NTNU
Norwegian University of
Science and Technology

Permutation Polynomials and Polynomial Quasigroups defined over $\mathbb{Z}_{p^w}$

Simona Samardjiska

Department of Telematics, NTNU, Norway
simonas@item.ntnu.no

University of Oulu, 14.11.2011

Introduction

Permutation polynomial

- $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ over a finite ring $(R, +, \cdot)$ is a *permutation polynomial* if P permutes the elements of R.

Polynomial binary quasigroup

- (Q, q) can be represented as a polynomial $P(x, y)$ over a finite ring $(Q, +, \cdot)$ such that

$$q(x, y) = P(x, y) \text{ for every } x, y \in Q.$$

Most interesting case - when the ring is $(\mathbb{Z}_{2^w}, +, \cdot)$, w - positive integer.

Introduction

Permutation polynomial

- $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ over a finite ring $(R, +, \cdot)$ is a *permutation polynomial* if P permutes the elements of R.

Polynomial binary quasigroup

- (Q, q) can be represented as a polynomial $P(x, y)$ over a finite ring $(Q, +, \cdot)$ such that

$$q(x, y) = P(x, y) \quad \text{for every } x, y \in Q.$$

Most interesting case - when the ring is $(\mathbb{Z}_{2^w}, +, \cdot)$, w - positive integer.

NTNU
Norwegian University of Science and Technology

Introduction

Permutation polynomial

- $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ over a finite ring $(R, +, \cdot)$ is a *permutation polynomial* if P permutes the elements of R.

Polynomial binary quasigroup

- (Q, q) can be represented as a polynomial $P(x, y)$ over a finite ring $(Q, +, \cdot)$ such that

$$q(x, y) = P(x, y) \quad \text{for every } x, y \in Q.$$

Most interesting case - when the ring is $(\mathbb{Z}_{2^w}, +, \cdot)$, w - positive integer.

NTNU
Norwegian University of Science and Technology

Rivest - simple criteria for permutation polynomials and binary polynomial quasigroups

$P(x) = a_0 + a_1x + \cdots + a_dx^d$ - with integral coefficients is a permutation polynomial modulo 2^w, $w \geq 2$, if and only if a_1 - odd, $(a_2 + a_4 + a_6 + \ldots)$ - even, $(a_3 + a_5 + a_7 + \ldots)$ - even.

$P(x, y)$, represents a quasigroup operation in $\mathbb{Z}_{2^w}$, $w \geq 2$, if and only if the four univariate polynomials

$$P(x, 0),\ P(x, 1),\ P(0, y) \text{ and } P(1, y),$$

are all permutation polynomials in $\mathbb{Z}_{2^w}$.

NTNU
Norwegian University of Science and Technology

Rivest - simple criteria for permutation polynomials and binary polynomial quasigroups

$P(x) = a_0 + a_1 x + \dots + a_d x^d$ - with integral coefficients is a permutation polynomial modulo 2^w, $w \geq 2$, if and only if a_1 - odd, $(a_2 + a_4 + a_6 + \dots)$ - even, $(a_3 + a_5 + a_7 + \dots)$ - even.

$P(x, y)$, represents a quasigroup operation in $\mathbb{Z}_{2^w}$, $w \geq 2$, if and only if the four univariate polynomials

$$P(x,0),\ P(x,1),\ P(0,y) \text{ and } P(1,y),$$

are all permutation polynomials in $\mathbb{Z}_{2^w}$.

Permutation Polynomials, Polynomial Quasigroups

- We have a complete characterization,
- A rather simple one!

Several important questions about polynomial quasigroups:

- What is the simplest form?
- How many are there?
- Can we distinguish some special properties?
- What about n-ary polynomial quasigroups? Over different finite rings?
- What is the relation to other quasigroups of order 2^w?

NTNU
Norwegian University of Science and Technology

Permutation Polynomials, Polynomial Quasigroups

- We have a complete characterization,
- A rather simple one!

Several important questions about polynomial quasigroups:

- What is the simplest form?
- How many are there?
- Can we distinguish some special properties?
- What about n-ary polynomial quasigroups? Over different finite rings?
- What is the relation to other quasigroups of order 2^w?

Polynomials and Polynomial Functions over $\mathbb{Z}_{p^w}$

$G_d(\mathbb{Z}_{p^w})$ - the set of all d-ary polynomial functions over $\mathbb{Z}_{p^w}$
$f \in G_d(\mathbb{Z}_{p^w})$, $f : \mathbb{Z}_{p^w}^d \to \mathbb{Z}_{p^w}$ - a polynomial function

$$f(\boldsymbol{x}) \equiv p_1(\boldsymbol{x}) \pmod{n}, \quad \forall \boldsymbol{x} = (x_1, \dots x_d) \in \mathbb{Z}_{p^w}^d,$$
$$f(\boldsymbol{x}) \equiv p_2(\boldsymbol{x}) \pmod{n}, \quad \forall \boldsymbol{x} = (x_1, \dots x_d) \in \mathbb{Z}_{p^w}^d,$$
$$f(\boldsymbol{x}) \equiv p_3(\boldsymbol{x}) \pmod{n}, \quad \forall \boldsymbol{x} = (x_1, \dots x_d) \in \mathbb{Z}_{p^w}^d,$$
$$\dots$$

We need the simplest,
canonical form of the polynomial function f.

Polynomials and Polynomial Functions over $\mathbb{Z}_{p^w}$

$G_d(\mathbb{Z}_{p^w})$ - the set of all d-ary polynomial functions over $\mathbb{Z}_{p^w}$
$f \in G_d(\mathbb{Z}_{p^w})$, $f : \mathbb{Z}_{p^w}^d \to \mathbb{Z}_{p^w}$ - a polynomial function

$$
\begin{aligned}
f(\boldsymbol{x}) &\equiv p_1(\boldsymbol{x}) \pmod{n}, \quad \forall \boldsymbol{x} = (x_1, \ldots x_d) \in \mathbb{Z}_{p^w}^d, \\
f(\boldsymbol{x}) &\equiv p_2(\boldsymbol{x}) \pmod{n}, \quad \forall \boldsymbol{x} = (x_1, \ldots x_d) \in \mathbb{Z}_{p^w}^d, \\
f(\boldsymbol{x}) &\equiv p_3(\boldsymbol{x}) \pmod{n}, \quad \forall \boldsymbol{x} = (x_1, \ldots x_d) \in \mathbb{Z}_{p^w}^d, \\
&\ldots
\end{aligned}
$$

We need the simplest,
canonical form of the polynomial function f.

Polynomials and Polynomial Functions over $\mathbb{Z}_{p^w}$

$G_d(\mathbb{Z}_{p^w})$ - the set of all d-ary polynomial functions over $\mathbb{Z}_{p^w}$
$f \in G_d(\mathbb{Z}_{p^w})$, $f : \mathbb{Z}_{p^w}^d \to \mathbb{Z}_{p^w}$ - a polynomial function

$$
\begin{aligned}
f(\boldsymbol{x}) &\equiv p_1(\boldsymbol{x}) \pmod n, \quad \forall \boldsymbol{x} = (x_1, \ldots x_d) \in \mathbb{Z}_{p^w}^d, \\
f(\boldsymbol{x}) &\equiv p_2(\boldsymbol{x}) \pmod n, \quad \forall \boldsymbol{x} = (x_1, \ldots x_d) \in \mathbb{Z}_{p^w}^d, \\
f(\boldsymbol{x}) &\equiv p_3(\boldsymbol{x}) \pmod n, \quad \forall \boldsymbol{x} = (x_1, \ldots x_d) \in \mathbb{Z}_{p^w}^d, \\
&\ldots
\end{aligned}
$$

We need the simplest,
canonical form of the polynomial function f.

NTNU
Norwegian University of Science and Technology

Polynomials and Polynomial Functions over $\mathbb{Z}_{p^w}$

$G_d(\mathbb{Z}_{p^w})$ - the set of all d-ary polynomial functions over $\mathbb{Z}_{p^w}$
$f \in G_d(\mathbb{Z}_{p^w})$, $f : \mathbb{Z}_{p^w}^d \rightarrow \mathbb{Z}_{p^w}$ - a polynomial function

$$\begin{aligned} f(\boldsymbol{x}) &\equiv p_1(\boldsymbol{x}) \pmod{n}, \quad \forall \boldsymbol{x} = (x_1, \ldots x_d) \in \mathbb{Z}_{p^w}^d, \\ f(\boldsymbol{x}) &\equiv p_2(\boldsymbol{x}) \pmod{n}, \quad \forall \boldsymbol{x} = (x_1, \ldots x_d) \in \mathbb{Z}_{p^w}^d, \\ f(\boldsymbol{x}) &\equiv p_3(\boldsymbol{x}) \pmod{n}, \quad \forall \boldsymbol{x} = (x_1, \ldots x_d) \in \mathbb{Z}_{p^w}^d, \\ &\ldots \end{aligned}$$

We need the simplest,
canonical form of the polynomial function f.

Canonical form of a polynomial function

Theorem (Hungerbuhler and Specker)

Let $\boldsymbol{x}^{\boldsymbol{k}} = \prod_{i=1}^{d} x_i^{k_i}$, $\boldsymbol{k!} = \prod_{i=1}^{d} k_i!$, and

$$\nu_p(\boldsymbol{k!}) = max\left\{x \in \mathbb{N}_0 : p^x \mid \boldsymbol{k!}\right\}$$

Then every polynomial function $f \in G_d(\mathbb{Z}_{p^w})$ has a unique representation of the form

$$f(\boldsymbol{x}) \equiv \sum_{\substack{\boldsymbol{k} \in \mathbb{N}_0^d \\ \nu_p(\boldsymbol{k!}) < w}} \alpha_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}},$$

where $\alpha_{\boldsymbol{k}} \in \left\{0, 1, \ldots, p^{w-\nu_p(\boldsymbol{k!})} - 1\right\}$.

Number of polynomial functions (H. & S.)

$G_d(\mathbb{Z}_{p^w})$ - the set of all d-ary polynomial functions over $\mathbb{Z}_{p^w}$

$$|G_d(\mathbb{Z}_{p^w})| = exp_p\left(\sum_{\substack{\boldsymbol{k} \in \mathbb{N}_0^d \\ \nu_p(\boldsymbol{k}!) < w}} (w - \nu_p(\boldsymbol{k}!))\right)$$

Number of permutation polynomials over $\mathbb{Z}_{2^w}$

$PP(\mathbb{Z}_{p^w})$ - the set of all permutations over $\mathbb{Z}_{p^w}$

$$|PP(\mathbb{Z}_{2^w})| = \frac{|G(\mathbb{Z}_{2^w})|}{2^3}$$

NTNU
Norwegian University of Science and Technology

Number of polynomial functions (H. & S.)

$G_d(\mathbb{Z}_{p^w})$ - the set of all d-ary polynomial functions over $\mathbb{Z}_{p^w}$

$$|G_d(\mathbb{Z}_{p^w})| = exp_p\Big(\sum_{\substack{\boldsymbol{k} \in \mathbb{N}_0^d \\ \nu_p(\boldsymbol{k}!) < w}} (w - \nu_p(\boldsymbol{k}!))\Big)$$

Number of permutation polynomials over $\mathbb{Z}_{2^w}$

$PP(\mathbb{Z}_{p^w})$ - the set of all permutations over $\mathbb{Z}_{p^w}$

$$|PP(\mathbb{Z}_{2^w})| = \frac{|G(\mathbb{Z}_{2^w})|}{2^3}$$

NTNU
Norwegian University of
Science and Technology

Example: $|PP(\mathbb{Z}_8)| = 2^7$

x	$3x$	$5x$	$7x$
$x+2x^2$	$3x+2x^2$	$5x+2x^2$	$7x+2x^2$
$x+2x^3$	$3x+2x^3$	$5x+2x^3$	$7x+2x^3$
$x+2x^2+2x^3$	$3x+2x^2+2x^3$	$5x+2x^2+2x^3$	$7x+2x^2+2x^3$
$1+x$	$1+3x$	$1+5x$	$1+7x$
$1+x+2x^2$	$1+3x+2x^2$	$1+5x+2x^2$	$1+7x+2x^2$
$1+x+2x^3$	$1+3x+2x^3$	$1+5x+2x^3$	$1+7x+2x^3$
$1+x+2x^2+2x^3$	$1+3x+2x^2+2x^3$	$1+5x+2x^2+2x^3$	$1+7x+2x^2+2x^3$
$2+x$	$2+3x$	$2+5x$	$2+7x$
$2+x+2x^2$	$2+3x+2x^2$	$2+5x+2x^2$	$2+7x+2x^2$
$2+x+2x^3$	$2+3x+2x^3$	$2+5x+2x^3$	$2+7x+2x^3$
$2+x+2x^2+2x^3$	$2+3x+2x^2+2x^3$	$2+5x+2x^2+2x^3$	$2+7x+2x^2+2x^3$
$\dots$			
$7+x$	$7+3x$	$7+5x$	$7+7x$
$7+x+2x^2$	$7+3x+2x^2$	$7+5x+2x^2$	$7+7x+2x^2$
$7+x+2x^3$	$7+3x+2x^3$	$7+5x+2x^3$	$7+7x+2x^3$
$7+x+2x^2+2x^3$	$7+3x+2x^2+2x^3$	$7+5x+2x^2+2x^3$	$7+7x+2x^2+2x^3$

Number of polynomial quasigroups of order 2^w (S.'09)

$PQ(\mathbb{Z}_{p^w})$ - the set of all polynomial quasigroups of order 2^w

$$|PQ(\mathbb{Z}_{2^w})| = \frac{|G_2(\mathbb{Z}_{2^w})|}{2^{11}} = \Bigg(\prod_{\substack{\langle k_1,k_2\rangle\in\mathbb{N}_0^2 \\ \nu_2(k_1!\,k_2!)<w}} 2^{w-\nu_2(k_1!\,k_2!)} \Bigg) \cdot 2^{-11}$$

$\mathbb{Z}_{2^w}$	$\mathbb{Z}_2$	$\mathbb{Z}_{2^2}$	$\mathbb{Z}_{2^3}$	$\mathbb{Z}_{2^4}$	$\mathbb{Z}_{2^5}$	$\mathbb{Z}_{2^6}$	$\mathbb{Z}_{2^7}$	$\mathbb{Z}_{2^8}$
$\|PQ(\mathbb{Z}_{2^w})\|$	2	2^5	2^{21}	2^{45}	2^{84}	2^{132}	2^{185}	2^{252}

$\mathbb{Z}_{2^w}$	$\mathbb{Z}_{2^9}$	$\mathbb{Z}_{2^{10}}$	$\mathbb{Z}_{2^{11}}$	$\mathbb{Z}_{2^{12}}$	$\mathbb{Z}_{2^{13}}$	$\mathbb{Z}_{2^{14}}$	$\mathbb{Z}_{2^{15}}$	...
$\|PQ(\mathbb{Z}_{2^w})\|$	2^{341}	2^{437}	2^{549}	2^{692}	2^{852}	2^{1020}	2^{1209}	...

NTNU
Norwegian University of Science and Technology

Example $|PQ(\mathbb{Z}_{2^2})| = 2^5$.

$$\begin{array}{rcccccccccc} q(x,y) & = & \alpha_{00} & + & \alpha_{01}\,y & + & \alpha_{02}\,y^2 & + & \alpha_{03}\,y^3 & + \\ & + & \alpha_{10}\,x & + & \alpha_{11}\,xy & + & \alpha_{12}\,xy^2 & + & \alpha_{13}\,xy^3 & + \\ & + & \alpha_{20}\,x^2 & + & \alpha_{21}\,x^2y & + & & & & \\ & + & \alpha_{30}\,x^3 & + & \alpha_{31}\,x^3y & & & & & \end{array}$$

$$\alpha_{k_1,k_2} \in \left\{0, 1, \ldots, 2^{2-\nu_2(k_1!\,k_2!)} - 1\right\}.$$

coef.	possibilities	coef.	possibilities
α_{00}	$2^{2-\nu_2(0!\,0!)}$	α_{01}	$2^{2-\nu_2(0!\,1!)-1}$
α_{10}	$2^{2-\nu_2(1!\,0!)-1}$	α_{02}	$2^{2-\nu_2(0!\,2!)-1}$
α_{20}	$2^{2-\nu_2(2!\,0!)-1}$	α_{03}	$2^{2-\nu_2(0!\,3!)-1}$
α_{30}	$2^{2-\nu_2(3!\,0!)-1}$	α_{11}	$2^{2-\nu_2(1!\,1!)-1}$
α_{12}	$2^{2-\nu_2(1!\,2!)-1}$	α_{21}	$2^{2-\nu_2(2!\,1!)-1}$
α_{13}	$2^{2-\nu_2(1!\,3!)-1}$	α_{31}	$2^{2-\nu_2(3!\,1!)-1}$

Parastrophe operations of quasigroups

For a permutation $\sigma \in \mathcal{S}_3$, and a binary quasigroup (Q, q), the operation ${}^{\sigma}q$ defined by

$$ {}^{\sigma}q(x_{\sigma(1)}, x_{\sigma(2)}) = x_{\sigma(3)} \quad \Leftrightarrow \quad q(x_1, x_2) = x_3, $$

is called a σ- parastrophe of the quasigroup (Q, q).

- Each of the parastrophes ${}^{\sigma}q$ also defines a binary quasigroup $(Q, {}^{\sigma}q)$.
- Notations: q by "$*$", ${}^{(13)}q$ by "$/$", and ${}^{(23)}q$ by "$\backslash$".

Parastrophe operations of quasigroups

For a permutation $\sigma \in \mathcal{S}_3$, and a binary quasigroup (Q, q), the operation ${}^{\sigma}q$ defined by

$$ {}^{\sigma}q(x_{\sigma(1)}, x_{\sigma(2)}) = x_{\sigma(3)} \quad \Leftrightarrow \quad q(x_1, x_2) = x_3, $$

is called a σ- parastrophe of the quasigroup (Q, q).

- Each of the parastrophes ${}^{\sigma}q$ also defines a binary quasigroup $(Q, {}^{\sigma}q)$.
- Notations: q by "$*$", ${}^{(13)}q$ by "$/$", and ${}^{(23)}q$ by "$\backslash$".

NTNU
Norwegian University of Science and Technology

(Q, q) - binary polynomial quasigroup.

Are the parastrophes polynomial?

If there is a polynomial that defines $(Q, {}^{(23)}q)$, then all the parastrophes are polynomial as well, since:

$$\begin{aligned} {}^{(12)}q(x_1, x_2) &= q(x_2, x_1), \\ {}^{(123)}q(x_1, x_2) &= {}^{(12)}({}^{(13)}q)(x_1, x_2), \\ {}^{(132)}q(x_1, x_2) &= {}^{(12)}({}^{(23)}q)(x_1, x_2), \\ {}^{(13)}q(x_1, x_2) &= {}^{(23)}({}^{(12)}({}^{(23)}q))(x_1, x_2). \end{aligned}$$

Focus on ${}^{(23)}q$ ("\").

NTNU
Norwegian University of Science and Technology

(Q, q) - binary polynomial quasigroup.

Are the parastrophes polynomial?

If there is a polynomial that defines $(Q, {}^{(23)}q)$, then all the parastrophes are polynomial as well, since:

$$\begin{aligned} {}^{(12)}q(x_1, x_2) &= q(x_2, x_1), \\ {}^{(123)}q(x_1, x_2) &= {}^{(12)}({}^{(13)}q)(x_1, x_2), \\ {}^{(132)}q(x_1, x_2) &= {}^{(12)}({}^{(23)}q)(x_1, x_2), \\ {}^{(13)}q(x_1, x_2) &= {}^{(23)}({}^{(12)}({}^{(23)}q))(x_1, x_2). \end{aligned}$$

Focus on ${}^{(23)}q$ ("\").

NTNU
Norwegian University of Science and Technology

The parastrophes are polynomial! (S.'10)

$q_1, q_2 \in \mathcal{Q}_n$ - set of all left quasigroup operations over the set Q of n elements.

$$(q_1 \circ q_2)(x, y) = q_1(x, q_2(x, y))$$

Theorem (Norton): $(\mathcal{Q}_n, \circ)$ is a group of order $(n!)^n$.

- $e(x, y) = y$ - the identity element.
- q^{-1} is defined by: $q^{-1}(x, y) = z \Leftrightarrow q(x, z) = y$.

- For every polynomial quasigroup (Q, q), $q \in \mathcal{Q}_n$.
- $q^{-1} = \backslash = q^{r-1}$
- **Corollary:** $(Q, \backslash)$ is polynomial!

NTNU
Norwegian University of Science and Technology

The parastrophes are polynomial! (S.'10)

$q_1, q_2 \in \mathcal{Q}_n$ - set of all left quasigroup operations over the set Q of n elements.

$$(q_1 \circ q_2)(x, y) = q_1(x, q_2(x, y))$$

Theorem (Norton): $(\mathcal{Q}_n, \circ)$ is a group of order $(n!)^n$.

- $e(x, y) = y$ - the identity element.
- q^{-1} is defined by: $q^{-1}(x, y) = z \Leftrightarrow q(x, z) = y$.

- For every polynomial quasigroup (Q, q), $q \in \mathcal{Q}_n$.
- $q^{-1} = \backslash = q^{r-1}$
- **Corollary:** $(Q, \backslash)$ is polynomial!

NTNU
Norwegian University of Science and Technology

The parastrophes are polynomial! (S.'10)

$q_1, q_2 \in \mathcal{Q}_n$ - set of all left quasigroup operations over the set Q of n elements.

$$(q_1 \circ q_2)(x, y) = q_1(x, q_2(x, y))$$

Theorem (Norton): $(\mathcal{Q}_n, \circ)$ is a group of order $(n!)^n$.

- $e(x, y) = y$ - the identity element.
- q^{-1} is defined by: $q^{-1}(x, y) = z \iff q(x, z) = y$.

- For every polynomial quasigroup (Q, q), $q \in \mathcal{Q}_n$.
- $q^{-1} = \backslash = q^{r-1}$
- **Corollary:** $(Q, \backslash)$ is polynomial!

The parastrophes are polynomial! (S.'10)

$q_1, q_2 \in \mathcal{Q}_n$ - set of all left quasigroup operations over the set Q of n elements.

$$(q_1 \circ q_2)(x, y) = q_1(x, q_2(x, y))$$

Theorem (Norton): $(\mathcal{Q}_n, \circ)$ is a group of order $(n!)^n$.

- $e(x, y) = y$ - the identity element.
- q^{-1} is defined by: $q^{-1}(x, y) = z \ \Leftrightarrow \ q(x, z) = y$.

- For every polynomial quasigroup (Q, q), $q \in \mathcal{Q}_n$.
- $q^{-1} = \backslash = q^{r-1}$
- **Corollary:** $(Q, \backslash)$ is polynomial!

NTNU
Norwegian University of Science and Technology

The parastrophes are polynomial! (S.'10)

$q_1, q_2 \in \mathcal{Q}_n$ - set of all left quasigroup operations over the set Q of n elements.

$$(q_1 \circ q_2)(x, y) = q_1(x, q_2(x, y))$$

Theorem (Norton): $(\mathcal{Q}_n, \circ)$ is a group of order $(n!)^n$.

- $e(x, y) = y$ - the identity element.
- q^{-1} is defined by: $q^{-1}(x, y) = z \;\Leftrightarrow\; q(x, z) = y$.

- For every polynomial quasigroup (Q, q), $q \in \mathcal{Q}_n$.
- $q^{-1} = \backslash = q^{r-1}$
- **Corollary:** $(Q, \backslash)$ is polynomial!

NTNU
Norwegian University of Science and Technology

The parastrophes are polynomial! (S.'10)

$q_1, q_2 \in \mathcal{Q}_n$ - set of all left quasigroup operations over the set Q of n elements.

$$(q_1 \circ q_2)(x, y) = q_1(x, q_2(x, y))$$

Theorem (Norton): $(\mathcal{Q}_n, \circ)$ is a group of order $(n!)^n$.

- $e(x, y) = y$ - the identity element.
- q^{-1} is defined by: $q^{-1}(x, y) = z \;\Leftrightarrow\; q(x, z) = y$.

- For every polynomial quasigroup (Q, q), $q \in \mathcal{Q}_n$.
- $q^{-1} = \backslash = q^{r-1}$
- **Corollary:** $(Q, \backslash)$ is polynomial!

Some properties:

- Very structured!
  - Property of being a polynomial over $\mathbb{Z}_{2^w}$

$$P(x, y + l2^m) \equiv P(x, y) \pmod{2^m},$$
$$P(x + l2^m, y) \equiv P(x, y) \pmod{2^m}.$$

- Orthogonality:
  - (Rivest) No pairs of orthogonal polynom. quasigroups exist
- Unit element:
  - $q(x, y)$ has a unit e iff

$$q(x, y) = q'(x + e, y + e) - e \quad \text{where}$$

$$q'(x, y) \equiv \alpha_{0,0} + x + y + \sum_{\substack{\langle k_1, k_2 \rangle \in \mathbb{N}^2 \\ \nu_2(k_1!\, k_2!) < w}} \alpha_{k_1,k_2} x^{k_1} y^{k_2} \quad \text{is a quasigroup}$$

and $\alpha_{k_1,k_2} \in \left\{0, 1, \ldots, 2^{w-\nu_2(k_1!\, k_2!)} - 1\right\}$.

Some properties:

- Very structured!
  - Property of being a polynomial over $\mathbb{Z}_{2^w}$

$$P(x, y + l2^m) \equiv P(x, y) \pmod{2^m},$$
$$P(x + l2^m, y) \equiv P(x, y) \pmod{2^m}.$$

- Orthogonality:
  - (Rivest) No pairs of orthogonal polynom. quasigroups exist
- Unit element:
  - $q(x, y)$ has a unit e iff

$$q(x, y) = q'(x + e, y + e) - e \quad \text{where}$$

$$q'(x, y) \equiv \alpha_{0,0} + x + y + \sum_{\substack{\langle k_1, k_2 \rangle \in \mathbb{N}^2 \\ \nu_2(k_1!\, k_2!) < w}} \alpha_{k_1,k_2} x^{k_1} y^{k_2} \quad \text{is a quasigroup}$$

and $\alpha_{k_1,k_2} \in \left\{0, 1, \ldots, 2^{w-\nu_2(k_1!\, k_2!)} - 1\right\}$.

NTNU
Norwegian University of Science and Technology

Some properties:

- Very structured!
  - Property of being a polynomial over $\mathbb{Z}_{2^w}$

$$P(x, y + l2^m) \equiv P(x, y) \pmod{2^m},$$
$$P(x + l2^m, y) \equiv P(x, y) \pmod{2^m}.$$

- Orthogonality:
  - (Rivest) No pairs of orthogonal polynom. quasigroups exist

- Unit element:
  - $q(x, y)$ has a unit e iff

$$q(x, y) = q'(x + e, y + e) - e \quad \text{where}$$

$$q'(x, y) \equiv \alpha_{0,0} + x + y + \sum_{\substack{\langle k_1, k_2\rangle \in \mathbb{N}^2 \\ \nu_2(k_1!\, k_2!) < w}} \alpha_{k_1,k_2} x^{k_1} y^{k_2} \quad \text{is a quasigroup}$$

and $\alpha_{k_1,k_2} \in \left\{0, 1, \ldots, 2^{w-\nu_2(k_1!\, k_2!)} - 1\right\}$.

NTNU
Norwegian University of
Science and Technology

Yet to be investigated:

- Associativity: Characterization of polynomial semigroups,
- Polynomial Moufang loops,
- ....

Single Cycle Permutation Polynomials

Characterization (Larin, '02):
A permutation polynomial $P(x) = a_0 + a_1x + \cdots + a_dx^d$ defines a single cycle permutation modulo 2^w, $w \geq 3$, iff

- a_0 - odd,
- $(a_2 + a_4 + a_6 + \dots) + (a_3 + a_5 + a_7 + \dots) + 2a_{1,1} \equiv 0 \pmod 4$,
- $(a_2 + a_4 + a_6 + \dots) + 2a_{2,0} + 2a_{1,1} \equiv 0 \pmod 4$

Interesting:

- possible application for stream ciphers,
- some weaknesses found - linear equations (Wang & Qi),
- What about quasigroups containing single cycle translations???

NTNU
Norwegian University of Science and Technology

Single Cycle Permutation Polynomials

Characterization (Larin, '02):

A permutation polynomial $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ defines a single cycle permutation modulo 2^w, $w \geq 3$, iff

- a_0 - odd,
- $(a_2 + a_4 + a_6 + \dots) + (a_3 + a_5 + a_7 + \dots) + 2a_{1,1} \equiv 0 \pmod 4$,
- $(a_2 + a_4 + a_6 + \dots) + 2a_{2,0} + 2a_{1,1} \equiv 0 \pmod 4$

Interesting:

- possible application for stream ciphers,
- some weaknesses found - linear equations (Wang & Qi),
- What about quasigroups containing single cycle translations???

NTNU
Norwegian University of
Science and Technology

Single Cycle Permutation Polynomials

Characterization (Larin, '02):

A permutation polynomial $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ defines a single cycle permutation modulo 2^w, $w \geq 3$, iff

- a_0 - odd,
- $(a_2 + a_4 + a_6 + \ldots) + (a_3 + a_5 + a_7 + \ldots) + 2a_{1,1} \equiv 0 \pmod 4$,
- $(a_2 + a_4 + a_6 + \ldots) + 2a_{2,0} + 2a_{1,1} \equiv 0 \pmod 4$

Interesting:

- possible application for stream ciphers,
- some weaknesses found - linear equations (Wang & Qi),
- What about quasigroups containing single cycle translations???

Single Cycle Permutation Polynomials

Characterization (Larin, '02):

A permutation polynomial $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ defines a single cycle permutation modulo 2^w, $w \geq 3$, iff

- a_0 - odd,
- $(a_2 + a_4 + a_6 + \dots) + (a_3 + a_5 + a_7 + \dots) + 2a_{1,1} \equiv 0 \pmod 4$,
- $(a_2 + a_4 + a_6 + \dots) + 2a_{2,0} + 2a_{1,1} \equiv 0 \pmod 4$

Interesting:

- possible application for stream ciphers,
- some weaknesses found - linear equations (Wang & Qi),
- What about quasigroups containing single cycle translations???

NTNU
Norwegian University of Science and Technology

Permutation Polynomials over $\mathbb{Z}_{p^w}$

A direct consequence of Theorem 123 from Hardy and Wright's, "An Introduction to the Theory of Numbers"'

Characterization (S.'07):
A polynomial $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ with integral coefficients is a permutation polynomial modulo p^w, p-prime, $w \geq 2$ if and only if:

1. $P(x)$ is a permutation polynomial modulo p, i.e. $\forall i, j \in \mathbb{Z}_p$ and $i \neq j$, $P(j) - P(i) \neq 0 \pmod p$
2. $\forall i \in \mathbb{Z}_p$, $P'(i) = a_1 + 2ia_2 + \cdots + di^{d-1}a_d \neq 0 \pmod p$

NTNU
Norwegian University of Science and Technology

Polynomial n-ary quasigroups

(Q, q) is an n-ary quasigroup if the unary operations

$$q_{a_1,\dots,a_{i-1},a_{i+1},\dots,a_n}(x) = q(a_1,\dots,a_{i-1},x,a_{i+1},\dots,a_n)$$

are permutations on Q.

Generalization of Rivest's result (S.'07):

Let $P(x_1, x_2, \dots, x_n)$ - polynomial over $(\mathbb{Z}_{p^w}, +, \cdot)$, p- prime.
$P(x_1, x_2, \dots, x_n)$ defines an n-ary quasigroup, $n \geq 2$, iff
$\forall\ (a_1, \dots, a_{n-1}) \in \mathbb{Z}_p^{n-1}$

$$P_1(x_1) = P(x_1, a_1, \dots, a_{n-1}),$$
$$P_2(x_2) = P(a_1, x_2, \dots, a_{n-1}),$$
$$\vdots$$
$$P_n(x_n) = P(a_1, \dots, a_{n-1}, x_n).$$

are permutation polynomials over $(\mathbb{Z}_{p^w}, +, \cdot)$.

NTNU
Norwegian University of Science and Technology

Polynomial n-ary quasigroups

(Q, q) is an n-ary quasigroup if the unary operations

$$q_{a_1,\dots,a_{i-1},a_{i+1},\dots,a_n}(x) = q(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$$

are permutations on Q.

Generalization of Rivest's result (S.'07):

Let $P(x_1, x_2, \dots, x_n)$ - polynomial over $(\mathbb{Z}_{p^w}, +, \cdot)$, p- prime. $P(x_1, x_2, \dots, x_n)$ defines an n-ary quasigroup, $n \geq 2$, iff $\forall\ (a_1, \dots, a_{n-1}) \in \mathbb{Z}_p^{n-1}$

$$P_1(x_1) = P(x_1, a_1, \dots, a_{n-1}),$$
$$P_2(x_2) = P(a_1, x_2, \dots, a_{n-1}),$$
$$\vdots$$
$$P_n(x_n) = P(a_1, \dots, a_{n-1}, x_n).$$

are permutation polynomials over $(\mathbb{Z}_{p^w}, +, \cdot)$.

NTNU
Norwegian University of Science and Technology

More applicable Generalizations

- Distinguishing Property:

$$P(x, y + l2^m) \equiv P(x, y) \pmod{2^m},$$
$$P(x + l2^m, y) \equiv P(x, y) \pmod{2^m}.$$

- **Other non-polynomial functions exist with the same property!**

Wider class: T-functions

- Klimov and Shamir
- Anashin - general theory of T-functions using p-adic analysis
  - continuous with respect to p-adic distance

NTNU
Norwegian University of Science and Technology

More applicable Generalizations

- Distinguishing Property:

$$P(x, y + l2^m) \equiv P(x, y) \pmod{2^m},$$
$$P(x + l2^m, y) \equiv P(x, y) \pmod{2^m}.$$

- **Other non-polynomial functions exist with the same property!**

Wider class: T-functions

- Klimov and Shamir
- Anashin - general theory of T-functions using p-adic analysis
  - continuous with respect to p-adic distance

NTNU
Norwegian University of Science and Technology

More applicable Generalizations

- Distinguishing Property:

$$P(x, y + l2^m) \equiv P(x, y) \pmod{2^m},$$
$$P(x + l2^m, y) \equiv P(x, y) \pmod{2^m}.$$

- **Other non-polynomial functions exist with the same property!**

Wider class: T-functions

- Klimov and Shamir
- Anashin - general theory of T-functions using p-adic analysis
  - continuous with respect to p-adic distance

More applicable Generalizations

- Distinguishing Property:

$$P(x, y + l2^m) \equiv P(x, y) \pmod{2^m},$$
$$P(x + l2^m, y) \equiv P(x, y) \pmod{2^m}.$$

- **Other non-polynomial functions exist with the same property!**

Wider class: T-functions

- Klimov and Shamir
- Anashin - general theory of T-functions using p-adic analysis
  - continuous with respect to p-adic distance

NTNU
Norwegian University of Science and Technology

T-Multivariate Permutations (S.'10)

The vector valued Boolean function

$$p = (p^{(1)}, p^{(2)}, \ldots, p^{(w)}) : \mathbb{F}_2^w \to \mathbb{F}_2^w$$

such that $\forall s = 1, \ldots, w$,

$$p^{(s)}(x_1, \ldots, x_w) = x_s + \left(\sum_{j=(j_{s+1},\ldots,j_w)\in\mathbb{F}_2^{w-s}} \alpha_j^{(s)} x_{s+1}^{j_{s+1}} x_{s+2}^{j_{s+2}} \ldots x_w^{j_w} \right),$$

defines a permutation on the set $\mathbb{F}_2^w$.

NTNU
Norwegian University of Science and Technology

T-Multivariate Quasigroups (S.'10)

The vector valued Boolean function

$$q = (q^{(1)}, q^{(2)}, \ldots, q^{(w)}) : \mathbb{F}_2^{2w} \to \mathbb{F}_2^w$$

such that $\forall s = 1, \ldots, w$,

$$q^{(s)}(x_1, \ldots, x_w, y_1, \ldots, y_w) = x_s + y_s +$$
$$+ \left(\sum_{\substack{k=(k_{s+1},\ldots,k_w)\in \mathbb{F}_2^{w-s} \\ j=(j_{s+1},\ldots,j_w)\in \mathbb{F}_2^{w-s}}} \alpha_{k,j}^{(s)} x_{s+1}^{k_{s+1}} x_{s+2}^{k_{s+2}} \ldots x_w^{k_w} y_{s+1}^{j_{s+1}} y_{s+2}^{j_{s+2}} \ldots y_w^{j_w} \right),$$

defines a quasigroup of order 2^w.

NTNU
Norwegian University of Science and Technology

T-Multivariate Quasigroups

Many properties preserved from polynomial quasigroups

- same structure
- no pairs of orthogonal quasigroups
- same condition for loops
- ...

But, can be used

- for creation of new Multivariate Quasigroups
- pairs of orthogonal quasigroups (Klimov, Shamir)

New idea: Left Multivariate Quasigroups

T-Multivariate Quasigroups

Many properties preserved from polynomial quasigroups

- same structure
- no pairs of orthogonal quasigroups
- same condition for loops
- ...

But, can be used

- for creation of new Multivariate Quasigroups
- pairs of orthogonal quasigroups (Klimov, Shamir)

New idea: Left Multivariate Quasigroups

T-Multivariate Quasigroups

Many properties preserved from polynomial quasigroups

- same structure
- no pairs of orthogonal quasigroups
- same condition for loops
- ...

But, can be used

- for creation of new Multivariate Quasigroups
- pairs of orthogonal quasigroups (Klimov, Shamir)

New idea: **Left Multivariate Quasigroups**

Crypto world:

Multivariate Public Key Cryptography

Algorithms based on Multivariate Quadratic Quasigroups (MQQ)

- MQQ PKC (Gligoroski et al. 2008)
- MQQ-sig (Gligoroski et al. 2011)
- MQQ-enc . . . ongoing work . . .
- . . .

Thank you for your attention!