From r-Linearized Polynomial Equations to r^m-Linearized Polynomial Equations

Neranga Fernando

Joint work with Xiang-dong Hou

Department of Mathematics
Northeastern University

Fq12, Saratoga Springs, NY

July 13 - 17 ,2015

Outline

- Introduction
- r-Linearized and r^m-Linearized Equations
- Applications to Permutation Polynomials
  - A Criterion
  - The Polynomial $g_{n,q}$
  - Applications to $g_{n,q}$

Introduction

Let p be a prime and $\mathbb{F}_{q_1}, \mathbb{F}_{q_2} \subset \overline{\mathbb{F}}_p$, where $\overline{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$. A q_1-linearized polynomial over $\mathbb{F}_{q_2}$ is a polynomial of the form

$$f = a_0 \mathtt{X}^{q_1^0} + a_1 \mathtt{X}^{q_1^1} + \cdots + a_n \mathtt{X}^{q_1^n} \in \mathbb{F}_{q_2}[\mathtt{X}].$$

If $f \in \mathbb{F}_{q_2}[\mathtt{X}]$ is q_1-linearized and $g \in \mathbb{F}_{q_1}[\mathtt{X}]$ is q_2-linearized, then $f \circ g = g \circ f$.

Introduction (Contd.)

Let $f = \sum_{i=0}^{n} a_i \mathtt{X}^{q^i} \in \overline{\mathbb{F}}_p[\mathtt{X}]$ be a q-linearized polynomial.

- The conventional associate of f is the polynomial $\widetilde{f} = \sum_{i=0}^{n} a_i x^i \in \overline{\mathbb{F}}_p[\mathtt{X}]$.
- Let $f, g \in \mathbb{F}_q[\mathtt{X}]$ be q-linearized polynomials. Then $\gcd(f, g)$ is a q-linearized polynomial over $\mathbb{F}_q[\mathtt{X}]$ with $\widetilde{\gcd(f, g)} = \gcd(\widetilde{f}, \widetilde{g})$.

Introduction (Contd.)

Let r be a prime power.
Let $\mathbb{F}_r \subset \overline{\mathbb{F}}_p$ and $q = r^m$. Assume that $z \in \overline{\mathbb{F}}_p$ satisfies an equation

$$\sum_{i=0}^{m-1} a_i f_i(z)^{r^i} = 0, \tag{1}$$

where $a_i \in \mathbb{F}_q$ and $f_i \in \mathbb{F}_r[\mathtt{X}]$ is q-linearized.

(1) is an r-linearized equation with coefficients in $\mathbb{F}_q$.

Question: Is it possible to derive from (1) a q-linearized equation with coefficients in $\mathbb{F}_r$?

r-Linearized and r^m-Linearized Equations

Let p be a prime, $\mathbb{F}_r \subset \overline{\mathbb{F}}_p$ and $q = r^m$. Let R_q denote the set of all q-linearized polynomials over $\mathbb{F}_q$.

Assume that for $0 \le i \le m-1$, $a_i \in \mathbb{F}_q$ and $f_i \in \mathbb{F}_r[\mathtt{X}]$ is q-linearized.

Define

$$M = \begin{bmatrix} a_0 f_0 & a_1 f_1 & \cdots & a_{m-1} f_{m-1} \\ a_{m-1}^r f_{m-1} \circ \mathtt{X}^q & a_0^r f_0 & \cdots & a_{m-2}^r f_{m-2} \\ \vdots & \vdots & & \vdots \\ a_1^{r^{m-1}} f_1 \circ \mathtt{X}^q & a_2^{r^{m-1}} f_2 \circ \mathtt{X}^q & \cdots & a_0^{r^{m-1}} f_0 \end{bmatrix} \in \mathrm{M}_{n\times n}(R_q). \tag{2}$$

r-Linearized and r^m-Linearized Equations (Contd.)

Theorem

Assume that for $0 \leq i \leq m-1$, $a_i \in \mathbb{F}_q$ and $f_i \in \mathbb{F}_r[\mathtt{X}]$ is q-linearized. Assume that $z \in \overline{\mathbb{F}}_p$ satisfies the equation

$$\sum_{i=0}^{m-1} a_i f_i^{r^i}(z) = 0. \tag{3}$$

Then we have

$$(\det M)(z) = 0, \tag{4}$$

where $\det M$ is a q-linearized polynomial over $\mathbb{F}_r$.

$$\sum_{i=0}^{m-1} a_i f_i^{r^i}(z) = 0. \tag{5}$$

Raise the left side of (5) to the power of r^j, $0 \le j \le m-1$, and express the results in a matrix form. We have

$$\Bigg(\sum_{j=0}^{m-1} \begin{bmatrix} a_j f_j^{r^j} \\ a_{j-1}^{r} f_{j-1}^{r^j} \\ \vdots \\ a_0^{r^j} f_0^{r^j} \\ a_{m-1}^{r^{j+1}} f_{m-1}^{r^j} \circ \mathtt{X}^q \\ \vdots \\ a_{j+1}^{r^{m-1}} f_{j+1}^{r^j} \circ \mathtt{X}^q \end{bmatrix}\Bigg)(z) = 0. \tag{6}$$

$$M = \begin{bmatrix} a_0 f_0 & a_1 f_1 & \cdots & a_{m-1} f_{m-1} \\ a_{m-1}^r f_{m-1} \circ \mathtt{X}^q & a_0^r f_0 & \cdots & a_{m-2}^r f_{m-2} \\ \vdots & \vdots & & \vdots \\ a_1^{r^{m-1}} f_1 \circ \mathtt{X}^q & a_2^{r^{m-1}} f_2 \circ \mathtt{X}^q & \cdots & a_0^{r^{m-1}} f_0 \end{bmatrix} \in \mathrm{M}_{n\times n}(R_q). \tag{7}$$

Label the rows and columns of M from 0 through $m-1$. Let M_0 be the submatrix M with its 0th column deleted, and, for $0 \le i \le m-1$, let $M_{i,0}$ be the submatrix of M_0 with its ith row deleted. Put $D_i = (-1)^i \det M_{i,0}$, $0 \le i \le m-1$.

$$0 = \left([D_0, \cdots, D_{m-1}] \circ \begin{bmatrix} a_0 f_0 \\ a_{m-1}^r f_{m-1} \circ \mathtt{X}^q \\ \vdots \\ a_1^{r^{m-1}} f_1 \circ \mathtt{X}^q \end{bmatrix} \right)(z) = (\det M)(z).$$

Applications to Permutation Polynomials

A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if the mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$.

Let m and e be positive integers, r a prime power and $q = r^m$. Define $S_e = \mathtt{X}^{q^0} + \mathtt{X}^{q^1} + \cdots + \mathtt{X}^{q^{e-1}}$.

A Criterion

A polynomial $f \in \mathbb{F}_{q^e}[\mathtt{X}]$ is a PP of $\mathbb{F}_{q^e}$ if the following three conditions are satisfied.

(i) There exists a PP $\bar{f} \in \mathbb{F}_q[\mathtt{X}]$ of $\mathbb{F}_q$ such that the diagram

$$\begin{tikzcd} \mathbb{F}_{q^e} \arrow[r, "f"] \arrow[d, "S_e"'] & \mathbb{F}_{q^e} \arrow[d, "S_e"] \\ \mathbb{F}_q \arrow[r, "\bar{f}"'] & \mathbb{F}_q \end{tikzcd}$$

commutes.

(ii) For each $c \in \mathbb{F}_q$, there exist q-linearized polynomials $f_{c,i} \in \mathbb{F}_r[\mathtt{X}]$ and $a_{c,i} \in \mathbb{F}_q$, $0 \le i \le m-1$, and $b_c \in \mathbb{F}_{q^e}$ such that

$$f(x) = f_c(x) + b_c \quad \text{for all } x \in S_e^{-1}(c), \tag{8}$$

where

$$f_c = \sum_{i=0}^{m-1} a_{c,i} f_{c,i}^{r^i}. \tag{9}$$

(iii) For each $c \in \mathbb{F}_q$,

$$\gcd\big(\det A_c,\ (\mathtt{X}^e - 1)/(\mathtt{X} - 1)\big) = 1, \tag{10}$$

where

$$A_c = \begin{bmatrix} a_{c,0}\widetilde{f}_{c,0} & a_{c,1}\widetilde{f}_{c,1} & \cdots & a_{c,m-1}\widetilde{f}_{c,m-1} \\ a^r_{c,m-1}\widetilde{f}_{c,m-1}\mathtt{X} & a^r_{c,0}\widetilde{f}_{c,0} & \cdots & a^r_{c,m-2}\widetilde{f}_{c,m-2} \\ \vdots & \vdots & & \vdots \\ a^{r^{m-1}}_{c,1}\widetilde{f}_{c,1}\mathtt{X} & a^{r^{m-1}}_{c,2}\widetilde{f}_{c,2}\mathtt{X} & \cdots & a^{r^{m-1}}_{c,0}\widetilde{f}_{c,0} \end{bmatrix}, \tag{11}$$

and $\widetilde{(\ )}$ denotes the conventional associate of a q-linearized polynomial over $\mathbb{F}_q$.

Applications to Permutation Polynomials (Contd.)

The Polynomial $g_{n,q}$

Let $p = \operatorname{char} \mathbb{F}_q$. For each integer $n \geq 0$, there is a polynomial $g_{n,q} \in \mathbb{F}_p[\mathtt{X}]$ defined by the functional equation

$$\sum_{c \in \mathbb{F}_q} (\mathtt{X} + c)^n = g_{n,q}(\mathtt{X}^q - \mathtt{X}). \tag{12}$$

• X. Hou, *Two classes of permutation polynomials over finite fields*, J. Combin. Theory Ser. A **118** (2011), 448 – 454.

Question: When is $g_{n,q}$ a permutation polynomial(PP) of $\mathbb{F}_{q^e}$?

If $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$, we call triple $(n, e; q)$ **desirable**.

$$g_{0,q} = \ldots = g_{q-2,q} = 0,$$
$$g_{q-1,q} = -1,$$

$$g_{n,q} = x g_{n-q,q} + g_{n-q+1,q} \ , \quad n \geq q$$

(1) X. Hou, *A new approach to permutation polynomials over finite fields*, Finite Fields Appl. **18** (2012), 492 – 521.

(2) N. Fernando, X. Hou, S. D. Lappano, *A new approach to permutation polynomials over finite fields, II*, Finite Fields Appl. **22** (2013), 122 – 158.

(3) N. Fernando, X. Hou, S. D. Lappano, *Permutation polynomials over finite fields involving* $\mathtt{x} + \mathtt{x}^q + \cdots + \mathtt{x}^{q^{a-1}}$, Discrete Math. **315** (2014), 173 – 184.

- Computer searches for desirable triples with small values of q and e were conducted.
- A table of **desirable** triples when $q = 4$ and $e \leq 6$ was given in (2).

For each integer $a \geq 0$, define $S_a = \mathtt{X} + \mathtt{X}^q + \cdots + \mathtt{X}^{q^{a-1}}$.

Proposition

Let $q = 4$ and $n = 1 + q^a + q^b + q^e + q^{e+k}$, where a, b, e, and k are positive integers. Then

$$g_{n,q} \equiv S_a S_b + (S_a + S_b + S_e) S_k + S_e^2 \pmod{\mathtt{X}^{q^e} - \mathtt{X}}. \qquad (13)$$

If $\gcd(e, 2k) = 1$ and $a = k$ or $b = k$, then $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Outline of the proof $g_{n,q} \equiv S_k^2 + S_e^2 + S_e S_k \pmod{\mathtt{X}^{q^e} - \mathtt{X}}$.
Let $S_e = c$.

$$\overline{f} = \mathtt{X}^2, f_{c,0} = f_{c,1} = S_k, \; a_{c,0} = c, \; a_{c,1} = 1, \; b_c = c^2.$$

Proposition

Let $q = 4$ and $n = 1 + 3q^a + q^e + 2q^{e+a}$, where e and a are positive integers. Then

$$g_{n,q} \equiv \mathtt{X}^{q^a} + S_e + S_a^2 S_e^2 + S_a S_e^3 \pmod{\mathtt{X}^{q^e} - \mathtt{X}}.$$

If $2 \mid e$ and $\gcd(e, 2a+1) = 1$, then $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Proposition

Let $q = 4$ and $n = 1 + 2q^2 + q^4 + q^e + 2q^{e+2}$, where e is a positive integer. Then

$$g_{n,q} \equiv \mathtt{X}^{q^3} + S_e + S_2^2 S_e^2 + S_4 S_e^3 \pmod{\mathtt{X}^{q^e} - \mathtt{X}}.$$

If $2 \mid e$ but $5 \nmid e$, then $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Proposition

Let $q = 4$ and $n = 1 + 2q^1 + 2q^{e-1} + 2q^{e+1}$, where $e > 1$ is an integer. Then

$$g_{n,q} \equiv S_2 + \mathtt{X}^2 S_e^2 + S_{e-1}^2 S_e^2 \pmod{\mathtt{X}^{q^e} - \mathtt{X}}.$$

If e is odd, then $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

A Generalization

Let $q = 4$ and $f = S_a + \mathtt{X}^2 S_e^2 + S_b^2 S_e^2$, where a, b, and e are positive integers. Then f is a PP of $\mathbb{F}_{q^e}$ if $2 \mid (a + b)$, $\gcd(e, a) = 1$, and

$$\gcd\left(\frac{\mathtt{X}^{2a} + 1 + \mathtt{X}^{2b+1} + \mathtt{X}^3}{(\mathtt{X}+1)^2}, \frac{\mathtt{X}^e + 1}{\mathtt{X}+1}\right) = 1.$$

Proposition

Let $q = 4$ and $n = 1 + 2q^1 + q^3 + q^e + 2q^{e+1}$, where e is a positive integer. Then

$$g_{n,q} \equiv \mathtt{X}^{q^2} + S_e + \mathtt{X}^2 S_e^2 + S_3 S_e^3 \pmod{\mathtt{X}^{q^e} - \mathtt{X}}.$$

If $2 \mid e$ but $3 \nmid e$, then $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

A Generalization

Let $q = 4$ and $f = S_a + S_b + S_e + \mathtt{X}^2 S_e^2 + S_b S_e^3$, where a, b, and e are positive integers. Then f is a PP of $\mathbb{F}_{q^e}$ if $2 \mid (a + e)$, $\gcd(e, a - b) = 1$, and

$$\gcd\left(\frac{\mathtt{X}^{2a} + \mathtt{X}^3 + \mathtt{X} + 1}{(\mathtt{X}+1)^2}, \frac{\mathtt{X}^e + 1}{\mathtt{X}+1}\right) = 1.$$

Table

$*$ - [Hou 2012], [Fernando, Hou, Lappano 2013] $\bullet$ - New Results

Table : Desirable triples $(n, e; 4)$, $e \leq 6$, $w_4(n) > 4$

e	n	base 4 digits of n	reference
2	59	3,2,3	$*$
2	127	3,3,3,1	$*$
3	29	1,3,1	$*$
3	101	1,1,2,1	$*$
3	149	1,1,1,2	
3	163	3,0,2,2	$*$
3	281	1,2,1,0,1	$*$
3	307	3,0,3,0,1	$*$
3	329	1,2,0,1,1	$*$
3	341	1,1,1,1,1	$*$
3	2047	3,3,3,3,3,1	$*$
4	281	1,2,1,0,1	$*$
4	307	3,0,3,0,1	
4	401	1,0,1,2,1	$*$

Table (Contd.)

$*$ - [Hou 2012], [Fernando, Hou, Lappano 2013] $\bullet$ - New Results

Table : Desirable triples $(n, e; 4)$, $e \leq 6$, $w_4(n) > 4$

e	n	base 4 digits of n	reference
4	547	3,0,2,0,2	$*$
4	779	3,2,0,0,3	$*$
4	787	3,0,1,0,3	$*$
4	817	1,0,3,0,3	
4	899	3,0,0,2,3	$*$
4	1469	1,3,3,2,1,1	
4	2201	1,2,1,2,0,2	
4	2317	1,3,0,0,1,2	$\bullet$
4	2321	1,0,1,0,1,2	$*$
4	2377	1,2,0,1,1,2	$\bullet$
4	2441	1,2,0,2,1,2	
4	4387	3,0,2,0,1,0,1	
4	32767	3,3,3,3,3,3,3,1	$*$
5	29	1,3,1	$*$

Table (Contd.)

$*$ - [Hou 2012], [Fernando, Hou, Lappano 2013] • - New Results

Table : Desirable triples $(n, e; 4)$, $e \leq 6$, $w_4(n) > 4$

e	n	base 4 digits of n	reference
5	1049	1,2,1,0,0,1	$*$
5	1061	1,1,2,0,0,1	$*$
5	1169	1,0,1,2,0,1	$*$
5	1289	1,2,0,0,1,1	$*$
5	1409	1,0,0,2,1,1	$*$
5	1541	1,1,0,0,2,1	$*$
5	1601	1,0,0,1,2,1	$*$
5	2083	3,0,2,0,0,2	$*$
5	2563	3,0,0,0,2,2	$*$
5	4229	1,1,0,2,0,0,1	$*$
5	4289	1,0,0,3,0,0,1	
5	4387	3,0,2,0,1,0,1	
5	5129	1,2,0,0,0,1,1	$*$

Table (Contd.)

$*$ - [Hou 2012], [Fernando, Hou, Lappano 2013] $\bullet$ - New Results

Table : Desirable triples $(n, e; 4)$, $e \leq 6$, $w_4(n) > 4$

e	n	base 4 digits of n	reference
5	5141	1,1,1,0,0,1,1	$*$
5	5189	1,1,0,1,0,1,1	$*$
5	5249	1,0,0,2,0,1,1	$*$
5	5381	1,1,0,0,1,1,1	$*$
5	8713	1,2,0,0,2,0,2	$\bullet$
5	9281	1,0,0,1,0,1,2	$*$
5	17429	1,1,1,0,0,1,0,1	$\bullet$
5	17441	1,0,2,0,0,1,0,1	$*$
5	17489	1,0,1,1,0,1,0,1	$\bullet$
5	17681	1,0,1,0,1,1,0,1	$\bullet$
5	524287	3,3,3,3,3,3,3,3,3,1	$*$
6	4361	1,2,0,0,1,0,1	$*$
6	6161	1,0,1,0,0,2,1	$*$
6	6401	1,0,0,0,1,2,1	$*$

Table (Contd.)

$*$ - [Hou 2012], [Fernando, Hou, Lappano 2013] • - New Results

Table : Desirable triples $(n, e; 4)$, $e \leq 6$, $w_4(n) > 4$

e	n	base 4 digits of n	reference
6	8227	3,0,2,0,0,0,2	$*$
6	8707	3,0,0,0,2,0,2	$*$
6	12299	3,2,0,0,0,0,3	$*$
6	12307	3,0,1,0,0,0,3	$*$
6	14339	3,0,0,0,0,2,3	$*$
6	37121	1,0,0,0,1,0,1,2	$*$
6	65801	1,2,0,0,1,0,0,0,1	$*$
6	65921	1,0,0,2,1,0,0,0,1	
6	66307	3,0,0,0,3,0,0,0,1	$*$
6	135209	1,2,2,0,0,0,1,0,2	
6	135217	1,0,3,0,0,0,1,0,2	•
6	135457	1,0,2,0,1,0,1,0,2	•
6	137249	1,0,2,0,0,2,1,0,2	
6	8388607	3,3,3,3,3,3,3,3,3,3,3,1	$*$

For more details

N. Fernando, X. Hou, *From r-linearized polynomial equations to r^m-linearized polynomial equations*, (2015). arXiv: 1503.03162

References

(1) A. Akbary, D. Ghioca, Q. Wang, *On constructing permutations of finite fields*, Finite Fields Appl. **17** (2011), 51 – 67.

(2) X. Caruso, J. Le Borgne, *Some algorithms for skew polynomials over finite fields*, arXiv1212.3582, 2012.

(3) M. Giesbrecht, *Factoring in skew-polynomial rings over finite fields*, J. Symbolic Comput. **26** (1998), 463 – 486.

(4) M. Hall, *A combinatorial problem on abelian groups*, Proc. Amer. Math. Soc. **3** (1952), 584 – 587.

(5) X. Hou, *Proof of a conjecture on permutation polynomials over finite fields*, Finite Fields Appl. **24** (2013) 192 – 195.

Thank You!