NTNU
Norwegian University of
Science and Technology

Towards a Characterization of Left Quasigroup Polynomials of Small Degree Over $\mathbb{F}_{2^k}$

Simona Samardjiska (joint work with Danilo Gligoroski)

Department of Telematics, NTNU, Norway

simonas@item.ntnu.no,danilog@item.ntnu.no

MileHigh, August 11 – 17, 2013, Denver

Introduction - Permutation Polynomials (PP)

A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if the induced function $f : c \to f(c)$ from $\mathbb{F}_q$ to itself is a permutation of $\mathbb{F}_q$.

- Hermite criterion
  $f(x) \in \mathbb{F}_q[x]$ is a PP of $\mathbb{F}_q$ iff
  - *f has a unique root in $\mathbb{F}_q$*
  - $\forall n,\ 1 \leq n \leq q-2,\ (n,q) = 1,\ Deg(f^n) \leq q-2 \pmod{x^q - x}$
- A small amount of classes known
- Characterization- open problem
- In characteristic 2
  - Dickson (1896) - up to degree 5
  - Li et al. (2010) - degrees 6, 7

NTNU
Norwegian University of Science and Technology

Introduction - Permutation Polynomials (PP)

A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if the induced function $f : c \to f(c)$ from $\mathbb{F}_q$ to itself is a permutation of $\mathbb{F}_q$.

- Hermite criterion
  $f(x) \in \mathbb{F}_q[x]$ *is a PP of* $\mathbb{F}_q$ *iff*
  - f *has a unique root in* $\mathbb{F}_q$
  - $\forall n,\ 1 \le n \le q-2,\ (n,q)=1,\ Deg(f^n) \le q-2 \pmod{x^q - x}$
- A small amount of classes known
- Characterization- open problem
- In characteristic 2
  - Dickson (1896) - up to degree 5
  - Li et al. (2010) - degrees 6, 7

NTNU
Norwegian University of Science and Technology

Introduction - Permutation Polynomials (PP)

A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if the induced function $f : c \to f(c)$ from $\mathbb{F}_q$ to itself is a permutation of $\mathbb{F}_q$.

- Hermite criterion
  $f(x) \in \mathbb{F}_q[x]$ is a PP of $\mathbb{F}_q$ iff
  - *f has a unique root in $\mathbb{F}_q$*
  - $\forall n,\ 1 \leq n \leq q-2,\ (n,q) = 1,\ Deg(f^n) \leq q-2 \pmod{x^q - x}$

- A small amount of classes known
- Characterization- open problem
- In characteristic 2
  - Dickson (1896) - up to degree 5
  - Li et al. (2010) - degrees 6, 7

Permutation Polynomials of Degree ≤ 5 over $\mathbb{F}_{2^k}$

[Dickson]

All normalized PP:

x	all k
x^2	all k
x^3	$(2^k-1,3)=1$
x^4+ax^2+bx	$x=0$ is the only root
x^5	$(2^k-1,5)=1$
$x^5+ax^3+a^2x$	$2^k=\pm 2 \pmod 5$

Permutation Polynomials of Degree 6 over $\mathbb{F}_{2^k}$ [Li et al.]

- k - odd: x^6
- $k = 3$:

$x^6 + x^5 + x^3 + \alpha x^2 + \alpha x$	$x^6 + x^5 + \alpha x^3$
$x^6 + x^5 + x^3 + x^2 + x$	$x^6 + x^5 + x^4$
$x^6 + x^5 + x^4 + x^3 + x^2$	$x^6 + x^3 + x^2$
$x^6 + x^5 + x^4 + x^3 + x$	$x^6 + x^5 + x^4 + \alpha^3 x^3 + \alpha^4 x^2 + \alpha^6 x$

  and α is a root of $x^3 + x + 1$.

- $k = 4$:

$$x^6 + x^5 + x^3 + \beta^3 x^2 + \beta^5 x$$
$$x^6 + x^5 + \beta^3 x^4 + x^3 + \beta x^2 + \beta^6 x$$
$$x^6 + x^5 + \beta^3 x^4 + x^3 + \beta^8 x^2 + \beta^{13} x$$

  and β is a root of $x^4 + x + 1$.

- $k = 5$: $x^6 + x^5 + x^2$

NTNU
Norwegian University of Science and Technology

Left Quasigroup Polynomials (LQP) over $\mathbb{F}_{2^k}$

A polynomial $g(x,y) \in \mathbb{F}_q[x,y]$ is called a Left Quasigroup Polynomial (LQP) of $\mathbb{F}_q$ if for all $u \in \mathbb{F}_q$, $g(u,y)$ is a permutation polynomial of $\mathbb{F}_q$.

- Natural extension of PPs
- Natural question:

Can we characterize LQPs for small degrees?

- Ex: Algebraic Degree 1

$$g(x,y) = L_1(x) + L_2(y)$$

L_1, L_2 linearized polynomials, L_2 - no other roots but 0.

Left Quasigroup Polynomials (LQP) over $\mathbb{F}_{2^k}$

A polynomial $g(x,y) \in \mathbb{F}_q[x,y]$ is called a Left Quasigroup Polynomial (LQP) of $\mathbb{F}_q$ if for all $u \in \mathbb{F}_q$, $g(u,y)$ is a permutation polynomial of $\mathbb{F}_q$.

- Natural extension of PPs
- Natural question:

Can we characterize LQPs for small degrees?

- Ex: Algebraic Degree 1

$$g(x,y) = L_1(x) + L_2(y)$$

L_1, L_2 linearized polynomials, L_2 - no other roots but 0.

NTNU
Norwegian University of Science and Technology

Left Quasigroup Polynomials (LQP) over $\mathbb{F}_{2^k}$

A polynomial $g(x,y) \in \mathbb{F}_q[x,y]$ is called a Left Quasigroup Polynomial (LQP) of $\mathbb{F}_q$ if for all $u \in \mathbb{F}_q$, $g(u,y)$ is a permutation polynomial of $\mathbb{F}_q$.

- Natural extension of PPs
- Natural question:

Can we characterize LQPs for small degrees?

- Ex: Algebraic Degree 1

$$g(x,y) = L_1(x) + L_2(y)$$

L_1, L_2 linearized polynomials, L_2 - no other roots but 0.

NTNU
Norwegian University of
Science and Technology

Left Quasigroup Polynomials (LQP) over $\mathbb{F}_{2^k}$

A polynomial $g(x,y) \in \mathbb{F}_q[x,y]$ is called a Left Quasigroup Polynomial (LQP) of $\mathbb{F}_q$ if for all $u \in \mathbb{F}_q$, $g(u,y)$ is a permutation polynomial of $\mathbb{F}_q$.

- Natural extension of PPs
- Natural question:

  Can we characterize LQPs for small degrees?

- **Focus on LQPs over $\mathbb{F}_{2^k}$ of algebraic degree 2**
  - notation - $_2$**LQPs**
  - known as MQQs when defined over $\mathbb{F}_2^k$

$$g(x,y) = h(x,y)y + f(x)$$

Left Quasigroup Polynomials (LQP) over $\mathbb{F}_{2^k}$

A polynomial $g(x,y) \in \mathbb{F}_q[x,y]$ is called a Left Quasigroup Polynomial (LQP) of $\mathbb{F}_q$ if for all $u \in \mathbb{F}_q$, $g(u,y)$ is a permutation polynomial of $\mathbb{F}_q$.

- Natural extension of PPs
- Natural question:

  Can we characterize LQPs for small degrees?

- **Focus on LQPs over $\mathbb{F}_{2^k}$ of algebraic degree 2**
  - notation - $_2$**LQPs**
  - known as MQQs when defined over $\mathbb{F}_2^k$

$$g(x,y) = h(x,y)y + f(x)$$

Left Quasigroup Polynomials (LQP) over $\mathbb{F}_{2^k}$

A polynomial $g(x,y) \in \mathbb{F}_q[x,y]$ is called a Left Quasigroup Polynomial (LQP) of $\mathbb{F}_q$ if for all $u \in \mathbb{F}_q$, $g(u,y)$ is a permutation polynomial of $\mathbb{F}_q$.

- Natural extension of PPs
- Natural question:

  Can we characterize LQPs for small degrees?

- **Focus on LQPs over $\mathbb{F}_{2^k}$ of algebraic degree 2**

  Degree 2: $g(x,y) = ay^2 + bxy$, $ab = 0$

NTNU
Norwegian University of Science and Technology

Left Quasigroup Polynomials (LQP) over $\mathbb{F}_{2^k}$

A polynomial $g(x,y) \in \mathbb{F}_q[x,y]$ is called a Left Quasigroup Polynomial (LQP) of $\mathbb{F}_q$ if for all $u \in \mathbb{F}_q$, $g(u,y)$ is a permutation polynomial of $\mathbb{F}_q$.

- Natural extension of PPs
- Natural question:

  Can we characterize LQPs for small degrees?

- **Focus on LQPs over $\mathbb{F}_{2^k}$ of algebraic degree 2**

  Degree 3: $g(x,y) = (x+y)^3$, k - odd

  $g(x,y) = (x^2+x+b)y$, x^2+x+b - irreducible

NTNU
Norwegian University of Science and Technology

${}_2$LQPs over $\mathbb{F}_{2^k}$

f_1, f_2, f_3 - linearized polynomials

Degree 4 :

$$\begin{aligned} g(x,y) &= ay^4 + cy^3 + f_2(x)y^2 + f_3(x)y \\ &\quad deg(f_2), deg(f_3) \leq 2 \end{aligned}$$

Degree 5 :

$$\begin{aligned} g(x,y) &= ay^5 + f_1(x)y^4 + cy^3 + f_2(x)y^2 + f_3(x)y \\ &\quad deg(f_1) \leq 1,\ deg(f_2) \leq 2, deg(f_3) \leq 4 \end{aligned}$$

Degree 6 :

$$\begin{aligned} g(x,y) &= ay^6 + by^5 + f_1(x)y^4 + cy^3 + f_2(x)y^2 + f_3(x)y \\ &\quad deg(f_1) \leq 2,\ deg(f_2) \leq 4, deg(f_3) \leq 4 \end{aligned}$$

NTNU
Norwegian University of
Science and Technology

$_2$LQPs over $\mathbb{F}_{2^k}$

Case I:

Degree 4 :

$$g(x,y) = ay^4 + cy^3 + f_2(x)y^2 + f_3(x)y$$
$$deg(f_2), deg(f_3) \leq 2$$

Degree 5 :

$$g(x,y) = ay^5 + f_1(x)y^4 + cy^3 + f_2(x)y^2 + f_3(x)y$$
$$deg(f_1) \leq 1,\ deg(f_2) \leq 2, deg(f_3) \leq 4$$

Degree 6 :

$$g(x,y) = ay^6 + by^5 + f_1(x)y^4 + cy^3 + f_2(x)y^2 + f_3(x)y$$
$$deg(f_1) \leq 2,\ deg(f_2) \leq 4, deg(f_3) \leq 4$$

${}_2$LQPs over $\mathbb{F}_{2^k}$

$$g(x,y) = cy^3 + f_2(x)y^2 + f_3(x)y$$

defines a ${}_2$LQP of $deg \leq 6$, iff one of the following is true

- $g(x,y) = f_3(x)y$,
  where $f_3(x)$ - linearized pol. without roots and $deg(f_3) \leq 4$
- $g(x,y) = f_2(x)y^2 + f_3(x)y$,
  where
  - $k = 2,\ f_2(x) = \prod_{i=1}^{2}(x-\alpha_i),\ f_3(x) = \prod_{i=3}^{4}(x-\alpha_i)$
  - $k = 3,\ f_2(x) = \prod_{i=1}^{4}(x-\alpha_i),\ f_3(x) = \prod_{i=5}^{8}(x-\alpha_i)$

  and α_i are all the elements of $\mathbb{F}_{2^k}$.
- $g(x,y) = (y + f_2(x))^3$,
  where k - odd, $deg(f_2) \leq 2$

NTNU
Norwegian University of Science and Technology

${}_2$LQPs over $\mathbb{F}_{2^k}$

Case II:

Degree 4 :

$$\begin{aligned} g(x,y) &= ay^4 + cy^3 + f_2(x)y^2 + f_3(x)y \\ &\quad deg(f_2), deg(f_3) \leq 2 \end{aligned}$$

Degree 5 :

$$\begin{aligned} g(x,y) &= \mathbf{a}y^5 + f_1(x)y^4 + cy^3 + f_2(x)y^2 + f_3(x)y \\ &\quad deg(f_1) \leq 1, deg(f_2) \leq 2, deg(f_3) \leq 4 \end{aligned}$$

Degree 6 :

$$\begin{aligned} g(x,y) &= \mathbf{a}y^6 + \mathbf{b}y^5 + f_1(x)y^4 + cy^3 + f_2(x)y^2 + f_3(x)y \\ &\quad deg(f_1) \leq 2, deg(f_2) \leq 4, deg(f_3) \leq 4 \end{aligned}$$

NTNU
Norwegian University of Science and Technology

${}_2$LQPs over $\mathbb{F}_{2^k}$

$$g(x,y) = y^5 + f_1(x)y^4 + cy^3 + f_2(x)y^2 + f_3(x)y$$

defines a ${}_2$LQP of $deg \leq 6$, iff one of the following is true

- $g(x,y) = (y + f_1(x))^5$,
  where $(2^k - 1, 5) = 1$, $deg(f_1) \leq 2$
- $g(x,y) = (y + f_1(x))^5 + a(y + f_1(x))^3 + a^2(y + f_1(x))$,
  where $2^k = \pm 2 \pmod 5$, a - arbitrary, $deg(f_1) = 1$,
  $(deg(f_1) \leq 2$ for $k = 3)$

${}_2$LQPs over $\mathbb{F}_{2^k}$

$$g(x,y) = y^6 + by^5 + f_1(x)y^4 + cy^3 + f_2(x)y^2 + f_3(x)y$$

defines a ${}_2$LQP of $deg = 6$, iff one of the following is true

- $g(x,y) = (y + f_1(x))^6$,
  where k - odd, $deg(f_1) = 1$
- $g(x,y) = p(y + f(x))$,
  where $k = 3$, $deg(f_1) = 1$, and p is one of
  - $p(x) = x^6 + x^5 + \alpha x^3$
  - $p(x) = x^6 + x^5 + x^4 + \alpha^3 x^3 + \alpha^4 x^2 + \alpha^6 x$
  - $p(x) = x^6 + x^3 + x^2$
  - $p(x) = x^6 + x^5 + x^4$

  and α is a root of $x^3 + x + 1$.

NTNU
Norwegian University of Science and Technology

${}_2$LQPs over $\mathbb{F}_{2^k}$

$$g(x,y) = y^6 + by^5 + f_1(x)y^4 + cy^3 + f_2(x)y^2 + f_3(x)y$$

defines a ${}_2$LQP of $deg = 6$, iff one of the following is true

- $g(x,y) = p(y + f(x))$,
  where $k = 4$, $deg(f_1) = 1$, and p is one of
  - $p(x) = x^6 + x^5 + x^3 + \beta^3 x^2 + \beta^5 x$
  - $p(x) = x^6 + x^5 + \beta x^4 + x^3 + \beta x^2 + \beta^6 x$
  - $p(x) = x^6 + x^5 + \beta x^4 + x^3 + \beta^8 x^2 + \beta^{13} x$

  and β is a root of $x^4 + x + 1$.

- $g(x,y) = p(y + f(x))$,
  where $k = 5$, $deg(f_1) = 1$, and $p(x) = x^6 + x^5 + x^2$

NTNU
Norwegian University of
Science and Technology

${}_2$LQPs over $\mathbb{F}_{2^k}$

- $g(x,y) = y^6 + y^5 + f_1(x)y^4 + y^3 + f_2(x)y^2 + f_3(x)y,$

  $k = 3$, $deg(f_1) = 1$ and
  - $f_1(x) = 0,$
$f_2(x) = g(x+u_1)(x+u_2)(x+u_3)(x+u_4) + 1,$
$f_3(x) = f_2(x)$, $C = \alpha$, or
  - $f_1(x) = 1,$
$f_2(x) = g(x+u_1)(x+u_2)(x+u_3)(x+u_4),$
$f_3(x) = f_2(x) + 1$, $C = 0$,

  where $\alpha^3 + \alpha + 1$, and $u_i, g \in \mathbb{F}^*_{2^k}$ satisfy

$$\begin{aligned} g(x+u_1)(x+u_2)(x+u_3)(x+u_4) &+ \\ g(x+u_5)(x+u_6)(x+u_7)(x+u_8) &= 1 + C \end{aligned}$$

  for every $x \in \mathbb{F}_{2^k}$.

NTNU
Norwegian University of Science and Technology

$_2$LQPs over $\mathbb{F}_{2^k}$

Case III:

Degree 4 :

$$g(x,y) = ay^4 + cy^3 + f_2(x)y^2 + f_3(x)y$$
$$deg(f_2), deg(f_3) \leq 2$$

Degree 5 :

$$g(x,y) = ay^5 + f_1(x)y^4 + cy^3 + f_2(x)y^2 + f_3(x)y$$
$$deg(f_1) \leq 1, deg(f_2) \leq 2, deg(f_3) \leq 4$$

Degree 6 :

$$g(x,y) = ay^6 + by^5 + f_1(x)y^4 + cy^3 + f_2(x)y^2 + f_3(x)y$$
$$deg(f_1) \leq 2, deg(f_2) \leq 4, deg(f_3) \leq 4$$

NTNU
Norwegian University of Science and Technology

${}_2$LQPs over $\mathbb{F}_{2^k}$

Case III:

Degree 4 :

$$g(x,y) = ay^4 + \cancel{cy^3 +} f_2(x)y^2 + f_3(x)y$$
$$deg(f_2), deg(f_3) \leq 2$$

Degree 5 :

$$g(x,y) = ay^5 + f_1(x)y^4 + \cancel{cy^3 +} f_2(x)y^2 + f_3(x)y$$
$$deg(f_1) \leq 1, deg(f_2) \leq 2, deg(f_3) \leq 4$$

Degree 6 :

$$g(x,y) = ay^6 + by^5 + f_1(x)y^4 + \cancel{cy^3 +} f_2(x)y^2 + f_3(x)y$$
$$deg(f_1) \leq 2, deg(f_2) \leq 4, deg(f_3) \leq 4$$

$_2$LQPs over $\mathbb{F}_{2^k}$

Case III: f_1, f_2, f_3 - linearized polynomials
$deg(f_1) \leq 2, deg(f_2) \leq 4, deg(f_3) \leq 4$

$$g(x,y) = f_1(x)y^4 + f_2(x)y^2 + f_3(x)y$$

$g(x,y)$ is a $_2$LQP iff $\dfrac{g(x,y)}{y}$ has no roots in $\mathbb{F}_{2^k}$, $\forall x \in \mathbb{F}_{2^k}$.

- Hard to characterize
- Many open questions

- Some necessary conditions
- Sieving approach
- Some classes excluded
- Small fields feasible

NTNU
Norwegian University of Science and Technology

${}_2$LQPs over $\mathbb{F}_{2^k}$

Case III: f_1, f_2, f_3 - linearized polynomials
$deg(f_1) \leq 2, deg(f_2) \leq 4, deg(f_3) \leq 4$

$$g(x,y) = f_1(x)y^4 + f_2(x)y^2 + f_3(x)y$$

$g(x,y)$ is a ${}_2$LQP iff $\dfrac{g(x,y)}{y}$ has no roots in $\mathbb{F}_{2^k}$, $\forall x \in \mathbb{F}_{2^k}$.

- Hard to characterize
- Many open questions

- Some necessary conditions
- Sieving approach
- Some classes excluded
- Small fields feasible

NTNU
Norwegian University of
Science and Technology

${}_2$LQPs over $\mathbb{F}_{2^k}$

Case III: f_1, f_2, f_3 - linearized polynomials
$deg(f_1) \leq 2, deg(f_2) \leq 4, deg(f_3) \leq 4$

$$g(x,y) = f_1(x)y^4 + f_2(x)y^2 + f_3(x)y$$

$g(x,y)$ is a ${}_2$LQP iff $\dfrac{g(x,y)}{y}$ has no roots in $\mathbb{F}_{2^k}$, $\forall x \in \mathbb{F}_{2^k}$.

- Hard to characterize
- Many open questions

- Some necessary conditions
- Sieving approach
- Some classes excluded
- Small fields feasible

${}_2$LQPs over $\mathbb{F}_{2^k}$

Sieving condition 1

Let
$$g(x,y) = f_1(x)y^4 + f_2(x)y^2 + f_3(x)y$$
be an ${}_2$LQP. Then the following holds:

k - odd

If for a given $i \in \{1,2,3\}$, $f_i(u) = 0$, $u \in \mathbb{F}_{2^k}$
then $f_j(u) = 0$ for exactly one $j \in \{1,2,3\} \setminus \{i\}$

k - even

$$\begin{aligned} f_1(u) = 0 &\quad \Rightarrow \quad (f_2(u) = 0 \veebar f_3(u) = 0) \\ f_3(u) = 0 &\quad \Rightarrow \quad (f_1(u) = 0 \veebar f_2(u) = 0) \\ f_2(u) = 0 &\quad \Rightarrow \quad (f_1(u) = 0 \veebar f_3(u) = 0) \veebar \frac{f_3(u)}{f_1(u)} \text{ is non} - \text{cube} \end{aligned}$$

Bluher polynomials

Gao & Mullen, Dobbertin,
Bluher, Helleseth & Kholosha, Charpin et al....

$$P_a(x) = D_3(x) + a, \quad a \in \mathbb{F}_{2^k}^*$$

- Conditions for number of roots

Bluher polynomials

Gao & Mullen, Dobbertin,
Bluher, Helleseth & Kholosha, Charpin et al....

$$P_a(x) = x^3 + x + a, \quad a \in \mathbb{F}_{2^k}^*$$

- Conditions for number of roots

NTNU
Norwegian University of Science and Technology

Bluher polynomials

Gao & Mullen, Dobbertin,
Bluher, Helleseth & Kholosha, Charpin et al....

$$P_a(x) = x^3 + x + a, \quad a \in \mathbb{F}_{2^k}^*$$

- Conditions for number of roots

Bluher polynomials

Gao & Mullen, Dobbertin,
Bluher, Helleseth & Kholosha, Charpin et al....

$$P_a(x) = x^3 + x + a, \quad a \in \mathbb{F}_{2^k}^*$$

- Conditions for number of roots

M_i - the number of a s.t. $P_a(x)$ has i roots.

- k - odd: $M_0 = \dfrac{2^k+1}{3}, \; M_1 = 2^{k-1} - 1, \; M_3 = \dfrac{2^{k-1}-1}{3}$
- k - even: $M_0 = \dfrac{2^k-1}{3}, \; M_1 = 2^{k-1}, \; M_3 = \dfrac{2^{k-1}-2}{3}$

Bluher polynomials

Gao & Mullen, Dobbertin,
Bluher, Helleseth & Kholosha, Charpin et al....

$$P_a(x) = x^3 + x + a, \quad a \in \mathbb{F}_{2^k}^*$$

- Conditions for number of roots
- $P_a(x)$ has exactly one root iff $Tr(a^{-1} + 1) = 1$
- $P_a(x)$ is irreducible iff:
  - k - even: $a = \xi + \xi^{-1}$, where ξ is a non-cube in $\mathbb{F}_{2^k}$
  - k - odd: $a = \xi^{\frac{2^k-1}{2}} + \xi^{-\frac{2^k-1}{2}}$, where ξ is a non-cube in $\mathbb{F}_{2^{2k}}$

NTNU
Norwegian University of Science and Technology

${}_2$LQPs over $\mathbb{F}_{2^k}$

$$g(x,y) = f_1(x)y^4 + f_2(x)y^2 + f_3(x)y$$

Let $R = \{x \in \mathbb{F}_{2^k} | f_1(x) \neq 0, f_2(x) \neq 0, f_3(x) \neq 0\}$

- Sieving condition 1 for $x \in \mathbb{F}_{2^k} \setminus R$
- For $x \in R$,

  $h_R(x,y) = \dfrac{g(x,y)}{y}|_R$ has no roots in $\mathbb{F}_{2^k}$, $\forall x \in R$ iff

$$P_R(x,y) = y^3 + y + \frac{f_3(x)(f_1(x))^{1/2}}{(f_2(x))^{3/2}}$$

has no roots in $\mathbb{F}_{2^k}$, $\forall x \in R$.

NTNU
Norwegian University of Science and Technology

${}_2$LQPs over $\mathbb{F}_{2^k}$

Reduce the problem to:

Find properties of the value set of $\dfrac{f_1(x)(f_3(x))^2}{(f_2(x))^3}$ for $x \in R$

- In general, not an easy task
- **Sieving conditions:**
  - If $|VS(\dfrac{f_1(x)(f_3(x))^2}{(f_2(x))^3})| \geq M_0$, $g(x,y)$ is not an ${}_2$LQP.
  - If $\exists x_0 \in R,$ s.t. $Tr(\dfrac{(f_2(x_0))^3}{f_1(x_0)(f_3(x_0))^2} + 1) = 1,$ $g(x,y)$ is not a ${}_2$LQP.

NTNU
Norwegian University of Science and Technology

${}_2$LQPs over $\mathbb{F}_{2^k}$

Reduce the problem to:

Find properties of the value set of $\dfrac{f_1(x)(f_3(x))^2}{(f_2(x))^3}$ for $x \in R$

- In general, not an easy task
- **Sieving conditions:**
  - If $|VS(\frac{f_1(x)(f_3(x))^2}{(f_2(x))^3})| \geq M_0$, $g(x,y)$ is not an ${}_2$LQP.
  - If $\exists x_0 \in R,$ s.t. $Tr(\frac{(f_2(x_0))^3}{f_1(x_0)(f_3(x_0))^2} + 1) = 1,$ $g(x,y)$ is not a ${}_2$LQP.

NTNU
Norwegian University of Science and Technology

Benefits from the sieving conditions

k - odd:

Degree 4: There are no ${}_2$LQPs for Case III, except possibly when f_2, f_3 are irreducible of degree 2.

- open for f_2, f_3 - irreducible
- Conjecture: There are no ${}_2$LQPs of degree 4 for Case III ???
- Checked for small values of k

Degree 5: 12 different possible types for g.

- for k=3, 7 of them are ${}_2$LQPs

Degree 6: 34 different possible types for g.

- for k=3, 27 of them are ${}_2$LQPs

NTNU
Norwegian University of Science and Technology

Benefits from the sieving conditions

k - odd:

Degree 4: There are no $_2$LQPs for Case III, except possibly when f_2, f_3 are irreducible of degree 2.

- open for f_2, f_3 - irreducible
- Conjecture: There are no $_2$LQPs of degree 4 for Case III ???
- Checked for small values of k

Degree 5: 12 different possible types for g.

- for k=3, 7 of them are $_2$LQPs

Degree 6: 34 different possible types for g.

- for k=3, 27 of them are $_2$LQPs

NTNU
Norwegian University of Science and Technology

Characterization of ${}_2$LQPs for $k=3$

Sieving conditions + Hermite criterion $\Rightarrow$ All ${}_2$LQPs of $Deg \leq 6$

Degree 5:

$g(x,y)$ defines an ${}_2$LQP only if it is one of:

- f_1, f_2 - const., $deg(f_3)=4,\ f_3$ has no roots
- f_1 - const., $f_2(x)=x(x+u),\ f_3(x)=t(f_2(x))^2$
- f_1 - const., $f_2(x)=x(x+u),\ f_3(x)=f_2(x)f_3'(x)$, $deg(f_3')=2,\ f_3'$ has no roots
- f_1 - const., $deg(f_2)=2,\ deg(f_3)=4,\ f_2, f_3$ have no roots
- $f_1(x)=x,\ f_2(x)=t_1(x+u),\ f_3(x)=t_2(f_1(x)f_2(x))^2$
- $f_1(x)=x,\ f_2(x)=t_1x(x+u),\ f_3(x)=t(x+u)^2$
- $f_1(x)=x,\ f_2(x)=t_1(x+u)^2,\ f_3(x)=tx(x+u)f_3'(x)$, $deg(f_3')=2,\ f_3'$ has no roots

Characterization of ${}_2$LQPs for $k = 3$

Degree 6:

$g(x,y)$ defines an ${}_2$LQP only if it is one of:

- f_1, f_3 - const., $deg(f_2) = 4$, f_2 has no roots
- f_1 - const., $f_2(x) = x(x+u)f_2'(x)$, $f_3(x) = tx(x+u)f_3'(x)$, $deg(f_2') = 2, deg(f_3') = 2$, f_2', f_3' have no roots
- f_1 - const., $deg(f_2) = 4$, $deg(f_3) = 2, 4$, f_2, f_3 have no roots
- f_1 - const., $f_2(x) = x(x+u)f_2'(x)$, $f_3(x) = tx(x+u)$, $deg(f_2') = 4$, f_3' has no roots
- f_1 - const., $f_2(x) = x(x+u)f_2'(x)$, $f_3(x) = t(x(x+u))^2$, $deg(f_2') = 4$, f_2' has no roots
- f_1 - const., $f_2(x) = (x(x+u))^2$, $f_3(x) = tx(x+u)f_3'(x)$, $deg(f_3') = 2$, f_3' has no roots
- f_1 - const., $f_2(x) = x(x+u_1)(x+u_2)(x+u_3)$, $f_3(x) = tf_2(x)$

NTNU
Norwegian University of Science and Technology

Characterization of $_2$LQPs for $k = 3$

Degree 6:

$g(x, y)$ defines an $_2$LQP only if it is one of:

- $f_1(x) = x,\ f_2(x) = t_1(x+u)^4,\ f_3(x) = t_2x(x+u)$
- $f_1(x) = x,\ f_2(x) = t_1x(x+u)f_2'(x),\ f_3(x) = t_2(x+u)^4,$ $deg(f_2') = 2,\ f_2'$ has no roots
- $f_1(x) = x,\ f_2(x) = t_1(x(x+u))^2,\ f_3(x) = t_2(x+u)^4$
- $f_1(x) = x,\ f_2(x) = t_1(x(x+u))^2,\ f_3(x) = t(x+u)$
- $f_1(x) = x,\ f_3(x) = txf_3'(x),\ deg(f_2) = 4,\ deg(f_3') = 3,\ f_2, f_3'$ have no roots
- $f_1(x) = x,\ f_2(x) = txf_2'(x),\ deg(f_2') = 3,\ deg(f_3') = 4,\ f_2, f_3'$ have no roots

$\ldots$ 14 more cases $\ldots$

$\ldots$ and complicated if conditions $\ldots$

NTNU
Norwegian University of Science and Technology

Open questions and future work

- How close can we get to characterisation of ${}_2$LQPs of degree 4, 5, 6, ...?
  - Closer look at the value sets of the possible rational functions
- Complete characterization for degree 4
- k - even
- $k = 3$: More unified look of the long list of cases
- Apply the sieving to bigger fields
  - some tried - not ${}_2$LQPs
  - we expect "less" ${}_2$LQPs
  - feasibility issues

NTNU
Norwegian University of Science and Technology

Open questions and future work

- How close can we get to characterisation of ${}_2$LQPs of degree 4, 5, 6, ...?
  - Closer look at the value sets of the possible rational functions
- Complete characterization for degree 4
- k - even
- $k = 3$: More unified look of the long list of cases
- Apply the sieving to bigger fields
  - some tried - not ${}_2$LQPs
  - we expect “less” ${}_2$LQPs
  - feasibility issues

Thank you for listening!

NTNU
Norwegian University of
Science and Technology