Maximal Fermat Varieties

Iwan Duursma

RICAM Workshop
Algebraic curves over finite fields
Linz, Austria, November 11-15, 2013

Let k be a finite field. In how many ways can $0 \in k$ be written as a sum of $r+1$ d-th powers?

(Weil, 1954) Let X/k be the Fermat hypersurface

$$x_0^d + x_1^d + \cdots + x_r^d = 0.$$

For a field k that contains the d-th roots of unity,

$$\#X(k) = \#\mathbb{P}^{r-1}(k) + \sum_{\alpha \in A} j(\alpha).$$

Where

$$j(\alpha) = \frac{1}{q} g(a_0) \cdots g(a_r)$$

$$A = \left\{ (a_0, a_1, \ldots, a_r) \;\middle|\; \begin{array}{l} a_i \in \mathbb{Z}/d\mathbb{Z}, a_i \not\equiv 0 \\ a_0 + a_1 + \cdots + a_r \equiv 0 \end{array} \right\}$$

For a nontrivial additive character

$$\psi : k \longrightarrow \mathbb{C}$$

and for a multiplicative character

$$\chi : k^*/(k^*)^d \longrightarrow \mathbb{C}^*$$

both fixed once and for all, the Gauss sum $g(a)$, for $a \in \mathbb{Z}/d\mathbb{Z}$, is defined as

$$g(a) = \sum_{x \in k} \chi^a(x)\psi(x).$$

Although the Gauss sums may depend on the choice of multiplicative character χ, this choice does not effect the Jacobi sums in the expression for $\#X(k)$.

The Gauss sums have absolute value $\sqrt{q}$.

Thus $M^- \leq \#X(k) \leq M^+$, where

$$M^{\pm} = (q^r - 1)/(q - 1) \pm |A| q^{(r-1)/2}.$$

For the Fermat hypersurface X/k,

$$|A| = (d-1)((d-1)^r - (-1)^r)/d).$$

The right side is the Chern class for a smooth hypersurface of degree d in $\mathbb{P}^r$.

For what values of q, r, d,

$$M^- = \#X(k) \quad \text{or} \quad \#X(k) = M^+ \ ?$$

It follows from the Davenport-Hasse relations for Gauss sums that X/k has zeta function

$$Z_X(T) = Z_{\mathbb{P}^{r-1}}(T)P(T)^{\pm}$$

Where

$$P(T) = \prod_{\alpha \in A} (1 - (-1)^r j(\alpha)T),$$

$$\pm = (-1)^r.$$

Special case:

$$X/k : x_0^3 + x_1^3 + x_2^3 + x_3^3 = 0 \quad (\mu_3 \subset k)$$

$$A = \left\{ (a_0, a_1, \ldots, a_r) \;\middle|\; \begin{array}{l} a_i \in \mathbb{Z}/d\mathbb{Z}, a_i \not\equiv 0 \\ a_0 + a_1 + \cdots + a_r \equiv 0 \end{array} \right\}$$

$$= \{\text{permutations of } (1,1,2,2)\}$$

$$j(\alpha) = \frac{1}{q} g(a_0) \cdots g(a_3) = q$$

$$\#X/k = (q^2 + q + 1) + 6q = M^+$$

Theorem

The Fermat variety $X \subset \mathbb{P}^r$ of degree d and dimension $r-1$ over a field k of q elements is maximal over k if and only if one of the following holds.

1. $d > 3$, q is a square, and $d|\sqrt{q}+1$.

2. $d = 3$, $3|q-1$, and $r-1 = 2$.

3. $d = 2$, $q \equiv 1 \pmod 4$.

4. $d = 2$, $q \equiv 3 \pmod 4$, $r-1$ is even.

X is minimal over k if and only if r is even and there exists a subfield $k' \subset k$ of even index such that X is maximal over k'.

Main idea: Use the inductive structure among Fermat varieties of same degree d but different dimension $r-1$.

A variety X_d^{r-1} of degree $d > 3$ is maximal or minimal only as a special case of (A) or (B).

(A) X_d^{r-1} is maximal over k, for all r.

(B) $\begin{cases} X_d^{r-1} \text{ is minimal over } k, \text{ for even } r, \text{ and} \\ X_d^{r-1} \text{ is maximal over } k, \text{ for odd } r. \end{cases}$

Proposition

For $d > 2$ and r even,

X_d^{r-1} is maximal over k if and only if (A).

X_d^{r-1} is minimal over k if and only if (B).

For $d > 3$ and r odd,

X_d^{r-1} is maximal over k if and only if (A) or (B).

Because of the inductive structure, the proofs reduce to the cases of curves and surfaces.

Lemma 1.

Let $d > 2$. The Fermat curve X_d^1 is maximal (resp. minimal) if and only if, for some d-th root of unity ζ, the gauss sums $g(a) = \zeta^a\sqrt{q}$ (resp. $-\sqrt{q}$).

Lemma 2.

Let $d > 3$. The Fermat surface X_d^2 is maximal if and only if, for some d-th root of unity ζ and for $r = \pm\sqrt{q}$, the gauss sums $g(a) = \zeta^a r$.

Gauss sums with these properties were characterized by Evans (1981) and by (Baumert-Mills-Ward, 1982). That completes the proof of the theorem.

A graph theoretic approach to counting solutions on diagonal hypersurfaces.

Let $D = \{x^d : x \in k^*\}$ be the subgroup of index d in k^*. Define the Cayley graph for $D \subset k$ as the directed graph with vertex set k and $(u, v) \in k \times k$ an edge if and only if $v - u \in D$. The graph becomes an undirected graph when $D = -D$.

Let A be the adjacency matrix of the graph. The number of affine solutions to the Fermat equations corresponds, up to a factor d^{r+1}, to the number N of paths of length $r + 1$ in the Cayley graph.

$$N = \frac{1}{|k|}\text{Trace}((I + dA)^{r+1}).$$

X/k of degree d is maximal in any dimension r if and only if the matrix $I + dA$ has nontrivial eigenvalues $(d-1)\sqrt{q}$ and $-\sqrt{q}$ if and only if the Cayley graph of $D \subset k^*$ is a Pseudo-Latin graph $L_\sigma(\sqrt{q})$ (a special type of strongly regular graph).

X/k of degree d is maxima in even dimension and minimal in odd dimension if and only if the Cayley graph of $D \subset k^*$ is a Negative Latin graph $L_\sigma(\sqrt{q})$.

It appears that the combination of (1) graph-theoretic approach, (2) interpretation of the Cayley graph as counting points on Fermat varieties, and (3) relating the point counting on Fermat varieties to properties of Gauss sums gives an independent proof of the results by (Evans, 1981) and (Baumert-Mills-Ward, 1982).

Ueber eine Verallgemeinerung der Kreistheilung (Stickelberger, 1890)

—

On Fermat varieties (Katsura-Shioda, 1979)

On the Jacobian variety of the Fermat curve (Yui, 1980)

Pure Gauss sums (Evans, 1981)

Uniform cyclotomy (Baumert-Mills-Ward, 1982)

Two-weight irreducible cyclic codes / Characters and cyclotomic fields in finite geometry (Schmidt, 2002)

Maximal Fermat curves (D, 1989)

Certain maximal curves and Cartier operators (Garcia-Tafazolian, 2008) / Maximal and minimal Fermat curves (Tafazolian, 2010)

Smooth models for the Suzuki and Ree curves
Abdulla Eid and Iwan Duursma
arXiv upload available today November 11, 2013

1 - Function fields

2 - Automorphism groups and Polarity

3- Deligne-Lusztig varieties

k a finite field of size q, $q = q_0^2$.

The Hermitian curve has function field $L = k(x, y)$ over $F = k(x)$ with

$$y^{q_0} + y = x^{q_0+1}.$$

It is the ray class field extension of F of conductor $q_0 + 2$ in which all finitie $k-$rational points of F split completely.

In projective 2-space,

$$P(1 : x : y) \in \ell(y^{q_0} : x^{q_0} : 1).$$

And

$$\ell(x^{q_0} : y^{q_0} : 1) \in L(1 : x^q : y^q)$$

k a finite field of size q, $2q = (2q_0)^2$.

The Suzuki curve has function field $L = k(x, y)$ over $F = k(x)$ with

$$L/F \ : \ y^q - y = x^{q_0}(x^q - x).$$

$F \subset L$ contains a subextension $F \subset K \subset L$ defined by

$$\mathrm{Y}^2 - \mathrm{Y} = x^{q_0}(x^q - x)$$

Or, equivalently, by

$$K/F \ : \ v^2 - v = x^{2q_0+1} - x^{q_0+1}$$

This is an Artin-Schreier extension with conductor $2q_0 + 2$ in which all finite $k-$rational points of F split completely.

The extension L/F is the compositum of the family $\{v^2 - v = (ax)^{2q_0+1} - (ax)^{q_0+1} \ : \ a \in k^*\}$. It is the ray class field extension of F of conductor $2q_0+2$ in which all finitie $k-$rational points of F split completely.

k a finite field of size q, $3q = (3q_0)^2$.

The Ree curve has function field $L = k(x, y_1, y_2)$ over $F = k(x)$ with $L = L_1 L_2$,

$$\begin{aligned} L_1/F &: y_1^q - y_1 = x^{q0}(x^q - x). \\ L_2/F &: y_2^q - y_2 = x^{2q0}(x^q - x). \end{aligned}$$

$F \subset L_i$ contains a subextension $F \subset K_i \subset L_i$ defined by

$$\begin{aligned} K_1/F &: v_1^3 - v_1 = x^{3q_0+1} - x^{q_0+1}. \\ K_2/F &: v_2^3 - v_2 = x^{3q_0+2} - x^{2q_0+1}. \end{aligned}$$

These are Artin-Schreier extensions with conductor $3q_0{+}2, 3q_0{+}3$ in which all finite $k-$rational points of F split completely.

The extensions L_i/F are the compositum of the family of twists of K_i/F.

The compositum $L = L_1 L_2$ is the ray class field extension of F of conductor $3q_0{+}3$ in which all finitie $k-$rational points of F split completely.

The definition of the curves as compositum of Artin-Schreier extensions *immediately* reveales their genus, number of rational points, their zeta function, part of (the p-part) of their automorphism group, but *not* the full automorphism groups, which are *large*.

To see the full automorphism group we follow Chevalley (1955), Suzuki (1960), Ree (1961), Tits (1960/61). (This approach explains the stabilizer of the set of rational points which agrees with the full automprhism group of the curve)

The automorphism groups are of type $2A2$, $2B2$, $2G2$, i.e. are twists of the algebraic groups of type $A2, B2, G2$.

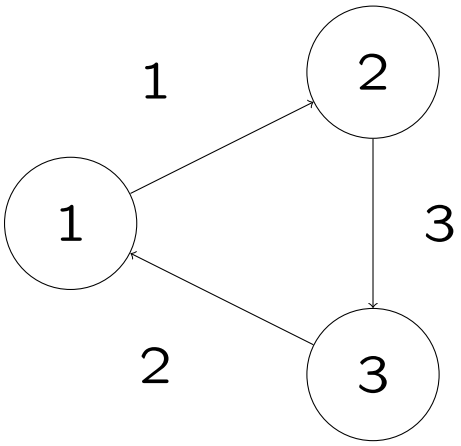
In all cases the twist can be explained through a polarity in projective 3−space.

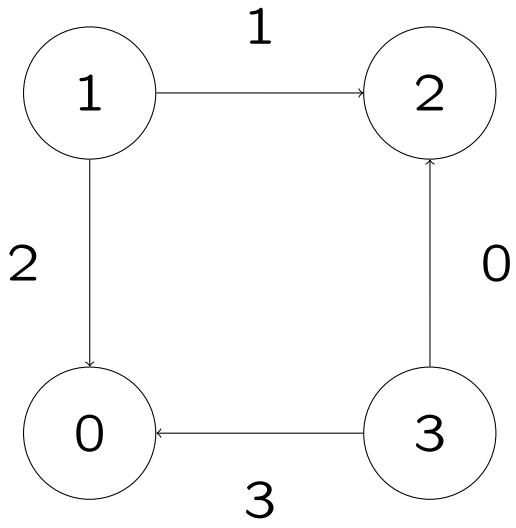
Given a point-hyperplane incidence $P \in H$ in projective 3−space we seek to describe the pencil of lines $\{\ell : P \in \ell, \ell \in H\}$.

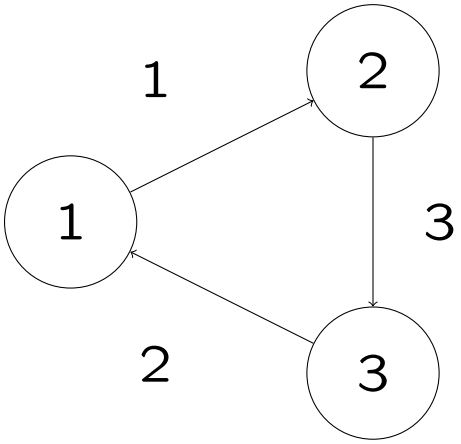
That is we seek to describe the completions $P \subset \ell \subset H \subset \mathbb{P}^3$ of the partial flag $P \subset H \subset \mathbb{P}^3$.

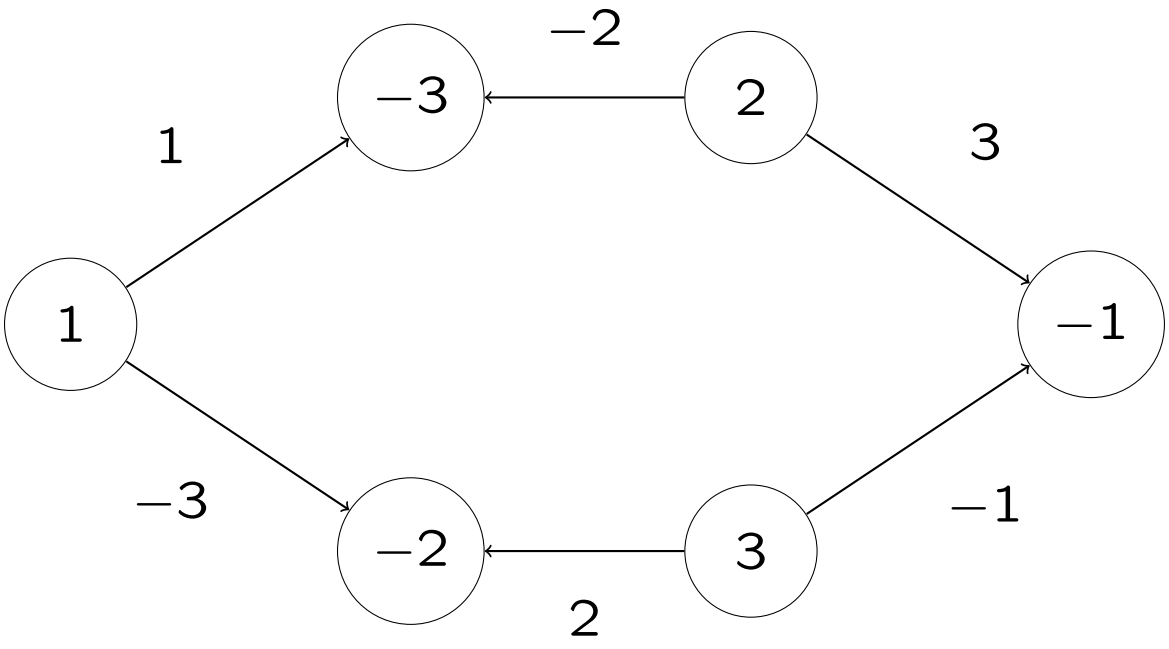
Fix $P = (x_0 : x_1 : x_2 : x_3)$ and write $L = \{\ell : P \in \ell, \ell \in H\}$. Then

(H)	$H = (1 : 0 : 0 : 0)$	$L = P.$
(S)	$H = (x_3 : x_2 : x_1 : x_0)$	$L = P^{(2)}.$
(R)	$H = (x_0 : x_{-1} : x_{-2} : x_{-3})$	$L = (P^{(3)}, H^{(3)}).$


1
2
1
3
2
3


1
1
2
2
0
0
3
3


1
2
1
3
2
3


−2
−3
2
1
3
1
−1
−3
−2
3
−1
2