Counting 10-arcs in the Projective Plane

Rachel Lawrence, Luke Peilen, and Max Weinreich

Yale University

Projective Space over Finite Fields

Definition (Projective Plane over a Finite Field)

The **projective plane over** $\mathbb{F}_q$, denoted $\mathbb{P}^2(\mathbb{F}_q)$, is the set of all triples $(a : b : c)$ with $a, b, c \in \mathbb{F}_q$, except the triple $(0 : 0 : 0)$.

Projective Space over Finite Fields

Definition (Projective Plane over a Finite Field)

The **projective plane over** $\mathbb{F}_q$, denoted $\mathbb{P}^2(\mathbb{F}_q)$, is the set of all triples $(a : b : c)$ with $a, b, c \in \mathbb{F}_q$, except the triple $(0 : 0 : 0)$.

We consider two triples $(a : b : c)$ and $(d : e : f)$ the same if there exists some scalar $\lambda \in \mathbb{F}_q$ so that $(\lambda a, \lambda b, \lambda c) = (d, e, f)$.

Projective Space over Finite Fields

Definition (Projective Plane over a Finite Field)

The **projective plane over** $\mathbb{F}_q$, denoted $\mathbb{P}^2(\mathbb{F}_q)$, is the set of all triples $(a : b : c)$ with $a, b, c \in \mathbb{F}_q$, except the triple $(0 : 0 : 0)$.

We consider two triples $(a : b : c)$ and $(d : e : f)$ the same if there exists some scalar $\lambda \in \mathbb{F}_q$ so that $(\lambda a, \lambda b, \lambda c) = (d, e, f)$.

For instance, in $\mathbb{F}_7$ we have $(1 : 2 : 3) = (3 : 6 : 2)$. This is an example of a **point** in $\mathbb{P}^2(\mathbb{F}_7)$.

Arcs in Projective Space

Definition (n-arc)

An **n-arc** in $\mathbb{P}^2(\mathbb{F}_q)$ is a collection of n points in the projective plane, no three of which lie on a line.

Arcs in Projective Space

Definition (n-arc)

An **n-arc** in $\mathbb{P}^2(\mathbb{F}_q)$ is a collection of n points in the projective plane, no three of which lie on a line.

Our Goal: Find a formula in q, the size of the finite field, for how many arcs exist in the projective plane over a given finite field.

Known formulae for the number of n-arcs

- $\#(\text{1-arcs}) = q^2 + q + 1$

Known formulae for the number of n-arcs

- $\#(\text{1-arcs}) = q^2 + q + 1$
- $\#(\text{2-arcs}) = \frac{1}{2!}(q^2 + q + 1)(q^2 + q)$

Known formulae for the number of n-arcs

- $\#(\text{1-arcs}) = q^2 + q + 1$
- $\#(\text{2-arcs}) = \frac{1}{2!}(q^2 + q + 1)(q^2 + q)$
- $\#(\text{3-arcs}) = \frac{1}{3!}(q^2 + q + 1)(q^2 + q)(q^2)$

Known formulae for the number of n-arcs

- $\#(\text{1-arcs}) = q^2 + q + 1$
- $\#(\text{2-arcs}) = \frac{1}{2!}(q^2 + q + 1)(q^2 + q)$
- $\#(\text{3-arcs}) = \frac{1}{3!}(q^2 + q + 1)(q^2 + q)(q^2)$
- #(4-arcs), #(5-arcs) and #(6-arcs) of a similar form, but...

Known formulae for the number of n-arcs

Glynn [1988]:

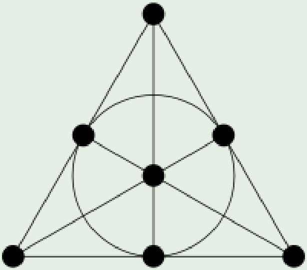
- $\#$(7-arcs) $= \frac{1}{7!}(q^2+q+1)(q^2+q)q^3(q-1)^2(q-3)(q-5)(q^4-20q^3+148q^2-468q+498) - A_7$

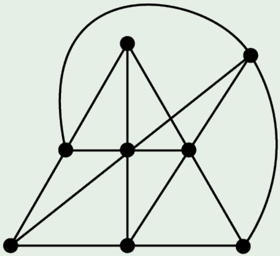
Known formulae for the number of n-arcs

Glynn [1988]:

- $\#(\text{7-arcs}) = \frac{1}{7!}(q^2+q+1)(q^2+q)q^3(q-1)^2(q-3)(q-5)(q^4-20q^3+148q^2-468q+498) - A_7$
- $\#(\text{8-arcs}) = \frac{1}{8!}(q^2+q+1)(q+1)q^3(q-1)^2(q-5)(q^7-43q^6+788q^5-7937q^4+47097q^3-162834q^2+299280q-222960) - (q^2-20q+78)A_7 + A_8$

Example (A_7 and A_8)





9-arcs and Beyond

Iampolskaia, Skorobogatov, and Sorokin [1995]:

#(9-arcs)=

$$
\begin{aligned}
&(q-1)^8 \times (q^{10} - 75q^9 \\
&+2530q^8 - 50466q^7 + 657739q^6 - 5835825q^5 \\
&+35563770q^4 - 146288034q^3 + 386490120q^2 \\
&-588513120q + 389442480 \\
&-1080(q^4 - 47q^3 + 807q^2 - 5921q + 15134)a(q) \\
&+840(9q^2 - 243q + 1684)b(q) \\
&+30240(-9c(q) + 9d(q) + 2e(q))),
\end{aligned}
$$

where

$$
\begin{aligned}
a(q) &= 1, \text{ if } q \text{ is a power of } 2, \text{ and } a(q) = 0, \text{otherwise} \\
b(q) &= \#\{x \in \boldsymbol{F}_q \text{ such that } x^2 + x + 1 = 0\} \\
c(q) &= 1, \text{ if } q \text{ is a power of } 3, \text{ and } c(q) = 0, \text{otherwise} \\
d(q) &= \#\{x \in \boldsymbol{F}_q, \text{ such that } x^2 + x - 1 = 0\} \\
e(q) &= \#\{x \in \boldsymbol{F}_q, \text{ such that } x^2 + 1 = 0\}.
\end{aligned}
$$

Superfigurations

There are certain incidence structures, called "Superfigurations," which play a key role in the combinatorial geometry of $\mathbb{P}^2(\mathbb{F}_q)$.

Superfigurations

There are certain incidence structures, called "Superfigurations," which play a key role in the combinatorial geometry of $\mathbb{P}^2(\mathbb{F}_q)$.

Definition (Superfiguration)

A superfiguration is a collection of points and any number of lines such that:

Superfigurations

There are certain incidence structures, called "Superfigurations," which play a key role in the combinatorial geometry of $\mathbb{P}^2(\mathbb{F}_q)$.

Definition (Superfiguration)

A superfiguration is a collection of points and any number of lines such that:

- Two lines intersect each other at no more than one point.

Superfigurations

There are certain incidence structures, called "Superfigurations," which play a key role in the combinatorial geometry of $\mathbb{P}^2(\mathbb{F}_q)$.

Definition (Superfiguration)

A superfiguration is a collection of points and any number of lines such that:

- Two lines intersect each other at no more than one point.
- Two points are connected by no more than one line.

Superfigurations

There are certain incidence structures, called "Superfigurations," which play a key role in the combinatorial geometry of $\mathbb{P}^2(\mathbb{F}_q)$.

Definition (Superfiguration)

A superfiguration is a collection of points and any number of lines such that:

- Two lines intersect each other at no more than one point.
- Two points are connected by no more than one line.
- There are at least 3 points on each line, and at least 3 lines through each point.

Game Plan

Theorem (Glynn)

Let S be the set of superfigurations on up to 10 points. In general, for #(10-arcs) we can expect an expression of the form

$$f(q) + \sum_{s \in S} g_s(q) A_s$$

where A_s is the number of copies of s in $\mathbb{P}^2(\mathbb{F}_q)$ and $g_s(q)$ and $f(q)$ are polynomials in q.

Game Plan

Theorem (Glynn)

$$\#\text{(10-arcs)} = f(q) + \sum_{s \in S} g_s(q) A_s$$

In order to find all the terms of this polynomial, a number of subproblems arise:

1. Finding Superfigurations (Combinatorics problem)

Game Plan

Theorem (Glynn)

$$\#\text{(10-arcs)} = f(q) + \sum_{s \in S} g_s(q) A_s$$

In order to find all the terms of this polynomial, a number of subproblems arise:

1. Finding Superfigurations (Combinatorics problem)
2. Realizability of Superfigurations (Algebra problem)

Game Plan

Theorem (Glynn)

$$\#\textit{(10-arcs)} = f(q) + \sum_{s \in S} g_s(q) A_s$$

In order to find all the terms of this polynomial, a number of subproblems arise:

1. Finding Superfigurations (Combinatorics problem)
2. Realizability of Superfigurations (Algebra problem)
3. Finding Coefficients (Computational problem)

Finding Superfigurations

Theorem (LPW 2015)

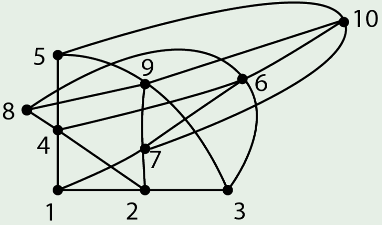
There are 151 superfigurations on 10 points.

Finding Superfigurations

Theorem (LPW 2015)

There are 151 superfigurations on 10 points.

Example

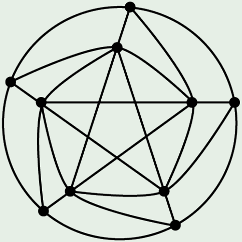


Finding Superfigurations

Theorem (LPW 2015)

There are 151 superfigurations on 10 points.

Example



10-Arcs Formula

#(10-arcs) =

$$f(q) + \sum_{s \in S} g_s(q) A_s$$

We now know the contents of the set S of all superfigurations on up to 10 points. We still need to determine A_s for each $s \in S$, and the polynomials $g_s(q)$.

Realizability of Superfigurations

Definition (Realizability)

A superfiguration $\mathscr{C}$ is ***q*-realizable** if there exists some assignment φ of coordinates in $\mathbb{P}^2(\mathbb{F}_q)$ to points of the superfiguration such that φ preserves the collinearity (or lack of collinearity) of every subset of 3 points in $\mathscr{C}$.

Realizability of Superfigurations

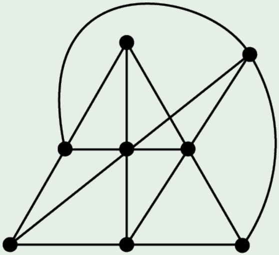
Definition (Realizability)

A superfiguration $\mathscr{C}$ is ***q*-realizable** if there exists some assignment φ of coordinates in $\mathbb{P}^2(\mathbb{F}_q)$ to points of the superfiguration such that φ preserves the collinearity (or lack of collinearity) of every subset of 3 points in $\mathscr{C}$.

For each of the 151 superfigurations, we want to determine for which $\mathbb{F}_q$ the configuration can be realized, and if so, how many different ways there are to assign the coordinates to the points.

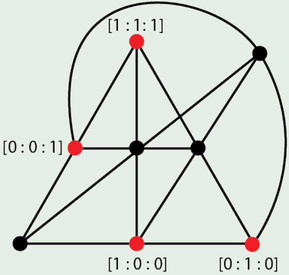
Realizability of Superfigurations

Example (Computing Realizability)



Realizability of Superfigurations

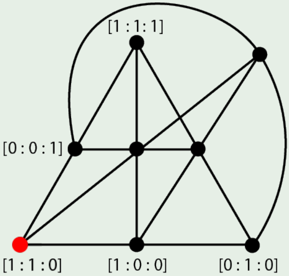
Example (Computing Realizability)



Add coordinates for 4 points in general position.

Realizability of Superfigurations

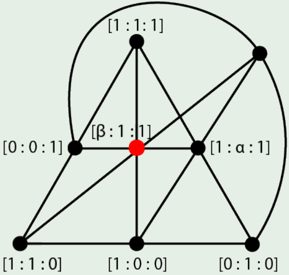
Example (Computing Realizability)



Deduce additional point.

Realizability of Superfigurations

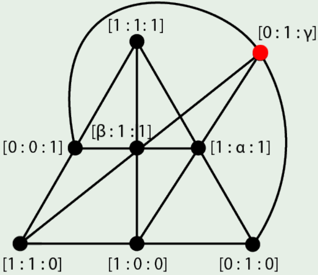
Example (Computing Realizability)



Deduce additional point.

Realizability of Superfigurations

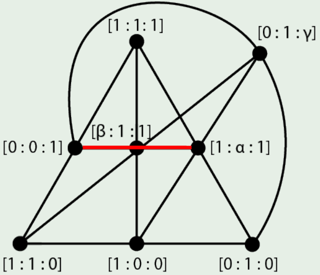
Example (Computing Realizability)



Deduce additional point.

Realizability of Superfigurations

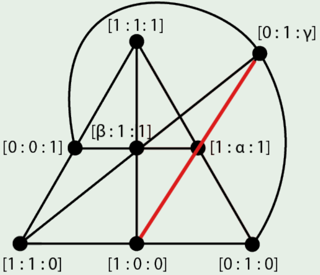
Example (Computing Realizability)



$$\begin{vmatrix} 0 & 0 & 1 \\ \beta & 1 & 1 \\ 1 & \alpha & 1 \end{vmatrix} = \alpha\beta - 1 = 0.$$

Realizability of Superfigurations

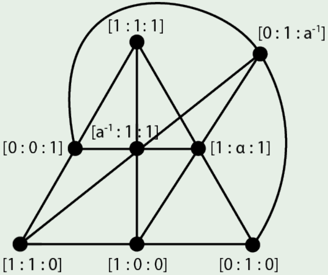
Example (Computing Realizability)



$$\begin{vmatrix} 1 & 0 & 0 \\ 1 & \alpha & 1 \\ 0 & 1 & \gamma \end{vmatrix} = \alpha\gamma - 1 = 0.$$

Realizability of Superfigurations

Example (Computing Realizability)

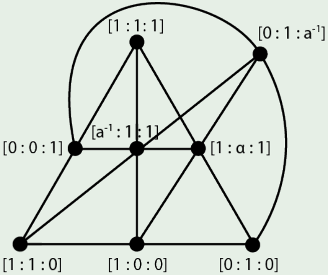


$$\begin{vmatrix} 1 & 1 & 0 \\ \alpha^{-1} & 1 & 1 \\ 0 & 1 & \alpha^{-1} \end{vmatrix}$$

$$= -\alpha^{-2} + \alpha^{-1} - 1 = 0$$

Realizability of Superfigurations

Example (Computing Realizability)



$$\begin{vmatrix} 1 & 1 & 0 \\ \alpha^{-1} & 1 & 1 \\ 0 & 1 & \alpha^{-1} \end{vmatrix}$$

$$= -\alpha^{-2} + \alpha^{-1} - 1 = 0$$

$$\implies \alpha^2 - \alpha + 1 = 0$$

Weak and Strong Realizations

Weak and Strong Realizations

Definition (Weak Realization)

A **weak realization** of a superfiguration $\mathscr{C}$ is an assignment φ of coordinates in $\mathbb{P}^2(\mathbb{F}_q)$ to points of $\mathscr{C}$ such that φ at least preserves all collinearities of $\mathscr{C}$.

Weak and Strong Realizations

Definition (Weak Realization)

A **weak realization** of a superfiguration $\mathscr{C}$ is an assignment φ of coordinates in $\mathbb{P}^2(\mathbb{F}_q)$ to points of $\mathscr{C}$ such that φ at least preserves all collinearities of $\mathscr{C}$.

Definition (Strong Realization)

A **strong realization** of a superfiguration $\mathscr{C}$ is a weak realization of $\mathscr{C}$ that induces no additional collinearities.

Weak and Strong Realizations

Definition (Weak Realization)

A **weak realization** of a superfiguration $\mathscr{C}$ is an assignment φ of coordinates in $\mathbb{P}^2(\mathbb{F}_q)$ to points of $\mathscr{C}$ such that φ at least preserves all collinearities of $\mathscr{C}$.

Definition (Strong Realization)

A **strong realization** of a superfiguration $\mathscr{C}$ is a weak realization of $\mathscr{C}$ that induces no additional collinearities.

- We say that a superfiguration is **nondegenerate** if all points and lines remain unique after assigning coordinates.

Realizability Results

Theorem (LPW 2015)

Each superfiguration S may be associated with a system of polynomial equations so that S appears in $\mathbb{P}^2(\mathbb{F}_q)$ if and only if that system of equations has solutions over $\mathbb{F}_q$.

Example

Mobius-Kantor appears in $\mathbb{P}^2(\mathbb{F}_q)$ when $x^2 - x + 1$ has solutions over $\mathbb{F}_q$.

Realizability Results

Of the 151 superfigurations, we have computed all of the previously unknown polynomial systems. We find that:

Theorem

There are 31 superfigurations which cannot be realized in $\mathbb{P}^2(\mathbb{F}_q)$ for any q.

Realizability Results

Example

The following polynomials show up in the realizability computations of superfigurations:

$$5 = 0$$

$$x^3 + x^2 - 1 = 0$$

$$x^2y^3 - (2x^3 - x^2)y^2 + (4x^3 - 7x^2 + 3x)y$$
$$-(2x^3 - 5x^2 + 4x - 1) = 0$$

The numbers A_S mentioned earlier may be characterized as the number of distinct solutions of each polynomial over $\mathbb{F}_q$.

10-arcs Formula

#(10-arcs) =

$$f(q) + \sum_{s \in S} g_s(q) A_s$$

We now have a way to find A_s for each $s \in S$, and just need the polynomials $g_s(q)$.

Computing $g_s(q)$ and $f(q)$

Definition (Boolean n-function)

Generalizing the notion of superfigurations, we define a boolean n-function

$$B : \mathcal{P}(\{1, 2, \cdots, n\}) \to \mathbb{1}_C$$

where $\mathbb{1}_C$ is the indicator function denoting whether the points in the set are collinear.

Computing $g_s(q)$ and $f(q)$

Definition (Boolean n-function)

Generalizing the notion of superfigurations, we define a boolean n-function

$$B : \mathcal{P}(\{1, 2, \cdots, n\}) \to \mathbb{1}_C$$

where $\mathbb{1}_C$ is the indicator function denoting whether the points in the set are collinear.

We adapt an algorithm from Glynn, Rolland, and Skorobogatov to compute the $g_s(q)$ and $f(q)$ by examining a partial ordering on all boolean n-functions for $n \leq 10$.

Computing $g_s(q)$ and $f(q)$

Algorithm Sketch:

Computing $g_s(q)$ and $f(q)$

Algorithm Sketch:

- Set $n = 1$.

Computing $g_s(q)$ and $f(q)$

Algorithm Sketch:

- Set $n = 1$.
- Create a partial ordering under "constriction" on all boolean n-functions.

Computing $g_s(q)$ and $f(q)$

Algorithm Sketch:

- Set $n = 1$.
- Create a partial ordering under "constriction" on all boolean n-functions.
- For each boolean n-function b_f, compute the number of weak realizations $n_q(b_f)$ as a function of all $n_q(b_g)$ such that $b_g \preceq b_f$.

Computing $g_s(q)$ and $f(q)$

Algorithm Sketch:

- Set $n = 1$.
- Create a partial ordering under "constriction" on all boolean n-functions.
- For each boolean n-function b_f, compute the number of weak realizations $n_q(b_f)$ as a function of all $n_q(b_g)$ such that $b_g \preceq b_f$.
- Compute the strong realizations $m_q(b_f)$ of each b_f using the Möbius inversion

$$m_q(b_f) = \sum_{b_g \geq b_f} (-1)^{\#b_g^{-1}(1) - \#b_f^{-1}(1)} n_q(b_g)$$

Computing $g_s(q)$ and $f(q)$

Algorithm Sketch:

- Set $n = 1$.
- Create a partial ordering under "constriction" on all boolean n-functions.
- For each boolean n-function b_f, compute the number of weak realizations $n_q(b_f)$ as a function of all $n_q(b_g)$ such that $b_g \preceq b_f$.
- Compute the strong realizations $m_q(b_f)$ of each b_f using the Möbius inversion

$$m_q(b_f) = \sum_{b_g \geq b_f} (-1)^{\#b_g^{-1}(1) - \#b_f^{-1}(1)} n_q(b_g)$$

- Increment n for $n \leq 10$.

Applications

- Error-Correcting Codes

Applications

- Error-Correcting Codes
  - Specifically, there is a bijection between n-arcs in $\mathbb{P}^2(\mathbb{F}_q)$ and $[n, 3]$ Maximum Distance Separable (MDS) Codes

Applications

- Error-Correcting Codes
  - Specifically, there is a bijection between n-arcs in $\mathbb{P}^2(\mathbb{F}_q)$ and $[n, 3]$ Maximum Distance Separable (MDS) Codes
- Existence of abstract projective planes

Applications

- Error-Correcting Codes
  - Specifically, there is a bijection between n-arcs in $\mathbb{P}^2(\mathbb{F}_q)$ and $[n, 3]$ Maximum Distance Separable (MDS) Codes
- Existence of abstract projective planes
  - There is no projective plane of order six!

Thank you!