Permutation polynomials over finite fields and their applications to Cryptography

Francesco Pappalardi

Beirut, March 9th, 2002

Finite Fields

- Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \dots, p-1\}$ (field if p prime);
- Given $f \in \mathbb{F}_p[x]$ irreducible $(m = \partial(f))$

$$\boxed{\mathbb{F}_p[x]/(f) = \{a_0 + a_1 t + \cdots + a_{m-1} t^{m-1} \mid a_i \in \mathbb{F}_p,\}}$$

- $\mathbb{F}_p[x]/(f)$ is a field ($g_1 \star g_2 \in \mathbb{F}_p[x]/(f)$ is $g_1 g_2 \bmod f$)
- $\mathbb{F}_p[x]/(f)$ does not depend on f
  (i.e. if $h \in \mathbb{F}_p[x]$ irreducible, $\partial f = \partial h \Longrightarrow \mathbb{F}_p[x]/(f) \cong \mathbb{F}_p[x]/(h)$)

$$\boxed{\mathbb{F}_{p^m} = \mathbb{F}_p[x]/(f)}$$

  any choice of f with $m = \partial f$ is the same

- $|\mathbb{F}_{p^m}| = p^m$

Producing $\mathbb{F}_q$

Set $q = p^m$

- Produce $\mathbb{F}_q \iff$ find $f \in I_m(q)$;
  $(I_m(q) = \{f \in \mathbb{F}_p[x], f \text{ irreducible}, \partial f = m\})$;
- $\sum_{d|m} dI_d(q) = q^m$;
- $I_m(q) = \frac{q^m - q}{m}$ (if m is prime) $I_m(q) \sim \frac{q^m}{m}$;
- If $m \nmid p-1$ & m is prime $\Longrightarrow \frac{x^m-1}{x-1} \in I_{m-1}(q)$;
- Some fields: $\mathbb{F}_{2^{503}} = \mathbb{F}_2[x]/(x^{503} + x^3 + 1), \mathbb{F}_{5323^{20}} = \mathbb{F}_{5323}[x]/(f)$

  $f = x^{20} + 1451x^{18} + 5202x^{17} + 752x^{16} + 3778x^{15} + 4598x^{14} + 2563x^{13} + 5275x^{12} + 4260x^{11} + 862x^{10} + 4659x^9 + 3484x^8 + 1510x^7 + 4556x^6 + 2317x^5 + 2171x^4 + 3100x^3 + 4100x^2 + 682x + 5110$
- Good to find f sparse.

Interpolation on $\mathbb{F}_q$

Given $h : \mathbb{F}_q \to \mathbb{F}_q$ a function.

h can always be interpolated with a polynomial in $\mathbb{F}_q[x]$!

- LAGRANGE INTERPOLATION.

$$f_h(x) = \sum_{c \in \mathbb{F}_q} h(c) \prod_{\substack{d \in \mathbb{F}_q \\ d \neq c}} \frac{x-d}{c-d} \in \mathbb{F}_q[x]$$

- FINITE FIELDS INTERPOLATION.

$$f_h(x) = \sum_{c \in \mathbb{F}_q} h(c) \left(1 - (x-c)^{q-1}\right) \in \mathbb{F}_q[x]$$

$\mathbb{F}_q^*$ is a (ciclic) group under multiplication

$$\Longrightarrow d^{q-1} = \begin{cases} 1 & d \neq 0 \\ 0 & d = 0. \end{cases}$$

More on interpolation in $\mathbb{F}_q$

- If $f_1, f_2 \in \mathbb{F}_q[x]$ with $f_1(c) = f_2(c) \forall c \in \mathbb{F}_q$,
$\boxed{\Longrightarrow x^q - x \mid f_1(x) - f_2(x)}$;
- The interpolant polynomial is unique mod $x^q - x$
$\boxed{\Longrightarrow \text{unique with degree} \leq q-1}$;
- If $c_h = \#\{c \in \mathbb{F}_q \mid h(c) \neq c\}$,
$\boxed{q - c_h \leq \partial f_h \leq q - 2;}$
- **Problem.** *Find functions with sparse interpolation polynomial.*

Permutation polynomials

$$\mathcal{S}(\mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma(1:1)\}$$

permutations of $\mathbb{F}_q$.

- $f \in \mathbb{F}_q[x]$ is called permutation polynomial (PP) if

  "*f (as a funtion) is a permutation*";

  (i.e. $\exists \sigma \in \mathcal{S}(\mathbb{F}_q), \sigma(c) = f(c)\ \forall c \in \mathbb{F}_q$)

- If $f_\sigma(x) = \sum_{c \in \mathbb{F}_q} \sigma(c)\left(1 - (x-c)^{q-1}\right) \in \mathbb{F}_q[x] \Longrightarrow$

  $$\boxed{f \in \mathbb{F}_q[x] \text{ is PP} \iff \exists \sigma \in \mathcal{S}(\mathbb{F}_q), f \equiv f_\sigma \bmod x^q - x.}$$

- **Examples:**
  - $ax + b, \qquad a, b \in \mathbb{F}_q, a \neq 0;$
  - $x^k, \qquad (k, q-1) = 1;$

More examples of PP

- **Composition.** $f \circ g$ is PP if f, g are PP;
- $x^{(q+m-1)/m} + ax$ is a PP if $m|q-1$;
- **Linearized Polynomials.** Let $q = p^m$,

$$\boxed{L(x) = \sum_{s=0}^{r-1} \alpha_s x^{q^s}} \qquad (\alpha_s \in \mathbb{F}_{p^m})$$

  - $L(c_1 + c_2) = L(c_1) + L(c_2)$;
  - $L \in \mathrm{GL}_m(\mathbb{F}_p) \subset \mathcal{S}(\mathbb{F}_{p^m}) \iff \det(\alpha_{i-j}^{q^j}) \neq 0.$
    $\iff L(x) = 0$ has 1 solution.

One more example of PP

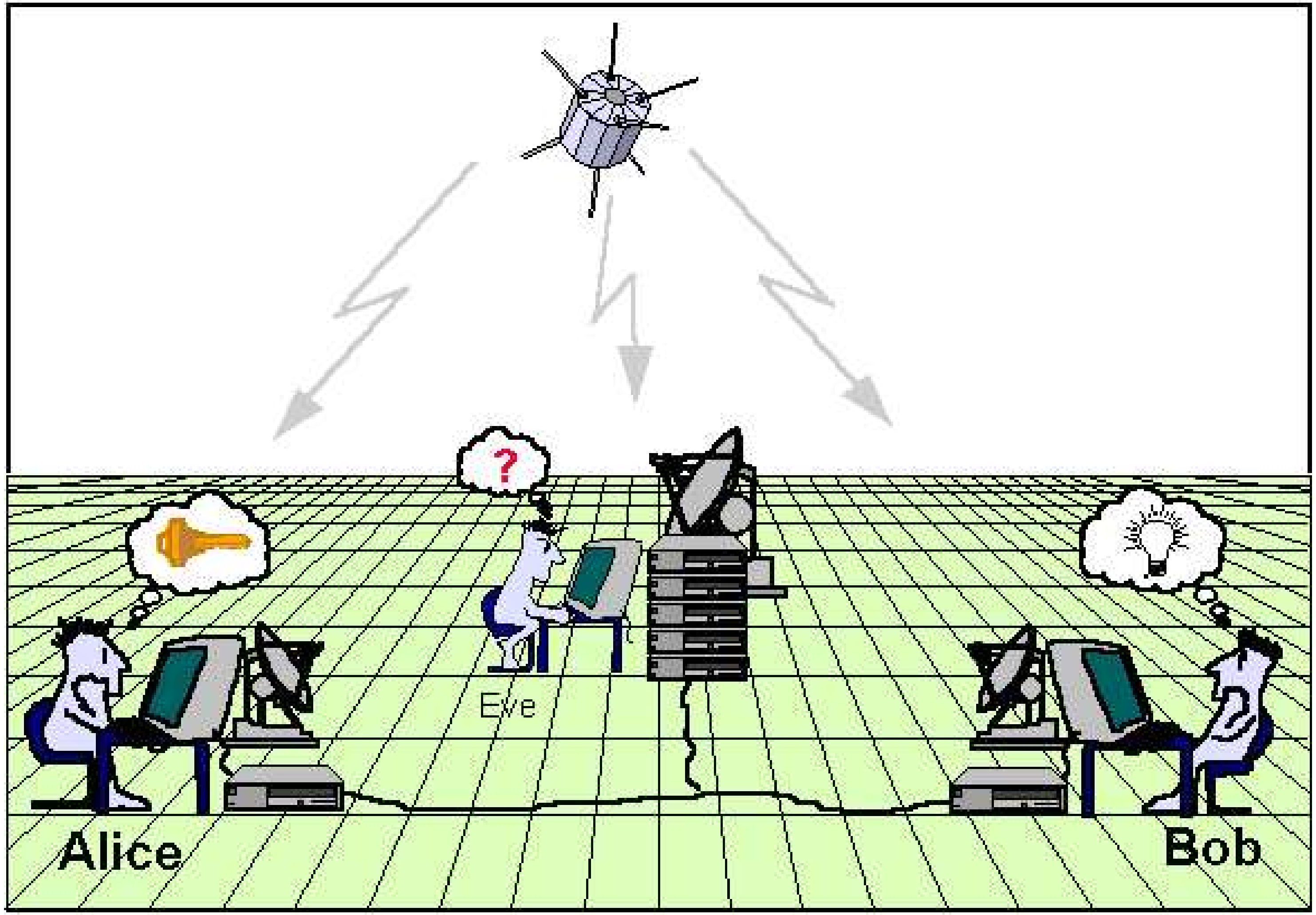
✎ DICKSON POLYNOMIALS. If $a \in \mathbb{F}_q$, $k \in \mathbb{N}$

$$\boxed{D_k(x,a) = \sum_{j=0}^{[k/2]} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}}$$

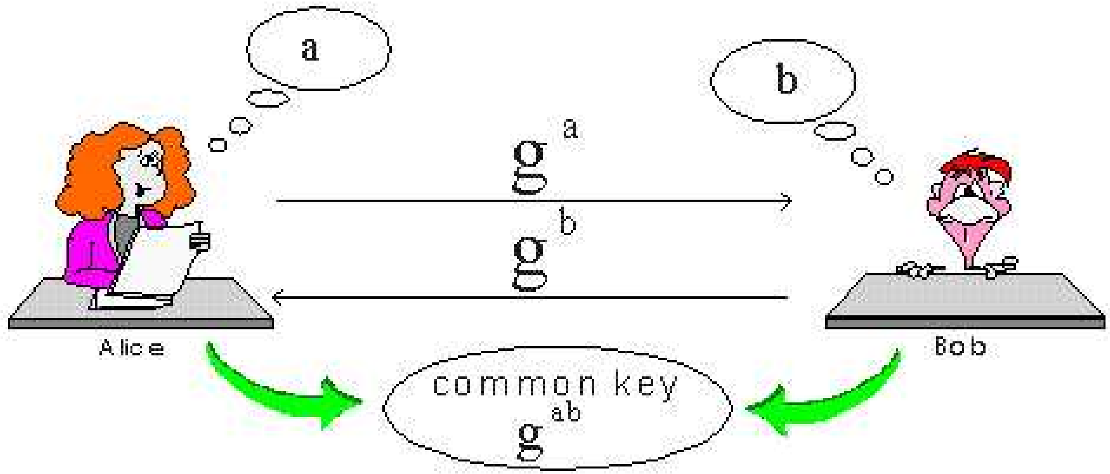
- if $a \neq 0$, $D_k(x,a)$ is a PP $\iff$ $(k, q^2-1) = 1$;
- $D_k(x,0) = x^k$ is a PP $\iff$ $(k, q-1) = 1$.
- **Note:** if $(mn, q^2-1) = 1$,

$$\boxed{D_m(D_n(x,\pm 1), \pm 1) = D_{mn}(x, \pm 1)}.$$

Diffie–Hellmann key exchange 1/2



Diffie–Hellmann key exchange 2/2



1. **Alice** and **Bob** agree on a finite field $\mathbb{F}_q$, and a generator $g \in \mathbb{F}_q$;
2. **Alice** picks a secret $a \in [0, q-1]$, **Bob** picks a secret $b \in [0, q-1]$;
3. They compute and publish g^a (**Alice**) and g^b (**Bob**);
4. The common secret key is g^{ab}.

Dickson analogue of DH Key–exchange

① **Alice** and **Bob** agree on a finite field $\mathbb{F}_q$, and a $\gamma \in \mathbb{F}_q$ (γ *not necessarily a generator*);

② **Alice** picks a secret $a \in [0, q^2 - 1]$, **Bob** picks a secret $b \in [0, q^2 - 1]$;

③ They compute and publish $D_a(\gamma, 1)$ (**Alice**) and $D_b(\gamma, 1)$ (**Bob**);

④ The common secret key is

$$\boxed{D_{ab}(\gamma, 1) = D_a(D_b(\gamma, 1, 1)) = D_b(D_a(\gamma, 1, 1))}.$$

NOTE. There is a fast algorithm to compute the value of a Dickson polynomial at an element of $\mathbb{F}_q$.

Problem. Find new classes of PP.

The problem of enumeration of PP by degree

$$\boxed{N_d(q) = \{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) = d\}}$$

Problem. *Compute* $N_d(q)$

- $\displaystyle\sum_{d \leq q-2} N_d(q) = q!$ $\quad(\partial f_\sigma \leq q-2)$;
- $N_1(q) = q(q-1)$;
- $N_d(q) = 0$ if $d | q-1$ $\quad$ (Hermite criterion);
- $N_d(q)$ is known for $d \leq 6$;
- *Almost all permutation polynomials have degree* $q-2$.

(S. Konyagin, FP) $M_q = \{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial f_\sigma < q-2\}$

$$|\#M_q - (q-1)!| \leq \sqrt{2e/\pi}\, q^{q/2}$$

Other ways of counting

If $\sigma \in \mathcal{S}(\mathbb{F}_q)$, $\boxed{c_\sigma = \#\{a \in \mathbb{F}_q \mid \sigma(a) \neq a\}}$

$$\sigma \neq id \Longrightarrow q - c_\sigma \leq \partial f_\sigma \leq q - 2$$

(since $f_\sigma(x) - x$ has at least $q - c_\sigma$ roots)

Consequences.

- 2–cycles have degree $q-2$;
- 3–cycles have degree $q-2$ or $q-3$;
- k–cycles have degree in $[q-k, q-2]$.

(*Wells*) $$\boxed{\#\{\sigma \in 3\text{–cyle},\ \partial(f_\sigma) = q-3\} = \begin{cases} \frac{2}{3}q(q-1) & q \equiv 1 \bmod 3 \\ 0 & q \equiv 0 \bmod 3 \\ \frac{1}{3}q(q-1) & q \equiv 0 \bmod 3 \end{cases}}$$

More enumeration functions

- σ_1, σ_2 conjugated $\Longrightarrow \; c_{\sigma_1} = c_{\sigma_2}$;
- $\mathcal{C}$ *conjugation class of permutations*;
- $c_{\mathcal{C}} = \#\{$ elements $\in \mathbb{F}_q$ moved by any $\sigma \in \mathcal{C}\}$;
  (i.e. $c_{\mathcal{C}} = c_\sigma$ for any $\sigma \in \mathcal{C} \qquad q - c_{\mathcal{C}} \leq f_\sigma$)
- $\mathcal{C} = [k]$=k–cycles $\Longrightarrow \quad c_{[k]} = k$.
- Natural enumeration functions:
  - ✗ $m_{\mathcal{C}}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma = q - c_{\mathcal{C}}\}$ (*minimal degree*);
  - ✗ $M_{\mathcal{C}}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma < q - 2\}$ (*non-maximal degree*).

Permutation Classes with non maximal degree

Let $\mathcal{C} = (m_1, \dots, m_t)$ be the class of permutations with m_1 1-cycles, ..., m_t t-cycles. The number $c_\mathcal{C}$ of elements in $\mathbb{F}_q$ moved by any element of $\mathcal{C}$ is

$$c_\mathcal{C} = 2m_2 + 3m_3 + \cdots + tm_t.$$

$$\boxed{M_\mathcal{C}(q) = \#\{\sigma \in \mathcal{C}, \partial f_\sigma < q-2\}}$$

Theorem 1 (C. Malvenuto, FP). $\exists N = N_\mathcal{C} \in \mathbb{N}$, $f_1, \cdots, f_N \in \mathbb{Z}[x]$, f_i monic, $\partial f_i = c_\mathcal{C} - 3$ such that if $q \equiv a \bmod N$, then

$$M_\mathcal{C}(q) = \frac{q(q-1)}{m_2! 2^{m_2} \cdots m_t! t^{m_t}} f_a(q).$$

Consequences of Theorem 1

- $\dfrac{M_{\mathcal{C}}(q)}{\#\mathcal{C}} = \dfrac{1}{q} + O\left(\dfrac{1}{q^2}\right);$
- If $\mathcal{C}$ is fixed,

$$\mathrm{Prob}(\partial f_\sigma < q-2 \mid \sigma \in \mathcal{C}) \sim \frac{1}{q};$$

- If $q = 2^r$, $\mathcal{C}_r$ is the conjugation class of r transposition,

$$M_{\mathcal{C}_r}(q) = \frac{q!}{r!2^r(q-2r+1)!} - \frac{q-2(r-1)(2r-1)}{2r} M_{\mathcal{C}_{r-1}}(q);$$

- One can compute $M_{\mathcal{C}}(q)$ for $c_{\mathcal{C}} \leq 6$.

Table 1. $\#c_{\mathcal{C}} \leq 6$, (q odd)

- $$M_{[4]}(q) = \frac{1}{4}q(q-1)\left(q-5-2\eta(-1)-4\eta(-3)\right)$$

- $$M_{[2\ 2]}(q) = \frac{1}{8}q(q-1)(q-4)\left\{1+\eta(-1)\right\}$$

- $$\begin{aligned} M_{[5]}(q) = &\ \frac{1}{5}q(q-1)\left(q^2-(9-\eta(5)-5\eta(-1)+5\eta(-9))\,q+\right.\\ &\left.+26+5\eta(-7)+15\eta(-3)+15\eta(-1)\right) \end{aligned}$$

- $$\begin{aligned} M_{[2\ 3]}(q) = &\ \frac{1}{6}q(q-1)\left(q^2-(9+\eta(-3)+3\eta(-1))q+\right.\\ &\left.+(24+6\eta(-3)+18\eta(-1)+6\eta(-7))\right)+\\ &\eta(-1)(1-\eta(9))q(q-5). \end{aligned}$$

Table 2. $\#c_{\mathcal{C}} \leq 6$, (q even)

- $M_{[4]}(2^n) = \frac{1}{4}2^n(2^n-1)(2^n-4)(1+(-1)^n)$
- $M_{[2\ 2]}(2^n) = \frac{1}{8}2^n(2^n-1)(2^n-2)$
- $M_{[5]}(2^n) = \frac{1}{5}2^n(2^n-1)(2^n-3-(-1)^n)(2^n-6-3(-1)^n)$
- $M_{[2\ 3]}(2^n) = \frac{1}{6}2^n(2^n-1)(2^n-3-(-1)^n)(2^n-6)$.

Table 3. $\#c_{\mathcal{C}} = 6$, (q odd, $3 \nmid q$)

$$
\begin{aligned}
M_{[6]}(q) &= \tfrac{q(q-1)}{6}\{q^3 - 14\,q^2 + [68 - 6\,\eta(5) - 6\,\eta(50)]q - \\
&\quad [154 + 66\,\eta(-3) + 93\,\eta(-1) + 12\,\eta(-2) + 54\,\eta(-7)]\} \\
M_{[4\ 2]}(q) &= \tfrac{q(q-1)}{8}(q^3 - [14 - \eta(2)]q^2 + \\
&\quad [71 + 12\,\eta(-1) + \eta(-2) + 4\,\eta(-3) - 8\,\eta(50)]q \\
&\quad -[148 + 100\,\eta(-1) + 24\,\eta(-2) + 44\,\eta(-3) + 40\,\eta(-7)]) \\
M_{[3\ 3]}(q) &= \tfrac{q(q-1)}{18}(q^3 - 13\,q^2 + [62 + 9\,\eta(-1) + 4\,\eta(-3)]q \\
&\quad -[150 + 99\,\eta(-1) + 42\,\eta(-3) + 72\,\eta(-7)]) \\
M_{[2\ 2\ 2]}(q) &= \tfrac{q(q-1)}{48}(q^3 - [14 + 3\,\eta(-1)]q^2 + [70 + 36\,\eta(-1) + 6\,\eta(-2)]q \\
&\quad -[136 + 120\,\eta(-1) + 48\,\eta(-2) + 8\,\eta(-3)])
\end{aligned}
$$

Table 4. $\#c_{\mathcal{C}} = 6$

$$M_{[6]}(3^n) = \frac{3^n(3^n-1)}{6}\{3^{3n} - [14+2(-1)^n]3^{2n} + [71+39(-1)^n]3^n - [162+147(-1)^n]\}$$

$$M_{[4\ 2]}(3^n) = \frac{3^n(3^n-1)}{8}\{3^{3n} - [14+3\,(-1)^n]3^{2n} + [72+40\,(-1)^n]3^n - [164+140\,(-1)^n]\}$$

$$M_{[3\ 3]}(3^n) = \frac{3^n(3^n-1)}{18}\{(1+(-1)^n)\,3^{3\,n} - [14+15\ (-1)^n]3^{2\,n} + [71+81\ (-1)^n]3^n - [150+171\ (-1)^n]\}$$

$$M_{[2\ 2\ 2]}(3^n) = \frac{3^n(3^n-1)}{48}\{3^{3n} - [14+3(-1)^n]3^{2n} + [76+36(-1)^n]3^n - +[168+120(-1)^n]\}$$

Table 5. $\#c_{\mathcal{C}} = 6)$

$$M_{[6]}(2^n) = \frac{2^n(2^n-1)}{6} \{(2^n - 3 - (-1)^n)(2^{2n} - (11 - (-1)^n)2^n + (41 + 7(-1)^n))\}$$

$$M_{[4\ 2]}(2^n) = \frac{2^n(2^n-1)}{8} \{(2^n - 3 - (-1)^n)(2^{2n} - 11 \cdot 2^n + 37 + (-1)^n)\}$$

$$M_{[3\ 3]}(2^n) = \frac{2^n(2^n-1)}{18} \{(2^n - 3 - (-1)^n)(2^{2n} - (10 - (-1)^n)2^n + 45 - 3(-1)^n))\}$$

$$M_{[2\ 2\ 2]}(2^n) = \frac{2^n(2^n-1)}{48} \{(2^n - 2)(2^n - 4)(2^n - 8)\}.$$

k–cycles with minimal degree

$$\boxed{m_{[k]}(q) = \#\{\sigma\ k\text{–cycle}, \partial f_\sigma = q-k\}}$$

THEOREM 2 (C. Malvenuto, FP).

- If $q \equiv 1 \bmod k \quad \Longrightarrow$

$$m_{[k]}(q) \geq \frac{\varphi(k)}{k} q(q-1).$$

- If $q = p^f$, $p \geq 2 \cdot 3^{[k/3]-1} \quad \Longrightarrow$

$$m_{[k]}(q) \leq \frac{(k-1)!}{k} q(q-1).$$

Sketch of the Proof of Theorem 2. (1/3)

STEP 1. Translate the problem into one on counting points of an algebraic varieties;

$$m_k(q) = \frac{q(q-1)}{k} n_k(q)$$

where $n_k(q) = \{\sigma \in [k] \mid \partial f_\sigma = q-k, \sigma(0) = 1\}$.
Need to show $|n_k(q)| \leq (k-1)!$. Now

$$f_\sigma(x) = \sum_{c \in \mathbb{F}_q} \sigma(c)\left(1 - (x-c)^{q-1}\right) = A_1 x^{q-2} + A_2 x^{q-3} + \cdots + A_{q-1}.$$

with $A_j = \sum_{c \in \mathbb{F}_q} \sigma(c) c^j = \sum_{c \in \mathbb{F}_q} \sigma(c)\left(c^j - c^{j-1}\right) = \sum_{\substack{c \in \mathbb{F}_q \\ \sigma(c) \neq c}} (\sigma(c) - c) c^j.$

Sketch of the Proof of Theorem 2. (2/3)

If $\sigma = (0,\ 1,\ x_1,\ x_2,\ \ldots,\ x_{k-2}) \in \mathcal{S}(\mathbb{F}_q)$,

$$A_j(\sigma) = (1 - x_1) + (x_1 - x_2)x_1^j + \cdots (x_{k-2} - x_{k-2})x_{k-3}^j + x_{k-2}^{j+1}.$$

Def. (Affine k–th Silvia set)

$$\mathcal{A}_k : \left\{ \begin{array}{rcl} (1 - x_1) + x_1(x_1 - x_2) + \cdots + x_{k-3}(x_{k-3} - x_{k-2}) + x_{k-2}^2 & = & 0 \\ (1 - x_1) + x_1^2(x_1 - x_2) + \cdots + x_{k-3}^2(x_{k-3} - x_{k-2}) + x_{k-2}^3 & = & 0 \\ & \vdots & \\ (1 - x_1) + x_1^{k-2}(x_1 - x_2) + \cdots + x_{k-3}^{k-2}(x_{k-3} - x_{k-2}) + x_{k-2}^{k-1} & = & 0 \end{array} \right.$$

$$n_k(q) = \#\{\underline{x} = (x_1, \ldots, x_{k-2}) \in \mathbb{F}_q^{k-2} \mid \underline{x} \in \mathcal{A}_k(\mathbb{F}_q), x_i \neq x_j\} \leq \#\mathcal{A}_k(\mathbb{F}_q)$$

$$\boxed{\dim_{\overline{\mathbb{F}}_q} \mathcal{A}_k = 0 \quad \overset{\text{Bezout Thm.}}{\Longrightarrow} \quad \#\mathcal{A}(\mathbb{F}_q) \leq (k-1)!}$$

Sketch of the Proof of Theorem 2. (3/3)

Step 2.

Theorem. If $\mathbf{K}$ is an algebrically closed field,

$$\mathrm{char}(\mathbf{K}) = \begin{cases} 0 & \text{or} \\ > 2 \cdot 3^{[k/3]-1}. & \end{cases}$$

Then

$$\boxed{\dim_{\mathbf{K}} \mathcal{A}_k = 0.}$$

NOTE.

- Proof is based on finding projective hyperplanes disjoint from $\mathcal{A}_k$;
- There are examples of small values of q with $\dim_{\mathbf{K}} \mathcal{A}_k > 0$;

Numerical Examples (4–cycles)

$$m_{[4]}(\mathbb{F}_q) = \frac{1}{4}q(q-1)\cdot\begin{cases} 6 & \text{if } q \equiv 1 \pmod{20} \\ 4 & \text{if } q \equiv 11 \pmod{20} \\ 2 & \text{if } q \equiv 9, 13, 17 \pmod{20} \\ 0 & \text{if } q \equiv 3, 7, 19 \pmod{20}, \end{cases}$$

$$m_{[4]}(\mathbb{F}_{5^n}) = \frac{1}{2}5^n(5^n-1), \quad m_{[4]}(\mathbb{F}_{2^n}) = \begin{cases} 2^n(2^n-1) & \text{if } 4|n \\ 0 & \text{otherwise.} \end{cases}$$

Numerical Examples (5–cycles)

$$\text{If } q \notin \{2, 13, 61, 3719, 3100067\} \Rightarrow m_{[5]}(\mathbb{F}_q) = \frac{q(q-1)}{5}(r_q + t_q + u_q),$$

$$t_q = \begin{cases} 4 & \text{if } q \equiv 1 \pmod 5 \\ 1 & \text{if } q \equiv 0 \pmod 5 \\ 0 & \text{otherwise,} \end{cases} \quad u_q = \begin{cases} -1 & \text{if } p = 11, 41 \\ 0 & \text{otherwise,} \end{cases} \quad r_q = \#\{ \begin{matrix} \mathbb{F}_q - \text{roots} \\ \text{of } g_2 \end{matrix} \}$$

$$\begin{aligned} g_2(x) = \ & 2\,x^{20} - 29\,x^{19} + 229\,x^{18} - 1249\,x^{17} + 5187\,x^{16} - 17222\,x^{15} + \\ & 47040\,x^{14} - 107505\,x^{13} + 207622\,x^{12} - 340496\,x^{11} + 474638\,x^{10} - \\ & 560999\,x^{9} + 559052\,x^{8} - 465487\,x^{7} + 319628\,x^{6} - 177653\,x^{5} + \\ & 77807\,x^{4} - 25797\,x^{3} + 6074\,x^{2} - 904\,x + 64. \end{aligned}$$

$$\boxed{g_2(\alpha) = 0, \sigma_\alpha = (0, 1, \alpha, y(\alpha), z(\alpha)) \;\Rightarrow\; \partial f_{\sigma_\alpha} = q - 5 \text{ (minimal)}}$$

$$\begin{aligned}
y(x) = {} & \frac{1}{(2)^3(13)(61)(3719)(3100067)} (6245340990732510 - 7427524702034847 7\,x \\
& +4258973674796274 11\,x^2 - 1556772755104088477\,x^3 + 4068122356423765520\,x^4 \\
& -8092377944341897339\,x^5 + 12739155747072503154\,x^6 - 16281608694400072277\,x^7 + \\
& 17191467892889878476\,x^8 - 15176855331347725064\,x^9 + 11289210111615920188\,x^{10} \\
& -7103742513094855073\,x^{11} + 3782081407301444460\,x^{12} - 1696979431552752820\,x^{13} \\
& +635807089991226023\,x^{14} - 195705738631474759\,x^{15} + 48121368022605621\,x^{16} \\
& -9009616966592957\,x^{17} + 1165803130533438\,x^{18} - 82558295396232\,x^{19}
\end{aligned}$$

$$\begin{aligned}
z(x) = {} & \frac{1}{(2)^3(13)(61)(3719)(3100067)} \quad -292290150269490\,x^{19} + 3950333490943181\,x^{18} \\
& -29484664428617801\,x^{17} + 152268243151302965\,x^{16} - 599002775464475543\,x^{15} \\
& +1880438345917167218\,x^{14} - 4841135989461751552\,x^{13} + 10378374551469856881\,x^{12} \\
& -18679878403151115130\,x^{11} + 28303942873286020848\,x^{10} - 36041151267474587782\,x^9 \\
& +38336702176933085823\,x^8 - 33711958096174593304\,x^7 + 24129466512539278343\,x^6 \\
& -13742359416000756136\,x^5 + 6020424561116746133\,x^4 - 1925677501494324283\,x^3 \\
& +413273185040891961\,x^2 - 51203861193252214\,x + 2593061963570136)
\end{aligned}$$

Numerical Examples (6–cycles)

$$\text{If } p \gg 1 \quad \Rightarrow \quad m_{[6]}(\mathbb{F}_p) = \frac{p(p-1)}{6}(s_1 + s_2 + s_3 + s_4) \quad \text{where}$$

$$s_i = \# \left\{ \begin{array}{c} \mathbb{F}_q - \text{roots} \\ \text{of } f_i \end{array} \right\},$$

$$f_1(x) = x^2 - 3\,x + 3;$$
$$f_2(x) = x^4 - 3\,x^3 + 9\,x^2 - 9\,x + 3;$$
$$f_3(x) = x^6 - 4\,x^5 + 12\,x^4 - 22\,x^3 + 25\,x^2 - 14\,x + 3;$$
$$f_4(x) = \textbf{ Devil's Hat}.$$

Galois Structure of the Silvia set

$$\mathrm{Gal}(\mathbb{Q}(f_1)/\mathbb{Q})) \cong \mathbb{Z}/2\mathbb{Z} \text{ (cyclotomic permutations)}$$

$$\mathrm{Gal}(\mathbb{Q}(f_2)/\mathbb{Q})) \cong D_4$$

$$\mathrm{Gal}(\mathbb{Q}(f_3)/\mathbb{Q})) \cong (\mathbb{Z}/3\mathbb{Z})^2 \rtimes S_2$$

$$\mathrm{Gal}(\mathbb{Q}(\textit{Devil's Hat})) \cong ???$$

(exponent probably $= (2)^5(3)^3(5)(7)(11)(13)(17)$)

Later discovered that

$$\mathrm{Gal}(\mathbb{Q}(\textit{Devil's Hat})) \leq (\mathbb{Z}/6\mathbb{Z})^{18} \rtimes S_{18}$$