When is $x^{-1} + L(x)$ a permutation?

Faruk Göloğlu

Claude Shannon Institute, University College Dublin

with Gary McGuire

WCC 2013
Bergen, April 18, 2013

Permutations of finite fields

- A polynomial

$$f(x) = \sum_{i=0}^{q-1} a_i x^i$$

Permutations of finite fields

- A polynomial

$$f(x) = \sum_{i=0}^{q-1} a_i x^i$$

is a PP (permutation polynomial) if it permutes the elements of $\mathbb{F}_q$.

Permutations of finite fields

- A polynomial

$$f(x) = \sum_{i=0}^{q-1} a_i x^i$$

  is a PP (permutation polynomial) if it permutes the elements of $\mathbb{F}_q$.

- Characterisations:

Permutations of finite fields

- A polynomial

$$f(x) = \sum_{i=0}^{q-1} a_i x^i$$

  is a PP (permutation polynomial) if it permutes the elements of $\mathbb{F}_q$.
- Characterisations:
  - Monomials $ax^d + b$

Permutations of finite fields

- A polynomial
$$f(x)=\sum_{i=0}^{q-1} a_i x^i$$
is a PP (permutation polynomial) if it permutes the elements of $\mathbb{F}_q$.
- Characterisations:
  - Monomials ax^d+b iff $\gcd(d,q-1)=1$

Permutations of finite fields

- A polynomial

$$f(x) = \sum_{i=0}^{q-1} a_i x^i$$

  is a PP (permutation polynomial) if it permutes the elements of $\mathbb{F}_q$.

- Characterisations:
  - Monomials $ax^d + b$ iff $\gcd(d, q-1) = 1$
  - Dickson polynomials $D_d(x)$

Permutations of finite fields

- A polynomial

$$f(x) = \sum_{i=0}^{q-1} a_i x^i$$

is a PP (permutation polynomial) if it permutes the elements of $\mathbb{F}_q$.

- Characterisations:
  - Monomials $ax^d + b$ iff $\gcd(d, q-1) = 1$
  - Dickson polynomials $D_d(x)$ $\gcd(d, q^2-1) = 1$

Permutations of finite fields

- A polynomial

$$f(x) = \sum_{i=0}^{q-1} a_i x^i$$

  is a PP (permutation polynomial) if it permutes the elements of $\mathbb{F}_q$.

- Characterisations:
  - Monomials $ax^d + b$ iff $\gcd(d, q-1) = 1$
  - Dickson polynomials $D_d(x)$ $\gcd(d, q^2 - 1) = 1$
  - Binomials $x^d + ax^e$?

Permutations of finite fields

- A polynomial

$$f(x) = \sum_{i=0}^{q-1} a_i x^i$$

  is a PP (permutation polynomial) if it permutes the elements of $\mathbb{F}_q$.

- Characterisations:
  - Monomials $ax^d + b$ iff $\gcd(d, q-1) = 1$
  - Dickson polynomials $D_d(x)$ $\gcd(d, q^2 - 1) = 1$
  - Binomials $x^d + ax^e$?
    Carlitz; Masuda, Zieve; X.D. Hou; Masuda, Panario, Wang; Niederreiter, Robinson; Turnwald; D. Wan; Sarkar, Bhattacharya, Çesmelioğlu;

Permutations of finite fields

- A polynomial

$$f(x) = \sum_{i=0}^{q-1} a_i x^i$$

  is a PP (permutation polynomial) if it permutes the elements of $\mathbb{F}_q$.
- Characterisations:
  - Monomials $ax^d + b$ iff $\gcd(d, q-1) = 1$
  - Dickson polynomials $D_d(x)$ $\gcd(d, q^2-1) = 1$
  - Binomials $x^d + ax^e$?
    Carlitz; Masuda, Zieve; X.D. Hou; Masuda, Panario, Wang; Niederreiter, Robinson; Turnwald; D. Wan; Sarkar, Bhattacharya, Çesmelioğlu;
- Complete mappings:

Permutations of finite fields

- A polynomial

$$f(x) = \sum_{i=0}^{q-1} a_i x^i$$

  is a PP (permutation polynomial) if it permutes the elements of $\mathbb{F}_q$.

- Characterisations:
  - Monomials $ax^d + b$ iff $\gcd(d, q-1) = 1$
  - Dickson polynomials $D_d(x)$ $\gcd(d, q^2-1) = 1$
  - Binomials $x^d + ax^e$?
    Carlitz; Masuda, Zieve; X.D. Hou; Masuda, Panario, Wang; Niederreiter, Robinson; Turnwald; D. Wan; Sarkar, Bhattacharya, Çesmelioğlu;

- Complete mappings: both $f(x)$ and $f(x) + x$ are PPs.

- Linearised polynomials:

$$L(x) = a_0 x + a_1 x^p + a_2 x^{p^2} + \cdots + a_{m-1} x^{p^{m-1}}$$

- Linearised polynomials:

$$L(x) = a_0 x + a_1 x^p + a_2 x^{p^2} + \cdots + a_{m-1} x^{p^{m-1}}$$

- (Generalized) Walsh transform

$$\widehat{f}(\alpha, \beta) = \sum_{x \in \mathbb{F}_q} \chi(\alpha f(x) + \beta x)$$

where $\chi(\cdot) = \zeta^{\mathrm{Tr}(\cdot)}$.

- Linearised polynomials:

$$L(x) = a_0 x + a_1 x^p + a_2 x^{p^2} + \cdots + a_{m-1} x^{p^{m-1}}$$

- (Generalized) Walsh transform

$$\widehat{f}(\alpha, \beta) = \sum_{x \in \mathbb{F}_q} \chi(\alpha f(x) + \beta x)$$

where $\chi(\cdot) = \zeta^{\mathrm{Tr}(\cdot)}$.

- A criterion for being PP:

- Linearised polynomials:

$$L(x) = a_0 x + a_1 x^p + a_2 x^{p^2} + \cdots + a_{m-1} x^{p^{m-1}}$$

- (Generalized) Walsh transform

$$\widehat{f}(\alpha, \beta) = \sum_{x \in \mathbb{F}_q} \chi(\alpha f(x) + \beta x)$$

where $\chi(\cdot) = \zeta^{\mathrm{Tr}(\cdot)}$.

- A criterion for being PP: f is PP if and only if

$$\sum_{x \in \mathbb{F}_q} \chi(\alpha f(x)) = 0$$

for all $\alpha \in \mathbb{F}_q^*$.

- Consider polynomials of the form:

$$f(x) = L_1(x^d) + L_2(x)$$

- Consider polynomials of the form:

$$f(x) = L_1(x^d) + L_2(x)$$

- Now

$$\sum_{x \in \mathbb{F}_q} \chi(\alpha[L_1(x^d) + L_2(x)]) = 0$$

- Consider polynomials of the form:

$$f(x) = L_1(x^d) + L_2(x)$$

- Now

$$\begin{aligned} \sum_{x \in \mathbb{F}_q} \chi(\alpha[L_1(x^d) + L_2(x)]) &= 0 \\ \sum_{x \in \mathbb{F}_q} \chi(L_1^*(\alpha)x^d + L_2^*(\alpha)x) &= 0 \end{aligned}$$

Where adjoint of L is defined as:

$$L^*(x) = \sum_{i=0}^{m-1} a_i^{p^{m-i}} x^{p^{m-i}}.$$

- Consider polynomials of the form:

$$f(x) = L_1(x^d) + L_2(x)$$

- Now

$$\begin{aligned} \sum_{x\in\mathbb{F}_q} \chi(\alpha[L_1(x^d) + L_2(x)]) &= 0 \\ \sum_{x\in\mathbb{F}_q} \chi(L_1^*(\alpha)x^d + L_2^*(\alpha)x) &= 0 \end{aligned}$$

Where adjoint of L is defined as:

$$L^*(x) = \sum_{i=0}^{m-1} a_i^{p^{m-i}} x^{p^{m-i}}.$$

- If one can describe Walsh zeroes of x^d, then one may find permutation polynomials.

Previous work

- Description of Walsh zeroes known for some d,

Previous work

- Description of Walsh zeroes known for some d, i.e.,
  - $p = 2$ and $d = 1, 3, 2^k + 1, 2^{2k} - 2^k + 1$

Previous work

- Description of Walsh zeroes known for some d, i.e.,
  - $p = 2$ and $d = 1, 3, 2^k + 1, 2^{2k} - 2^k + 1$
  - $p =$ odd, and $d = 1, p + 1, p^k + 1$

Previous work

- Description of Walsh zeroes known for some d, i.e.,
  - $p = 2$ and $d = 1, 3, 2^k + 1, 2^{2k} - 2^k + 1$
  - $p =$ odd, and $d = 1, p + 1, p^k + 1$

  Carlitz; Gold, Dillon, Dobbertin; Coulter

Previous work

- Description of Walsh zeroes known for some d, i.e.,
    - $p = 2$ and $d = 1, 3, 2^k + 1, 2^{2k} - 2^k + 1$
    - $p =$ odd, and $d = 1, p + 1, p^k + 1$
    Carlitz; Gold, Dillon, Dobbertin; Coulter
- PPs coming from these ideas

Previous work

- Description of Walsh zeroes known for some d, i.e.,
  - $p = 2$ and $d = 1, 3, 2^k + 1, 2^{2k} - 2^k + 1$
  - $p =$ odd, and $d = 1, p + 1, p^k + 1$
    Carlitz; Gold, Dillon, Dobbertin; Coulter
- PPs coming from these ideas Pasalic, Charpin; Y. Li, M. Wang;

Previous work

- Description of Walsh zeroes known for some d, i.e.,
  - $p = 2$ and $d = 1, 3, 2^k + 1, 2^{2k} - 2^k + 1$
  - $p =$ odd, and $d = 1, p + 1, p^k + 1$

    Carlitz; Gold, Dillon, Dobbertin; Coulter
- PPs coming from these ideas   Pasalic, Charpin; Y. Li, M. Wang;
- PPs of type $P(x) + \gamma \mathrm{Tr}\,(Q(x))$

Previous work

- Description of Walsh zeroes known for some d, i.e.,
  - $p = 2$ and $d = 1, 3, 2^k + 1, 2^{2k} - 2^k + 1$
  - $p =$ odd, and $d = 1, p + 1, p^k + 1$

    Carlitz; Gold, Dillon, Dobbertin; Coulter
- PPs coming from these ideas Pasalic, Charpin; Y. Li, M. Wang;
- PPs of type $P(x) + \gamma \mathrm{Tr}\,(Q(x))$ Charpin, Kyureghyan

Previous work

- Description of Walsh zeroes known for some d, i.e.,
  - $p = 2$ and $d = 1, 3, 2^k + 1, 2^{2k} - 2^k + 1$
  - $p =$ odd, and $d = 1, p + 1, p^k + 1$
    Carlitz; Gold, Dillon, Dobbertin; Coulter
- PPs coming from these ideas Pasalic, Charpin; Y. Li, M. Wang;
- PPs of type $P(x) + \gamma \mathrm{Tr}\,(Q(x))$ Charpin, Kyureghyan
- If $\gcd(d, q-1) > 1$ then $x^d + L(x)$ ($L(x)$ with binary coefficients) are not permutations ($p = 2$)

Previous work

- Description of Walsh zeroes known for some d, i.e.,
  - $p = 2$ and $d = 1, 3, 2^k + 1, 2^{2k} - 2^k + 1$
  - $p =$ odd, and $d = 1, p + 1, p^k + 1$
    Carlitz; Gold, Dillon, Dobbertin; Coulter
- PPs coming from these ideas Pasalic, Charpin; Y. Li, M. Wang;
- PPs of type $P(x) + \gamma \mathrm{Tr}\left(Q(x)\right)$ Charpin, Kyureghyan
- If $\gcd(d, q-1) > 1$ then $x^d + L(x)$ ($L(x)$ with binary coefficients) are not permutations ($p = 2$) Pasalic

$x^{-1} + L(x)$

- If $p = 2$ then $x^{-1} + L(x)$ is not PP on $\mathbb{F}_{2^n}$ (for $n \geq 5$) Li, Wang

$x^{-1} + L(x)$

- If $p = 2$ then $x^{-1} + L(x)$ is not PP on $\mathbb{F}_{2^n}$ (for $n \geq 5$) Li, Wang
- Our exponential some now becomes:

$$\sum_{x \in \mathbb{F}_q} \chi(x^{-1} + \alpha L^*(\alpha) x) = 0.$$

$x^{-1} + L(x)$

- If $p = 2$ then $x^{-1} + L(x)$ is not PP on $\mathbb{F}_{2^n}$ (for $n \geq 5$) Li, Wang
- Our exponential some now becomes:

$$\sum_{x \in \mathbb{F}_q} \chi(x^{-1} + \alpha L^*(\alpha)x) = 0.$$

You only need $\widehat{f}(1, a)$ modulo some number for negative results.

$x^{-1} + L(x)$

- If $p = 2$ then $x^{-1} + L(x)$ is not PP on $\mathbb{F}_{2^n}$ (for $n \geq 5$) Li, Wang
- Our exponential some now becomes:

$$\sum_{x \in \mathbb{F}_q} \chi(x^{-1} + \alpha L^*(\alpha)x) = 0.$$

  You only need $\widehat{f}(1, a)$ modulo some number for negative results.
- Kloosterman sum is defined by

$$K(a) = \sum_{x \in \mathbb{F}_q} \chi(x^{-1} + ax).$$

$x^{-1} + L(x)$

- If $p = 2$ then $x^{-1} + L(x)$ is not PP on $\mathbb{F}_{2^n}$ (for $n \geq 5$) Li, Wang
- Our exponential some now becomes:

$$\sum_{x \in \mathbb{F}_q} \chi(x^{-1} + \alpha L^*(\alpha)x) = 0.$$

  You only need $\widehat{f}(1, a)$ modulo some number for negative results.
- Kloosterman sum is defined by

$$K(a) = \sum_{x \in \mathbb{F}_q} \chi(x^{-1} + ax).$$

- When $p = 2$, we know $K(a)$ modulo $8, 16, \ldots, 256$ Van der Geer, Van der Vlugt; Helleseth, Zinoviev; G., Lisonek, McGuire, Moloney;

$x^{-1} + L(x)$

- If $p = 2$ then $x^{-1} + L(x)$ is not PP on $\mathbb{F}_{2^n}$ (for $n \geq 5$) Li, Wang
- Our exponential some now becomes:

$$\sum_{x \in \mathbb{F}_q} \chi(x^{-1} + \alpha L^*(\alpha)x) = 0.$$

You only need $\widehat{f}(1, a)$ modulo some number for negative results.

- Kloosterman sum is defined by

$$K(a) = \sum_{x \in \mathbb{F}_q} \chi(x^{-1} + ax).$$

- When $p = 2$, we know $K(a)$ modulo $8, 16, \ldots, 256$ Van der Geer, Van der Vlugt; Helleseth, Zinoviev; G., Lisonek, McGuire, Moloney;
- When $p = 3$, we know $K(a)$ modulo $9, 27$ G., McGuire, Moloney;

$x^{-1} + L(x)$

- If $p = 2$ then $x^{-1} + L(x)$ is not PP on $\mathbb{F}_{2^n}$ (for $n \geq 5$) Li, Wang
- Our exponential some now becomes:

$$\sum_{x \in \mathbb{F}_q} \chi(x^{-1} + \alpha L^*(\alpha)x) = 0.$$

  You only need $\widehat{f}(1, a)$ modulo some number for negative results.
- Kloosterman sum is defined by

$$K(a) = \sum_{x \in \mathbb{F}_q} \chi(x^{-1} + ax).$$

- When $p = 2$, we know $K(a)$ modulo $8, 16, \ldots, 256$ Van der Geer, Van der Vlugt; Helleseth, Zinoviev; G., Lisonek, McGuire, Moloney;
- When $p = 3$, we know $K(a)$ modulo $9, 27$ G., McGuire, Moloney; 4

$x^{-1} + L(x)$

- If $p = 2$ then $x^{-1} + L(x)$ is not PP on $\mathbb{F}_{2^n}$ (for $n \geq 5$) Li, Wang
- Our exponential some now becomes:

$$\sum_{x \in \mathbb{F}_q} \chi(x^{-1} + \alpha L^*(\alpha)x) = 0.$$

You only need $\widehat{f}(1, a)$ modulo some number for negative results.

- Kloosterman sum is defined by

$$K(a) = \sum_{x \in \mathbb{F}_q} \chi(x^{-1} + ax).$$

- When $p = 2$, we know $K(a)$ modulo $8, 16, \ldots, 256$ Van der Geer, Van der Vlugt; Helleseth, Zinoviev; G., Lisonek, McGuire, Moloney;
- When $p = 3$, we know $K(a)$ modulo $9, 27$ G., McGuire, Moloney; 4
- When $p > 3$, no Kloosterman zeroes Kononen, Rinta-aho, Väänänen

Modulo 4 characterisation

Theorem (G. ('12), Garaschuk, Lisoněk ('08))

Let $a \in \mathbb{F}_{3^m}$. Then

$$K(a) \equiv \begin{cases} 0 \pmod 4 & \text{if } a = 0 \text{ or } a = b^2 \text{ with } \mathrm{Tr}(b) = 1 \\ & \text{and } -b \text{ is not a square,} \\ 2m+3 \pmod 4 & \text{if } a = t^2 - t^3 \text{ for some } t \in \mathbb{F}_q \setminus \{0,1\} \\ & \text{and at least one of } t, 1-t \text{ is a square,} \\ 2 \pmod 4 & \text{if } a = b^2 \text{ with } \mathrm{Tr}(b) = 1 \\ & \text{and } -b \text{ is a square.} \\ 2m+1 \pmod 4 & \text{if } a = t^2 - t^3 \text{ for some } t \in \mathbb{F}_q \setminus \{0,1\} \\ & \text{and none of } t, 1-t \text{ is a square.} \end{cases}$$

Odd cases Garaschuk, Lisoněk; Even cases G.

A theorem of Carlitz

Theorem (Carlitz)

Let $f(x)$ be a polynomial over $\mathbb{F}_q[x]$ such that $f(0) = 0, f(1) = 1$, and

$$\eta(f(a) - f(b)) = \eta(a - b) \quad (1)$$

for all $a, b \in \mathbb{F}_q$. Then $f(x) = x^{p^d}$ for some $0 \leq d < m$.

A theorem of Carlitz

Theorem (Carlitz)

Let $f(x)$ be a polynomial over $\mathbb{F}_q[x]$ such that $f(0) = 0, f(1) = 1$, and

$$\eta(f(a) - f(b)) = \eta(a - b) \tag{1}$$

for all $a, b \in \mathbb{F}_q$. Then $f(x) = x^{p^d}$ for some $0 \leq d < m$.

We modify condition (1) as follows:

$$\eta(f(a) - f(b))\ \eta(a - b) \in \{0, 1\}. \tag{2}$$

A theorem of Carlitz

Theorem (Carlitz)

Let $f(x)$ be a polynomial over $\mathbb{F}_q[x]$ such that $f(0) = 0, f(1) = 1$, and

$$\eta(f(a) - f(b)) = \eta(a - b) \tag{1}$$

for all $a, b \in \mathbb{F}_q$. Then $f(x) = x^{p^d}$ for some $0 \leq d < m$.

We modify condition (1) as follows:

$$\eta(f(a) - f(b))\ \eta(a - b) \in \{0, 1\}. \tag{2}$$

If $f = L$ is linearized then the condition (2) is equivalent to

$$\eta(aL(a)) \in \{0, 1\}.$$

A related theorem

Theorem (G., McGuire)

Let $L(x)$ be a linearized polynomial. Then $Im(xL(x)) \subseteq \mathrm{Sq} \cup \{0\}$ if and only if $L(x) = 0$ or $L(x) = ax^{p^d}$ for some $a \in \mathrm{Sq}$ and some $0 \le d < m$.

A related theorem

Theorem (G., McGuire)

Let $L(x)$ be a linearized polynomial. Then $Im(xL(x)) \subseteq \mathrm{Sq} \cup \{0\}$ if and only if $L(x) = 0$ or $L(x) = ax^{p^d}$ for some $a \in \mathrm{Sq}$ and some $0 \leq d < m$.

Sketch of Proof

$$H_\alpha^{(c)} = \{x \in \mathbb{F}_q \ : \ \mathrm{Tr}(\alpha x) = c\}$$

A related theorem

Theorem (G., McGuire)

Let $L(x)$ be a linearized polynomial. Then $Im(xL(x)) \subseteq \mathrm{Sq} \cup \{0\}$ if and only if $L(x) = 0$ or $L(x) = ax^{p^d}$ for some $a \in \mathrm{Sq}$ and some $0 \leq d < m$.

Sketch of Proof

$$H_\alpha^{(c)} = \{x \in \mathbb{F}_q \ : \ \mathrm{Tr}(\alpha x) = c\}$$

$$S_\alpha^{(c)} = \sum_{x \in H_\alpha^{(c)}} \eta(x)$$

A related theorem

Theorem (G., McGuire)

Let $L(x)$ be a linearized polynomial. Then $Im(xL(x)) \subseteq \mathrm{Sq} \cup \{0\}$ if and only if $L(x) = 0$ or $L(x) = ax^{p^d}$ for some $a \in \mathrm{Sq}$ and some $0 \leq d < m$.

Sketch of Proof

$$H_\alpha^{(c)} = \{x \in \mathbb{F}_q \ : \ \mathrm{Tr}(\alpha x) = c\}$$

$$S_\alpha^{(c)} = \sum_{x \in H_\alpha^{(c)}} \eta(x)$$

We show the (exact) p-divisibility of $S_\alpha^{(c)}$ is $\frac{m-1}{2}$ when $c \neq 0$.

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.
- For $x \in K$, $\eta(L(x)) = 0$.

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.
- For $x \in K$, $\eta(L(x)) = 0$.
- For nonzero $v \in V$, since $\eta((x+v)L(x+v)) = 1$ we must have $\eta(x+v) = \eta(L(v))$,

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.
- For $x \in K$, $\eta(L(x)) = 0$.
- For nonzero $v \in V$, since $\eta((x+v)L(x+v)) = 1$ we must have $\eta(x+v) = \eta(L(v))$, i.e., η is constant on nonzero cosets of K.

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.
- For $x \in K$, $\eta(L(x)) = 0$.
- For nonzero $v \in V$, since $\eta((x+v)L(x+v)) = 1$ we must have $\eta(x+v) = \eta(L(v))$, i.e., η is constant on nonzero cosets of K.
- Now since $K \subseteq H_\alpha^{(0)}$

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.
- For $x \in K$, $\eta(L(x)) = 0$.
- For nonzero $v \in V$, since $\eta((x+v)L(x+v)) = 1$ we must have $\eta(x+v) = \eta(L(v))$, i.e., η is constant on nonzero cosets of K.
- Now since $K \subseteq H_\alpha^{(0)}$ and the (exact) p-divisibility of $S_\alpha^{(c)}$ is $\frac{m-1}{2}$,

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.
- For $x \in K$, $\eta(L(x)) = 0$.
- For nonzero $v \in V$, since $\eta((x+v)L(x+v)) = 1$ we must have $\eta(x+v) = \eta(L(v))$, i.e., η is constant on nonzero cosets of K.
- Now since $K \subseteq H_\alpha^{(0)}$ and the (exact) p-divisibility of $S_\alpha^{(c)}$ is $\frac{m-1}{2}$, dimension of K cannot be large,

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.
- For $x \in K$, $\eta(L(x)) = 0$.
- For nonzero $v \in V$, since $\eta((x+v)L(x+v)) = 1$ we must have $\eta(x+v) = \eta(L(v))$, i.e., η is constant on nonzero cosets of K.
- Now since $K \subseteq H_\alpha^{(0)}$ and the (exact) p-divisibility of $S_\alpha^{(c)}$ is $\frac{m-1}{2}$, dimension of K cannot be large, (viz., $\mathrm{val}_p(t|K|) = \frac{m-1}{2}$).

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.
- For $x \in K$, $\eta(L(x)) = 0$.
- For nonzero $v \in V$, since $\eta((x+v)L(x+v)) = 1$ we must have $\eta(x+v) = \eta(L(v))$, i.e., η is constant on nonzero cosets of K.
- Now since $K \subseteq H_\alpha^{(0)}$ and the (exact) p-divisibility of $S_\alpha^{(c)}$ is $\frac{m-1}{2}$, dimension of K cannot be large, (viz., $\mathrm{val}_p(t|K|) = \frac{m-1}{2}$).
- Since $\eta(L(v))$ is $+1$ and -1 equal number of times for $v \in V^*$,

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.
- For $x \in K$, $\eta(L(x)) = 0$.
- For nonzero $v \in V$, since $\eta((x+v)L(x+v)) = 1$ we must have $\eta(x+v) = \eta(L(v))$, i.e., η is constant on nonzero cosets of K.
- Now since $K \subseteq H_\alpha^{(0)}$ and the (exact) p-divisibility of $S_\alpha^{(c)}$ is $\frac{m-1}{2}$, dimension of K cannot be large, (viz., $\mathrm{val}_p(t|K|) = \frac{m-1}{2}$).
- Since $\eta(L(v))$ is $+1$ and -1 equal number of times for $v \in V^*$, (note that $\sum_{x \in \mathbb{F}_q} \eta(x) = 0$),

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.
- For $x \in K$, $\eta(L(x)) = 0$.
- For nonzero $v \in V$, since $\eta((x+v)L(x+v)) = 1$ we must have $\eta(x+v) = \eta(L(v))$, i.e., η is constant on nonzero cosets of K.
- Now since $K \subseteq H_\alpha^{(0)}$ and the (exact) p-divisibility of $S_\alpha^{(c)}$ is $\frac{m-1}{2}$, dimension of K cannot be large, (viz., $\mathrm{val}_p(t|K|) = \frac{m-1}{2}$).
- Since $\eta(L(v))$ is $+1$ and -1 equal number of times for $v \in V^*$, (note that $\sum_{x \in \mathbb{F}_q} \eta(x) = 0$), and $V \subseteq H_\beta^{(0)}$,

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.
- For $x \in K$, $\eta(L(x)) = 0$.
- For nonzero $v \in V$, since $\eta((x+v)L(x+v)) = 1$ we must have $\eta(x+v) = \eta(L(v))$, i.e., η is constant on nonzero cosets of K.
- Now since $K \subseteq H_\alpha^{(0)}$ and the (exact) p-divisibility of $S_\alpha^{(c)}$ is $\frac{m-1}{2}$, dimension of K cannot be large, (viz., $\mathrm{val}_p(t|K|) = \frac{m-1}{2}$).
- Since $\eta(L(v))$ is $+1$ and -1 equal number of times for $v \in V^*$, (note that $\sum_{x \in \mathbb{F}_q} \eta(x) = 0$), and $V \subseteq H_\beta^{(0)}$, we have $S_\beta^{(c)}$ strictly less than $|K|$, it cannot be small.

Sketch of Proof (cont'd)

- Assume $\eta(xL(x)) \in 0, 1$ for all x and $L(x) \neq 0$ or ax^{p^k}.
- Let K be kernel of L and $K \oplus V = \mathbb{F}_q$.
- For $x \in K$, $\eta(L(x)) = 0$.
- For nonzero $v \in V$, since $\eta((x+v)L(x+v)) = 1$ we must have $\eta(x+v) = \eta(L(v))$, i.e., η is constant on nonzero cosets of K.
- Now since $K \subseteq H_\alpha^{(0)}$ and the (exact) p-divisibility of $S_\alpha^{(c)}$ is $\frac{m-1}{2}$, dimension of K cannot be large, (viz., $\mathrm{val}_p(t|K|) = \frac{m-1}{2}$).
- Since $\eta(L(v))$ is $+1$ and -1 equal number of times for $v \in V^*$, (note that $\sum_{x \in \mathbb{F}_q} \eta(x) = 0$), and $V \subseteq H_\beta^{(0)}$, we have $S_\beta^{(c)}$ strictly less than $|K|$, it cannot be small.
- A number cannot be both small and large! QED.

The nonexistence result

Theorem (G., McGuire)

If p is odd then $x^{-1} + L(x)$ is a PP if and only if

(i) $L(x) = 0$, *or*

(ii) $q = 3$ *and* $L(x) = x$, *or*

(iii) $q = 9$ *and* $L(x) = \omega^2 x^3$ *or* $L(x) = \omega^6 x^3$, *where* ω *generates* $\mathbb{F}_9^*$.

The nonexistence result

Theorem (G., McGuire)

If p is odd then $x^{-1} + L(x)$ is a PP if and only if

(i) $L(x) = 0$, *or*

(ii) $q = 3$ *and* $L(x) = x$, *or*

(iii) $q = 9$ *and* $L(x) = \omega^2 x^3$ *or* $L(x) = \omega^6 x^3$, *where* ω *generates* $\mathbb{F}_9^*$.

Sketch of Proof

By the result giving Kloosterman sums modulo 4, if $xL(x)$ is always square or 0, then $L(x) = 0$ or $L(x) = ax^{p^k}$.

The nonexistence result

Theorem (G., McGuire)

If p is odd then $x^{-1} + L(x)$ is a PP if and only if

(i) $L(x) = 0$, *or*

(ii) $q = 3$ *and* $L(x) = x$, *or*

(iii) $q = 9$ *and* $L(x) = \omega^2 x^3$ *or* $L(x) = \omega^6 x^3$, *where* ω *generates* $\mathbb{F}_9^*$.

Sketch of Proof

By the result giving Kloosterman sums modulo 4, if $xL(x)$ is always square or 0, then $L(x) = 0$ or $L(x) = ax^{p^k}$.
We have to show now $x^{-1} + ax^{p^k}$ cannot be permutation.

The nonexistence result

Theorem (G., McGuire)

If p is odd then $x^{-1} + L(x)$ is a PP if and only if

(i) $L(x) = 0$, *or*

(ii) $q = 3$ *and* $L(x) = x$, *or*

(iii) $q = 9$ *and* $L(x) = \omega^2 x^3$ *or* $L(x) = \omega^6 x^3$, *where* ω *generates* $\mathbb{F}_9^*$.

Sketch of Proof

By the result giving Kloosterman sums modulo 4, if $xL(x)$ is always square or 0, then $L(x) = 0$ or $L(x) = ax^{p^k}$.
We have to show now $x^{-1} + ax^{p^k}$ cannot be permutation.
Use Hermite condition.

Sketch of Proof (cont'd)

Theorem (Hermite's criterion)

A polynomial $f \in \mathbb{F}_{p^m}[x]$ is a permutation polynomial if and only if

1. *f has exactly one root in $\mathbb{F}_{p^m}$,*
2. *for each d with $1 \le d \le p^m - 2$ and $d \not\equiv 0 \pmod{p}$, the degree of $f(x)^d \pmod{x^{p^m} - x}$ is less than $p^m - 1$.*

Sketch of Proof (cont'd)

Theorem (Hermite's criterion)

A polynomial $f \in \mathbb{F}_{p^m}[x]$ is a permutation polynomial if and only if

1. *f has exactly one root in $\mathbb{F}_{p^m}$,*
2. *for each d with $1 \leq d \leq p^m - 2$ and $d \not\equiv 0 \pmod{p}$, the degree of $f(x)^d \pmod{x^{p^m} - x}$ is less than $p^m - 1$.*

This leaves a few exceptions. For them we use the result giving Kloosterman sums modulo 4.

An announcement
F.G., Robert Granger, Gary McGuire, Jens Zumbrägel

- **The Discrete Logarithm Problem on Finite Fields:**

An announcement

F.G., Robert Granger, Gary McGuire, Jens Zumbrägel

- **The Discrete Logarithm Problem on Finite Fields:** Fix a generator g of $\mathbb{F}_{q^n}^*$. Given $c \in \mathbb{F}_{q^n}^*$, find i such that $c = g^i$.

An announcement
F.G., Robert Granger, Gary McGuire, Jens Zumbrägel

- **The Discrete Logarithm Problem on Finite Fields:** Fix a generator g of $\mathbb{F}_{q^n}^*$. Given $c \in \mathbb{F}_{q^n}^*$, find i such that $c = g^i$.
- It is a challenge to compute Discrete Logarithms on the largest possible Finite Field $\mathbb{F}_{q^n}$.

An announcement
F.G., Robert Granger, Gary McGuire, Jens Zumbrägel

- **The Discrete Logarithm Problem on Finite Fields:** Fix a generator g of $\mathbb{F}_{q^n}^*$. Given $c \in \mathbb{F}_{q^n}^*$, find i such that $c = g^i$.
- It is a challenge to compute Discrete Logarithms on the largest possible Finite Field $\mathbb{F}_{q^n}$.
- **Highlights of our method:** For $q = 2^l$, when $k \mid l$ and $l/k \geq 3$, the following family of polynomials has probability $\approx 1/2^{3k}$ of splitting:

$$x^{2^k+1} + ax^{2^k} + bx + c, \quad a, b, c \in \mathbb{F}_q,$$

(the work on these polynomials due to Bluher and Helleseth-Kholosha) which is much higher than the random $1/(2^k + 1)!$. We effectively use these polynomials in our polynomial time relation generation (the first polynomial time algorithm for relation generation).

- **Highlights of our method:** A very effective descent method to find individual logarithms (involves algorithms on polynomials over $\mathbb{F}_q$).

- **Highlights of our method:** A very effective descent method to find individual logarithms (involves algorithms on polynomials over $\mathbb{F}_q$).
- **Highlights of our method:** An $L_{q^n}(1/3, (2/3)^{2/3})$ overall algorithm.

- **Highlights of our method:** A very effective descent method to find individual logarithms (involves algorithms on polynomials over $\mathbb{F}_q$).
- **Highlights of our method:** An $L_{q^n}(1/3, (2/3)^{2/3})$ overall algorithm.
- **World record progress:**

bitlength	who/when	running time
127	Coppersmith 1984	N/A
...		
521	Joux-Lercier 2001	$>$ 3000 core hours
607	Thomé 2001	$>$ 800000 core hours
...		
923	Hayashi et al. 2010	$>$ 800000 core hours
1175	Joux Dec. 2012	$>$ 30000 core hours
1425	Joux Jan. 2013	$>$ 30000 core hours
1778	Joux 11/2/2013	215 core hours

- **Highlights of our method:** A very effective descent method to find individual logarithms (involves algorithms on polynomials over $\mathbb{F}_q$).
- **Highlights of our method:** An $L_{q^n}(1/3, (2/3)^{2/3})$ overall algorithm.
- **World record progress:**

bitlength	who/when	running time
127	Coppersmith 1984	N/A
...		
521	Joux-Lercier 2001	$>$ 3000 core hours
607	Thomé 2001	$>$ 800000 core hours
...		
923	Hayashi et al. 2010	$>$ 800000 core hours
1175	Joux Dec. 2012	$>$ 30000 core hours
1425	Joux Jan. 2013	$>$ 30000 core hours
1778	Joux 11/2/2013	215 core hours
1971	GGMZ 19/2/2013	3132 core hours

- **Highlights of our method:** A very effective descent method to find individual logarithms (involves algorithms on polynomials over $\mathbb{F}_q$).
- **Highlights of our method:** An $L_{q^n}(1/3, (2/3)^{2/3})$ overall algorithm.
- **World record progress:**

bitlength	who/when	running time
127	Coppersmith 1984	N/A
...		
521	Joux-Lercier 2001	$>$ 3000 core hours
607	Thomé 2001	$>$ 800000 core hours
...		
923	Hayashi et al. 2010	$>$ 800000 core hours
1175	Joux Dec. 2012	$>$ 30000 core hours
1425	Joux Jan. 2013	$>$ 30000 core hours
1778	Joux 11/2/2013	215 core hours
1971	GGMZ 19/2/2013	3132 core hours
4080	Joux 22/3/2013	14100 core hours

- **Highlights of our method:** A very effective descent method to find individual logarithms (involves algorithms on polynomials over $\mathbb{F}_q$).
- **Highlights of our method:** An $L_{q^n}(1/3, (2/3)^{2/3})$ overall algorithm.
- **World record progress:**

bitlength	who/when	running time
127	Coppersmith 1984	N/A
...		
521	Joux-Lercier 2001	$>$ 3000 core hours
607	Thomé 2001	$>$ 800000 core hours
...		
923	Hayashi et al. 2010	$>$ 800000 core hours
1175	Joux Dec. 2012	$>$ 30000 core hours
1425	Joux Jan. 2013	$>$ 30000 core hours
1778	Joux 11/2/2013	215 core hours
1971	GGMZ 19/2/2013	3132 core hours
4080	Joux 22/3/2013	14100 core hours
6120	GGMZ 11/4/2013	750 core hours

Thanks for your attention.