On the maximum size of arcs in the projective plane and some length optimal codes

Eun Ju Cheon

The Department of Mathematics and RINS
Gyeongsang National University

July 3, 2018
Shanghai University, China

Projective plane $PG(2,q)$ over $\mathbb{F}_q$

Let $\mathbb{F}_q$ be the finite field of order q. The set of n-tuples

$$\mathbb{F}_q^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{F}_q\}$$

is the n-dimensional vector space over $\mathbb{F}_q$.
Let $PG(2,q)$ be the projective plane over $\mathbb{F}_q$, which consists of all lines through the origin of $\mathbb{F}_q^3$ over $\mathbb{F}_q$, that is,

$$\left(\mathbb{F}_q^3 \setminus \{(0,0,0)\}\right) / \sim,$$

where $(a,b,c) \sim (x,y,z) \iff (a,b,c) = \lambda(x,y,z)$ for some $\lambda \in \mathbb{F}_q \setminus \{0\}$.

We can express $PG(2,q)$ as

$$PG(2,q) = \{(a,b,1) \mid a,b \in \mathbb{F}_q\} \cup \{(a,1,0) \mid a \in \mathbb{F}_q\} \cup \{(1,0,0)\}.$$

Thus we have $|PG(2,q)| = q^2 + q + 1$.

The linear equation

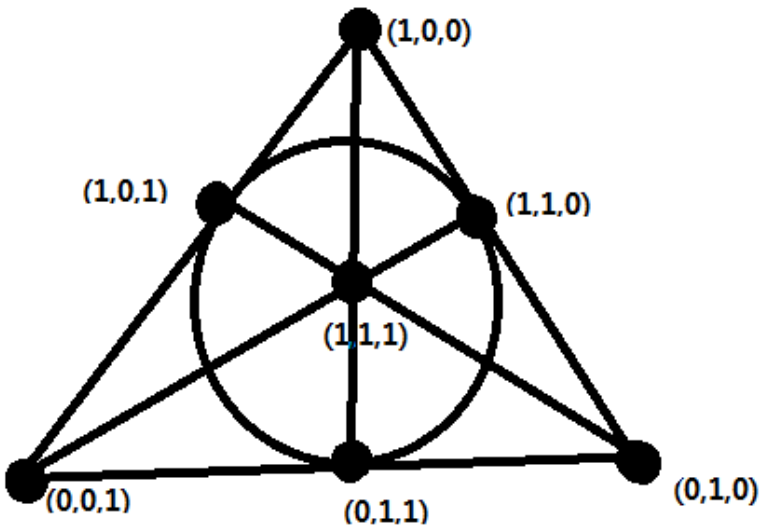
$$ax + by + cz = 0, \quad a,b,c \in \mathbb{F}_q, \quad (a,b,c) \neq (0,0,0)$$

is the equation of a line ℓ in $PG(2,q)$, simply denoted $\ell = [a,b,c]$, i.e.,

$$\ell := \{(x_0,x_1,x_2) \in PG(2,q) \mid ax_0 + bx_1 + cx_2 = 0\}.$$

Example 1.

(1) The projective plane $PG(2,2)$ consists of 7 points and 7 lines. The set of points in $PG(2,2)$ is $\{(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$, and the set of lines in $PG(2,2)$ is $\{[0,0,1],[0,1,0],[0,1,1],[1,0,0],[1,0,1],[1,1,0],[1,1,1]\}$. The line $x+y+z=0$ is $[1,1,1] := \{(0,1,1),(1,0,1),(1,1,0)\}$.



(2) The set of points in $PG(2,3)$ is

$$\{(0,0,1),(0,1,1),(0,2,1),(1,0,1),(1,1,1),(1,2,1),$$
$$(2,0,1),(2,1,1),(2,2,1),(0,1,0),(1,1,0),(2,1,0),(1,0,0)\},$$

and the set of lines in $PG(2,3)$ is

$$\{[0,0,1],[0,1,1],[0,2,1],[1,0,1],[1,1,1],[1,2,1],$$
$$[2,0,1],[2,1,1],[2,2,1],[0,1,0],[1,1,0],[2,1,0],[1,0,0]\}.$$

The line $x+y+z=0$ is
$[1,1,1] := \{(0,2,1),(1,1,1),(2,0,1),(2,1,0)\}$.

We note that $PG(2,3)$ has 13 points and 13 lines and each line has 4 points in $PG(2,3)$.

The following hold in $PG(2, q)$.

Points and lines in $PG(2, q)$

1. $PG(2, q)$ consists of $q^2 + q + 1$ points and $q^2 + q + 1$ lines.
2. Every line contains $q + 1$ points.
3. Two distinct lines meet at a point.
4. There are $q + 1$ lines passing through a point in $PG(2, q)$.

Consider quadrics in $PG(2,q)$

$$F := ax^2 + by^2 + cz^2 + dxy + eyz + fxz,$$

where $a, b, c, d, e, f \in \mathbb{F}_q$.

Define $v(F)$ as the zero set of F in $PG(2,q)$, i.e.,

$$v(F) := \{(x_0, x_1, x_2) \in PG(2,q) \mid F(x_0, x_1, x_2) = 0\}.$$

A conic means a nonsingular quadric.
Any conic has $q+1$ (rational) points in $PG(2,q)$ with no three collinear.
A zero set of a singular quadric is a repeated line or a pair of distince lines or a point.

Arcs

An $(n, r)_q$-arc

An $(n, r)_q$-arc is a set $\mathcal{K}$ of n points of $PG(2, q)$ such that some r but no $r + 1$ of them, are collinear, i.e., $|\mathcal{K} \cap \ell| \leq r$ for any line ℓ and $|\mathcal{K} \cap \ell| = r$ for some line ℓ in $PG(2, q)$.

For an $(n, r)_q$-arc $\mathcal{K}$, the line ℓ is called i-line if $|\ell \cap \mathcal{K}| = i$.
Define a_i as the number of i-lines to $\mathcal{K}$, i.e.,

$$a_i := \#\{\ell \mid |\ell \cap \mathcal{K}| = i\}.$$

Note that $a_i = 0$ for $i \geq r + 1$.
The $(r + 1)$-tuple $(a_0, a_1, \ldots, a_r)$ is called the spectrum of the arc $\mathcal{K}$.

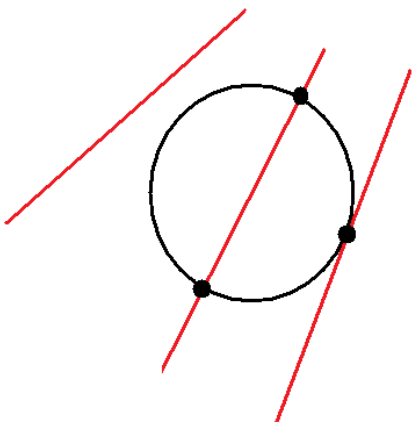
Example 2.

Let $\mathcal{C}$ be a conic in $PG(2,q)$ with the equation $y^2 = xz$.

(1) The conic $\mathcal{C}$ is a $(q+1,2)_q$-arc in $PG(2,q)$.
We note that the conic

$$\mathcal{C} = \{(t^2, t, 1) \mid t \in \mathbb{F}_q\} \cup \{(1,0,0)\}.$$

Thus $|\mathcal{C}| = q+1$ and for any line ℓ, we have $|\mathcal{C} \cap \ell| = 0$ or 1 or 2.
Thus $\mathcal{C}$ is a $(q+1,2)_q$-arc.



(2) For a conic $\mathcal{C}$, we have its spectrum as

$$a_0 = \frac{(q-1)q}{2}, \quad a_1 = q+1, \quad a_2 = \frac{(q+1)q}{2}.$$

Since the tangent lines of $\mathcal{C}$ is 1-line, we have $a_1 = q+1$.
And each 2-line contains exactly two points of $\mathcal{C}$.
Thus we have

$$a_2 = \binom{q+1}{2} = \frac{(q+1)q}{2},$$

and hence

$$a_0 = q^2 + q + 1 - (a_1 + a_2) = \frac{(q-1)q}{2}.$$

Hence the spectrum is

$$a_0 = \frac{(q-1)q}{2}, \quad a_1 = q+1, \quad a_2 = \frac{(q+1)q}{2}.$$

The value of $m_r(2,q)$

Let $m_r(2,q)$ denote the largest n for which there exists an $(n,r)_q$-arc for given r and q.

We call $(m_r(2,q),r)_q$ -arc the largest arc for given r and q.

An interesting problem in finite geometry is to determine the exact values of $m_r(2,q)$. Obviously, we have the bound for $m_r(2,q)$;

$$m_r(2,q) \leq (r-1)q + r.$$

Linear codes

For two vectors $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ in $\mathbb{F}_q^n$, the Hamming distance between $\mathbf{x}$ and $\mathbf{y}$, denoted by $d(\mathbf{x}, \mathbf{y})$ is the number of positions in which they differ.

An $[n, k, d]_q$ linear code C is a k-dimensional linear subspace of $\mathbb{F}_q^n$ over $\mathbb{F}_q$ with minimum distance d, where

$$\begin{aligned} d &= \min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\} \\ &= \min\{w(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}. \end{aligned}$$

Here the weight $w(\mathbf{x})$ of $\mathbf{x}$ is the number of nonzero positions in $\mathbf{x}$.

A good code will have small n (for fast transmission of messages), large k (for a wide variety of messages) and large d (to correct many errors).

Optimal linear codes problems

Optimize one of the parameters n, k, d for given values of the other two for a given field $\mathbb{F}_q$.

Optimal linear code problems

Optimal linear codes problems by Hill

1. Find $B_q(n, d)$, the largest number q^k of codewords for which there exists an $[n, k, d]_q$ code.
2. Find $d_q(n, k)$, the largest minimum distance d for which there exists an $[n, k, d]_q$ code.
3. Find $n_q(k, d)$, the smallest length n of codewords for which there exists an $[n, k, d]_q$ code.

A code which achieves one of the above values is called optimal, that is, we call dimension optimal, distance optimal and length optimal, respectively.

We note that the following;

A code is length optimal $\Longrightarrow$ distance optimal,
$\Longrightarrow$ dimension optimal.

Example 1.

Let C_1 be a $[7, 2, 4]_2$ linear code with a generator matrix

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}_{2\times 7}.$$

Then C_1 is a distance optimal because there is no $[7, 2, 5]_2$ code. But C_1 is not a length optimal and a dimension optimal because there is a $[6, 2, 4]_2$ code and a $[7, 3, 4]_2$ code, respectively.

Griesmer bound

Griesmer bound

For an $[n, k, d]_q$ linear code, we have

$$n \geq g_q(k, d) := d + \left\lceil \frac{d}{q} \right\rceil + \left\lceil \frac{d}{q^2} \right\rceil + \cdots + \left\lceil \frac{d}{q^{k-1}} \right\rceil .$$

A linear code for which equality holds is called a Griesmer code.

We note that the Griesmer bound is an important lower bound of $n_q(k, d)$, that is,

$$n_q(k, d) \geq g_q(k, d).$$

Every Griesmer code is a length optimal.

Linear codes and arcs

Let C be an $[n, 3, d]_q$ code with a generator matrix G.
Consider multi-set S whose elements are columns of G.
Then S can be regarded as a multi-set in $PG(2, q)$.

Thus we have the following;

Theorem

An $[n, 3, d]_q$ linear code gives an $(n, n-d)_q$-arc in $PG(2, q)$.

Equivalently, an $(n, r)_q$-arc gives an $[n, 3, n-r]_q$ linear code.

Recall $m_r(2,q)$ denotes the largest arc for given r and q, and $m_r(2,q) \leq (r-1)q+r$.

Theorem.

For $(r-2)q+r < m_r(2,q) \leq (r-1)q+r$, the largest $(m_r(2,q),r)_q$-arc corresponds to a Griesmer code(length optimal code).

We can easily see the following;

1. For $r = 1$, the value $m_1(2, q) = 1$ and the arc is a singleton set.
2. For $r = q$, the value $m_q(2, q) = q^2$ and the arc is the complement of a line ℓ_0, i.e., $PG(2, q) \setminus \ell_0$.
3. For $r = q + 1$, the value $m_{q+1}(2, q) = q^2 + q + 1$ and the arc is the projective plane $PG(2, q)$.

A few values of $m_r(2, q)$, $(2 \leq r \leq q - 1)$ are known for general q.

Known results on $m_r(2,q)$

Theorem. Bose (1947): On the values of $m_2(2,q)$

We have

$$m_2(2,q) = \begin{cases} q+1, & q \text{ odd}, \\ q+2, & q \text{ even}. \end{cases}$$

Theorem. Barlotti (1965) and Ball(1996)

For q odd prime, we have

$$m_r(2,q) = (r-1)q+1 \quad \text{for} \quad r = \frac{q+1}{2} \quad \text{or} \quad r = \frac{q+3}{2}.$$

Theorem. Denniston (1969)

For q even, we have

$$m_r(2,q) = (r-1)q+r \quad \text{for} \quad r = 2^e \leq q.$$

The values of $m_r(2, q)$

r/q	3	4	5	7	8	9	11	13	16	17
2	4	6	6	8	10	10	12	14	18	18
3		9	11	15	15	17	21	23	28	28–33
4			16	22	28	28	32	38–40	52	48–52
5				29	33	37	43–45	49–53	65	61–69
6				36	42	48	56	64–66	78–82	79–86
7					49	55	67	79	93–97	95–103
8						65	78	92	120	114–120
9							89–90	105	129–130	137
10							100–102	118–119	142–148	154
11								132–133	159–164	166–171
12								145–147	180–181	183–189
13									195–199	205–207
14									210–214	221–225
15									231	239–243
16										256–261

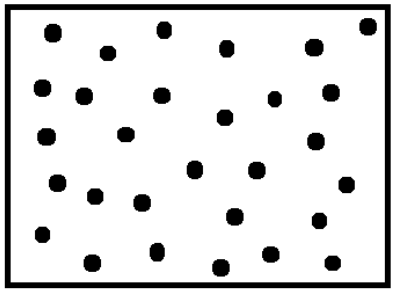
From S. Ball, http://www-ma4.upc.es/ simeon/codebounds.html

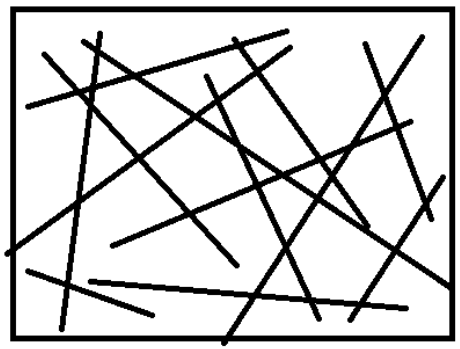
Problems

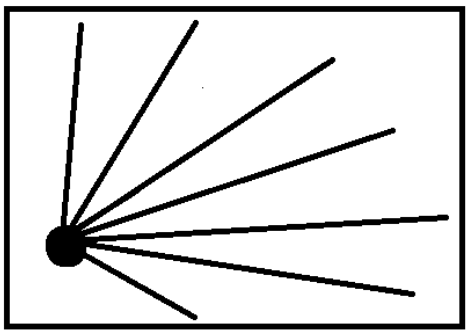
Let r be an integer with $2 \leq r \leq q-1$.

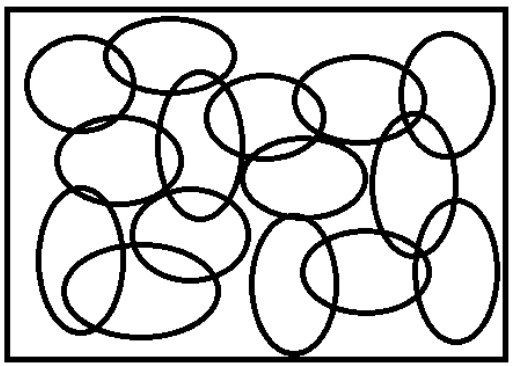
1. Find $m_r(2,q)$, the maximum value of n for which an (n,r)-arc exists in $PG(2,q)$.
   Equivalently, find length optimal codes meeting the Griesmer codes.
2. Classify (n,r)-arcs in $PG(2,q)$ for $n = m_r(2,q)$ up to projective equivalence.

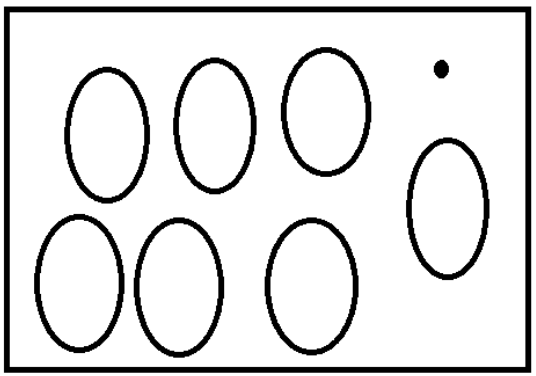
Consider $PG(2, q)$ as follows;











A partition of $PG(2, q)$

For odd prime q, we denote by QR the set of quadratic residues $\bmod q$ and by NQR the set of quadratic nonresidues $\bmod q$.

We consider a conic with the equation $ax^2 + by^2 + cz^2 + xy$ for $(a, b, c) \in PG(2, q)$, denoted by $f_{(a,b,c)}$.
Let $\mathcal{F} := \{f_{(a,b,c)} \mid (a, b, c) \in PG(2, q)\}$.

Lemma 1

For odd prime q, the conic $4xy - z^2$ and a line $[u, v, w]$ has no common point in $PG(2, q)$ if $w^2 - uv \in NQR$.

We express the line $[u, v, w]$ as follows;

$$[u, v, w] := \{(a, b, 1) \in PG(2, q) \mid au + bv + w = 0\} \cup \{(-v, u, 0)\}.$$

For two points $(a, b, 1), (a', b', 1) \in [u, v, w]$, consider two conics $C_1 := ax^2 + by^2 + z^2 + xy$ and $C_2 := a'x^2 + b'y^2 + z^2 + xy$.
We have the following;

Lemma 2

Two conics C_1 and C_2 in $\mathcal{F}$ which is given above are disjoint if $uv \in NQR$.

Next theorem shows that projective plane can be partitioned into disjoint conics and a point.

Theorem 3

For odd prime q, the projective plane $PG(2,q)$ consists of q disjoint conics and a point.

Proof) Choose q conics in $\mathcal{F}$ such that $(a,b,c) \in [u,v,w]$ and $(a,b,c) \neq (-v,u,0)$.
Here u, v and w satisfies that

$$uv \in NQR \text{ and } w^2 - uv \in NQR.$$

We note that such a line $[u,v,w]$ exists.
And the point $(0,0,1)$ is outside of the conics in $\mathcal{F}$. Thus we have

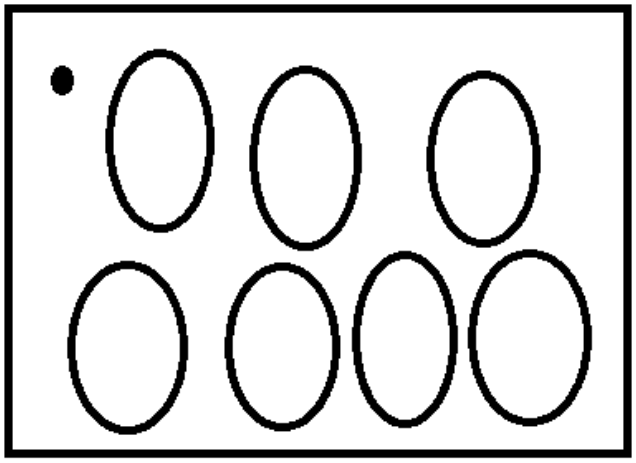
$$PG(2,q) = \{(0,0,1)\} \cup \dot{\bigcup}_{(a,b,c)\in[u,v,w]\setminus\{(-v,u,0)\}} f_{(a,b,c)}.$$

The case $q = 7$

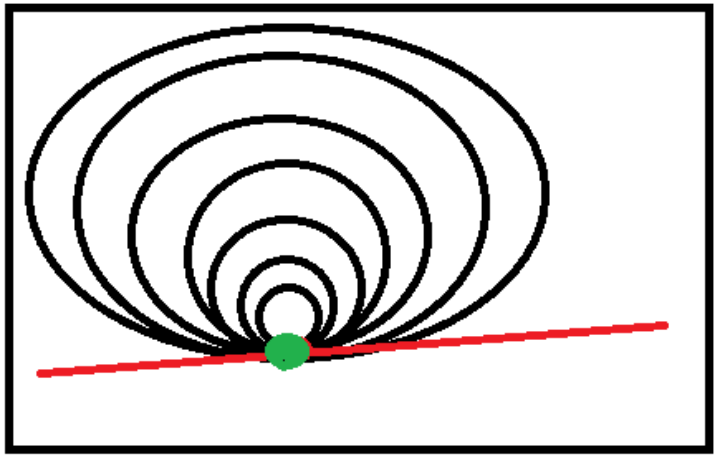
Consider conics in $\mathcal{F}$ with the equation

$$f_{(a,b,c)} = ax^2 + by^2 + cz^2 + xy,$$

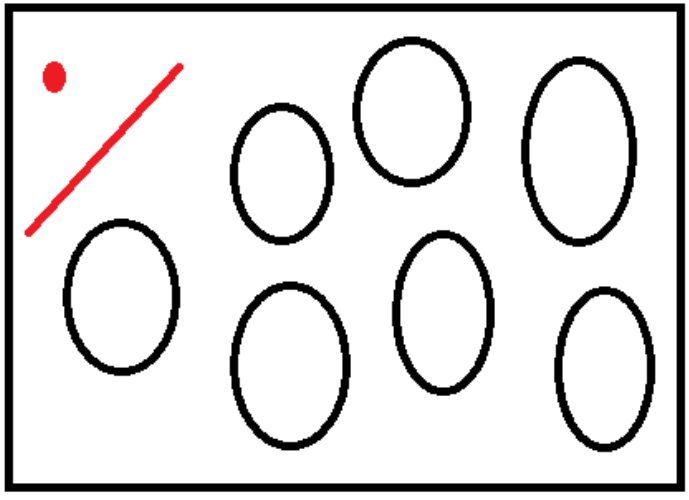
and a line $[3, 1, 1]$. Then the line [3,1,1] satisfies
$uv = 3 \in NQR$ and $w^2 - uv = 1 - 3 \equiv -2 \equiv 5 \in NQR$.
Choose 7 points (a, b, c)
on the line $[3, 1, 1]$, $(a, b, c) \neq (-1, 3, 0) = (2, 1, 0)$, where $[3, 1, 1] =$
$\{(2, 0, 1), (0, 6, 1), (5, 5, 1), (1, 3, 1)(6, 2, 1), (4, 1, 1), (3, 4, 1), (2, 1, 0)\}$.
Then the union of 7 conics and a point $\{(0, 0, 1)\}$ is the whole
plane $PG(2, 7)$.



Theorem 3



Theorem 4



Theorem 10

Conics with one common point

We consider the conics in $\mathcal{F}$ with $f_{(a,b,c)}$, where (a,b,c) is on the line $[0,1,0] = \{(a,0,1) \mid a \in \mathbb{F}_q\} \cup \{(1,0,0)\}$.
Then the intersection of $f_{(a,b,c)}, (a,b,c) \in [0,1,0]$ is the point $(0,1,0)$.

Next theorem gives another geometrical configuration of $PG(2,q)$.

Theorem 4

For odd prime q, the projective plane $PG(2,q)$ consists of q conics with a common point P and common tangent line at P.

Proof) Consider the line $[0,1,0] = \{(a,0,1) \mid a \in \mathbb{F}_q\}$.
Choose q conics $f_{(a,0,1)}$ with $a \in \mathbb{F}_q, a \neq 1$.
Then the intersection of q conics $f_{(a,0,1)}$, $a \neq 1$ is the point $(0,1,0)$.
Note that the common tangent line of q conics $f_{(a,0,1)}$ is the line $[1,0,0]$. Then

$$PG(2,q) = [1,0,0] \cup \bigcup_{a \in \mathbb{F}_q, a \neq 1} f_{(a,0,1)}.$$

□

For $a \in \mathbb{F}_q \setminus \{0\}$, we have

$$\#\{a \in \mathbb{F}_q \mid 1 - a \in NQR, \quad a \neq 0\} = \frac{q-1}{2},$$

and

$$\#\{a \in \mathbb{F}_q \mid 1 - a \in NQR \cup \{0\}, \quad a \neq 0\} = \frac{q+1}{2}.$$

Using this, we have the following;

Theorem 5

(1) The union of $f_{(a,0,1)}$ satisfying $1-a \in NQR$ is $(\frac{q(q-1)}{2}+1, \frac{q+1}{2})_q$ maximal arc with the spectrum

$$a_0 = q, \quad a_1 = 1, \quad a_{\frac{q-1}{2}} = \frac{(q-1)q}{2}, \quad a_{\frac{q+1}{2}} = \frac{(q+1)q}{2}.$$

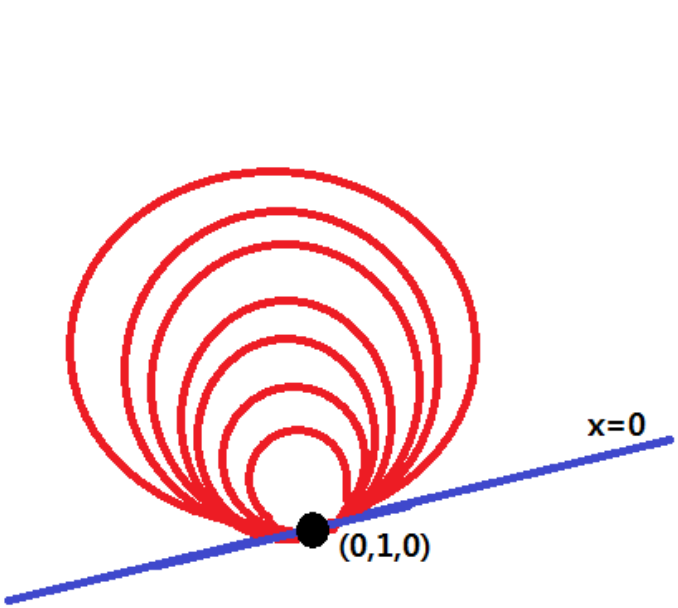
(2) The union of $f_{(a,0,1)}$ satisfying $1-a \in NQR \cup \{0\}$ is $(\frac{q(q+1)}{2}+1, \frac{q+3}{2})_q$ maximal arc with the spectrum

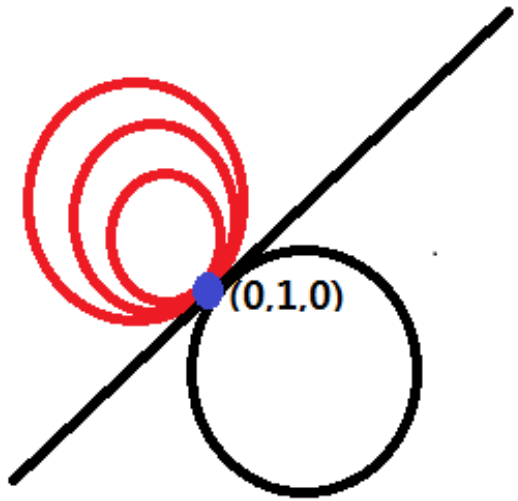
$$a_0 = 0, \quad a_1 = q+1, \quad a_{\frac{q+1}{2}} = \frac{(q-1)q}{2}, \quad a_{\frac{q+3}{2}} = \frac{(q+1)q}{2}.$$

Remark

The maximal arcs in Theorem 5 is exactly same arcs with one 's of Barlotti (1965) and Ball(1996). That is, for a given conic $\mathcal{C}$, if $t = \frac{q-1}{2}$, the arcs is the union of a point of $\mathcal{C}$ and its internal set $\mathcal{I}(\mathcal{C})$ and $t = \frac{q+1}{2}$, the arcs is the union of the conic $\mathcal{C}$ and its internal set $\mathcal{I}(\mathcal{C})$.

For $q = 7$, we have



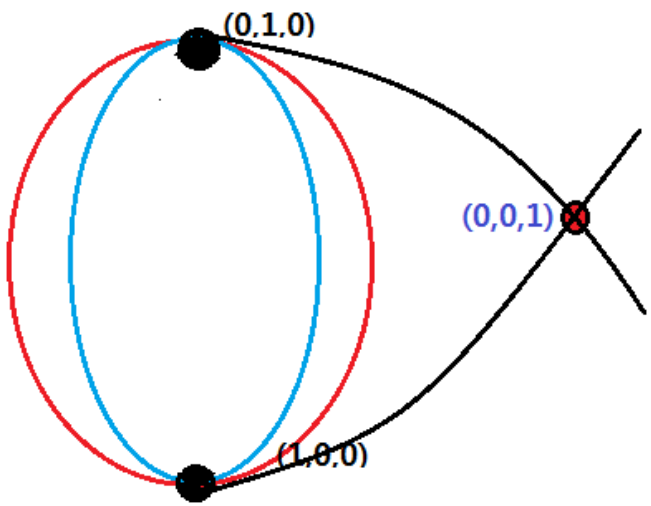


The case $q = 7$

In $PG(2, 7)$, consider two conics with two common points $(0, 1, 0)$ and $(1, 0, 0)$ as follows;

$$C_1 := z^2 + xy, \quad C_2 := 6z^2 + xy.$$

Then the union of C_1, C_2 and the point $\{(0, 0, 1)\}$ is the largest $(15, 3)_7$-arc with spectrum $a_0 = 12, \quad a_1 = 0, \quad a_2 = 15, \quad a_3 = 30.$

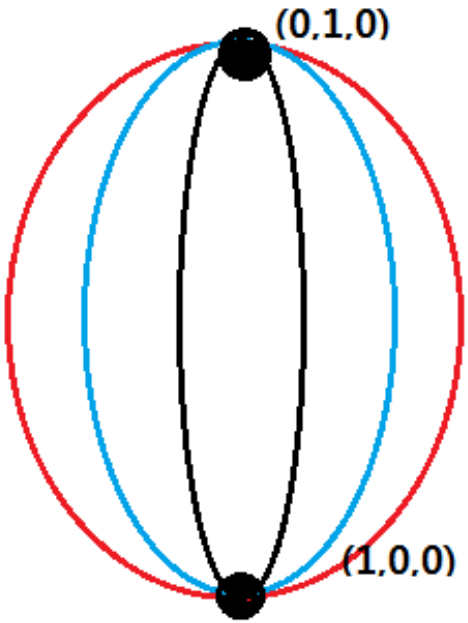


The case $q = 13$

In $PG(2, 13)$, consider three conics with two common points $(0, 1, 0)$ and $(1, 0, 0)$ as follows;

$$C_1 := 4z^2 + xy, \quad C_2 := 5z^2 + xy \quad C_3 := 12z^2 + xy.$$

Then the union of C_1, C_2 and C_3 is a $(38, 4)_{13}$ maximal arc.



The case $q = 8$

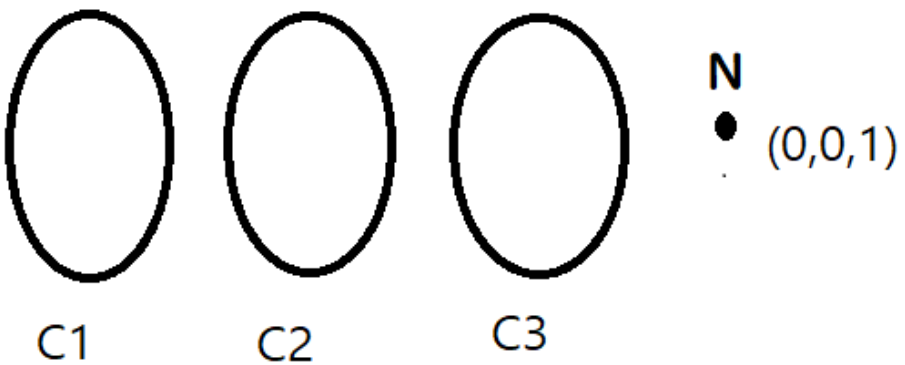
When q is even, we consider only $q = 8$.
It is known that the largest $(28, 4)_8$-arc exists uniquely upto projective equivalence and it's spectrum is $a_0 = 10$ and $a_4 = 63$.

We represent that $(28, 4)_8$-arc as several ways.
Let α be a primitive element of $\mathbb{F}_8$ with $\alpha^3 + \alpha + 1 = 0$.
Here we express the arc with conics.

(1) The $(28, 4)_8$-arc is expressed as the union of three disjoint conics with common nucleus.
Let C_i $(i = 1, 2, 3)$ be a conic defined by the equation

$$C_i : x^2 + y^2 + \lambda_i z^2 + xy = 0,$$

where $\{\lambda_1, \lambda_2, \lambda_3\} = \{1, \alpha, \alpha^3\}$. Then the point $(0, 0, 1)$ is the nucleus of C_i $(i = 1, 2, 3)$. The set $C_1 \cup C_2 \cup C_3 \cup \{(0, 0, 1)\}$ forms the $(28, 4)_8$-arc.



(2) The $(28, 4)_8$-arc is expressed using four conics passing through two points.

Let C_i $(i = 1, \ldots, 4)$ be a conic defined by the equation

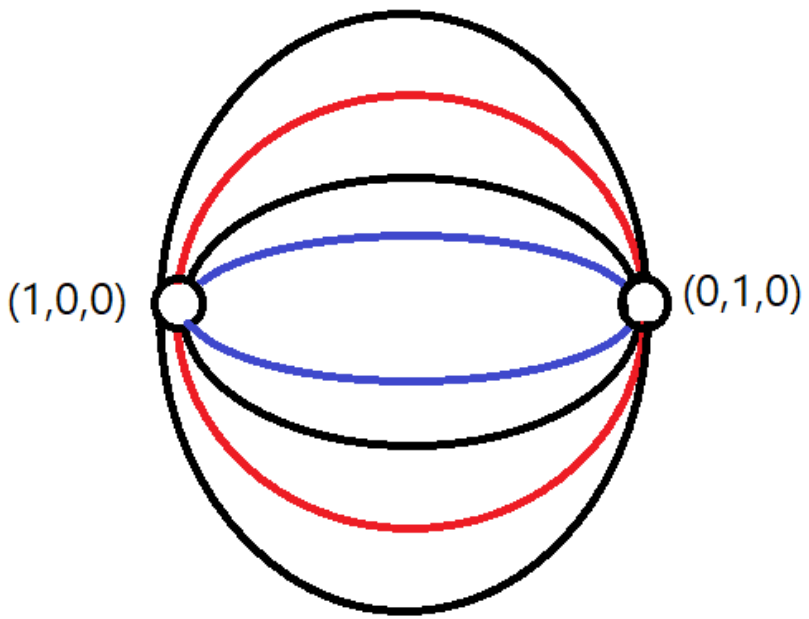
$$C_i : \mu_i z^2 + xy = 0,$$

where $\{\mu_1, \mu_2, \mu_3, \mu_4\} = \{1, \alpha^3, \alpha^5, \alpha^6\}$.

Then the point $(0, 0, 1)$ is the nucleus of C_i $(i = 1, \ldots, 4)$.

For $i \neq j$, $C_i \cap C_j = \{(1, 0, 0), (0, 1, 0)\}$.

The set $\cup_{i=1}^{4} C_i \setminus \{(1, 0, 0), (0, 1, 0)\}$ is a $(28, 4)_8$-arc.



(3) For a conic C in $PG(2,8)$, the conic C has the spectrum $a_0 = 28,\ a_1 = 9,\ a_2 = 36$.
Then the number of 0-lines is 28.
Those lines forms a dual $(28,4)_8$-arc, i.e., the set $\{(a,b,c) \in PG(2,8) \mid [a,b,c]$ is a 0-line of $C\}$ is the $(28,4)_8$-arc.

Zero set of a polynomial

Theorem 6. (Homma and Kim, 2018)

Let k be an integer with $1 \leq k \leq n$, and $PG(k-1,q)$ the linear subspace defined by $x_k = x_{k+1} = \cdots = x_n = 0$. Then the ideal of $PG(n,q) \setminus PG(k-1,q)$ in $\mathbb{F}_q[x_0,\ldots,x_n]$ is generated by

$$\{x_i^q x_j - x_i x_j^q \mid 0 \leq i < j \leq n\}$$
$$\cup \{x_s \prod_{i=k}^{n} (x_i^{q-1} - x_s^{q-1}) \mid s = 0,1,\ldots,k-1\}.$$

Corollary 7.

The ideal of $PG(n,q) \setminus \{(1,0,\ldots,0)\}$ in $\mathbb{F}_q[x_0,\ldots,x_n]$ is generated by $\{x_i^q x_j - x_i x_j^q \mid 0 \le i < j \le n\} \cup \{x_0 \prod_{i=1}^{n}(x_i^{q-1} - x_0^{q-1})\}$.

Corollary 8.

Let $P_0 \in PG(n,q)$. Then there is a homogeneous polynomial F of degree d in $\mathbb{F}_q[x_0,\ldots,x_n]$ such that the hypersurface H defined by $F = 0$ satisfies $H(\mathbb{F}_q) = PG(n,q) \setminus \{P_0\}$ if and only if $d \ge (q-1)n + 1$.

Corollary 9.

Let $P_0 \in PG(2,q)$. Then there is a homogeneous polynomial F of degree d in $\mathbb{F}_q[x_0,x_1,x_2]$ such that the curve H defined by $F = 0$ satisfies $H(\mathbb{F}_q) = PG(2,q) \setminus \{P_0\}$ if and only if $d \ge 2q - 1$.

Another partition of $PG(2,q)$ with conics

Next theorem gives another partition of $PG(2,q)$ with conics.

For odd q, the following holds.

Theorem 10.

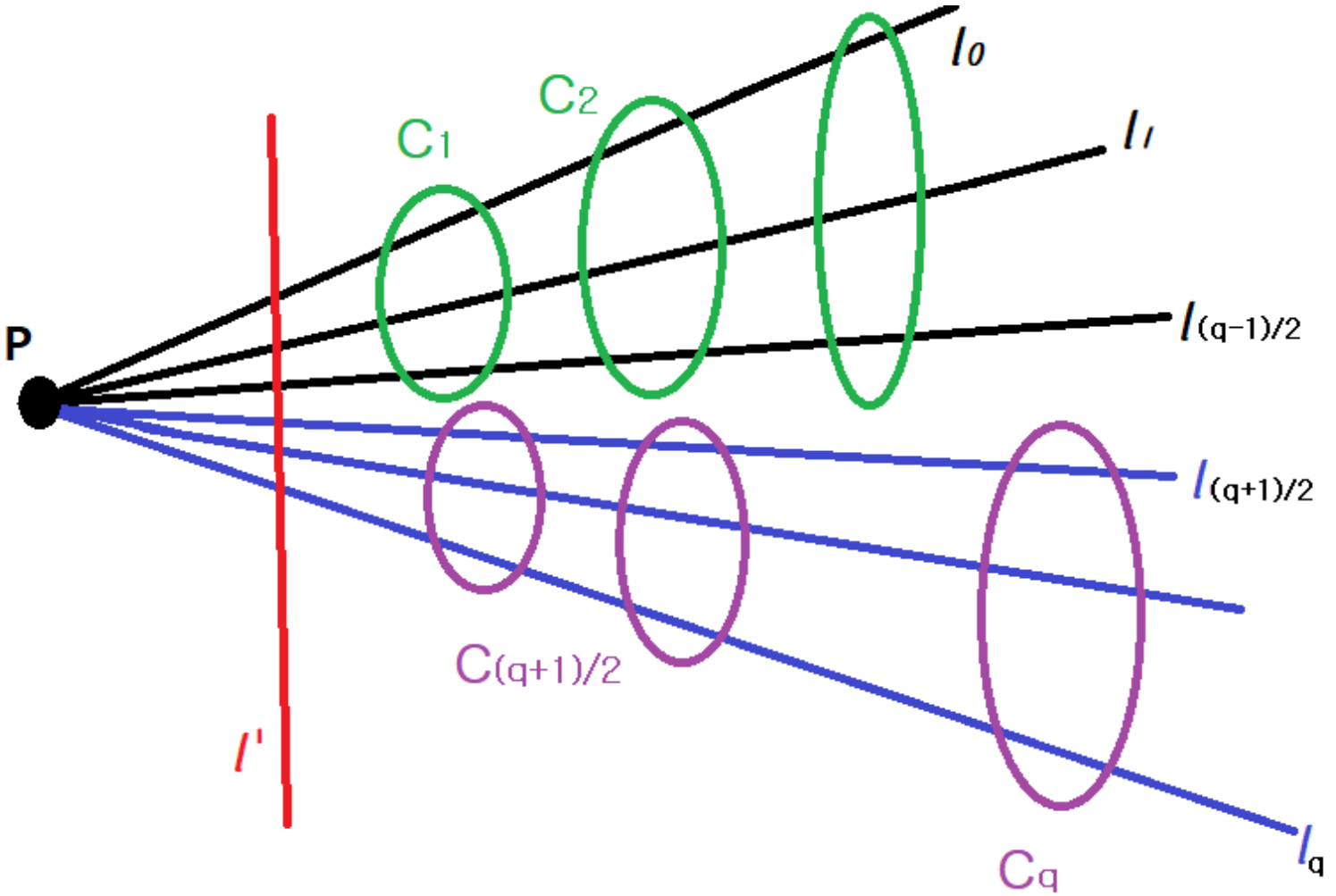
Let P be a point in $PG(2,q)$ and let ℓ_i $(i = 0,\ldots,q)$ be $q+1$ lines passing through P. Then there exists disjoint $q-1$ conics $C_1,\ldots,C_{q-1}$, a line ℓ' and satisfying the following conditions;

$$PG(2,q) = \cup_{i=1}^{q-1} C_i \cup \ell' \cup \{P\}.$$

and

$$\cup_{i=1}^{\frac{q-1}{2}} C_i \subset \cup_{i=0}^{\frac{q-1}{2}} \ell_i \text{ and } \cup_{i=\frac{q+1}{2}}^{q-1} C_i \subset \cup_{i=\frac{q+1}{2}}^{q+1} \ell_i,$$

by renumbering the lines ℓ_i.


P
l0
l1
l(q−1)/2
l(q+1)/2
lq
l'
C1
C2
C(q+1)/2
Cq

Let H be the set $(\cup_{i=2}^{\frac{q-1}{2}} C_i) \cup (\cup_{i=\frac{q+1}{2}}^{q+1} \ell_i) \cup \ell'$.

Then H is the complement of the conic C_1, and of degree

$$(q-3) + \frac{q+1}{2} + 1 = \frac{3}{2}(q-1).$$

We obtained a polynomial H whose zero set is the complement of the conic C_1.

Now we prove that the $\deg H$ is the minimum of such polynomials whose zero set is the complement of C_1.

Theorem 11.

We have

$$\min\{\deg f \mid v(f) = PG(2,q) \setminus C_1\} = \frac{3}{2}(q-1).$$

Proof. Suppose that there exists a polynomial f of degree $\leq \frac{3}{2}(q-1)-1$ such that $v(f) = PG(2,q) \setminus C_1$.
Let $\{Q_0, Q_1, \ldots, Q_q\} = C_1$.
Consider $\frac{q-1}{2}$ lines $\overline{Q_1Q_2}, \ldots, \overline{Q_{q-2}Q_{q-1}}$ and any line ℓ containing Q_q but not Q_0. Then the product of f and these $\frac{q+1}{2}$ lines is the polynomial of degree $\leq 2q-2$, whose zero set is exactly $PG(2,q) \setminus \{Q_0\}$. It contradicts the Corollalry 9. □

Thank you for your attention!!

References

- [1] S. Ball and J.W.P. Hirschfeld, Bounds on (n, r)-arcs and their application to linear codes, *Finit fields and their applications*, 11, 326–336, 2005
- [2] R.H.F. Denniston, Some maximal arcs in finite projective planes, *Jounral of Combinatorial Theory*, 6, 317–319, 1969
- [3] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields*, Clarendon Press Oxford, 1998.
- [4] M. Homma and S.J. Kim, The second largest number of points on plane curves over finite fields, *Finite Fields and Their Applications* 49, 80–93, 2018.