Ambiguity, deficiency and differential spectrum of normalized permutation polynomials over finite fields

Daniel Panario
School of Mathematics and Statistics
Carleton University
daniel@math.carleton.ca

Dedicated to Claude Carlet on his $2^6 + 2^2 + 2$ birthday

Boolean Functions and their Applications
Florence, June 16-21, 2019

Introduction

Let G_1 and G_2 be two finite Abelian groups of the same cardinality and $f : G_1 \to G_2$. We focus on the study of the differential map

$$\Delta_{f,a}(x) = f(x+a) - f(x).$$

Given $a \neq 0 \in G_1$ and $b \in G_2$, what is the number of solutions of

$$f(x+a) - f(x) = b?$$

The differential map notion is related to several important problems including Costas array (for radar and sonar communications) and perfect non-linear (PN) almost perfect non-linear (APN) functions (for cryptography).

Costas arrays as a difference map

A Costas array of order n is an $n \times n$ array of dots and blanks which satisfies

- n dots, $n(n-1)$ blanks, with exactly one dot in each row and column; and
- all segments between pairs of dots are different.

A Costas array can be represented by

$f(1)$	$f(2)$	$\cdots$	$f(n)$

such that $f(j) = i$ if (i, j)-position has a dot, and for $x \neq y$, $a \neq 0$

$$f(x+a) - f(x) \neq f(y+a) - f(y).$$

PN and APN functions

Definition

Let G_1 and G_2 be finite Abelian groups of the same cardinality and $f : G_1 \to G_2$. Then f is a perfect non-linear (PN) function if

$$\Delta_{f,a}(x) = f(x+a) - f(x) = b$$

has exactly one solution for all $a \neq 0 \in G_1$ and all $b \in G_2$.

Perfect non-linear permutations do not exist. Furthermore, perfect non-linear functions cannot exist in finite fields of characteristic 2 (the most important for implementations). An alternate definition for the best-possible differential structure of a function is APN.

APN functions

Definition

Let G_1 and G_2 be finite Abelian groups of the same cardinality and $f : G_1 \to G_2$. Then, f is an almost perfect non-linear (APN) function if

$$\Delta_{f,a}(x) = f(x+a) - f(x) = b$$

has at most two solutions for all $a \neq 0 \in G_1$ and all $b \in G_2$.

Example. The inverse function $f : x \mapsto x^{2^n-2}$ in $\mathbb{F}_{2^n}$ is APN if and only if n is odd. This function is used in AES but $n = 8$!

Theorem. Let $f(x) = x^{2^n-2}$ over $\mathbb{F}_{2^n}$. The function f is APN if and only if n is odd. Furthermore, if n is even, then $\Delta_{f,a}$ is differential 4-uniform, and is optimally so (for monomials).

Differential spectrum

Let G_1 and G_2 be finite Abelian groups of the same cardinality and $f : G_1 \to G_2$. For any $a \in G_1^*$ and $b \in G_2$, we consider

$$\Delta_{f,a}(x) = f(x+a) - f(x) = b$$

and denote $\lambda_{a,b}(f) = \#\Delta_{f,a}^{-1}(b)$. Over finite fields, for $0 \leq i \leq q$, let

$$n_i(f) = \#\{(a,b) \in G_1^* \times G_2 \mid \lambda_{a,b}(f) = i\}.$$

The differential spectrum of a function f is the vector $[n_0(f), \ldots, n_q(f)]$.

Providing differential spectrum of a function leads to important differential knowledge on the function. As an example, the differential spectra of monomial functions $f(x) = x^{2^t-1} \in \mathbb{F}_{2^n}[x]$, $1 < t < n$, is considered by Blondeau, Canteaut and Charpin (IEEE-IT, 2011).

Ambiguity and deficiency

Panario, Sakzad, Stevens and Wang (IEEE-IT, 2011) attempt to understand the injectivity and surjectivity of $\Delta_{f,a}$ when f is a bijection. How close a bijection f is to be APN?

Again, for any $a \in G_1^*$ and $b \in G_2$, we consider

$$\Delta_{f,a}(x) = f(x+a) - f(x) = b$$

and denote $\lambda_{a,b}(f) = \#\Delta_{f,a}^{-1}(b)$. Over finite fields, for $0 \leq i \leq q$, let

$$n_i(f) = \#\{(a,b) \in G_1^* \times G_2 \mid \lambda_{a,b}(f) = i\}.$$

The deficiency of f, denoted by $D(f)$, is n_0. Hence, $D(f)$ measures the number of pairs (a,b) such that $\Delta_{f,a}(x) = b$ has no solutions.

This is a measure of the surjectivity of $\Delta_{f,a}$: the lower the deficiency the closer the $\Delta_{f,a}$ are to surjective.

Ambiguity and deficiency (cont.)

Moreover, we define the (weighted) ambiguity of f as

$$A(f) = \sum_{0 \leq i \leq q} n_i(f) \binom{i}{2}.$$

The weighted ambiguity of f measures the total replication of pairs of x and x' such that $\Delta_{f,a}(x) = \Delta_{f,a}(x')$ for some $a \in G_1^*$.

This is a measure of the injectivity of the function $\Delta_{f,a}$: the lower the ambiguity of f the closer the $\Delta_{f,a}$ are to injective.

Remark. Deficiency does not require knowledge of the full differential spectrum, but computing the exact ambiguity of a function does require this information. Tight upper and lower bounds for deficiency and ambiguity are given both in general for finite Abelian groups, and in particular for bijections in finite fields, not requiring spectrum knowledge.

Related measures: dispersion

The dispersion of a permutation P on the set $\{0, 1, \ldots, p-1\}$ is the cardinality of the set

$$\{(j-i, P(j)-P(i)) \colon 0 \leq i < j \leq p-1\}.$$

Dispersion has been used as a random measure for interleavers in turbo codes; see the book by Heegard and Wicker, 1999.

Dispersion is related to deficiency but deficiency is invariant under extended affine equivalence and dispersion is not; see Çeşmelioğlu, Meidl and Topuzoğlu (Journal of Computational and Applied Mathematics, 2014).

In that paper dispersion is used to provide permutations of given Carlitz rank with prescribed cycle decomposition and dispersion.

Related measures: non-balancedness

Let G_1 and G_2 be finite Abelian groups and $f : G_1 \to G_2$. The mean of the (uniform) random variable $|f^{-1}(b)|$ is $|G_1|/|G_2|$; then f is balanced if the random variable is constant. The coalescence, that is the variance of this random variable giving the distribution of the preimage sizes, is

$$\frac{1}{|G_2|} \sum_{b \in G_2} \left(|f^{-1}(b)| - \frac{|G_1|}{|G_2|} \right)^2 .$$

The non-balancedness of f is defined as

$$\mathbb{NB}(f) = \sum_{a \in G_1^*} \sum_{b \in G_2} \left(|\Delta_{f,a}^{-1}(b)| - \frac{|G_1|}{|G_2|} \right)^2 .$$

Non-balancedness is related to ambiguity; see Carlet and Ding (Finite Fields and their Applications, 2007). Non-balancedness is used to provide bounds on the non-linearity of the function.

Let us remember the title of this talk:

Ambiguity, deficiency and differential spectrum of normalized permutation polynomials over finite fields

We still need to define

normalized permutation polynomials over finite fields.

Normalized permutation polynomials

Let $\mathbb{F}_q$ be the finite field of q elements, q a prime power. If $f : \mathbb{F}_q \to \mathbb{F}_q$ induces a bijection, f is a permutation polynomial; if f is monic, $f(0) = 0$, and, when the degree n of f is not divisible by the characteristic of $\mathbb{F}_q$, the coefficient of x^{n-1} is zero, then f is in normalized form. Normalized permutation polynomials are known exhaustively up to degree six.

A list of all normalized permutation polynomials of degree less than six, taken from Chapter 7 of Lidl and Niederreiter (1983), is given next. The characterization of all normalized permutation polynomials of degree six is more recent (Shallue and Wanless, 2013).

The main results of this work are in the coming tables that provide exact formulas for the differential spectrum, deficiency and ambiguity of all normalized permutation polynomials of degree up to six over finite fields.

#	**Normalized PP in $\mathbb{F}_q$**	$\overline{q}$	**Differential Spectrum (Deficiency = n_0)**	**Ambiguity**
1)	x^2, $q \equiv 0 \pmod 2$	-	$[(q-1)^2, 0, \cdots, 0, q-1]$	$(q-1)\binom{q}{2}$
2)	x^3, $q \not\equiv 1 \pmod 3$			
a)	$q \equiv 0 \pmod 3$:	-	$[(q-1)^2, 0, \cdots, 0, q-1]$	$(q-1)\binom{q}{2}$
b)	$q = 2^m$, m odd:	-	$\left[(q-1)\frac{q}{2}, 0, (q-1)\frac{q}{2}, 0, \cdots, 0\right]$	$(q-1)\frac{q}{2}$
c)	$q \equiv 2 \pmod 3$, q odd:	-	$\left[\frac{(q-1)^2}{2}, q-1, \frac{(q-1)^2}{2}, 0, \cdots, 0\right]$	$\frac{(q-1)^2}{2}$
3)	$x^3 - wx$ $q \equiv 0 \pmod 3$, w is NS	-	$\left[(q-1)^2, 0, \cdots, 0, q-1\right]$	$(q-1)\binom{q}{2}$
4)	$x^4 \pm 3x$, $q = 7$	-	$[12, 18, 12, 0, \cdots, 0]$	12
5)	$x^4 + a_1x^2 + a_2x$ $q \equiv 0 \pmod 2$, only root in $\mathbb{F}_q$ is 0	-	$\left[(q-1)^2, 0, \cdots, 0, q-1\right]$	$(q-1)\binom{q}{2}$
6)	x^5, $q \not\equiv 1 \pmod 5$			
a)	$q = 2^m$, m even:	-	$\left[(q-1)\frac{3q}{4}, 0, 0, 0, (q-1)\frac{q}{4}, 0, \cdots, 0\right]$	$(q-1)\frac{q}{4}\binom{4}{2}$
b)	$q = 2^m$, m odd:	-	$\left[(q-1)\frac{q}{2}, 0, (q-1)\frac{q}{2}, 0, \cdots, 0\right]$	$(q-1)\frac{q}{2}$
c)	$q \equiv 0 \pmod 5$:	-	$\left[(q-1)^2, 0, \cdots, 0, q-1\right]$	$(q-1)\binom{q}{2}$
d)	$q \not\equiv 0, 1 \pmod 5$, q odd:	1	$\left[\frac{5(q-1)^2}{8}, 0, \frac{(q-1)(q+3)}{4}, q-1, \frac{(q-1)(q-9)}{8}, 0, \cdots, 0\right]$	$(q-1)(q-3)$
		3	$\left[\frac{(q-1)(5q+1)}{8}, 0, \frac{(q-1)(q-3)}{4}, q-1, \frac{(q-1)(q-3)}{8}, 0, \cdots, 0\right]$	$(q-1)q$
		5	$\left[\frac{(q-1)(5q-9)}{8}, q-1, \frac{(q-1)(q+3)}{4}, 0, \frac{(q-1)(q-5)}{8}, 0, \cdots, 0\right]$	$(q-1)(q-3)$
		7	$\left[\frac{(q-1)(5q-3)}{8}, q-1, \frac{(q-1)(q-3)}{4}, 0, \frac{(q-1)(q+1)}{8}, 0, \cdots, 0\right]$	$(q-1)q$

Table: Differential spectrum, deficiency and ambiguity of degree up to 5 normalized permutation polynomials ($\overline{q} = q \bmod 8$).

#	Normalized PP in $\mathbb{F}_q$	$\overline{q}$	Differential Spectrum (Deficiency = n_0)	Ambiguity
7)	$x^5 - wx$ $q \equiv 0 \pmod 5$ w not a 4^{th} power	-	$\left[(q-1)^2, 0, \cdots, 0, q-1\right]$	$(q-1)\binom{q}{2}$
8)	$x^5 + wx$ $q = 9,\ w^2 = 2$	-	$[40, 0, 24, 8, 0, \cdots, 0]$	48
9)	$x^5 \pm 2x^2$, $q = 7$	-	$[12, 24, 0, 6, 0, \cdots, 0]$	18
10)	$x^5 + wx^3 \pm x^2 + 3w^2x$ $q = 7$, w is NS	-	$[14, 18, 8, 0, 2, 0, \cdots, 0]$	20
12)	$x^5 + wx^3 + 3w^2x$ $q = 13$, w is NS	-	$[90, 6, 42, 6, 12, 0, \cdots, 0]$	132
13)	$x^5 - 2wx^3 + w^2x$ $q \equiv 0 \pmod 5$, w is NS	-	$\left[\frac{(q-1)^2}{2}, q-1, \frac{(q-1)^2}{2}, 0, \cdots, 0\right]$	$\frac{(q-1)^2}{2}$

Table: Differential spectrum, deficiency and ambiguity of degree up to 5 normalized permutation polynomials ($\overline{q} = q \bmod 8$).

$\chi(A)$ $\chi(B)$	$+1$	0	-1
$+1$	-2	$q-1$	0
0	$q-1$	0	$-(q-1)$
-1	0	$-(q-1)$	2

Table: Values of $S_{A,B}$.

#	Normalized PP in $\mathbb{F}_q$	$\overline{q}$	Differential Spectrum (Deficiency = n_0)	Ambiguity
11)	$x^5+wx^3+5^{-1}w^2x$ $w \in \mathbb{F}_q$, $q \equiv \pm 2 \pmod 5$			S is in previous table
a)	$q=2^m$, m odd:	-	$w=0$: $\left[(q-1)\frac{q}{2}, 0, (q-1)\frac{q}{2}, 0, \cdots, 0\right]$	$(q-1)\frac{q}{2}$
		-	$w \neq 0$: $\left[(q-1)\frac{q}{2}+\frac{(q-2)q}{8}, 0, \frac{q^2}{4}, 0, \frac{(q-2)q}{8}, 0, \cdots, 0\right]$	$(2q-3)\frac{q}{2}$
b)	q odd, $-\frac{6w}{5}$ is 0 or NS:	1	$\left[\frac{5(q-1)^2}{8}, \frac{q-1}{2}-\frac{S}{2}, \frac{(q-1)(q+1)}{4}+\frac{S}{2},\right.$ $\left.\frac{q-1}{2}+\frac{S}{2}, \frac{(q-1)(q-5)}{8}-\frac{S}{2}, 0, \cdots, 0\right]$	$(q-1)(q-2)-S$
		3	$\left[\frac{(q-1)(5q-3)}{8}-\frac{S}{2}, \frac{q-1}{2}+\frac{S}{2}, \frac{(q-1)(q-1)}{4}+\frac{S}{2},\right.$ $\left.\frac{q-1}{2}-\frac{S}{2}, \frac{(q-1)(q-3)}{8}, 0, \cdots, 0\right]$	$(q-1)^2-S$
		5	$\left[\frac{5(q-1)^2}{8}+\frac{S}{2}, \frac{q-1}{2}-\frac{S}{2}, \frac{(q-1)(q+1)}{4}-\frac{S}{2},\right.$ $\left.\frac{q-1}{2}+\frac{S}{2}, \frac{(q-1)(q-5)}{8}, 0, \cdots, 0\right]$	$(q-1)(q-2)+S$
		7	$\left[\frac{(5q-3)(q-1)}{8}, \frac{q-1}{2}+\frac{S}{2}, \frac{(q-1)(q-1)}{4}-\frac{S}{2},\right.$ $\left.\frac{q-1}{2}-\frac{S}{2}, \frac{(q-1)(q-3)}{8}+\frac{S}{2}, 0, \cdots, 0\right]$	$(q-1)^2+S$
c)	q odd, $-\frac{6w}{5} \neq 0$ is SQ:	1	$\left[\frac{(q-1)(5q-3)}{8}, \frac{q+1}{2}-\frac{S}{2}, \frac{(q-3)(q+1)}{4}+\frac{S}{2},\right.$ $\left.\frac{q-3}{2}+\frac{S}{2}, \frac{(q-3)(q-5)}{8}+\frac{q-1}{2}-\frac{S}{2}, 0, \cdots, 0\right]$	$(q-3)(q-2)+$ $3(q-1)-S$
		3	$\left[\frac{(q-3)(5q-3)}{8}+(q-1)-\frac{S}{2}, \frac{q+1}{2}+\frac{S}{2}, \frac{(q-1)(q+1)}{4}+\frac{S}{2},\right.$ $\left.\frac{q-3}{2}-\frac{S}{2}, \frac{(q-3)^2}{8}, 0, \cdots, 0\right]$	$(q-1)(q-2)-S$
		5	$\left[\frac{(q-1)(5q-3)}{8}+\frac{S}{2}, \frac{q+1}{2}-\frac{S}{2}, \frac{(q-3)(q+1)}{4}-\frac{S}{2},\right.$ $\left.\frac{q-3}{2}+\frac{S}{2}, \frac{(q-3)(q-5)}{8}+\frac{q-1}{2}, 0, \cdots, 0\right]$	$(q-3)(q-2)+$ $3(q-1)+S$
		7	$\left[\frac{(q-3)(5q-3)}{8}+(q-1), \frac{q+1}{2}+\frac{S}{2}, \frac{(q-1)(q+1)}{4}-\frac{S}{2},\right.$ $\left.\frac{q-3}{2}-\frac{S}{2}, \frac{(q-3)^2}{8}+\frac{S}{2}, 0, \cdots, 0\right]$	$(q-1)(q-2)+S$

#	Normalized PP in $\mathbb{F}_q$	Differential Spectrum (Deficiency = n_0)	Ambiguity
1)	$x^6 \pm 2x$, $q = 11$	$[40, 50, 0, 20, 0, \cdots, 0]$	60
2)	$x^6 + u^2vx^3 + ux^2 + 5vx$ $q = 11$, $u \neq 0$ is SQ, $v \in \{\pm 1\}$	$[52, 26, 22, 4, 2, 4, 0, \cdots, 0]$	86
3)	$x^6 + 4u^2vx^3 + ux^2 + 4vx$ $q = 11$, $u = 0$ or NS, $v \in \{\pm 1\}$	$u = 0$: $[40, 50, 0, 20, 0, \cdots, 0]$	60
		u is NS: $[46, 32, 20, 10, 2, 0, \cdots, 0]$	62
4)	$x^6 + u^2x^4 + u^7vx^3 + u^4x^2 + u(2v+1)x$, $q = 9$, $u \neq 0$ v a root of $x^6 - x^4 + x^3 + x^2 + x$	$[52, 0, 0, 18, 0, 0, 0, 0, 0, 2]$	126
5)	$x^6 + ux^5 + 2uvx^4 + (u^3 + uv^2 + 2v^3)x^3 + (2u^4 + uv^3)x^2 + (2u^5 + u^4v + 2uv^4)x$ $q = 9$, $u \neq 0$, v arbitrary	$[28, 22, 18, 2, 2, 0, \cdots, 0]$	36
6)	$x^6 + ux^5 + 2uvx^4 + (uv^2 + 2v^3 + u^3w)x^3 + (uv^3 + 2u^4w)x^2 + (u^5w^2 + 2uv^4 + u^4vw)x$, $q = 9$, $u \neq 0$, v arbitrary, w a root of $x^4 + 1$	$w \in \{z, 2z+1\}$: $[22, 30, 18, 2, 0, \cdots, 0]$	24
		$w \in \{2z, z+2\}$: $[28, 22, 18, 2, 2, 0, \cdots, 0]$	36
7)	$x^6 + ux^5 + 2uvx^4 + (2u^3 + uv^2 + 2v^3)x^3 + (u^4 + uv^3)x^2 + (2u^5 + u^5w + 2u^4v + 2uv^4)x$, $q = 9$, $u \neq 0$, v arbitrary, w a root of $x^2 + 1$	$[22, 42, 0, 2, 6, 0, \cdots, 0$	42
8)	$x^6 + ux^5 + 2uvx^4 + (uv^2 + 2v^3)x^3 + (2u^4 + uv^3)x^2 + (u^4v + 2uv^4)x$ $q = 27$, $u \neq 0$, v arbitrary	$[256, 252, 156, 14, 24, 0, \cdots, 0]$	342
9)	$x^6 + u^2x^4 + u^4x^2$ $q = 2^m$, m odd, $m \geq 3$, u arbitrary	$\left[(q-1)\frac{q}{2}, 0, (q-1)\frac{q}{2}, 0, \cdots, 0\right]$	$(q-1)\frac{q}{2}$

Table: Differential spectrum, deficiency and ambiguity of degree 6 normalized permutation polynomials ($\overline{q} = q \bmod 8$ and, in line 6, z is a root of $z^2 + 2z + 2 = 0$).

#	Normalized PP in $\mathbb{F}_q$	Differential Spectrum (Deficiency = n_0)	Ambiguity
10)	$x^6 + u^5v^2x^4 + u^4x^3 + (u^3 + u^3v + u^3v^4)x^2 + u^2v^2x$ $q = 8$, $u \neq 0$, v arbitrary	$[34, 0, 16, 0, 6, 0, 0, 0, 0]$	52
11)	$x^6 + ux^5 + u^2(v^2 + v)x^4 + u^3x^3 + u^4(v^2 + w)x^2 + u^5(v + w)x$, $q = 8$, $u \neq 0$, v a root of $x^4 + x^2 + x$, w a root of $x^4 + x^3 + x^2 + 1$	$[43, 0, 0, 0, 12, 0, 0, 0, 1]$	100
12)	$x^6 + ux^5 + u^2(v^2 + v)x^4 + u^3wx^3 + u^4(v^4 + vw)x^2 + u^5(v^4 + v^2w)x$ $q = 8$, $u \neq 0$, v arbitrary, w a root of $x^3 + x + 1$	$[28, 0, 28, 0, \cdots, 0]$	28
13)	$x^6 + ux^5 + u^2(v^2 + v + 1)x^4 + u^3x^3 + u^4(v^2 + 1)x^2 + u^5vx$ $q = 8$, $u \neq 0$, v arbitrary	$[43, 0, 0, 0, 12, 0, 0, 0, 1]$	100
14)	$x^6 + ux^5 + u^2(v^2 + v + 1)x^4 + u^3w^3x^3 + u^4(v^4 + vw^3 + w^4)x^2 + u^5(v^4 + v^2w^3 + w^3 + w^4)x$, $q = 8$, $u \neq 0$, v arbitrary, w a root of $x^4 + x^2 + x$	$[34, 0, 16, 0, 6, 0, 0, 0, 0]$	52
15)	$x^6 + ux^5 + u^2(v^6 + v^5 + w^4 + w^2 + w)x^4 + u^3x^3 + u^4(v^6 + v^5 + w^4 + w^2)x^2 + u^5(v + w)x$, $q = 16$, $u \neq 0$, v a root of $x^7 + x^4 + x^3 + x^2 + x$, w a root of $x^8 + x^4 + x^2 + x + 1$	$[183, 0, 0, 0, 56, 0, \cdots, 0, 1]$	456
16)	$x^6 + ux^5 + u^2(v^2 + v)x^4 + u^4(v^4 + 1)x^2 + u^5v^4x$, $q = 32$, $u \neq 0$, v arbit.	$[616, 0, 256, 0, 120, 0, \cdots, 0]$	976

Table: Differential spectrum, deficiency and ambiguity of degree 6 normalized permutation polynomials ($\overline{q} = q \bmod 8$).

The interesting cases

For some functions the results are easy to derive. This happens when q is a constant. Also, for example, if $q \equiv 0 \pmod 5$, the polynomial x^5 is linearized and we immediately obtain its ambiguity and deficiency as $A = (q-1)\binom{q}{2}$ and $D = (q-1)^2$ from previous works.

The cases in lines 6 and 11 of Table 1, corresponding, respectively, to the polynomials x^5 for $q \not\equiv 1 \pmod 5$, and $x^5 + wx^3 + 5^{-1}w^2x$ for arbitrary w and $q \equiv 2, 3 \pmod 5$, are more involved; we study the latter in detail and derive the former as a consequence.

To obtain our results in these harder cases we need to find solutions of quartic equations over finite fields. We use quadratic residuocity and Jacobi-like character sums for that task.

Sketch of the proof

The values of ambiguity and deficiency for a given field size q depend uniquely on the values of the spectrum vector n_i for i, in principle, ranging from $i = 0, \ldots, q$.

The vector n_i summarizes the distribution of values of the difference table: n_i counts how many times the value "i" occurs in the table of $\lambda_{a,b}(f)$.

Equivalently, each value $\lambda_{a,b}$ shows, for a fixed $a \in \mathbb{F}_q^*$, how many times (that is, for how many x's) a given $b \in \mathbb{F}_q$ is produced by the function $\Delta_{f,a}(x) = f(x+a) - f(x)$. As a consequence, for $F_w(x) = x^5 + wx^3 + 5^{-1}w^2x \in \mathbb{F}_q[x]$, q odd, $q \equiv \pm 2 \pmod 5$, the n_i's depend on the number of solutions, in the field $\mathbb{F}_q$, to the quartic equation

$$5ax^4 + 10a^2x^3 + (3aw + 10a^3)x^2 + (3a^2w + 5a^4)x + \frac{aw^2}{5} + a^3w + a^5 = b.$$

Sketch of the proof (cont)

$$5ax^4+10a^2x^3+(3aw+10a^3)x^2+(3a^2w+5a^4)x+\frac{aw^2}{5}+a^3w+a^5=b. \tag{1}$$

This equation can have a maximum of 4 roots, for all $a \in \mathbb{F}_q^*$ and for all $b \in \mathbb{F}_q$ (that is, $0 \leq i \leq 4$).

In summary, the search for a formula to compute spectrum vector, ambiguity and deficiency for $x^5+wx^3+5^{-1}w^2x$ over a given finite field of size q implies in the characterization, in $\mathbb{F}_q$, of the roots of Eq. (1).

Since $a \in \mathbb{F}_q^*$, a^{-1}, a^{-2} and a^{-5} always exist and we can have the following changes of variables: $y=\frac{x}{a}$, $v=\frac{w}{a^2}$ and $c=\frac{b}{a^5}$, obtaining

$$5y^4+10y^3+(3v+10)y^2+(3v+5)y+\frac{v^2}{5}+v+1=c. \tag{2}$$

Sketch of the proof (cont)

In Eq. (2), while b runs through all values in $\mathbb{F}_q$, so does c. Since we are only interested in the number of solutions of this equation, and not in the specific roots themselves, it does not matter whether we get x or x/a. Thus, for each v, the characterization of the roots of Eq. (1) can be done, without loss of generality, with the value of a fixed as 1. Hence, the equation to be analyzed can be simplified to $\Delta_{F_v,1}(x) = b$, or

$$x^4 + 2x^3 + \left(\frac{3v+10}{5}\right)x^2 + \left(\frac{5+3v}{5}\right)x + \frac{1}{5}\left(1 + \frac{v^2}{5} + v\right) = \frac{b}{5}. \quad (3)$$

According to a standard procedure in the solution of quartic equations, upon the change of variable $z = x + \frac{1}{2}$, Eq. (3) can be rewritten as

$$z^4 + \left(\frac{1}{2} + \frac{3v}{5}\right)z^2 + \left(\frac{v^2}{25} + \frac{v}{20} + \frac{1}{80} - \frac{b}{5}\right) = 0. \quad (4)$$

Sketch of the proof (cont)

Finally, since this is a biquadratic equation, we change once again to $t = z^2 = (x + \frac{1}{2})^2$ to obtain the main equation to characterize the structure of λ and, thereafter, spectrum, ambiguity and deficiency in $\mathbb{F}_q$:

$$t^2 + \left(\frac{1}{2} + \frac{3v}{5}\right)t + \left(\frac{v^2}{25} + \frac{v}{20} + \frac{1}{80} - \frac{b}{5}\right) = 0. \tag{5}$$

Depending on the discriminant δ_t of Eq. (5) being a square (SQ), a non-square (NS) or zero, we obtain the number of solutions for t, roots of Eq. (5), that are in the field $\mathbb{F}_q$. Then, based on each solution for t being SQ, NS or zero, we determine the exact number $(0, 1, 2, 3$ or $4)$ of solutions for z in $\mathbb{F}_q$.

Let $\alpha = \frac{1}{2} + \frac{3v}{5}$. The discriminant and the solutions for t of Eq. (5) are

$$\delta_t = \frac{(v+1)^2 + 4b}{5} \quad \text{and} \quad t = \frac{1}{2}\left(-\alpha \pm \sqrt{\delta_t}\right). \tag{6}$$

Sketch of the proof (cont)

The classification of the values of δ_t and t as SQ, NS or zero leads to a distribution of the b's among the multiplicities of the solutions for z. This distribution is based on the quadratic residuocity of δ_t and, in a second level, the quadratic residuocity of the t's accounts for the number of different solutions for z (roots) to Eq. (4).

The parameter δ_t, shown in Eq. (6), is linearly dependent on b, so it assumes all values in $\mathbb{F}_q$. Since q is odd, besides 0, exactly $\frac{q-1}{2}$ values in $\mathbb{F}_q$ can be squares. This gives the first level in the division of the q values of b into three categories. Further, the distribution of the solutions depends on the parameter α being zero or not. Then a complete characterization of the roots of $\Delta_{F_v,1}(x) = b$ in $\mathbb{F}_q$, according to the possible quantities of different solutions for z in $\mathbb{F}_q$ $(0, 1, 2, 3$ or $4)$, can be done.

The quantities corresponding to several branches in this classification are computed with the aid of multiplicative characters.

Characters

A character χ is a homomorphism from a finite Abelian group G into the multiplicative group U of complex numbers of absolute value 1 that satisfies, for all $g_1, g_2 \in G$, $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$. The trivial character ϵ is defined by $\epsilon(g) = 1$, for all $g \in G$. If $\chi \neq \epsilon$, we define $\chi(0) = 0$. In particular, a nontrivial character χ is quadratic if $\chi(a) = 1$ when a is nonzero square and -1 when a is nonsquare.

Let χ be the quadratic character of the multiplicative group of $\mathbb{F}_q$. It is well known that $\chi(a) = \left(\frac{a}{p}\right)$, the Legendre symbol, if $q = p$ is prime. In this case, $\chi(2) = (-1)^{\frac{p^2-1}{8}}$. Following similar arguments, for any finite field $\mathbb{F}_q$, we can obtain

$$\chi(2) = (-1)^{\frac{q^2-1}{8}}. \tag{7}$$

Characters (cont)

Theorem 5.48 in Lidl-Niederreiter Let $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$ with q odd and $a_2 \neq 0$. Put $d = a_1^2 - 4a_0a_2$ and let χ be a quadratic character of $\mathbb{F}_q$. Then

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = \begin{cases} -\chi(a_2) & \text{if } d \neq 0; \\ (q-1)\chi(a_2) & \text{if } d = 0. \end{cases}$$

Using this theorem, we compute the value of $S_{A,B} = \sum_{x \in \mathbb{F}_q^*} \chi(A + Bx^2)$, q odd, for some constants $A, B \in \mathbb{F}_q^*$. The results, shown in Table 3, are required to compute the full values of spectrum, ambiguity and deficiency.

Conclusions and further work

This fix a gap in the literature: give differential spectrum and related measures for low degree normalized polynomials. This implies in solving low degree equations over finite fields.

The boomerang uniformity of all normalized permutation polynomials of low degree over finite fields was recently studied by Y. Wang, Q. Wang and W.G. Zhang (talk at Fq14).

Further work:

- Degree 7? Only partial results exist.
- Crytographic use?

D. Panario, B. Stevens and Q. Wang,
Ambiguity and deficiency in Costas arrays and APN permutations. *LATIN 2010: Latin American Theoretical INformatics (Mexico, 2010)*, vol. 6034, *Lecture Notes in Comput. Sci.*, pp. 397–406, 2010.

D. Panario, A. Sakzad, B. Stevens and Q. Wang,
Ambiguity and deficiency of permutations from finite fields, *ITW 2011: Information Theory Workshop (Brazil, 2011)*, IEEE Xplore, 165-169, 2011.

D. Panario, A. Sakzad, B. Stevens and Q. Wang,
Two new measures for permutation: Ambiguity and deficiency. *IEEE Transactions on Information Theory*, vol. 57, 7648–7657, 2011.

D. Panario, A. Sakzad, B. Stevens, D. Thomson and Q. Wang,
Ambiguity and deficiency of permutations over finite fields with linearized difference map, *IEEE Transactions on Information Theory*, vol. 59, 5616–5626, 2013.

D. Panario, D. Santana, and Q. Wang,
Ambiguity, deficiency and differential spectrum of low degree normalized permutation polynomials over finite fields, *Finite Fields and their Applications*, vol. 47, 330–350, 2017.