Decompositions of Permutations in a Finite Field

Samuele Andreoli
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 $F : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ 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 $d^\circ(F) = \max_{\alpha_i \neq 0} w_p(i)$, where $w_p$ is the $p$–weight.

A power function is a monomial $x^k$, $1 \leq k < p^n - 1$ and $d^\circ(F) = w_p(k)$. 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 $d^\circ(F) = \max_{\alpha_i \neq 0} w_p(i)$, where $w_p$ is the $p$–weight.

A power function is a monomial $x^k$, $1 \leq k < p^n - 1$ and $d^\circ(F) = w_p(k)$. 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 $d^\circ(F) = \max_{\alpha_i \neq 0} w_p(i)$, where $w_p$ is the $p$–weight.

A power function is a monomial $x^k$, $1 \leq k < p^n - 1$ and $d^\circ(F) = w_p(k)$. An invertible power function is a power permutation.
A function $F : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ is called an $(n, n)$–function.

A $(n, n)$–function admits a representation as a univariate polynomial over $\mathbb{F}_p^n$, called \textit{univariate representation},

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

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

A \textit{power function} is a monomial $x^k$, $1 \leq k < p^n - 1$ and $d^\circ(F) = w_p(k)$. An invertible power function is a \textit{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, $\text{CCZ} \iff \text{Affine} \iff \text{Cyclotomic}$. 

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, $\text{CCZ} \iff \text{Affine} \iff \text{Cyclotomic}$.

*Differential uniformity* is defined as

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

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

We say that $F$ is *almost perfect nonlinear (APN)* if $\delta_F = 2$. 
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),
- \(\ell\) should also be as small as possible.
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),
- \(\ell\) 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),
- \(\ell\) should also be as small as possible.
1 Preliminaries

2 Decompositions using Carlitz

3 Decompositions using Stafford

4 Search of Decompositions

5 References
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 \( \ell \), using factors of \( p \)–weight \( \omega \), 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 \( \ell \), using factors of \( p \)-weight \( \omega \), 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 \( \ell \), using factors of \( p \)-weight \( \omega \), 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 $\mathbb{Z}_{p^n-1}^\ast$.
- Compute their orders $m_b$.
- Try all combinations of $\prod_i b_i^{e_i}$ 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 $\mathbb{Z}_{p^n-1}^*$.
- Compute their orders $m_b$.
- Try all combinations of $\prod_i b_i^{e_i}$ 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 $\mathbb{Z}_p^{*n-1}$.
- Compute their orders $m_b$.
- Try all combinations of $\prod_i b_i^{e_i}$ 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

\[ Q_n = \langle 2^i, 2^i + 1 \in \mathbb{Z}_{2^n-1}^* \rangle \leq \mathbb{Z}_{2^n-1}^* \]

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in \( Q_n \),

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

\[ Q_n = \langle 2^i, 2^i + 1 \in \mathbb{Z}_{2^n-1}^* \rangle \leq \mathbb{Z}_{2^n-1}^* \]

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in \( Q_n \).

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

\[ Q_n = \langle 2^i, 2^i + 1 \in \mathbb{Z}_{2^n}^* \rangle \leq \mathbb{Z}_{2^n}^* \]

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in \( Q_n \),

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

\[ \mathbb{Z}_{2^n}^* \text{ cyclic} \iff q \in \{2, 4, p^\ell, 2p^\ell\} \]
Our contribution

Consider

\[ Q_n = \langle 2^i, 2^i + 1 \in \mathbb{Z}_{2^n-1}^* \rangle \leq \mathbb{Z}_{2^n-1}^* \]

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in \( Q_n \),

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

\[ Q_n = \langle 2^i, 2^i + 1 \in \mathbb{Z}_{2^n-1}^* \rangle \leq \mathbb{Z}_{2^n-1}^* \]

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in \( Q_n \),

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

\[ Q_n = \langle 2^i, 2^i + 1 \in \mathbb{Z}_{2^n-1}^* \rangle \leq \mathbb{Z}_{2^n-1}^* \]

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in \( Q_n \),

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 \( 2^n - p^\ell = 1 \), and \( (x, y, a, b) = (2, p, n, l) \) would be a solution to \( x^a - y^b = 1 \).
Our contribution

Consider

\[ Q_n = \langle 2^j, 2^j + 1 \in \mathbb{Z}_{2^n-1}^* \rangle \leq \mathbb{Z}_{2^n-1}^* \]

We have one immediate observation:

- (Gold), Kasami, and Niho power functions belong in \( Q_n \),

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.

\[[\text{APB}^+23, \text{Theorem 3.3}]

Let \( 2^n - 1 = p \) be a prime. Then \( Q_n = \mathbb{Z}^{*}_{2^n-1} = \langle 3 \rangle \). 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

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

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\textsuperscript{+}23, Theorem 3.3]**

Let \( 2^n - 1 = p \) be a prime. Then \( Q_n = \mathbb{Z}_{2^n-1}^* = \langle 3 \rangle \). 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 \( \mathbb{Z}_p^* \).
Let $n = 4t$. If $k \not\equiv 2^i \pmod{2^4 - 1}$, then $k \not\in Q_n$.

It is computationally verified that $7, 13, 14 \not\in Q_4$.

- $Q_4$ is a subgroup of $Q_{4t}$, so $k \in Q_{4t} \implies k \mod 2^4 - 1 \in Q_4$.
- $n = 4t$, and $k = 7, 13, 14 \mod 2^4 - 1 \implies k \not\in Q_n$.

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

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

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

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

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

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

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

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

It is computationally verified that \( 7, 13, 14 \notin \mathbb{Q}_4 \).

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

Let \( n = 4t \). If \( k \in \mathbb{Q}_n \), 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 $n = 4t$, $\delta_{xd} < 16$.

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?
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 \( n \equiv 2, 3 \) (mod 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

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

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

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

- 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
\[
\text{sgn}(x^k) = \left( \frac{k}{2^n - 1} \right).
\]

Let \( \alpha \) 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 $\text{sgn}(x^k) = \left(\frac{k}{2^n-1}\right)$.

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

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

$$b \mapsto \alpha^b$$

is an isomorphism.
[APB$^+$23, Theorem 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 $4 \nmid n$. 
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 $\left(\frac{2^i+1}{2^n-1}\right)$.

Let $n \geq 3$. All permutations over $\mathbb{F}_{2^n}$ admit a decomposition using quadratic and affine permutations if and only if $4 \nmid n$. 
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 $\left(\frac{2^i + 1}{2^n - 1}\right)$.

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

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 $n \geq 3$, $n = 2^{
u_2(n)}s$, 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\textsuperscript{+}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\textsuperscript{+}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 $n$. 
1 Preliminaries

2 Decompositions using Carlitz

3 Decompositions using Stafford

4 Search of Decompositions

5 References
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 space 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 space 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 space 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 \( \mathcal{O}(2^{n\ell}) \).

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 space size and gives a complexity of \( \mathcal{O}(2^{n\ell}) \).
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 \( O(2^{2n\ell}) \).

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 space size and gives a complexity of \( O(2^{2n\ell}) \).
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 $\mathbb{F}_{2^4}$, $\text{C}5\text{6B90AD3EF84712}$,
- 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 $G = \{x^k\} \cup \{ax + b|a, b \in \mathbb{F}_q, a \neq 0\}$. If the hypotheses of Stafford's theorem are fulfilled, $\text{Sym}(\mathbb{F}_q) = \langle G \rangle$.

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

- Schreier and Sims presented an efficient algorithm in [SIM70].
- Knuth provided an implementation running time of $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 $G = \{ x^k \} \cup \{ ax + b | a, b \in \mathbb{F}_q, a \neq 0 \}$. If the hypotheses of Stafford’s theorem are fulfilled, $\text{Sym}(\mathbb{F}_q) = \langle G \rangle$.

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

- Schreier and Sims presented an efficient algorithm in [SIM70].
- Knuth provided an implementation running time of $O(q^5)$ 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 $G = \{ x^k \} \cup \{ ax + b \mid a, b \in \mathbb{F}_q, a \neq 0 \}$. If the hypotheses of Stafford's theorem are fulfilled, $\text{Sym}(\mathbb{F}_q) = \langle G \rangle$.

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

- Schreier and Sims presented an efficient algorithm in [SIM70].
- Knuth provided an implementation running time of $O(q^5)$ 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 $\text{Sym}(n)$ given a set of generators.
- Possible to derive an algorithm producing words of length $O(n2^n)$.

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 $\text{Sym}(n)$ given a set of generators.
- Possible to derive an algorithm producing words of length $O(n2^n)$.

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 $\text{Sym}(n)$ 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, $\ell \sim O(n^5)$
  - 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, $\ell \sim O(n^5)$
    - 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, $\ell \sim O(n^5)$
  - 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, $\ell \sim O(n^5)$
  - 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?


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.
