Decompositions of Permutations in a Finite Field

Samuele Andreoli

UNIVERSITY OF BERGEN

On Decompositions of Permutations in Quadratic Functions

Samuele Andreoli[1], Enrico Piccione[1], Lilya Budaghyan[1], Pantelimon Stănică[2], and Svetla Nikova[1,3]

[1]University of Bergen, Norway, {name.surname}@uib.no
[2]Naval Postgraduate School, Applied Mathematics Department, Monterey, CA 93955, USA, pstanica@nps.edu
[3]KU Leuven, Belgium, {name.surname}@esat.kuleuven.be

Based on [APB$^+$23].

A function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is called an $(n,n)-$*function*.

A $(n,n)-$function admits a representation as a univariate polynomial over $\mathbb{F}_{p^n}$, called *univariate representation*,

$$F(x) = \sum_{i=0}^{p^n-1} \alpha_i x^i.$$

The *algebraic degree* of F is $\mathrm{d}^\circ(F) = \max_{\alpha_i \neq 0} \mathrm{w}_p(i)$, where w_p is the $p-$weight.

A *power function* is a monomial x^k, $1 \leq k < p^n - 1$ and $\mathrm{d}^\circ(F) = \mathrm{w}_p(k)$. An invertible power function is a *power permutation*.

A function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is called an $(n, n)-$*function*.

A $(n, n)-$function admits a representation as a univariate polynomial over $\mathbb{F}_{p^n}$, called *univariate representation*,

$$F(x) = \sum_{i=0}^{p^n-1} \alpha_i x^i.$$

The *algebraic degree* of F is $\mathrm{d}^\circ(F) = \max_{\alpha_i \neq 0} \mathrm{w}_p(i)$, where w_p is the $p-$weight.

A *power function* is a monomial x^k, $1 \leq k < p^n - 1$ and $\mathrm{d}^\circ(F) = \mathrm{w}_p(k)$. An invertible power function is a *power permutation*.

A function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is called an $(n, n)-$*function*.

A $(n, n)-$function admits a representation as a univariate polynomial over $\mathbb{F}_{p^n}$, called *univariate representation*,

$$F(x) = \sum_{i=0}^{p^n-1} \alpha_i x^i.$$

The *algebraic degree* of F is $\mathrm{d}^\circ(F) = \max_{\alpha_i \neq 0} \mathrm{w}_p(i)$,
where w_p is the $p-$weight.

A *power function* is a monomial x^k, $1 \leq k < p^n - 1$ and $\mathrm{d}^\circ(F) = \mathrm{w}_p(k)$.
An invertible power function is a *power permutation*.

A function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is called an $(n, n)-$*function*.

A $(n, n)-$function admits a representation as a univariate polynomial over $\mathbb{F}_{p^n}$, called *univariate representation*,

$$F(x) = \sum_{i=0}^{p^n-1} \alpha_i x^i.$$

The *algebraic degree* of F is $\mathrm{d}^\circ(F) = \max_{\alpha_i \neq 0} \mathrm{w}_p(i)$, where w_p is the $p-$weight.

A *power function* is a monomial x^k, $1 \leq k < p^n - 1$ and $\mathrm{d}^\circ(F) = \mathrm{w}_p(k)$. An invertible power function is a *power permutation*.

Two power functions x^{d_1}, x^{d_2} are said *Cyclotomic Equivalent* if $x^{d_1} = x^{p^i} \circ x^{d_2}$

We say F and G are *Affine Equivalent* if there are affine permutations A and B such that

$$F = A \circ G \circ B.$$

We say that they are *CCZ-equivalent* if there is a linear permutation L mapping the graph of F into the graph of G.
For power functions, CCZ $\iff$ Affine $\iff$ Cyclotomic.

Differential uniformity is defined as

$$\delta_F = \max_{a,b \in \mathbb{F}_{p^n},\, a \neq 0} |\{x \in \mathbb{F}_{p^n} \mid F(x+a) - F(x) = b\}|.$$

We say that F is *perfect nonlinear (PN)* if $\delta_F = 1$.
We say that F is *almost perfect nonlinear (APN)* if $\delta_F = 2$.

Two power functions x^{d_1}, x^{d_2} are said *Cyclotomic Equivalent* if $x^{d_1} = x^{p^i} \circ x^{d_2}$
We say F and G are *Affine Equivalent* if there are affine permutations A and B such that

$$F = A \circ G \circ B.$$

We say that they are *CCZ-equivalent* if there is a linear permutation L mapping the graph of F into the graph of G.
For power functions, CCZ $\iff$ Affine $\iff$ Cyclotomic.

Differential uniformity is defined as

$$\delta_F = \max_{a,b \in \mathbb{F}_{p^n},\, a \neq 0} |\{x \in \mathbb{F}_{p^n} \mid F(x+a) - F(x) = b\}|.$$

We say that F is *perfect nonlinear (PN)* if $\delta_F = 1$.
We say that F is *almost perfect nonlinear (APN)* if $\delta_F = 2$.

Two power functions x^{d_1}, x^{d_2} are said *Cyclotomic Equivalent* if $x^{d_1} = x^{p^i} \circ x^{d_2}$
We say F and G are *Affine Equivalent* if there are affine permutations A and B such that

$$F = A \circ G \circ B.$$

We say that they are *CCZ-equivalent* if there is a linear permutation L mapping the graph of F into the graph of G.
For power functions, CCZ $\iff$ Affine $\iff$ Cyclotomic.

Differential uniformity is defined as

$$\delta_F = \max_{a,b \in \mathbb{F}_{p^n},\, a \neq 0} |\{x \in \mathbb{F}_{p^n} \mid F(x+a) - F(x) = b\}|.$$

We say that F is *perfect nonlinear (PN)* if $\delta_F = 1$.
We say that F is *almost perfect nonlinear (APN)* if $\delta_F = 2$.

Two power functions x^{d_1}, x^{d_2} are said *Cyclotomic Equivalent* if $x^{d_1} = x^{p^i} \circ x^{d_2}$
We say F and G are *Affine Equivalent* if there are affine permutations A and B such that

$$F = A \circ G \circ B.$$

We say that they are *CCZ-equivalent* if there is a linear permutation L mapping the graph of F into the graph of G.
For power functions, CCZ $\iff$ Affine $\iff$ Cyclotomic.

Differential uniformity is defined as

$$\delta_F = \max_{a,b \in \mathbb{F}_{p^n},\, a \neq 0} |\{x \in \mathbb{F}_{p^n} \mid F(x+a) - F(x) = b\}|.$$

We say that F is *perfect nonlinear (PN)* if $\delta_F = 1$.
We say that F is *almost perfect nonlinear (APN)* if $\delta_F = 2$.

Decomposition

A *decomposition* of a $(n, n)-$function F is a sequence of $(n, n)-$functions such that

$$F = G_1 \circ \cdots \circ G_\ell.$$

Applications in hardware implementations, especially masked implementations.

Goals:

- algebraic degree of G_i should be small (typically 2 or 3),
- ℓ should also be as small as possible.

Decomposition

A *decomposition* of a $(n, n)-$function F is a sequence of $(n, n)-$functions such that

$$F = G_1 \circ \cdots \circ G_\ell.$$

Applications in hardware implementations, especially masked implementations.

Goals:

- algebraic degree of G_i should be small (typically 2 or 3),
- ℓ should also be as small as possible.

Decomposition

A *decomposition* of a $(n, n)-$function F is a sequence of $(n, n)-$functions such that

$$F = G_1 \circ \cdots \circ G_\ell.$$

Applications in hardware implementations, especially masked implementations.

Goals:

- algebraic degree of G_i should be small (typically 2 or 3),
- ℓ should also be as small as possible.

Carlitz Theorem [Car53]

Let $\mathbb{F}_q$ be a finite field, then all permutation polynomials are generated by $x^{-1} = x^{q-2}$ and the affine polynomials $ax + b$, with $a, b \in \mathbb{F}_q$, $a \neq 0$.

Which means, for any $F(x)$ permutation polynomial in $\mathbb{F}_{p^n}[x]$,

$$F(x) = A_1(x) \circ x^{-1} \circ A_2(x) \circ x^{-1} \circ \cdots \circ A_{\ell-1}(x) \circ x^{-1} \circ A_\ell(x),$$

and $A_i(x) = a_i x + b_i$.

Further need to decompose x^{-1} into low algebraic degree functions G_i.

- use generic low degree polynomials,
- use low degree **power permutations**

Carlitz Theorem [Car53]

Let $\mathbb{F}_q$ be a finite field, then all permutation polynomials are generated by $x^{-1} = x^{q-2}$ and the affine polynomials $ax + b$, with $a, b \in \mathbb{F}_q$, $a \neq 0$.

Which means, for any $F(x)$ permutation polynomial in $\mathbb{F}_{p^n}[x]$,

$$F(x) = A_1(x) \circ x^{-1} \circ A_2(x) \circ x^{-1} \circ \cdots \circ A_{\ell-1}(x) \circ x^{-1} \circ A_\ell(x),$$

and $A_i(x) = a_i x + b_i$.

Further need to decompose x^{-1} into low algebraic degree functions G_i.

- use generic low degree polynomials,
- use low degree **power permutations**

Carlitz Theorem [Car53]

Let $\mathbb{F}_q$ be a finite field, then all permutation polynomials are generated by $x^{-1} = x^{q-2}$ and the affine polynomials $ax + b$, with $a, b \in \mathbb{F}_q$, $a \neq 0$.

Which means, for any $F(x)$ permutation polynomial in $\mathbb{F}_{p^n}[x]$,

$$F(x) = A_1(x) \circ x^{-1} \circ A_2(x) \circ x^{-1} \circ \cdots \circ A_{\ell-1}(x) \circ x^{-1} \circ A_\ell(x),$$

and $A_i(x) = a_i x + b_i$.

Further need to decompose x^{-1} into low algebraic degree functions G_i.

- use generic low degree polynomials,
- use low degree **power permutations**

Find decomposition

$$x^d = x^{e_1} \circ \ldots \circ x^{e_\ell},$$

where all power functions have algebraic degree no greater than two (or three).

The problem is equivalent to finding

$$d = e_1 \ldots e_\ell \pmod{p^n - 1},$$

where all factors have $p-$weight no greater than two (or three).

The existence of a decomposition of length ℓ, using factors of $p-$weight ω, is a cyclotomic invariant.

$$p^k d = p^k(e_1 \ldots e_\ell) = (p^k e_1) \ldots e_\ell \pmod{p^n - 1}$$

Find decomposition

$$x^d = x^{e_1} \circ \ldots \circ x^{e_\ell},$$

where all power functions have algebraic degree no greater than two (or three).

The problem is equivalent to finding

$$d = e_1 \ldots e_\ell \pmod{p^n - 1},$$

where all factors have $p-$weight no greater than two (or three).

The existence of a decomposition of length ℓ, using factors of $p-$weight ω, is a cyclotomic invariant.

$$p^k d = p^k(e_1 \ldots e_\ell) = (p^k e_1) \ldots e_\ell \pmod{p^n - 1}$$

Find decomposition

$$x^d = x^{e_1} \circ \ldots \circ x^{e_\ell},$$

where all power functions have algebraic degree no greater than two (or three).

The problem is equivalent to finding

$$d = e_1 \ldots e_\ell \pmod{p^n - 1},$$

where all factors have $p-$weight no greater than two (or three).

The existence of a decomposition of length ℓ, using factors of $p-$weight ω, is a cyclotomic invariant.

$$p^k d = p^k(e_1 \ldots e_\ell) = (p^k e_1) \ldots e_\ell \pmod{p^n - 1}$$

Previous Work

Search algorithm for $p = 2$ in [NNR19]

- Compute all exponents b of $2-$weight 2 in $Z^*_{p^n-1}$.
- Compute their orders m_b.
- Try all combinations of $\Pi_i b_i^{e_i}$ for $e_i = 0, \ldots, m_{b_i}$.

Later improved by Petrides in [Pet23].

Decompositions for the inverse for infinite values of n

- using only quadratic power permutations [Pet23]
- using quadratic and cubic power permutations [LSaa23].

Previous Work

Search algorithm for $p = 2$ in [NNR19]

- Compute all exponents b of $2-$weight 2 in $Z^*_{p^n-1}$.
- Compute their orders m_b.
- Try all combinations of $\Pi_i b_i^{e_i}$ for $e_i = 0, \ldots, m_{b_i}$.

Later improved by Petrides in [Pet23].

Decompositions for the inverse for infinite values of n

- using only quadratic power permutations [Pet23]
- using quadratic and cubic power permutations [LSaa23].

Previous Work

Search algorithm for $p = 2$ in [NNR19]

- Compute all exponents b of $2-$weight 2 in $Z^*_{p^n-1}$.
- Compute their orders m_b.
- Try all combinations of $\Pi_i b_i^{e_i}$ for $e_i = 0, \ldots, m_{b_i}$.

Later improved by Petrides in [Pet23].

Decompositions for the inverse for infinite values of n

- using only quadratic power permutations [Pet23]
- using quadratic and cubic power permutations [LSaa23].

Our contribution

Consider

$$\mathcal{Q}_n = \left\langle 2^j, 2^i + 1 \in \mathbb{Z}^*_{2^n-1} \right\rangle \leqslant \mathbb{Z}^*_{2^n-1}$$

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in $\mathcal{Q}_n$,

Moreover, $\mathbb{Z}^*_{2^n-1}$ is cyclic if and only if $2^n - 1$ is prime.

$$\mathbb{Z}^*_{2^n-1} \text{ cyclic} \iff q \in \{2, 4, p^\ell, 2p^\ell\}$$

Our contribution

Consider

$$\mathcal{Q}_n = \left\langle 2^j, 2^i + 1 \in \mathbb{Z}^*_{2^n-1} \right\rangle \leqslant \mathbb{Z}^*_{2^n-1}$$

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in $\mathcal{Q}_n$,

Moreover, $\mathbb{Z}^*_{2^n-1}$ is cyclic if and only if $2^n - 1$ is prime.

$$\mathbb{Z}^*_{2^n-1} \text{ cyclic } \iff q \in \left\{2, 4, p^\ell, 2p^\ell\right\}$$

Our contribution

Consider

$$\mathcal{Q}_n = \left\langle 2^j, 2^i + 1 \in \mathbb{Z}^*_{2^n-1} \right\rangle \leqslant \mathbb{Z}^*_{2^n-1}$$

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in $\mathcal{Q}_n$,

Moreover, $\mathbb{Z}^*_{2^n-1}$ is cyclic if and only if $2^n - 1$ is prime.

$$\mathbb{Z}^*_{2^n-1} \text{ cyclic } \iff q \in \left\{2, 4, p^\ell, 2p^\ell\right\}$$

Our contribution

Consider

$$\mathcal{Q}_n = \left\langle 2^j, 2^i + 1 \in \mathbb{Z}^*_{2^n-1} \right\rangle \leqslant \mathbb{Z}^*_{2^n-1}$$

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in $\mathcal{Q}_n$,

Moreover, $\mathbb{Z}^*_{2^n-1}$ is cyclic if and only if $2^n - 1$ is prime.

$$\mathbb{Z}^*_{2^n-1} \text{ cyclic } \iff q \in \left\{2, 4, p^\ell, 2p^\ell\right\}$$

Our contribution

Consider

$$\mathcal{Q}_n = \left\langle 2^j, 2^i + 1 \in \mathbb{Z}^*_{2^n-1} \right\rangle \leqslant \mathbb{Z}^*_{2^n-1}$$

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in $\mathcal{Q}_n$,

Moreover, $\mathbb{Z}^*_{2^n-1}$ is cyclic if and only if $2^n - 1$ is prime.

$$\mathbb{Z}^*_{2^n-1} \text{ cyclic} \iff q \in \left\{2, 4, p^\ell, 2p^\ell\right\}$$

Our contribution

Consider

$$\mathcal{Q}_n = \left\langle 2^j, 2^i + 1 \in \mathbb{Z}^*_{2^n-1} \right\rangle \leqslant \mathbb{Z}^*_{2^n-1}$$

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in $\mathcal{Q}_n$,

Moreover, $\mathbb{Z}^*_{2^n-1}$ is cyclic if and only if $2^n - 1$ is prime.

$$\mathbb{Z}^*_{2^n-1} \text{ cyclic} \iff q \in \{p^\ell\}$$

If $2^n - 1 = p^\ell$, then $2^n - p^l = 1$, and $(x, y, a, b) = (2, p, n, l)$ would be a solution to $x^a - y^b = 1$

Our contribution

Consider

$$\mathcal{Q}_n = \left\langle 2^j, 2^i + 1 \in \mathbb{Z}^*_{2^n-1} \right\rangle \leqslant \mathbb{Z}^*_{2^n-1}$$

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in $\mathcal{Q}_n$,

Moreover, $\mathbb{Z}^*_{2^n-1}$ is cyclic if and only if $2^n - 1$ is prime.

$$\mathbb{Z}^*_{2^n-1} \text{ cyclic} \iff 2^n - 1 = p$$

ERRATA A decomposition always exists for the inverse since $\left(\frac{3}{2^n-1}\right) = -1$, but 3 might not be a generator.

[APB+23, Theorem 3.3]

Let $2^n - 1 = p$ be a prime. Then $\mathcal{Q}_n = \mathbb{Z}^*_{2^n-1} =< 3 >$. If $p \equiv 3 \pmod 4$, then it is also generated by 5.

It is enough to compute the *Legendre Symbols* of 3 and 5, defined as

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}},$$

which are equal to -1 if and only if a is a primitive element of $\mathbb{Z}^*_p$

ERRATA A decomposition always exists for the inverse since $\left(\frac{3}{2^n-1}\right) = -1$, but 3 might not be a generator.

[APB+23, Theorem 3.3]

Let $2^n - 1 = p$ be a prime. Then $\mathcal{Q}_n = \mathbb{Z}^*_{2^n-1} =< 3 >$. If $p \equiv 3 \pmod 4$, then it is also generated by 5.

It is enough to compute the *Legendre Symbols* of 3 and 5, defined as

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}},$$

which are equal to -1 if and only if a is a primitive element of $\mathbb{Z}^*_p$

[APB+23, Lemma 3.1]

Let $n = 4t$. If $k \neq 2^i \pmod{2^4 - 1}$, then $k \notin \mathcal{Q}_n$.

It is computationally verified that $7, 13, 14 \notin \mathcal{Q}_4$.

- $\mathcal{Q}_4$ is a subgroup of $\mathcal{Q}_{4t}$, so $k \in \mathcal{Q}_{4t} \implies k \mod 2^4 - 1 \in \mathcal{Q}_4$.
- $n = 4t$, and $k = 7, 13, 14 \mod 2^4 - 1 \implies k \notin \mathcal{Q}_n$.

[APB+23, Lemma 3.1]

Let $n = 4t$. If $k \in \mathcal{Q}_n$, then $\delta_{x^k} \geq 16$.

By Lemma 3.1, we have that for any $x \in \mathbb{F}_{2^4}$

$$(x+1)^k + x^k = x^k + 1 + x^k = 1.$$

[APB+23, Lemma 3.1]

Let $n = 4t$. If $k \neq 2^i \pmod{2^4 - 1}$, then $k \notin \mathcal{Q}_n$.

It is computationally verified that $7, 13, 14 \notin \mathcal{Q}_4$.

- $\mathcal{Q}_4$ is a subgroup of $\mathcal{Q}_{4t}$, so $k \in \mathcal{Q}_{4t} \implies k \mod 2^4 - 1 \in \mathcal{Q}_4$.
- $n = 4t$, and $k = 7, 13, 14 \mod 2^4 - 1 \implies k \notin \mathcal{Q}_n$.

[APB+23, Lemma 3.1]

Let $n = 4t$. If $k \in \mathcal{Q}_n$, then $\delta_{x^k} \geq 16$.

By Lemma 3.1, we have that for any $x \in \mathbb{F}_{2^4}$

$$(x+1)^k + x^k = x^k + 1 + x^k = 1.$$

[APB+23, Lemma 3.1]

Let $n = 4t$. If $k \neq 2^i \pmod{2^4 - 1}$, then $k \notin \mathcal{Q}_n$.

It is computationally verified that $7, 13, 14 \notin \mathcal{Q}_4$.

- $\mathcal{Q}_4$ is a subgroup of $\mathcal{Q}_{4t}$, so $k \in \mathcal{Q}_{4t} \implies k \mod 2^4 - 1 \in \mathcal{Q}_4$.
- $n = 4t$, and $k = 7, 13, 14 \mod 2^4 - 1 \implies k \notin \mathcal{Q}_n$.

[APB+23, Lemma 3.1]

Let $n = 4t$. If $k \in \mathcal{Q}_n$, then $\delta_{x^k} \geq 16$.

By Lemma 3.1, we have that for any $x \in \mathbb{F}_{2^4}$

$$(x+1)^k + x^k = x^k + 1 + x^k = 1.$$

To sum up:

- ERRATA Existence result for $2^n - 1$ prime.
- Inexistence result for $n = 4t$, $\delta_{x^d} < 16$.

Intermediate cases are group membership problems.

To sum up:

- ERRATA Existence result for $2^n - 1$ prime.
- Inexistence result for $n = 4t$, $\delta_{x^d} < 16$.

Intermediate cases are group membership problems.

[Sta98, Theorem 1]

Let k, q be positive integers, $q = p^n > 2$, and $\gcd(k, q-1) = 1$. Then all permutation polynomials are generated by x^k and the affine polynomials $ax + b$, with $a, b \in \mathbb{F}_q, a \neq 0$, if and only if

- p is odd and $k \neq p^i$, or
- $p = 2$ and x^k is an odd permutation.

Which means, for any $F(x)$ permutation polynomial in $\mathbb{F}_{p^n}[x]$,

$$F = A_1(x) \circ x^k \circ A_2(x) \circ x^k \circ \cdots \circ A_{\ell-1}(x) \circ x^k \circ A_\ell(x).$$

No further need to decompose the power function x^k if chosen appropriately!

- For p odd, no particular work to do.
- For p even, how to characterize the parity of a power permutation?

[Sta98, Theorem 1]

Let k, q be positive integers, $q = p^n > 2$, and $\gcd(k, q-1) = 1$. Then all permutation polynomials are generated by x^k and the affine polynomials $ax + b$, with $a, b \in \mathbb{F}_q, a \neq 0$, if and only if

- p is odd and $k \neq p^i$, or
- $p = 2$ and x^k is an odd permutation.

Which means, for any $F(x)$ permutation polynomial in $\mathbb{F}_{p^n}[x]$,

$$F = A_1(x) \circ x^k \circ A_2(x) \circ x^k \circ \cdots \circ A_{\ell-1}(x) \circ x^k \circ A_\ell(x).$$

No further need to decompose the power function x^k if chosen appropriately!

- For p odd, no particular work to do.
- For p even, how to characterize the parity of a power permutation?

[Sta98, Theorem 1]

Let k, q be positive integers, $q = p^n > 2$, and $\gcd(k, q-1) = 1$. Then all permutation polynomials are generated by x^k and the affine polynomials $ax + b$, with $a, b \in \mathbb{F}_q, a \neq 0$, if and only if

- p is odd and $k \neq p^i$, or
- $p = 2$ and x^k is an odd permutation.

Which means, for any $F(x)$ permutation polynomial in $\mathbb{F}_{p^n}[x]$,

$$F = A_1(x) \circ x^k \circ A_2(x) \circ x^k \circ \cdots \circ A_{\ell-1}(x) \circ x^k \circ A_\ell(x).$$

No further need to decompose the power function x^k if chosen appropriately!

- For p odd, no particular work to do.
- For p even, how to characterize the parity of a power permutation?

Previous Work

There are earlier attempts to characterise the parity of power permutations [ÇÖ21]

- Efficient algorithm to compute the parity of a power permutation.
- Conjecture about the parity of quadratic power permutations:

[ÇÖ21, Conjecture 6.3]

- For all n odd integers, the power permutation x^3 is odd over $\mathbb{F}_{2^n}$,
- for all $n \equiv 2, 3 \pmod 4$, the power permutation x^5 is odd over $\mathbb{F}_{2^n}$,
- for all n multiples of 4 and not a power of 2, all quadratic permutations are even over $\mathbb{F}_{2^n}$.

Previous Work

There are earlier attempts to characterise the parity of power permutations [ÇÖ21]

- Efficient algorithm to compute the parity of a power permutation.
- Conjecture about the parity of quadratic power permutations:

[ÇÖ21, Conjecture 6.3]

- For all n odd integers, the power permutation x^3 is odd over $\mathbb{F}_{2^n}$,
- for all $n \equiv 2, 3 \pmod 4$, the power permutation x^5 is odd over $\mathbb{F}_{2^n}$,
- for all n multiples of 4 and not a power of 2, all quadratic permutations are even over $\mathbb{F}_{2^n}$.

Zolotoroff-Frobenius Lemma [Fro14]

Let a, b be positive integers, $b \geq 3$ odd, and $\gcd(a, b) = 1$. Let $\sigma_a : \mathbb{Z}_b \to \mathbb{Z}_b$ be the multiplication map $x \mapsto ax$. Then

$$sgn(\sigma_a) = \left(\frac{a}{b}\right).$$

Where the *Jacobi Symbol* for any odd $N = p_1^{e_1} \dots p_\ell^{e_\ell}$ is

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_\ell}\right)^{e_\ell}.$$

- Alternative proof of Gauss Law of Quadratic Reciprocity by Zolotoroff,
- extended by Frobenius to all **odd** N.

Our Contribution

[APB$^+$23, Lemma 4.1]

Let $n \geq 3$, and x^k a power permutation in $\mathbb{F}_{2^n}[x]$. Then $\operatorname{sgn}(x^k) = \left(\frac{k}{2^n-1}\right)$.

Let α be a primitive element of $\mathbb{F}_{2^n}$,

$$\Psi_\alpha : \mathbb{Z}_{2^n-1} \to \mathbb{F}_{2^n} \setminus \{0\}$$
$$b \mapsto \alpha^b$$

is an isomorphism.

Our Contribution

[APB$^+$23, Lemma 4.1]

Let $n \geq 3$, and x^k a power permutation in $\mathbb{F}_{2^n}[x]$. Then $\operatorname{sgn}(x^k) = \left(\frac{k}{2^n-1}\right)$.

Let α be a primitive element of $\mathbb{F}_{2^n}$,

$$\begin{aligned} \Psi_\alpha : \mathbb{Z}_{2^n-1} &\to \mathbb{F}_{2^n} \setminus \{0\} \\ b &\mapsto \alpha^b \end{aligned}$$

is an isomorphism.

[APB+23, Tehorem 4.1]

Let $n \geq 3$. Then

1. x^3 is an odd permutation over $\mathbb{F}_{2^n}$ if and only if $n \equiv 1 \pmod 2$,
2. x^5 is an odd permutation over $\mathbb{F}_{2^n}$ if and only if $n \equiv 2, 3 \pmod 4$,
3. quadratic power permutations over $\mathbb{F}_{2^n}$ are even for any $n \equiv 0 \pmod 4$.

- $(1-2)$ are direct computations of the Jacobi Symbol.
- (3) proved by induction on $n = 4t$, by manipulating $\left(\frac{2^i+1}{2^n-1}\right)$.

[APB+23, Theorem 4.2]

Let $n \geq 3$. All permutations over $\mathbb{F}_{2^n}$ admit a decomposition using quadratic and affine permutations if and only if $4 \nmid n$.

[APB$^+$23, Tehorem 4.1]

Let $n \geq 3$. Then

1. x^3 is an odd permutation over $\mathbb{F}_{2^n}$ if and only if $n \equiv 1 \pmod 2$,
2. x^5 is an odd permutation over $\mathbb{F}_{2^n}$ if and only if $n \equiv 2, 3 \pmod 4$,
3. quadratic power permutations over $\mathbb{F}_{2^n}$ are even for any $n \equiv 0 \pmod 4$.

- $(1-2)$ are direct computations of the Jacobi Symbol.
- (3) proved by induction on $n = 4t$, by manipulating $\left(\frac{2^i+1}{2^n-1}\right)$.

[APB$^+$23, Theorem 4.2]

Let $n \geq 3$. All permutations over $\mathbb{F}_{2^n}$ admit a decomposition using quadratic and affine permutations if and only if $4 \nmid n$.

[APB+23, Tehorem 4.1]

Let $n \geq 3$. Then

1. x^3 is an odd permutation over $\mathbb{F}_{2^n}$ if and only if $n \equiv 1 \pmod 2$,
2. x^5 is an odd permutation over $\mathbb{F}_{2^n}$ if and only if $n \equiv 2, 3 \pmod 4$,
3. quadratic power permutations over $\mathbb{F}_{2^n}$ are even for any $n \equiv 0 \pmod 4$.

- $(1-2)$ are direct computations of the Jacobi Symbol.
- (3) proved by induction on $n = 4t$, by manipulating $\left(\frac{2^i+1}{2^n-1}\right)$.

[APB+23, Theorem 4.2]

Let $n \geq 3$. All permutations over $\mathbb{F}_{2^n}$ admit a decomposition using quadratic and affine permutations if and only if $4 \nmid n$.

[APB+23, Theorem 4.3]

Let $n \geq 3$, $n = 2^{\nu_2(n)} s$, so that s is odd. Then x^{k_n} is an odd power permutation, where

- $k_n = 2^{2s} + 2^s + 1$, for any n, except when $s = 1$ and $\nu_2(n)$ is an odd integer,
- $k_n = 13$, if $s = 1$ and $\nu_2(n)$ is an odd integer.

Where both statements are proved by direct computations of the Jacobi Symbols case by case.

[APB+23, Theorem 4.4]

Let $n \geq 3$. All permutations on $\mathbb{F}_{2^n}$ admit a decomposition in cubic power permutations and affine permutations.

[APB+23, Theorem 4.3]

Let $n \geq 3$, $n = 2^{\nu_2(n)}s$, so that s is odd. Then x^{k_n} is an odd power permutation, where

- $k_n = 2^{2s} + 2^s + 1$, for any n, except when $s = 1$ and $\nu_2(n)$ is an odd integer,
- $k_n = 13$, if $s = 1$ and $\nu_2(n)$ is an odd integer.

Where both statements are proved by direct computations of the Jacobi Symbols case by case.

[APB+23, Theorem 4.4]

Let $n \geq 3$. All permutations on $\mathbb{F}_{2^n}$ admit a decomposition in cubic power permutations and affine permutations.

[APB+23, Theorem 4.3]

Let $n \geq 3$, $n = 2^{\nu_2(n)}s$, so that s is odd. Then x^{k_n} is an odd power permutation, where

- $k_n = 2^{2s} + 2^s + 1$, for any n, except when $s = 1$ and $\nu_2(n)$ is an odd integer,
- $k_n = 13$, if $s = 1$ and $\nu_2(n)$ is an odd integer.

Where both statements are proved by direct computations of the Jacobi Symbols case by case.

[APB+23, Theorem 4.4]

Let $n \geq 3$. All permutations on $\mathbb{F}_{2^n}$ admit a decomposition in cubic power permutations and affine permutations.

To sum up

- p odd, all nonlinear power permutations can be used to generate the permutation polynomials.
- $p = 2$:
  - Even permutations can be decomposed using quadratics iff n is not a power of 2.
  - Odd permutations can be decomposed using quadratics iff $4 \nmid n$.
  - All permutations can be decomposed using cubics for any n.

Search for decomposition of *reasonable* length.

$$F = (a_1 x + b_1) \circ x^k \circ \cdots \circ x^k \circ (a_\ell x + b_\ell)$$

Naive brute force search is $\mathcal{O}(2^{2n\ell})$.

Some simple observations can improve the situation drastically.

- Search up to affine equivalence:
  - incorporate $a_1 x + b_1$ and $a_\ell x + b_\ell$ in the affine permutations.
  - The check for Affine equivalence can be implemented efficiently.
  - Target the whole class of equivalence.
- $(ax+b)^k = a^k(x+ba^{-1})^k$, so only b_i need to be bruteforced.

This improves the search spaze size and gives a complexity of $\mathcal{O}(2^{2n\ell})$.

Search for decomposition of *reasonable* length.

$$F = (a_1 x + b_1) \circ x^k \circ \cdots \circ x^k \circ (a_\ell x + b_\ell)$$

Naive brute force search is $\mathcal{O}(2^{2n\ell})$.

Some simple observations can improve the situation drastically.

- Search up to affine equivalence:
  - incorporate $a_1 x + b_1$ and $a_\ell x + b_\ell$ in the affine permutations.
  - The check for Affine equivalence can be implemented efficiently.
  - Target the whole class of equivalence.
- $(ax + b)^k = a^k (x + ba^{-1})^k$, so only b_i need to be bruteforced.

This improves the search spaze size and gives a complexity of $\mathcal{O}(2^{2n\ell})$.

Search for decomposition of *reasonable* length.

$$F = (a_1 x + b_1) \circ x^k \circ \cdots \circ x^k \circ (a_\ell x + b_\ell)$$

Naive brute force search is $\mathcal{O}(2^{2n\ell})$.

Some simple observations can improve the situation drastically.

- Search up to affine equivalence:
  - incorporate $a_1 x + b_1$ and $a_\ell x + b_\ell$ in the affine permutations.
  - The check for Affine equivalence can be implemented efficiently.
  - Target the whole class of equivalence.
- $(ax + b)^k = a^k (x + ba^{-1})^k$, so only b_i need to be bruteforced.

This improves the search spaze size and gives a complexity of $\mathcal{O}(2^{2^{n\ell}})$.

Search for decomposition of *reasonable* length.

$$F = (a_1 x + b_1) \circ x^k \circ \cdots \circ x^k \circ (a_\ell x + b_\ell)$$

Naive brute force search is $\mathcal{O}(2^{2n\ell})$.

Some simple observations can improve the situation drastically.

- Search up to affine equivalence:
  - incorporate $a_1 x + b_1$ and $a_\ell x + b_\ell$ in the affine permutations.
  - The check for Affine equivalence can be implemented efficiently.
  - Target the whole class of equivalence.
- $(ax + b)^k = a^k (x + ba^{-1})^k$, so only b_i need to be bruteforced.

This improves the search spaze size and gives a complexity of $\mathcal{O}(2^{2n\ell})$.

Search for decomposition of *reasonable* length.

$$F = (a_1 x + b_1) \circ x^k \circ \cdots \circ x^k \circ (a_\ell x + b_\ell)$$

Naive brute force search is $\mathcal{O}(2^{2n\ell})$.

Some simple observations can improve the situation drastically.

- Search up to affine equivalence:
  - incorporate $a_1 x + b_1$ and $a_\ell x + b_\ell$ in the affine permutations.
  - The check for Affine equivalence can be implemented efficiently.
  - Target the whole class of equivalence.
- $(ax + b)^k = a^k (x + ba^{-1})^k$, so only b_i need to be bruteforced.

This improves the search spaze size and gives a complexity of $\mathcal{O}(2^{2n\ell})$.

Target the PRESENT S-Box [BKL+07]:

- Cubic permutation polynomial in $\mathbb{F}_{2^4}$, `C56B90AD3EF84712`,
- use the cubic power permutation x^7,
- no improvement in terms of degree, but now it can be expressed as power permutations and XORs.

The algorithm yields a decomposition of length 7 in a few seconds:

$$x^7 \circ (x+3) \circ x^7 \circ (x+4) \circ x^7 \circ (x+3) \circ x^7 \circ (x+3) \circ x^7 \circ (x+3) \circ x^7.$$

Searches for different examples are still ongoing with different targets.

Target the PRESENT S-Box [BKL+07]:

- Cubic permutation polynomial in $\mathbb{F}_{2^4}$, `C56B90AD3EF84712`,
- use the cubic power permutation x^7,
- no improvement in terms of degree, but now it can be expressed as power permutations and XORs.

The algorithm yields a decomposition of length 7 in a few seconds:

$$x^7 \circ (x+3) \circ x^7 \circ (x+4) \circ x^7 \circ (x+3) \circ x^7 \circ (x+3) \circ x^7 \circ (x+3) \circ x^7.$$

Searches for different examples are still ongoing with different targets.

Target the PRESENT S-Box [BKL+07]:

- Cubic permutation polynomial in $\mathbb{F}_{2^4}$, `C56B90AD3EF84712`,
- use the cubic power permutation x^7,
- no improvement in terms of degree, but now it can be expressed as power permutations and XORs.

The algorithm yields a decomposition of length 7 in a few seconds:

$$x^7 \circ (x+3) \circ x^7 \circ (x+4) \circ x^7 \circ (x+3) \circ x^7 \circ (x+3) \circ x^7 \circ (x+3) \circ x^7.$$

Searches for different examples are still ongoing with different targets.

Let $G = \{x^k\} \bigcup \{ax + b | a, b \in \mathbb{F}_q, a \neq 0\}$. If the hypotheses of Stafford's theorem are fulfilled, $\mathrm{Sym}(\mathbb{F}_q) =< G >$.

Finding a *word* $g_1 \circ \ldots \circ g_\ell = \pi \in \mathrm{Sym}(\mathbb{F}_q)$, $g_i \in G$ is an old problem.

- Schreier and Sims presented an efficient algorithm in [SIM70].
- Knuth provided an implementation running time of $\mathcal{O}(q^5)$ in [Knu91].

Problem

Schreier-Sims produces words including the inverse of generators. The inverse of a quadratic power permutation over $\mathbb{F}_{2^n}$ can have algebraic degree up to $\frac{n+1}{2}$ [Nyb93].

Let $G = \{x^k\} \bigcup \{ax + b | a, b \in \mathbb{F}_q, a \neq 0\}$. If the hypotheses of Stafford's theorem are fulfilled, $\mathrm{Sym}(\mathbb{F}_q) =< G >$.

Finding a *word* $g_1 \circ \ldots \circ g_\ell = \pi \in \mathrm{Sym}(\mathbb{F}_q)$, $g_i \in G$ is an old problem.

- Schreier and Sims presented an efficient algorithm in [SIM70].
- Knuth provided an implementation running time of $\mathcal{O}(q^5)$ in [Knu91].

Problem

Schreier-Sims produces words including the inverse of generators. The inverse of a quadratic power permutation over $\mathbb{F}_{2^n}$ can have algebraic degree up to $\frac{n+1}{2}$ [Nyb93].

Let $G = \left\{x^k\right\} \bigcup \left\{ax + b | a, b \in \mathbb{F}_q, a \neq 0\right\}$. If the hypotheses of Stafford's theorem are fulfilled, $\mathrm{Sym}\left(\mathbb{F}_q\right) =< G >$.

Finding a *word* $g_1 \circ \ldots \circ g_\ell = \pi \in \mathrm{Sym}\left(\mathbb{F}_q\right)$, $g_i \in G$ is an old problem.

- Schreier and Sims presented an efficient algorithm in [SIM70].
- Knuth provided an implementation running time of $\mathcal{O}(q^5)$ in [Knu91].

Problem

Schreier-Sims produces words including the inverse of generators. The inverse of a quadratic power permutation over $\mathbb{F}_{2^n}$ can have algebraic degree up to $\frac{n+1}{2}$ [Nyb93].

A different approach is presented in [Tan11].

- Main focus: a bound for the diameter of $\mathrm{Sym}\,(n)$ given a set of generators.
- Possible to derive an algorithm producing words of length $\mathcal{O}(n2^n)$.

This algorithm uses cycles of length 3 as stepping stones, so their representation is critical.

Problem

For $n = 4$, these permutations already have decompositions of length $\ell \geq 12$.
For $n = 5$, the computation is ongoing.

A different approach is presented in [Tan11].

- Main focus: a bound for the diameter of $\mathrm{Sym}(n)$ given a set of generators.
- Possible to derive an algorithm producing words of length $\mathcal{O}(n2^n)$.

This algorithm uses cycles of length 3 as stepping stones, so their representation is critical.

Problem

For $n = 4$, these permutations already have decompositions of length $\ell \geq 12$.
For $n = 5$, the computation is ongoing.

A different approach is presented in [Tan11].

- Main focus: a bound for the diameter of $\mathrm{Sym}\,(n)$ given a set of generators.
- Possible to derive an algorithm producing words of length $\mathcal{O}(n2^n)$.

This algorithm uses cycles of length 3 as stepping stones, so their representation is critical.

Problem

For $n = 4$, these permutations already have decompositions of length $\ell \geq 12$. For $n = 5$, the computation is ongoing.

Conclusions and Open Problems

- Power Functions
  - (Sub)Group Membership in $\mathbb{Z}^*_{2^n-1}$
  - Extend to $\mathbb{Z}^*_{p^n-1}$?
- Carlitz Decompositions
- Stafford Decomposition
  - Possible to further reduce the search space?
  - Group membership algorithms, $\ell \sim \mathcal{O}(n^5)$
  - Possible to have better membership algorithms, exploiting the shape of the generators?
- Better decompositions by relaxing the requisites on the algebraic degree?

Thank you!

Questions?

Conclusions and Open Problems

- Power Functions
  - (Sub)Group Membership in $\mathbb{Z}^*_{2^n-1}$
  - Extend to $\mathbb{Z}^*_{p^n-1}$?
- Carlitz Decompositions
- Stafford Decomposition
  - Possible to further reduce the search space?
  - Group membership algorithms, $\ell \sim \mathcal{O}(n^5)$
  - Possible to have better membership algorithms, exploiting the shape of the generators?
- Better decompositions by relaxing the requisites on the algebraic degree?

Thank you!

Questions?

Conclusions and Open Problems

- Power Functions
  - (Sub)Group Membership in $\mathbb{Z}^*_{2^n-1}$
  - Extend to $\mathbb{Z}^*_{p^n-1}$?
- Carlitz Decompositions
- Stafford Decomposition
  - Possible to further reduce the search space?
  - Group membership algorithms, $\ell \sim \mathcal{O}(n^5)$
  - Possible to have better membership algorithms, exploiting the shape of the generators?
- Better decompositions by relaxing the requisites on the algebraic degree?

Thank you!

Questions?

Conclusions and Open Problems

- Power Functions
  - (Sub)Group Membership in $\mathbb{Z}^*_{2^n-1}$
  - Extend to $\mathbb{Z}^*_{p^n-1}$?
- Carlitz Decompositions
- Stafford Decomposition
  - Possible to further reduce the search space?
  - Group membership algorithms, $\ell \sim \mathcal{O}(n^5)$
  - Possible to have better membership algorithms, exploiting the shape of the generators?
- Better decompositions by relaxing the requisites on the algebraic degree?

Thank you!

Questions?

Conclusions and Open Problems

- Power Functions
  - (Sub)Group Membership in $\mathbb{Z}^*_{2^n-1}$
  - Extend to $\mathbb{Z}^*_{p^n-1}$?
- Carlitz Decompositions
- Stafford Decomposition
  - Possible to further reduce the search space?
  - Group membership algorithms, $\ell \sim \mathcal{O}(n^5)$
  - Possible to have better membership algorithms, exploiting the shape of the generators?
- Better decompositions by relaxing the requisites on the algebraic degree?

Thank you!

Questions?

Samuele Andreoli, Enrico Piccione, Lilya Budaghyan, Pantelimon Stănică, and Svetla Nikova, *On decompositions of permutations in quadratic functions*, Cryptology ePrint Archive, Paper 2023/1632, 2023, https://eprint.iacr.org/2023/1632.

Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe, *PRESENT: an ultra-lightweight block cipher*, Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings (Pascal Paillier and Ingrid Verbauwhede, eds.), LNCS, vol. 4727, Springer, 2007, pp. 450–466.

Leonard Carlitz, *Permutations in a finite field*, Proc. AMS (1953), 538.

Pinar Çomak and Ferruh Özbudak, *On the parity of power permutations*, IEEE Access **9** (2021), 106806–106812.

Georg Ferdinand Frobenius, *Über das quadratische reziprozitätsgesetz i, ii*, Königliche Akademie der Wissenschaften, 1914.

- Donald E. Knuth, *Efficient representation of perm groups*, 1991.
- Florian Luca, Santanu Sarkar, and Pantelimon Stănică, *Representing the inverse map as a composition of quadratics in a finite field of characteristic* 2, arXiv (2023).
- Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen, *Decomposition of permutations in a finite field*, Cryptogr. Commun. **11** (2019), no. 3, 379–384.
- Kaisa Nyberg, *Differentially uniform mappings for cryptography*, Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings (Tor Helleseth, ed.), LNCS, vol. 765, Springer, 1993, pp. 55–64.
- George Petrides, *On decompositions of permutation polynomials into quadratic and cubic power permutations*, Cryptogr. Commun. **15** (2023), no. 1, 199–207.

CHARLES C. SIMS, *Computational methods in the study of permutation groups††this research was supported in part by the national science foundation.*, Computational Problems in Abstract Algebra (JOHN LEECH, ed.), Pergamon, 1970, pp. 169–183.

Richard M. Stafford, *Groups of permutation polynomials over finite fields*, Finite Fields and Their Applications **4** (1998), no. 4, 450–452.

Yan Shuo Tan, *On the diameter of cayley graphs of finite groups*, University of Chicago VIGRE REU (2011).