Codes from Polynomials over Finite Fields

Nathan Kaplan

University of California, Irvine

Colorado State Colloquium

February 8, 2021

I. Some Questions

Let $\mathbb{F}_q$ be a finite field of size q.

Question

1. *What is the maximum number of points in $\mathbb{P}^2(\mathbb{F}_q)$ such that no three points lie on a line?*

2. *What is the maximum n such that there exists a $3 \times n$ matrix with entries in $\mathbb{F}_q$ such that no 3×3 submatrix has determinant 0?*

3. *What is the maximum number of points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ such that no k points lie in a hyperplane?*

4. *What is the maximum n such that there exists a $k \times n$ matrix with entries in $\mathbb{F}_q$ such that no $k \times k$ submatrix has determinant 0?*

Main Conjecture for MDS Codes/MDS Conjecture

Questions II: Cubic Surfaces over Finite Fields

Question

1. *What is the maximum number of $\mathbb{F}_q$-points of a smooth cubic surface defined over $\mathbb{F}_q$?*

2. *A homogeneous cubic $f_3(w,x,y,z)$ is defined by 20 coefficients:*

$$f_3(w,x,y,z) = a_0 w^3 + a_1 w^2 x + \cdots + a_{19} z^3.$$

   How many of these q^{20} polynomials define a smooth cubic surface with this maximum number of $\mathbb{F}_q$-points?

3. *What about other numbers of $\mathbb{F}_q$-points?*

Questions III: Intersections of Cubic Curves

A homogeneous cubic polynomial in x, y, z is defined by 10 coefficients:

$$f_3(x, y, z) = a_0 x^3 + a_1 x^2 y + \cdots + a_9 z^3.$$

Question

How many of the q^{20} pairs of homogeneous cubic polynomials $f_3(x, y, z), g_3(x, y, z)$ do not share a common factor and have exactly 9 common $\mathbb{F}_q$-rational zeros?

◦ A cubic surface defined over $\mathbb{F}_q$ has 27 lines, but these lines are not necessarily defined over $\mathbb{F}_q$.

Theorem

The number of homogeneous cubic polynomials $f_3(w, x, y, z)$ such that $\{f_3 = 0\}$ is a smooth cubic surface with $q^2 + 7q + 1$ $\mathbb{F}_q$-points, the maximum possible, is

$$\frac{|\operatorname{GL}_4(\mathbb{F}_q)|(q-2)(q-3)(q-5)^2}{51840}.$$

◦ Three very different approaches: Betten-Karaoglu, Das, Elkies.

Theorem (K.-Matei)

The number of pairs of homogeneous cubic polynomials $f_3(x,y,z)$, $g_3(x,y,z)$ that do not have a common irreducible factor over $\overline{\mathbb{F}_q}$ and have exactly 9 common zeros in $\mathbb{P}^2(\mathbb{F}_q)$ is

$$\frac{1}{9!}(q-2)(q+1)^2(q-1)^4q^5(q^2+q+1)\cdot \left(q^6+2q^5-73q^4+344q^3-838q^2+1754q-2030\right).$$

◦ There are similar (more complicated) polynomial formulas for each number of common zeros between 0 and 9.

II. Coding Theory Basics

Coding Theory Basics

Let $\mathbb{F}_q$ be a finite field of size q.

Definition

- *A* code *over* $\mathbb{F}_q$ *of length* n *is a subset* $C \subseteq \mathbb{F}_q^n$.
- C *is a* linear code *if it is a linear subspace of* $\mathbb{F}_q^n$.
  That is, if $c_1, c_2 \in C$ *then* $c_1 + c_2 \in C$ *and* $\alpha c_1 \in C$ *for any* $\alpha \in \mathbb{F}_q$.
- *For* $\substack{x=(x_1,\ldots,x_n) \\ y=(y_1,\ldots,y_n)} \in \mathbb{F}_q^n$, *the* Hamming distance *between* x *and* y *is*

$$d(x,y) = \#\{i \mid x_i \neq y_i\}.$$

- *The* Hamming weight *of* x *is* $\mathrm{wt}(x) = d(x, \mathbf{0}) = \#\{i \mid x_i \neq 0\}$.
- *The* minimum distance *of a code* C *is*

$$d(C) = \min_{\substack{x,y \in C \\ x \neq y}} d(x,y).$$

- *If* C *is linear,* $d(C)$ *is the minimum weight of a nonzero* $c \in C$.

Main Problem in Combinatorial Coding Theory

The most interesting codes $C \subseteq \mathbb{F}_q^n$ have **large size** and **large minimum distance**.

Definition

Let $A_q(n,d)$ be the maximum size of a code $C \subseteq \mathbb{F}_q^n$ that has minimum distance at least d.

Main Problem in Combinatorial Coding Theory:
Compute values of $A_q(n,d)$.

On the Size of Optimal Three-Error-Correcting Binary Codes of Length 16

Patric R. J. Östergård

***Abstract*—Let $A(n,d)$ denote the maximum size of a binary code with length n and minimum distance d. It has been known for decades that $A(16,7) = A(17,8) = 36$ or 37, that is, that the size of optimal 3-error-correcting binary codes of length 16 is either 36 or 37. By a recursive classification via subcodes and a clique search in the final stage, it is shown that the size of optimal such codes is 36.**

attaining the lower bound have been constructed in [13], [14] (see also [10, pp. 57,58]) and the upper bound is from [3]. The problem of determining this particular value is also mentioned in [8, Research Problem 7.18]. The main result of this work is that the best known lower bound is the exact value: $A(17,8) = 36$.

MDS Codes

Proposition (Singleton Bound)

$$A_q(n, d) \leq q^{n-(d-1)}$$

Proof.

1. Let $C \subseteq \mathbb{F}_q^n$ have $|C| = A_q(n, d)$ and $d(C) \geq d$.
2. Write down all the $A_q(n, d)$ codewords.
3. Choose any $d - 1$ coordinates and erase them.
4. Get $A_q(n, d)$ **distinct** elements of $\mathbb{F}_q^{n-(d-1)}$.

□

Definition

A code for which equality holds, $|C| = q^{n-(d-1)}$ is called *Maximum Distance Separable* *or* *MDS*.

III. Reed-Solomon Codes

Reed-Solomon Codes

Let $p_1, p_2, \ldots, p_q$ be an ordering of the elements of $\mathbb{F}_q$.
Let V_d be the vector space of polynomials in $\mathbb{F}_q[x]$ of degree at most d.

Definition

The evaluation map is defined by

$$\begin{aligned} \mathrm{ev}\colon \quad V_d &\mapsto \mathbb{F}_q^q \\ \mathrm{ev}(f) &= (f(p_1), \ldots, f(p_q)) \in \mathbb{F}_q^q. \end{aligned}$$

- $\mathrm{ev}(f+g) = \mathrm{ev}(f) + \mathrm{ev}(g)$ and $\mathrm{ev}(\alpha f) = \alpha\,\mathrm{ev}(f)$.
  The image $\mathrm{ev}(V_d) \subseteq \mathbb{F}_q^q$ is a linear code.

  It is the Reed-Solomon code of length q and order d, $\mathrm{RS}(q,d)$.
- As long as there is no nonzero polynomial vanishing at every element of $\mathbb{F}_q$, this map is injective, and $\dim(\mathrm{RS}(q,d)) = \dim(V_d) = d+1$.

  $x^q - x$ vanishes at every element of $\mathbb{F}_q$, so suppose $q > d$.

Reed-Solomon Codes are MDS

Proposition

Let F be a field.
A nonzero $f \in F[x]$ with $\deg(f) = d$ has at most d distinct roots in F.

- Suppose $f, g \in \mathbb{F}_q[x]$ each have degree at most d.
  Then $f - g$ is either 0 or has at most d roots in $\mathbb{F}_q$.
- Conclude that $d(\mathrm{RS}(q, d)) = q - d$.
- $|\mathrm{RS}(q, d)| = q^{d+1} = q^{q-(d(\mathrm{RS}(q,d))-1)}$.
- Therefore, RS(q, d) is an MDS code.

Main Conjecture for MDS Codes

Definition

Let $M(k,q)$ be the maximum n such that a k-dimensional linear MDS code $C \subseteq \mathbb{F}_q^n$ exists.

Conjecture (Main Conjecture for MDS Codes)

1. *If $q \leq k$, $M(k,q) = k+1$. (Easy: Suppose now that $q > k$.)*
2. *If q is even and $k = 3$ or $k = q-1$, then $M(k,q) = q+2$.*
3. *Otherwise, $M(k,q) = q+1$.*

Reed-Solomon Example: For $q > d$, $M(d+1,q) \geq q$.

Projective Space over a Finite Field

Points of projective space are equivalence classes of affine points, where two points are equivalent if one is a scalar multiple of the other.

Definition

The *projective space* *of dimension* $n-1$ *over a finite field* $\mathbb{F}_q$ *is*

$$\mathbb{P}^{n-1}(\mathbb{F}_q) = \{(x_1,\ldots,x_n) \in \mathbb{F}_q^n \setminus (0,\ldots,0) \text{ where } (x_1,\ldots,x_n) \sim (\alpha x_1,\ldots,\alpha x_n) \text{ for any } \alpha \in \mathbb{F}_q^*\}.$$

Example

1. $\mathbb{P}^1(\mathbb{F}_q)$ has $q+1$ points, $[1:a]$ where $a \in \mathbb{F}_q$ and $[0:1]$.
2. $\mathbb{P}^2(\mathbb{F}_q)$ has q^2+q+1 points,

$$[1:a:b],\ [0:1:c],\ [0:0:1]$$

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

MDS Example: Projective Reed-Solomon Codes

Let V_d be the vector space of homogeneous polynomials in x, y of degree d.

Let $p'_1, p'_2, \ldots, p'_{q+1}$ be affine representatives for the points of $\mathbb{P}^1(\mathbb{F}_q)$.

Example: $(1, a)$, $(0, 1)$ where $a \in \mathbb{F}_q$.

Definition

The evaluation map is defined by

$$\begin{aligned} \mathrm{ev}\colon \quad V_d &\mapsto \mathbb{F}_q^{q+1} \\ \mathrm{ev}(f) = &\quad \big(f(p'_1), \ldots, f(p'_{q+1})\big) \in \mathbb{F}_q^{q+1} \end{aligned}$$

- If $d < q$, this map is injective.
  In this case, $\mathrm{ev}(V_d)$ is a $(d+1)$-dimensional linear subspace of $\mathbb{F}_q^{q+1}$, the Projective Reed-Solomon code $C_{1,d}$.
- This is an MDS code.
  Linear forms on $\mathbb{P}^1$ that agree at too many points are equal.

Main Conjecture for MDS Codes

Definition

Let $M(k, q)$ be the maximum n such that a k-dimensional linear MDS code $C \subseteq \mathbb{F}_q^n$ exists.

Conjecture (Main Conjecture for MDS Codes)

1. *If $q \leq k$, $M(k, q) = k + 1$. (Easy: Suppose now that $q > k$.)*
2. *If q is even and $k = 3$ or $k = q - 1$, then $M(k, q) = q + 2$.*
3. *Otherwise, $M(k, q) = q + 1$.*

Projective Reed-Solomon Example: For $q > d$, $M(d + 1, q) \geq q + 1$.

Question

When does there exist a longer k-dimensional MDS code defined over $\mathbb{F}_q$ than the one that comes from a Projective Reed-Solomon code?

Projective Reed-Solomon Code Example

- A k-dimensional linear code $C \subset \mathbb{F}_q^n$ is the row span of a $k \times n$ generator matrix G.
- Let $q = 5,\ d = 2$. $C_{1,2}$ is the row span of

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 1 & 4 & 4 & 1 & 1 \end{pmatrix}$$

- $C_{1,d}$ has minimum distance $q + 1 - d = 4$.
- No nonzero linear combination of rows has 0s in 3 or more coordinates.
- No 3×3 submatrix has determinant 0.

Main Conjecture for MDS Codes II

1. Let G be a $k \times n$ generator matrix for the k-dimensional code $C \subseteq \mathbb{F}_q^n$.
2. C is an MDS code if and only if every nonzero linear combination of the rows of G has at most $k-1$ coordinates equal to 0.
3. Equivalently, no $k \times k$ submatrix of G has determinant 0.

- $M(k,q)$ is the maximum n such that a k-dimensional linear MDS code $C \subset \mathbb{F}_q^n$ exists.
- $M(k,q)$ is the maximum n for which there exists a $k \times n$ matrix with entries in $\mathbb{F}_q$ such that none of its $\binom{n}{k}$ $k \times k$ submatrices have determinant 0.

- A nonzero column of a $k \times n$ matrix with entries in $\mathbb{F}_q$ gives a point in $\mathbb{P}^{k-1}(\mathbb{F}_q)$.
- k points lie in a hyperplane exactly when the corresponding $k \times k$ matrix has determinant 0.
- $M(k, q)$ is the maximum number of points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$ such that no k of them lie in a hyperplane.

Example

Let $q = 5,\ d = 2.$ $C_{1,2}$ is the row span of

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 1 & 4 & 4 & 1 & 1 \end{pmatrix}$$

This gives 6 points in $\mathbb{P}^2(\mathbb{F}_5)$:

$$[1:0:0], [1:1:1], [1:2:4], [1:3:4], [1:4:1], [0:0:1].$$

No three of these points lie on a line.

$k = 3$: Segre's Theorem

Idea: A smooth conic has $q+1$ $\mathbb{F}_q$-points, no three lie on a line.

Theorem (Segre)

1. *If q is odd, $M(3,q) = q+1$.*
   In fact, every collection of $q+1$ points with no three in a line is the set of rational points of a smooth conic.
2. *If q is even, $M(3,q) = q+2$.*
   (The classification of these hyperovals is not known.)

Definition. A curve X in $\mathbf{P}^n$ is *strange* if there is a point A which lies on all the tangent lines of X.

311

Example 3.8.2. A conic in $\mathbf{P}^2$ over a field of characteristic 2 is strange. For example, consider the conic $y = x^2$. Then $dy/dx \equiv 0$, so all the tangent lines are horizontal, so they all pass through the point at infinity on the x-axis.

Higher Dimensions

The $q + 1$ points in $\mathbb{P}^k(\mathbb{F}_q)$ corresponding to the Projective Reed-Solomon code $C_{1,k}$ are the $\mathbb{F}_q$-points of a rational normal curve.

Example: Image of the map $\nu_k \colon \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^k(\mathbb{F}_q)$

$$[x : y] \to [x^k : x^{k-1}y : \cdots : xy^{k-1} : y^k].$$

Theorem (Segre)

If q is odd, $M(4, q) = q + 1$.

In fact, every collection of $q + 1$ points in $\mathbb{P}^3(\mathbb{F}_q)$ with no 4 in a plane is the set of rational points of a twisted cubic curve.

Theorem

If q is odd, $M(5, q) = q + 1$.

Glynn's 10-**Arc**: 10 points in $\mathbb{P}^4(\mathbb{F}_9)$ with no 5 in a hyperplane, but they do not lie on a rational normal curve.

One of Nathan's Favorite Problems!

Question

What is the maximum number of points in $\mathbb{P}^2(\mathbb{F}_q)$ with no 4 on a line?

- A smooth plane cubic curve has no four points on a line.
  Can find one with at least $q + \lfloor 2\sqrt{q} \rfloor$ $\mathbb{F}_q$-points.
- Best upper bound: $2q$.
- Blokhuis offered a prize of 10,000 Hungarian forints to give an improvement in either direction:
  - Construction of $(1+\epsilon)q$ for infinitely many q,
  - Or, upper bound $(2-\epsilon)q$ that holds for infinitely many q.

Note: This prize is $\approx$ \$35.

IV. Projective Reed-Muller Codes

More Variables: Projective Reed-Muller Codes

Definition

- *Let* $N = |\mathbb{P}^n(\mathbb{F}_q)| = \frac{q^{n+1}-1}{q-1}$.

  1. *Choose an ordering of the points of* $\mathbb{P}^n(\mathbb{F}_q): \ p_1, \ldots, p_N$.
  2. *Choose an affine representative for each projective point:* $p'_1, \ldots, p'_N$.

- *Let* $V_{n,d}$ *be the* $\binom{n+d}{d}$*-dimensional vector space of homogeneous polynomials in* $x_0, x_1, \ldots, x_n$ *of degree* d.

- *The evaluation map is defined by*

$$\begin{aligned} \text{ev}: \quad V_{n,d} \quad &\mapsto \quad \mathbb{F}_q^N \\ \text{ev}(f) = \quad & \left(f(p'_1), \ldots, f(p'_N)\right) \in \mathbb{F}_q^N \end{aligned}$$

- *If* $d \leq q$*, this map is injective.*
  Image is the Projective Reed-Muller code $C_{n,d}$.

Projective Reed-Muller Codes

Question

1. *What is the minimum distance of $C_{n,d}$?*
2. *What is the maximum number of $\mathbb{F}_q$-points of a degree d hypersurface in $\mathbb{P}^n$?*

Idea [Serre]: Take the union of d hyperplanes through a common $n-2$ dimensional linear subspace.

For $n > 1$, the Projective Reed-Muller code $C_{n,d}$ is far from being MDS.

Definition

The *Hamming weight enumerator* *of* $C \subseteq \mathbb{F}_q^n$ *is*

$$W_C(X,Y) = \sum_{c \in C} X^{n-\mathrm{wt}(c)} Y^{\mathrm{wt}(c)} = \sum_{i=0}^{n} A_i \cdot X^{n-i} Y^i,$$

where $$A_i = \#\{c \in C \mid \mathrm{wt}(c) = i\}.$$

Example

For $C = \{(0,0,0),(1,1,1)\} \subset \mathbb{F}_2^3$, $\quad W_C(X,Y) = X^3 + Y^3$.

Question

- *What is the weight enumerator of* $C_{1,d}$*?*
- *How many* $f \in \mathbb{F}_q[x]$ *of degree at most* d *have exactly* m *distinct roots in* $\mathbb{F}_q$*?*

Fact: The weight enumerator of a k-dimensional MDS code $C \subseteq \mathbb{F}_q^n$ is determined by k and n.

A homogeneous cubic $f_3(w,x,y,z)$ is defined by 20 coefficients:

$$f_3(w,x,y,z) = a_0 w^3 + a_1 w^2 x + \cdots + a_{19} z^3.$$

Problem

1. *How many of the q^{20} homogeneous cubic polynomials $f_3(w,x,y,z)$ have exactly k zeros?*
2. *How many elements of $C_{3,3} \subset \mathbb{F}_q^{q^3+q^2+q+1}$ have exactly k coordinates equal to zero?*
3. *What is the $A_{q^3+q^2+q+1-k}$ coefficient of $W_{C_{3,3}}(X,Y)$?*

Projective Reed-Muller Codes: Examples

Example ($C_{n,1}$: Linear Forms on $\mathbb{P}^n$)

If $f(x_0, \ldots, x_n)$ is not zero, it defines a hyperplane with $\frac{q^n-1}{q-1}$ $\mathbb{F}_q$-points.

$$W_{C_{n,1}}(X,Y) = X^{\frac{q^{n+1}-1}{q-1}} + (q^{n+1}-1)X^{\frac{q^n-1}{q-1}}Y^{q^n}.$$

- We know $W_{C_{1,d}}(X,Y)$ and $W_{C_{n,2}}(X,Y)$.

Example ($C_{2,2}$ Plane Conics)

$(q-1)(q^5-q^2)$ polynomials $f_2(x,y,z)$ define a smooth conic.
All are projectively equivalent and have $q+1$ $\mathbb{F}_q$-points.

Some are singular:

Reducible Curve	# Polynomials	$\#\mathbb{F}_q$-points
Pair of Rational Lines	$(q-1)\binom{q^2+q+1}{2}$	$2q+1$
Pair of Galois-conjugate Lines	$(q-1)(\frac{q^4-q}{2})$	1
Double Line	$(q-1)(q^2+q+1)$	$q+1$

$C_{2,3}$: Plane Cubic Curves

- Reducible Cubics.
- Irreducible, Singular Cubics.
- Smooth Cubics.

A smooth cubic curve with an $\mathbb{F}_q$-rational point defines an elliptic curve.

Question

How many isomorphism classes of elliptic curves $E/\mathbb{F}_q$ have $\#E(\mathbb{F}_q) = q + 1 - t$?

Hasse's Theorem: 0 unless $|t| \leq 2\sqrt{q}$.
Deuring, Waterhouse: Answer involves class numbers of imaginary quadratic fields.

Question

Given an isomorphism class $E/\mathbb{F}_q$, how many smooth plane cubic curves C defined over $\mathbb{F}_q$ give an elliptic curve isomorphic to E?

Putting this together gives $W_{C_{2,3}}(X, Y)$.

- Reducible Cubics: (Three planes, etc.)
- Cone over a Plane Cubic.
- Everything Else.

Theorem (Weil)

An irreducible cubic surface S that is not a cone over a plane cubic has

$$\#S(\mathbb{F}_q) = q^2 + tq + 1,$$

where $t \in [-2, 7]$.

We know $W_{C_{3,3}}(X, Y)$ except for 10 coefficients:

$$A_{q^3-6q}, A_{q^3-5q}, \ldots, A_{q^3+3q}.$$

IV. The Dual of a Linear Code and the MacWilliams Identity

The Dual Code of a Linear Code

Definition

1. *For* $\begin{smallmatrix} x=(x_1,\ldots,x_N) \\ y=(y_1,\ldots,y_N) \end{smallmatrix} \in \mathbb{F}_q^N$ *let* $\langle x, y \rangle = \sum_{i=1}^N x_i y_i$.
2. *For a linear code* $C \subseteq \mathbb{F}_q^N$, *the dual code is defined by*

$$C^\perp = \left\{ y \in \mathbb{F}_q^N \mid \langle x, y \rangle = 0, \ \forall x \in C \right\}.$$

Example

Let $C = \{(0, \ldots, 0), (1, \ldots, 1)\} \subset \mathbb{F}_2^n$.
Then $C^\perp = \{y \in \mathbb{F}_2^n \mid \text{wt}(y) \text{ is even}\}$.
We see that

$$W_C(X, Y) = X^n + Y^n,$$

and

$$W_{C^\perp}(X, Y) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} X^{n-2i} Y^{2i} = \frac{(X+Y)^n + (X-Y)^n}{2}.$$

Theorem (MacWilliams)

For a linear code $C \subseteq \mathbb{F}_q^N$

$$W_{C^\perp}(X, Y) = \frac{1}{|C|} W_C\left(X + (q-1)Y, X - Y\right).$$

Example ($C_{2,1}$:Linear Forms on $\mathbb{P}^2$)

$$\begin{aligned} W_{C_{2,1}^\perp}(X, Y) &= \frac{1}{q^3} W_{C_{2,1}}\left(X + (q-1)Y, X - Y\right) \\ &= X^{q^2+q+1} + \frac{(q^3-1)(q^3-q)}{6} X^{q^2+q-2} Y^3 + \dots \end{aligned}$$

Computing Low-Weight Dual Code Coefficients

Example ($C_{2,1}$:Linear Forms on $\mathbb{P}^2$)

$C_{2,1}^{\perp}$ has no codewords of weight 1 or 2. Number of weight 3 codewords:

$$(q-1)(q^2+q+1)\binom{q+1}{3}.$$

This is $(q-1)$ times the number of collinear triples in $\mathbb{P}^2(\mathbb{F}_q)$.
A weight 3 dual codeword with nonzero entries a_i, a_j, a_k satisfies

$$a_i f_1(p_i) + a_j f_1(p_j) + a_k f_1(p_k) = 0$$

for all linear forms f_1.
If $f_1(p_i) = f_1(p_j) = 0$, then $f_1(p_k) = 0$. So $\{p_i, p_j, p_k\}$ must be collinear.

Interpolation Problems:
Dual codewords come from collections of points that fail to impose independent conditions on degree d curves in $\mathbb{P}^2$.

Points that 'Fail to Impose Independent Conditions'

$p_1, \ldots, p_N$ fail to impose independent conditions on degree d hypersurfaces in $\mathbb{P}^n$ if the dimension of the space of hypersurfaces containing them exceeds what it would be for generically chosen points.

Example: Three generic points in $\mathbb{P}^2$ are not contained in any lines, but if the three points are collinear then there is a line containing them.

Theorem (Chasles)

Let $X_1, X_2 \subset \mathbb{P}^2$ be cubic plane curves meeting in nine points $p_1, \ldots, p_9$. If $X \subset \mathbb{P}^2$ is any cubic containing $p_1, \ldots, p_8$, then X contains p_9 as well.

Let $N = \frac{q^4-1}{q-1} = |\mathbb{P}^3(\mathbb{F}_q)|$.

1. Determine $W_{C_{3,3}}(X,Y)$ up to 10 unknown coefficients.
2. Let

$$W_{C_{3,3}^{\perp}}(X,Y) = \sum_{i=0}^{N} B_i X^{n-i} Y^i.$$

By the MacWilliams identity, each B_j gives a linear relation satisfied by the unknown A_i coefficients.

Determine $B_0, B_1, \ldots, B_9$ and conclude with linear algebra.

Theorem

The number of homogeneous cubic polynomials $f_3(w,x,y,z)$ such that $\{f_3 = 0\}$ is a smooth cubic surface with q^2+7q+1 $\mathbb{F}_q$-points, the maximum possible, is

$$\frac{|\operatorname{GL}_4(\mathbb{F}_q)|(q-2)(q-3)(q-5)^2}{51840}.$$

Question

How many of the q^{20} pairs of homogeneous cubic polynomials $f_3(x, y, z), g_3(x, y, z)$ have exactly k common zeros?

- Question about a Second Hamming Weight Enumerator.
- Bézout's Theorem: Two cubic curves that intersect in more than 9 points must share a common component.
- Determine the Second Hamming Weight Enumerator up to 10 unknown coefficients.

Theorem (Entin)

As $q \to \infty$, the probability that a degree e polynomial in x, y, z and a degree d polynomial in x, y, z have exactly k common zeros approaches the *proportion of $\sigma \in S_{d \cdot e}$ with exactly k fixed points.*

Coding theory approach can give exact formulas for low-degree curves.

Theorem (K.-Matei)

The number of pairs of homogeneous cubic polynomials $f_3(x, y, z), g_3(x, y, z)$ *that do not have a common irreducible factor over* $\overline{\mathbb{F}_q}$ *and have exactly* 9 *common zeros in* $\mathbb{P}^2(\mathbb{F}_q)$ *is*

$$\frac{1}{9!}(q-2)(q+1)^2(q-1)^4q^5(q^2+q+1)\cdot$$
$$\left(q^6+2q^5-73q^4+344q^3-838q^2+1754q-2030\right).$$

◦ There are similar (more complicated) polynomial formulas for each number of common zeros between 0 and 9.