Further Existence Results of Decompositions of Permutation Polynomial

Samuele Andreoli, George Petrides

UNIVERSITY OF BERGEN

Why decompositions?

Permutation polynomials (PP) are at the base of many cryptographic primitives

- the inverse power function, notably, used for instance in AES
- generally, to achieve good cryptographic properties, have high degree

Much effort has gone into breaking down high degree PP into lower degree ones

- Reduce the area necessary for hardware implementations
- Enable area/latency tradeoffs
- Facilitate the usage of side-channel countermeasures, like masking or TIs

Why decompositions?

Permutation polynomials (PP) are at the base of many cryptographic primitives

- the inverse power function, notably, used for instance in AES
- generally, to achieve good cryptographic properties, have high degree

Much effort has gone into breaking down high degree PP into lower degree ones

- Reduce the area necessary for hardware implementations
- Enable area/latency tradeoffs
- Facilitate the usage of side-channel countermeasures, like masking or TIs

Preliminaries

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*.

Preliminaries

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*.

Preliminaries

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*.

Preliminaries

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*.

Decomposition

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

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

For applications in hardware implementations, especially masked implementations, goals are

- 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

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

For applications in hardware implementations, especially masked implementations, goals are

- 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).

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).

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 odd n

- using only quadratic power permutations [Pet23]
- using quadratic and cubic power permutations [LSaa23].
- using one quadratic power permutation [APB+23]

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 odd n

- using only quadratic power permutations [Pet23]
- using quadratic and cubic power permutations [LSaa23].
- using one quadratic power permutation [APB$^+$23]

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 odd n

- using only quadratic power permutations [Pet23]
- using quadratic and cubic power permutations [LSaa23].
- using one quadratic power permutation [APB$^+$23]

A criterion for the decomposition of the inverse

Lemma

Let n be an integer and x^d a power permutation of $\mathbb{F}_{2^n}$. The inversion power permutation in $\mathbb{F}_{2^n}$ admits a decomposition into the power function x^d if and only if $\mathrm{ord}\,(d)$ is even and $\gcd\left(2^n - 1, d^{\frac{\mathrm{ord}(d)}{2}} - 1\right) = 1$.

If $\mathrm{ord}\,(d)$ is even, then

$$d^{\mathrm{ord}(d)} - 1 \equiv \left(d^{\frac{\mathrm{ord}(d)}{2}} - 1\right)\left(d^{\frac{\mathrm{ord}(d)}{2}} + 1\right) \equiv 0 \pmod{2^n - 1}.$$

A criterion for the decomposition of the inverse

Lemma

Let n be an integer and x^d a power permutation of $\mathbb{F}_{2^n}$. The inversion power permutation in $\mathbb{F}_{2^n}$ admits a decomposition into the power function x^d if and only if $\operatorname{ord}(d)$ is even and $\gcd\left(2^n-1, d^{\frac{\operatorname{ord}(d)}{2}}-1\right)=1$.

If $\operatorname{ord}(d)$ is even, then

$$d^{\operatorname{ord}(d)}-1 \equiv \left(d^{\frac{\operatorname{ord}(d)}{2}}-1\right)\left(d^{\frac{\operatorname{ord}(d)}{2}}+1\right) \equiv 0 \pmod{2^n-1}.$$

Speeding up the search

- Efficient to check if the order is even computing the Jacobi Symbol
- Computing $\mathrm{ord}(d)/2$ and checking directly is more efficient than computing the gcd

Next step, try to reduce the search space with some equivalence relation.

Proposition

Let $n \geq 3$ and d be integers such that the conditions of the Lemma are satisfied. The conditions are also satisfied for n and $d' = 2^i d$ if and only if $\nu_2(n) \leq \nu_2(i)$.

- Only need to test $d' = 2^i d$ for $i = 0, \ldots, \nu_2(n)$ for each d.

Speeding up the search

- Efficient to check if the order is even computing the Jacobi Symbol
- Computing $\mathrm{ord}(d)/2$ and checking directly is more efficient than computing the gcd

Next step, try to reduce the search space with some equivalence relation.

Proposition

Let $n \geq 3$ and d be integers such that the conditions of the Lemma are satisfied. The conditions are also satisfied for n and $d' = 2^i d$ if and only if $\nu_2(n) \leq \nu_2(i)$.

- Only need to test $d' = 2^i d$ for $i = 0, \ldots, \nu_2(n)$ for each d.

Further improvement is possible for quadratic d.

Theorem. (A., Piccione, Budaghyan, Stănică, Nikova, 2023)

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

Test one representative d from each cyclotomic class, and $2d$ if n is even.

More efficient computational search than previously known, with caveats:

- Might return a longer than optimal decomposition
- It does not return for all possible n

We can further tweak the algorithm to achieve shorter decompositions.

Example. $n = 17, d = 3$

$3^{422} \equiv 2^8 \cdot 9 \pmod{2^{17}-1}$, then $-1 \equiv 3^{405} \equiv 2^8 \cdot 3 \cdot 9^{17} \pmod{2^{17}-1}$.
Repeat with 9^{17} to obtain the shortest decomposition.

Further improvement is possible for quadratic d.

Theorem. (A., Piccione, Budaghyan, Stănică, Nikova, 2023)

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

Test one representative d from each cyclotomic class, and $2d$ if n is even.

More efficient computational search than previously known, with caveats:

- Might return a longer than optimal decomposition
- It does not return for all possible n

We can further tweak the algorithm to achieve shorter decompositions.

Example. $n = 17, d = 3$

$3^{422} \equiv 2^8 \cdot 9 \pmod{2^{17} - 1}$, then $-1 \equiv 3^{405} \equiv 2^8 \cdot 3 \cdot 9^{17} \pmod{2^{17} - 1}$. Repeat with 9^{17} to obtain the shortest decomposition.

Further improvement is possible for quadratic d.

Theorem. (A., Piccione, Budaghyan, Stănică, Nikova, 2023)

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

Test one representative d from each cyclotomic class, and $2d$ if n is even.

More efficient computational search than previously known, with caveats:

- Might return a longer than optimal decomposition
- It does not return for all possible n

We can further tweak the algorithm to achieve shorter decompositions.

Example. $n = 17, d = 3$

$3^{422} \equiv 2^8 \cdot 9 \pmod{2^{17} - 1}$, then $-1 \equiv 3^{405} \equiv 2^8 \cdot 3 \cdot 9^{17} \pmod{2^{17} - 1}$. Repeat with 9^{17} to obtain the shortest decomposition.

Computational results

We run an exhaustive search for n up to 125 and we find many n for which the Lemma is satisfied.

$$3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 23, 26, 30, 31, 34, 38, 43, 46, \dots$$

Crucially, we might find families of **even** values of n.

The case of cubics: satisfied for all values up to 100, except

$$16, 32, 40, 48, 56, 60, 63, 64, 72, 75, 81, 84, 88, 96, \dots$$

- Optimal length achieved for some (sparse) values of n.
- Improvement of some order of magnitude for most decompositions found in [LSaa23].

Computational results

We run an exhaustive search for n up to 125 and we find many n for which the Lemma is satisfied.

$$3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 23, 26, 30, 31, 34, 38, 43, 46, \ldots$$

Crucially, we might find families of **even** values of n.

The case of cubics: satisfied for all values up to 100, except

$$16, 32, 40, 48, 56, 60, 63, 64, 72, 75, 81, 84, 88, 96, \ldots$$

- Optimal length achieved for some (sparse) values of n.
- Improvement of some order of magnitude for most decompositions found in [LSaa23].

Computational results

We run an exhaustive search for n up to 125 and we find many n for which the Lemma is satisfied.

$$3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 23, 26, 30, 31, 34, 38, 43, 46, \ldots$$

Crucially, we might find families of **even** values of n.

The case of cubics: satisfied for all values up to 100, except

$$16, 32, 40, 48, 56, 60, 63, 64, 72, 75, 81, 84, 88, 96, \ldots$$

- Optimal length achieved for some (sparse) values of n.
- Improvement of some order of magnitude for most decompositions found in [LSaa23].

The case of quadratics

Conjecture

The conditions of the Lemma are satisfied by some quadratic d for an odd integer n if and only if they are also satisfied for $2n$.

- Computationally verified for $n \geq 125$.

Why only a conjecture?

- Hard to prove the condition on the gcd if $2^n - 1$ has many factors.
- No single d can be used for all even n.

The case of quadratics

Conjecture

The conditions of the Lemma are satisfied by some quadratic d for an odd integer n if and only if they are also satisfied for $2n$.

- Computationally verified for $n \geq 125$.

Why only a conjecture?

- Hard to prove the condition on the gcd if $2^n - 1$ has many factors.
- No single d can be used for all even n.

Theorem

Let p be a prime such that $2^p - 1$ is also prime (a Mersenne prime). Then, the inversion power permutation in both $\mathbb{F}_{2^p}$ and $\mathbb{F}_{2^{2p}}$ has a decomposition into quadratic power permutations.

Proof by finding a suitable $d = 2^{p-1} + 1$ and proving it satisfies the conditions of the Lemma.

- Trivial for $n = p$.
- For $n = 2p$, the key is that $d^{-1} \equiv 2 \pmod{2^n - 1}$, so we can rewrite

$$\gcd\left(2^p + 1, d^{\frac{\mathrm{ord}_{2^{2p}-1}(d)}{2}} - 1\right) = \gcd\left(2^p + 1, 2^{\frac{\mathrm{ord}_{2^{2p}-1}(d)}{2}} - 1\right)$$

Work in progress

- Proving the conjecture for quadratics and using it to find other families.

The case of cubics

- The conjecture might also hold for cubics
- Harder to find patterns when most values of n have suitable d
- Finding families of d and n might be the right direction.

Tweak the algorithm to obtain shorter decompositions

- Is the greedy approach sufficient to produce short decompositions?
- Is there an approach to guarantee optimal decompositions?
- Can we theoretically prove the existence of such congruences?

Work in progress

- Proving the conjecture for quadratics and using it to find other families.

The case of cubics

- The conjecture might also hold for cubics
- Harder to find patterns when most values of n have suitable d
- Finding families of d and n might be the right direction.

Tweak the algorithm to obtain shorter decompositions

- Is the greedy approach sufficient to produce short decompositions?
- Is there an approach to guarantee optimal decompositions?
- Can we theoretically prove the existence of such congruences?

Work in progress

- Proving the conjecture for quadratics and using it to find other families.

The case of cubics

- The conjecture might also hold for cubics
- Harder to find patterns when most values of n have suitable d
- Finding families of d and n might be the right direction.

Tweak the algorithm to obtain shorter decompositions

- Is the greedy approach sufficient to produce short decompositions?
- Is there an approach to guarantee optimal decompositions?
- Can we theoretically prove the existence of such congruences?

Conclusions

- Criterion easy(ish) to use in proofs to find families
- First family of decompositions of the inverse for even values of n.
- With a small tweak, also efficient for computational searches
- Produce shorter decompositions than the state of the art

Thank you!

Questions?

Conclusions

- Criterion easy(ish) to use in proofs to find families
- First family of decompositions of the inverse for even values of n.
- With a small tweak, also efficient for computational searches
- Produce shorter decompositions than the state of the art

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.

L. Carlitz, *Permutations in a finite field*, 1953.

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.

George Petrides, *On decompositions of permutation polynomials into quadratic and cubic power permutations*, Cryptogr. Commun. **15** (2023), no. 1, 199–207.