Since $S \cup \{P_0, P_1\}$ is $(q + 2)$-arc, i.e., a hyperoval, every line in the plane is an 2-secant line or 0-secant line of it. Counting the number of points in $S \cup \{P_0, P_1\}$ implies that exactly $\frac{q}{2}$ lines through $P_q$ (or any $P_i$, $2 \leq i \leq q$) are 0-secant lines, equivalently $q$-point lines. Since $q \geq 5$, in fact $q \geq 8$, we have a contradiction using Lemma 6 again.

Thus there is no irreducible plane curve $C$ of degree $q$ over $\mathbb{F}_q$ with $N_q(C) = q^2 - q + 2$. By combining the fact mentioned below Lemma 2, we conclude there is no plane curve $C$ of degree $q$ with no $\mathbb{F}_q$-linear component with $N_q(C) = q^2 - q + 2$.

Therefore $M_q(q) = q^2 - q + 1$ for $q \geq 5$. Thus the proof of Theorem 1 is complete.
A proof of Theorem 2

Now we may assume that $C$ is a nonsingular plane curve over $\mathbb{F}_q$ of degree $d$ with $1 < d \leq q - 1$. We prove that $N_q(C) \leq (d - 1)q + 1$. A nonsingular plane curve $C$ defined over $\mathbb{F}_q$ is said to be $q$-Frobenius nonclassical if $F_q(P) \in T_P(C)$ for a general $\overline{\mathbb{F}}_q$-point $P$, where $F_q$ is the $q$-th power Frobenius map and $T_P(C)$ is the embedded tangent line at $P$ to $C$. Stöhr and Voloch showed that if $C$ is $q$-Frobenius classical of degree $d$, then

$$N_q(C) \leq \frac{1}{2} d(d + q - 1),$$

(3)

and Hefez and Voloch proved that if $C$ is $q$-Frobenius nonclassical of degree $d$, then $d \geq \sqrt{q} + 1$ and

$$N_q(C) = d(q - d + 2).$$

(4)
Each of these two estimates for $N_q(C)$ is stronger than the expected bound if $2 \leq d \leq q - 1$ for (3) or $d \geq \sqrt{q} + 1$ for (4). In fact,

$$(d - 1)q + 1 - \frac{1}{2}d(d + q - 1) = \frac{1}{2}(d - 2)(q - d - 1)$$

and

$$(d - 1)q + 1 - d(q - d + 2) = (d - \sqrt{q} - 1)(d + \sqrt{q} - 1).$$
References


