Cycle types of complete mappings

Talk at the Carleton Finite Fields eSeminar

Alexander Bors (j/w Qiang Wang)

Carleton University, Ottawa

29th of September, 2021

Overview

1. Introduction: Complete mappings and cycle types
2. Our main results
3. Proof sketch of Theorem 4
4. References

Current section

1 Introduction: Complete mappings and cycle types

2 Our main results

3 Proof sketch of Theorem 4

4 References

Complete mappings: Background 1

[1] H.B. Mann, The construction of orthogonal Latin squares, *Ann. Math. Statistics* **13**: 418–423, 1942.

[2] R.H. Schulz, On check digit systems using anti-symmetric mappings, in: I. Althöfer et al. (eds.), *Numbers, information and complexity*, Kluwer, Boston, 2000, pp. 295–310.

[3] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014.

[4] A.B. Evans, *Orthogonal Latin Squares Based on Groups*, Springer (Developments in Mathematics, 57), Cham, 2018. Chapter 3.

Complete mappings: Background 1

- group-theoretic concept

[1] H.B. Mann, The construction of orthogonal Latin squares, *Ann. Math. Statistics* **13**: 418–423, 1942.

[2] R.H. Schulz, On check digit systems using anti-symmetric mappings, in: I. Althöfer et al. (eds.), *Numbers, information and complexity*, Kluwer, Boston, 2000, pp. 295–310.

[3] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014.

[4] A.B. Evans, *Orthogonal Latin Squares Based on Groups*, Springer (Developments in Mathematics, 57), Cham, 2018. Chapter 3.

Complete mappings: Background 1

- group-theoretic concept
- introduced by H.B. Mann in 1942[1]

[1]H.B. Mann, The construction of orthogonal Latin squares, *Ann. Math. Statistics* **13**: 418–423, 1942.

[2]R.H. Schulz, On check digit systems using anti-symmetric mappings, in: I. Althöfer et al. (eds.), *Numbers, information and complexity*, Kluwer, Boston, 2000, pp. 295–310.

[3]A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014.

[4]A.B. Evans, *Orthogonal Latin Squares Based on Groups*, Springer (Developments in Mathematics, 57), Cham, 2018. Chapter 3.

Complete mappings: Background 1

- group-theoretic concept
- introduced by H.B. Mann in 1942[1]
- applications in
  - combinatorics (Latin squares[1]),

[1] H.B. Mann, The construction of orthogonal Latin squares, *Ann. Math. Statistics* **13**: 418–423, 1942.

[2] R.H. Schulz, On check digit systems using anti-symmetric mappings, in: I. Althöfer et al. (eds.), *Numbers, information and complexity*, Kluwer, Boston, 2000, pp. 295–310.

[3] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014.

[4] A.B. Evans, *Orthogonal Latin Squares Based on Groups*, Springer (Developments in Mathematics, 57), Cham, 2018. Chapter 3.

Complete mappings: Background 1

- group-theoretic concept
- introduced by H.B. Mann in 1942[1]
- applications in
  - combinatorics (Latin squares[1]),
  - check-digit systems[2],

[1] H.B. Mann, The construction of orthogonal Latin squares, *Ann. Math. Statistics* **13**: 418–423, 1942.

[2] R.H. Schulz, On check digit systems using anti-symmetric mappings, in: I. Althöfer et al. (eds.), *Numbers, information and complexity*, Kluwer, Boston, 2000, pp. 295–310.

[3] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014.

[4] A.B. Evans, *Orthogonal Latin Squares Based on Groups*, Springer (Developments in Mathematics, 57), Cham, 2018. Chapter 3.

Complete mappings: Background 1

- group-theoretic concept
- introduced by H.B. Mann in 1942[1]
- applications in
  - combinatorics (Latin squares[1]),
  - check-digit systems[2],
  - cryptography[3], etc.

---

[1]H.B. Mann, The construction of orthogonal Latin squares, *Ann. Math. Statistics* **13**: 418–423, 1942.

[2]R.H. Schulz, On check digit systems using anti-symmetric mappings, in: I. Althöfer et al. (eds.), *Numbers, information and complexity*, Kluwer, Boston, 2000, pp. 295–310.

[3]A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014.

[4]A.B. Evans, *Orthogonal Latin Squares Based on Groups*, Springer (Developments in Mathematics, 57), Cham, 2018. Chapter 3.

Complete mappings: Background 1

- group-theoretic concept
- introduced by H.B. Mann in 1942[1]
- applications in
  - combinatorics (Latin squares[1]),
  - check-digit systems[2],
  - cryptography[3], etc.
- also studied by pure group theorists (Hall-Paige Conjecture[4])

---

[1] H.B. Mann, The construction of orthogonal Latin squares, *Ann. Math. Statistics* **13**: 418–423, 1942.

[2] R.H. Schulz, On check digit systems using anti-symmetric mappings, in: I. Althöfer et al. (eds.), *Numbers, information and complexity*, Kluwer, Boston, 2000, pp. 295–310.

[3] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014.

[4] A.B. Evans, *Orthogonal Latin Squares Based on Groups*, Springer (Developments in Mathematics, 57), Cham, 2018. Chapter 3.

Complete mappings: Definition

Definition

$(G, +)$: group, n.n. abelian.

Complete mappings: Definition

Definition

$(G,+)$: group, n.n. abelian.

1. $f : G \to$ is a *complete mapping of G* if
   1. f is bijective, and
   2. $f + \mathrm{id} : x \mapsto f(x) + x$ is bijective.

Complete mappings: Definition

Definition

$(G, +)$: group, n.n. abelian.

1. $f : G \to$ is a *complete mapping of G* if
   1. f is bijective, and
   2. $f + \mathrm{id} : x \mapsto f(x) + x$ is bijective.
2. *Orthomorphism of G*: analogous def., replacing $f + \mathrm{id}$ by $f - \mathrm{id}$.

Complete mappings: Definition

Definition

$(G, +)$: group, n.n. abelian.

1. $f : G \to$ is a *complete mapping of G* if
   1. f is bijective, and
   2. $f + \mathrm{id} : x \mapsto f(x) + x$ is bijective.
2. *Orthomorphism of G*: analogous def., replacing $f + \mathrm{id}$ by $f - \mathrm{id}$.
3. *Strong complete mapping of G*: both properties at once.

Complete mappings: Definition

Definition

$(G, +)$: group, n.n. abelian.

1. $f : G \to$ is a *complete mapping of G* if
   1. f is bijective, and
   2. $f + \mathrm{id} : x \mapsto f(x) + x$ is bijective.
2. *Orthomorphism of G*: analogous def., replacing $f + \mathrm{id}$ by $f - \mathrm{id}$.
3. *Strong complete mapping of G*: both properties at once.

f is complete mapping $\Leftrightarrow$ $f + \mathrm{id}$ is orthomorphism.

Complete mappings: Background 2

[5] A.B. Evans, Applications of complete mappings and orthomorphisms of finite groups, *Quasigroups Related Systems* **23**: 5–30, 2015.

[6] H. Niederreiter and K.H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* **33**(2): 197–212, 1984.

Complete mappings: Background 2

- Orthomorphisms also have applications, see Evans' paper[5].

[5]A.B. Evans, Applications of complete mappings and orthomorphisms of finite groups, *Quasigroups Related Systems* **23**: 5–30, 2015.

[6]H. Niederreiter and K.H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* **33**(2): 197–212, 1984.

Complete mappings: Background 2

- Orthomorphisms also have applications, see Evans' paper[5].
- K: field. A (strong) complete mapping/orthomorphism of K is one of $(K, +)$.

[5] A.B. Evans, Applications of complete mappings and orthomorphisms of finite groups, *Quasigroups Related Systems* **23**: 5–30, 2015.

[6] H. Niederreiter and K.H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* **33**(2): 197–212, 1984.

Complete mappings: Background 2

- Orthomorphisms also have applications, see Evans' paper[5].
- K: field. A (strong) complete mapping/orthomorphism of K is one of $(K, +)$.
- Complete mappings of finite fields: First studied by Niederreiter and Robinson[6].

[5] A.B. Evans, Applications of complete mappings and orthomorphisms of finite groups, *Quasigroups Related Systems* **23**: 5–30, 2015.

[6] H. Niederreiter and K.H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* **33**(2): 197–212, 1984.

Complete mappings: Background 2

- Orthomorphisms also have applications, see Evans' paper[5].
- K: field. A (strong) complete mapping/orthomorphism of K is one of $(K, +)$.
- Complete mappings of finite fields: First studied by Niederreiter and Robinson[6].
- Studied by many authors since, especially w.r.t. polynomial representations. See e.g. [15], [29], [33], [34], [36] and [37] at the end of these slides.

[5] A.B. Evans, Applications of complete mappings and orthomorphisms of finite groups, *Quasigroups Related Systems* **23**: 5–30, 2015.

[6] H. Niederreiter and K.H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* **33**(2): 197–212, 1984.

Cycle types: Background

[7]H. Niederreiter, *Random number generation and quasi-Monte Carlo Methods*, SIAM (CBMS-NSF Regional Conference Series in Applied Mathematics, 63), Philadelphia, 1992. Section 7.2, p. 164.

[8]P. Charpin, S. Mesnager and S. Sarkar, Involutions over the Galois field $\mathbb{F}_{2^n}$, *IEEE Trans. Inform. Theory* **62**(4): 2266–2276, 2016. Introduction.

Cycle types: Background

- Ω: finite set, $\sigma \in \mathrm{Sym}(\Omega)$. σ has decomposition into disjoint cycles.

[7] H. Niederreiter, *Random number generation and quasi-Monte Carlo Methods*, SIAM (CBMS-NSF Regional Conference Series in Applied Mathematics, 63), Philadelphia, 1992. Section 7.2, p. 164.

[8] P. Charpin, S. Mesnager and S. Sarkar, Involutions over the Galois field $\mathbb{F}_{2^n}$, *IEEE Trans. Inform. Theory* **62**(4): 2266–2276, 2016. Introduction.

Cycle types: Background

- Ω: finite set, $\sigma \in \mathrm{Sym}(\Omega)$. σ has decomposition into disjoint cycles.
- *Cycle type of* σ, $\mathrm{CT}(\sigma)$: info how many cycles of each length σ has.

[7] H. Niederreiter, *Random number generation and quasi-Monte Carlo Methods*, SIAM (CBMS-NSF Regional Conference Series in Applied Mathematics, 63), Philadelphia, 1992. Section 7.2, p. 164.

[8] P. Charpin, S. Mesnager and S. Sarkar, Involutions over the Galois field $\mathbb{F}_{2^n}$, *IEEE Trans. Inform. Theory* **62**(4): 2266–2276, 2016. Introduction.

Cycle types: Background

- Ω: finite set, $\sigma \in \mathrm{Sym}(\Omega)$. σ has decomposition into disjoint cycles.
- *Cycle type of* σ, $\mathrm{CT}(\sigma)$: info how many cycles of each length σ has.
- Popular research topic: Study $\mathrm{CT}(\sigma)$ with $\sigma \in \mathrm{Sym}(K)$, K finite field, σ given by polynomial. See e.g. [6], [13], [26] and [27].

[7] H. Niederreiter, *Random number generation and quasi-Monte Carlo Methods*, SIAM (CBMS-NSF Regional Conference Series in Applied Mathematics, 63), Philadelphia, 1992. Section 7.2, p. 164.

[8] P. Charpin, S. Mesnager and S. Sarkar, Involutions over the Galois field $\mathbb{F}_{2^n}$, *IEEE Trans. Inform. Theory* **62**(4): 2266–2276, 2016. Introduction.

Cycle types: Background

- Ω: finite set, $\sigma \in \mathrm{Sym}(\Omega)$. σ has decomposition into disjoint cycles.
- *Cycle type of* σ, $\mathrm{CT}(\sigma)$: info how many cycles of each length σ has.
- Popular research topic: Study $\mathrm{CT}(\sigma)$ with $\sigma \in \mathrm{Sym}(K)$, K finite field, σ given by polynomial. See e.g. [6], [13], [26] and [27].
- Some applications require particular cycle types. For example:

[7] H. Niederreiter, *Random number generation and quasi-Monte Carlo Methods*, SIAM (CBMS-NSF Regional Conference Series in Applied Mathematics, 63), Philadelphia, 1992. Section 7.2, p. 164.

[8] P. Charpin, S. Mesnager and S. Sarkar, Involutions over the Galois field $\mathbb{F}_{2^n}$, *IEEE Trans. Inform. Theory* **62**(4): 2266–2276, 2016. Introduction.

Cycle types: Background

- Ω: finite set, $\sigma \in \mathrm{Sym}(\Omega)$. σ has decomposition into disjoint cycles.
- *Cycle type of* σ, $\mathrm{CT}(\sigma)$: info how many cycles of each length σ has.
- Popular research topic: Study $\mathrm{CT}(\sigma)$ with $\sigma \in \mathrm{Sym}(K)$, K finite field, σ given by polynomial. See e.g. [6], [13], [26] and [27].
- Some applications require particular cycle types. For example:
  - Pseudorandom number generation: long cycles[7].

[7] H. Niederreiter, *Random number generation and quasi-Monte Carlo Methods*, SIAM (CBMS-NSF Regional Conference Series in Applied Mathematics, 63), Philadelphia, 1992. Section 7.2, p. 164.

[8] P. Charpin, S. Mesnager and S. Sarkar, Involutions over the Galois field $\mathbb{F}_{2^n}$, *IEEE Trans. Inform. Theory* **62**(4): 2266–2276, 2016. Introduction.

Cycle types: Background

- Ω: finite set, $\sigma \in \mathrm{Sym}(\Omega)$. σ has decomposition into disjoint cycles.
- *Cycle type of* σ, $\mathrm{CT}(\sigma)$: info how many cycles of each length σ has.
- Popular research topic: Study $\mathrm{CT}(\sigma)$ with $\sigma \in \mathrm{Sym}(K)$, K finite field, σ given by polynomial. See e.g. [6], [13], [26] and [27].
- Some applications require particular cycle types. For example:
  - Pseudorandom number generation: long cycles[7].
  - Cryptography & Coding theory: involutions[8].

[7] H. Niederreiter, *Random number generation and quasi-Monte Carlo Methods*, SIAM (CBMS-NSF Regional Conference Series in Applied Mathematics, 63), Philadelphia, 1992. Section 7.2, p. 164.

[8] P. Charpin, S. Mesnager and S. Sarkar, Involutions over the Galois field $\mathbb{F}_{2^n}$, *IEEE Trans. Inform. Theory* **62**(4): 2266–2276, 2016. Introduction.

Cycle types of complete mappings: Research question

Question

What can be said about the cycle types of complete mappings of a finite group (field)?

Cycle types of complete mappings: Research question

Question

What can be said about the cycle types of complete mappings of a finite group (field)?

Two ways of "saying something":

Cycle types of complete mappings: Research question

Question

What can be said about the cycle types of complete mappings of a finite group (field)?

Two ways of "saying something":

1. negative results: necessary conditions, allowing to refute cycle types;

Cycle types of complete mappings: Research question

Question

What can be said about the cycle types of complete mappings of a finite group (field)?

Two ways of "saying something":

1. negative results: necessary conditions, allowing to refute cycle types;
2. positive results: give examples of possible cycle types (and corr. complete mappings).

Cycle types of complete mappings: Known negative results

- Only these elementary results are known:

Cycle types of complete mappings: Known negative results

- Only these elementary results are known:
  1. G: abelian group, f: compl. map. of G. Then f has no 2-cycle $(x, f(x))$.

Cycle types of complete mappings: Known negative results

- Only these elementary results are known:
  1. G: abelian group, f: compl. map. of G. Then f has no 2-cycle $(x, f(x))$. Otherwise,

     $$(f+\mathrm{id})(x) = f(x)+x = f(x)+f(f(x)) = f(f(x))+f(x) = (f+\mathrm{id})(f(x)),$$

Cycle types of complete mappings: Known negative results

- Only these elementary results are known:
  1. G: abelian group, f: compl. map. of G. Then f has no 2-cycle $(x, f(x))$. Otherwise,

     $$(f+\mathrm{id})(x) = f(x)+x = f(x)+f(f(x)) = f(f(x))+f(x) = (f+\mathrm{id})(f(x)),$$

     contradiction as $f + \mathrm{id}$ is injective.

Cycle types of complete mappings: Known negative results

- Only these elementary results are known:
  1. G: abelian group, f: compl. map. of G. Then f has no 2-cycle $(x, f(x))$. Otherwise,

     $$(f+\mathrm{id})(x) = f(x)+x = f(x)+f(f(x)) = f(f(x))+f(x) = (f+\mathrm{id})(f(x)),$$

     contradiction as $f + \mathrm{id}$ is injective.
  2. G: group, f: orthomor. of G. Then f has exactly 1 fixed point,

Cycle types of complete mappings: Known negative results

- Only these elementary results are known:
  1. G: abelian group, f: compl. map. of G. Then f has no 2-cycle $(x, f(x))$. Otherwise,

     $$(f+\mathrm{id})(x) = f(x)+x = f(x)+f(f(x)) = f(f(x))+f(x) = (f+\mathrm{id})(f(x)),$$

     contradiction as $f + \mathrm{id}$ is injective.
  2. G: group, f: orthomor. of G. Then f has exactly 1 fixed point, because $f(x) = x$ is equ. to $x = (f - \mathrm{id})^{-1}(0_G)$.

Cycle types of complete mappings: Known negative results

- Only these elementary results are known:
  1. G: abelian group, f: compl. map. of G. Then f has no 2-cycle $(x, f(x))$. Otherwise,

     $$(f+\mathrm{id})(x) = f(x)+x = f(x)+f(f(x)) = f(f(x))+f(x) = (f+\mathrm{id})(f(x)),$$

     contradiction as $f + \mathrm{id}$ is injective.
  2. G: group, f: orthomor. of G. Then f has exactly 1 fixed point, because $f(x) = x$ is equ. to $x = (f - \mathrm{id})^{-1}(0_G)$.
- If $x + x = 0_G$ for all $x \in G$, then f is compl. map. of $G \Leftrightarrow f$ is orthomor. of G.

Cycle types of complete mappings: Known positive results

[9] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014. Theorem 9.

Cycle types of complete mappings: Known positive results

- Regular complete mappings:

[9] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014. Theorem 9.

Cycle types of complete mappings: Known positive results

- Regular complete mappings:
  - K: fin. field, $a \in K$, $a \neq 0, -1$. Then $x \mapsto ax$ is a compl. map. of K.

[9] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014. Theorem 9.

Cycle types of complete mappings: Known positive results

- Regular complete mappings:
  - K: fin. field, $a \in K$, $a \neq 0, -1$. Then $x \mapsto ax$ is a compl. map. of K.
  - It has 1 fixed point (0_K) and $\frac{|K|-1}{\ell}$ cycles of length $\ell = \mathrm{ord}_{K^*}(a)$.

[9] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014. Theorem 9.

Cycle types of complete mappings: Known positive results

- Regular complete mappings:
  - K: fin. field, $a \in K$, $a \neq 0, -1$. Then $x \mapsto ax$ is a compl. map. of K.
  - It has 1 fixed point (0_K) and $\frac{|K|-1}{\ell}$ cycles of length $\ell = \mathrm{ord}_{K^*}(a)$.
  - Permutations with such a cycle type are called ℓ-*regular*.

[9] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014. Theorem 9.

Cycle types of complete mappings: Known positive results

- Regular complete mappings:
  - K: fin. field, $a \in K$, $a \neq 0, -1$. Then $x \mapsto ax$ is a compl. map. of K.
  - It has 1 fixed point (0_K) and $\frac{|K|-1}{\ell}$ cycles of length $\ell = \mathrm{ord}_{K^*}(a)$.
  - Permutations with such a cycle type are called *ℓ-regular*.
  - Focus so far mostly on constructing other examples of ℓ-regular complete mappings, see e.g. [17], [18], [23] and [35].

[9] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014. Theorem 9.

Cycle types of complete mappings: Known positive results

- Regular complete mappings:
  - K: fin. field, $a \in K$, $a \neq 0, -1$. Then $x \mapsto ax$ is a compl. map. of K.
  - It has 1 fixed point (0_K) and $\frac{|K|-1}{\ell}$ cycles of length $\ell = \mathrm{ord}_{K^*}(a)$.
  - Permutations with such a cycle type are called *ℓ-regular*.
  - Focus so far mostly on constructing other examples of ℓ-regular complete mappings, see e.g. [17], [18], [23] and [35].
- Fixed-point-free complete mappings: If $\mathrm{char}(K) > 2$, then K has compl. map. without fixed points (e.g., $x \mapsto x + 1$).

[9] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014. Theorem 9.

Cycle types of complete mappings: Known positive results

- Regular complete mappings:
  - K: fin. field, $a \in K$, $a \neq 0, -1$. Then $x \mapsto ax$ is a compl. map. of K.
  - It has 1 fixed point (0_K) and $\frac{|K|-1}{\ell}$ cycles of length $\ell = \mathrm{ord}_{K^*}(a)$.
  - Permutations with such a cycle type are called ℓ*-regular*.
  - Focus so far mostly on constructing other examples of ℓ-regular complete mappings, see e.g. [17], [18], [23] and [35].
- Fixed-point-free complete mappings: If $\mathrm{char}(K) > 2$, then K has compl. map. without fixed points (e.g., $x \mapsto x + 1$). For other examples, see [9].

[9] A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014. Theorem 9.

Current section

1 Introduction: Complete mappings and cycle types

2 Our main results

3 Proof sketch of Theorem 4

4 References

Overview of our main results

[10] A. Bors and Q. Wang, Cycle types of complete mappings of finite fields, to appear in *J. Algebra*, preprint available under `https://arxiv.org/abs/2105.00140`.

[11] A. Bors and Q. Wang, Coset-wise affine functions and cycle types of complete mappings, preprint (2021), `https://arxiv.org/abs/2109.03922`.

[12] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Overview of our main results

- positive results

[10] A. Bors and Q. Wang, Cycle types of complete mappings of finite fields, to appear in *J. Algebra*, preprint available under `https://arxiv.org/abs/2105.00140`.

[11] A. Bors and Q. Wang, Coset-wise affine functions and cycle types of complete mappings, preprint (2021), `https://arxiv.org/abs/2109.03922`.

[12] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Overview of our main results

- positive results
- two classes of functions $K \to K$, each with "piecewise" definitions:

[10] A. Bors and Q. Wang, Cycle types of complete mappings of finite fields, to appear in *J. Algebra*, preprint available under `https://arxiv.org/abs/2105.00140`.

[11] A. Bors and Q. Wang, Coset-wise affine functions and cycle types of complete mappings, preprint (2021), `https://arxiv.org/abs/2109.03922`.

[12] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Overview of our main results

- positive results
- two classes of functions $K \to K$, each with "piecewise" definitions:
  - first-order cyclotomic mappings, defined via multiplicative cosets of K. Results from [10].

[10] A. Bors and Q. Wang, Cycle types of complete mappings of finite fields, to appear in *J. Algebra*, preprint available under https://arxiv.org/abs/2105.00140.

[11] A. Bors and Q. Wang, Coset-wise affine functions and cycle types of complete mappings, preprint (2021), https://arxiv.org/abs/2109.03922.

[12] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Overview of our main results

- positive results
- two classes of functions $K \to K$, each with "piecewise" definitions:
  - first-order cyclotomic mappings, defined via multiplicative cosets of K. Results from [10].
  - coset-wise affine functions, defined via additive cosets of K. Results from [11].

[10] A. Bors and Q. Wang, Cycle types of complete mappings of finite fields, to appear in *J. Algebra*, preprint available under https://arxiv.org/abs/2105.00140.

[11] A. Bors and Q. Wang, Coset-wise affine functions and cycle types of complete mappings, preprint (2021), https://arxiv.org/abs/2109.03922.

[12] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Overview of our main results

- positive results
- two classes of functions $K \to K$, each with "piecewise" definitions:
  - first-order cyclotomic mappings, defined via multiplicative cosets of K. Results from [10].
  - coset-wise affine functions, defined via additive cosets of K. Results from [11].
- proved with methods from different areas:

---

[10] A. Bors and Q. Wang, Cycle types of complete mappings of finite fields, to appear in *J. Algebra*, preprint available under `https://arxiv.org/abs/2105.00140`.

[11] A. Bors and Q. Wang, Coset-wise affine functions and cycle types of complete mappings, preprint (2021), `https://arxiv.org/abs/2109.03922`.

[12] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Overview of our main results

- positive results
- two classes of functions $K \to K$, each with "piecewise" definitions:
  - first-order cyclotomic mappings, defined via multiplicative cosets of K. Results from [10].
  - coset-wise affine functions, defined via additive cosets of K. Results from [11].
- proved with methods from different areas:
  - wreath products from permutation group theory;

[10] A. Bors and Q. Wang, Cycle types of complete mappings of finite fields, to appear in *J. Algebra*, preprint available under `https://arxiv.org/abs/2105.00140`.

[11] A. Bors and Q. Wang, Coset-wise affine functions and cycle types of complete mappings, preprint (2021), `https://arxiv.org/abs/2109.03922`.

[12] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Overview of our main results

- positive results
- two classes of functions $K \to K$, each with "piecewise" definitions:
  - first-order cyclotomic mappings, defined via multiplicative cosets of K. Results from [10].
  - coset-wise affine functions, defined via additive cosets of K. Results from [11].
- proved with methods from different areas:
  - wreath products from permutation group theory;
  - combinatorial observations on cycle indices;

[10] A. Bors and Q. Wang, Cycle types of complete mappings of finite fields, to appear in *J. Algebra*, preprint available under `https://arxiv.org/abs/2105.00140`.

[11] A. Bors and Q. Wang, Coset-wise affine functions and cycle types of complete mappings, preprint (2021), `https://arxiv.org/abs/2109.03922`.

[12] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Overview of our main results

- positive results
- two classes of functions $K \to K$, each with "piecewise" definitions:
  - first-order cyclotomic mappings, defined via multiplicative cosets of K. Results from [10].
  - coset-wise affine functions, defined via additive cosets of K. Results from [11].
- proved with methods from different areas:
  - wreath products from permutation group theory;
  - combinatorial observations on cycle indices;
  - character sums (following & extending a method of Carlitz[12]) for the results on cycl. map.

[10] A. Bors and Q. Wang, Cycle types of complete mappings of finite fields, to appear in *J. Algebra*, preprint available under `https://arxiv.org/abs/2105.00140`.

[11] A. Bors and Q. Wang, Coset-wise affine functions and cycle types of complete mappings, preprint (2021), `https://arxiv.org/abs/2109.03922`.

[12] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

First-order cyclotomic mappings

First-order cyclotomic mappings

- $K = \mathbb{F}_q$, $d \mid q-1$, $C \ldots$ index d subgroup of $\mathbb{F}_q^* = \langle \omega \rangle$.

First-order cyclotomic mappings

- $K = \mathbb{F}_q$, $d \mid q-1$, $C \ldots$ index d subgroup of $\mathbb{F}_q^* = \langle \omega \rangle$.
- $C_i := \omega^i C$ for $i = 0, 1, \ldots, d-1$ are the cosets of C.

First-order cyclotomic mappings

- $K = \mathbb{F}_q$, $d \mid q-1$, $C \ldots$ index d subgroup of $\mathbb{F}_q^* = \langle \omega \rangle$.
- $C_i := \omega^i C$ for $i = 0, 1, \ldots, d-1$ are the cosets of C.
- $f : \mathbb{F}_q \to \mathbb{F}_q$ is a *first-order cyclotomic mapping (FOCM)* of index d of $\mathbb{F}_q$ if

First-order cyclotomic mappings

- $\underline{K = \mathbb{F}_q}$, $\underline{d \mid q-1}$, $\underline{C \ldots \text{index } d \text{ subgroup of } \mathbb{F}_q^* = \langle \omega \rangle}$.
- $C_i := \omega^i C$ for $i = 0, 1, \ldots, d-1$ are the cosets of C.
- $f : \mathbb{F}_q \to \mathbb{F}_q$ is a *first-order cyclotomic mapping (FOCM)* of index d of $\mathbb{F}_q$ if

$$f(x) = \begin{cases} 0, & \text{if } x = 0, \\ a_i x, & \text{if } x \in C_i, i \in \{0, \ldots, d-1\}. \end{cases}$$

  for some $a_i \in \mathbb{F}_q$.

First-order cyclotomic mappings

- $K = \mathbb{F}_q$, $d \mid q-1$, $C \ldots$ index d subgroup of $\mathbb{F}_q^* = \langle \omega \rangle$.
- $C_i := \omega^i C$ for $i = 0, 1, \ldots, d-1$ are the cosets of C.
- $f : \mathbb{F}_q \to \mathbb{F}_q$ is a *first-order cyclotomic mapping (FOCM)* of index d of $\mathbb{F}_q$ if

$$f(x) = \begin{cases} 0, & \text{if } x = 0, \\ a_i x, & \text{if } x \in C_i, i \in \{0, \ldots, d-1\}. \end{cases}$$

  for some $a_i \in \mathbb{F}_q$.
- Remark (generalizations):

First-order cyclotomic mappings

- $K = \mathbb{F}_q$, $d \mid q-1$, $C\ldots$ index d subgroup of $\mathbb{F}_q^* = \langle\omega\rangle$.
- $C_i := \omega^i C$ for $i = 0, 1, \ldots, d-1$ are the cosets of C.
- $f : \mathbb{F}_q \to \mathbb{F}_q$ is a *first-order cyclotomic mapping (FOCM)* of index d of $\mathbb{F}_q$ if

$$f(x) = \begin{cases} 0, & \text{if } x = 0, \\ a_i x, & \text{if } x \in C_i, i \in \{0, \ldots, d-1\}. \end{cases}$$

  for some $a_i \in \mathbb{F}_q$.
- Remark (generalizations):
  - "$a_i x$" $\to$ "$a_i x^r$": *r-th order cyclotomic mapping of index d.*

First-order cyclotomic mappings

- $K = \mathbb{F}_q$, $d \mid q-1$, $C \ldots$ index d subgroup of $\mathbb{F}_q^* = \langle \omega \rangle$.
- $C_i := \omega^i C$ for $i = 0, 1, \ldots, d-1$ are the cosets of C.
- $f : \mathbb{F}_q \to \mathbb{F}_q$ is a *first-order cyclotomic mapping (FOCM)* of index d of $\mathbb{F}_q$ if

$$f(x) = \begin{cases} 0, & \text{if } x = 0, \\ a_i x, & \text{if } x \in C_i, i \in \{0, \ldots, d-1\}. \end{cases}$$

  for some $a_i \in \mathbb{F}_q$.
- Remark (generalizations):
  - "$a_i x$" $\to$ "$a_i x^r$": *r-th order cyclotomic mapping of index d*.
  - "$a_i x$" $\to$ "$a_i x^{r_i}$": *generalized cyclotomic mapping of index d*

First-order cyclotomic mappings

- $K = \mathbb{F}_q$, $d \mid q-1$, $C \ldots$ index d subgroup of $\mathbb{F}_q^* = \langle \omega \rangle$.
- $C_i := \omega^i C$ for $i = 0, 1, \ldots, d-1$ are the cosets of C.
- $f : \mathbb{F}_q \to \mathbb{F}_q$ is a *first-order cyclotomic mapping (FOCM)* of index d of $\mathbb{F}_q$ if

$$f(x) = \begin{cases} 0, & \text{if } x = 0, \\ a_i x, & \text{if } x \in C_i, i \in \{0, \ldots, d-1\}. \end{cases}$$

  for some $a_i \in \mathbb{F}_q$.
- Remark (generalizations):
  - "$a_i x$" $\to$ "$a_i x^r$": *r-th order cyclotomic mapping of index d*.
  - "$a_i x$" $\to$ "$a_i x^{r_i}$": *generalized cyclotomic mapping of index d*
- Many authors have studied these kinds of functions, see e.g. [1], [2], [22], [30], [31] and [38].

First main result (Long cycles)

First main result (Long cycles)

- f: first-order cyclotomic permutation (FOCP) of $\mathbb{F}_q$.

First main result (Long cycles)

- f: first-order cyclotomic permutation (FOCP) of $\mathbb{F}_q$.
- Ass.: All cycles $\neq (0)$ of f are long and q is large enough.

First main result (Long cycles)

- f: first-order cyclotomic permutation (FOCP) of $\mathbb{F}_q$.
- Ass.: All cycles $\neq (0)$ of f are long and q is large enough.
- Then there ex. FOCP g of $\mathbb{F}_q$ s.t.:

First main result (Long cycles)

- f: first-order cyclotomic permutation (FOCP) of $\mathbb{F}_q$.
- Ass.: All cycles $\neq (0)$ of f are long and q is large enough.
- Then there ex. FOCP g of $\mathbb{F}_q$ s.t.:
  - $\mathrm{CT}(g) = \mathrm{CT}(f)$, and

First main result (Long cycles)

- f: first-order cyclotomic permutation (FOCP) of $\mathbb{F}_q$.
- Ass.: All cycles $\neq (0)$ of f are long and q is large enough.
- Then there ex. FOCP g of $\mathbb{F}_q$ s.t.:
  - $\mathrm{CT}(g) = \mathrm{CT}(f)$, and
  - g is a strong complete mapping.

First main result (Long cycles)

- f: first-order cyclotomic permutation (FOCP) of $\mathbb{F}_q$.
- Ass.: All cycles $\neq (0)$ of f are long and q is large enough.
- Then there ex. FOCP g of $\mathbb{F}_q$ s.t.:
  - $\mathrm{CT}(g) = \mathrm{CT}(f)$, and
  - g is a strong complete mapping.

Theorem 1

Let $d, n \in \mathbb{N}^+$ and $1 > \epsilon > 0$.

First main result (Long cycles)

- f: first-order cyclotomic permutation (FOCP) of $\mathbb{F}_q$.
- Ass.: All cycles $\neq (0)$ of f are long and q is large enough.
- Then there ex. FOCP g of $\mathbb{F}_q$ s.t.:
  - $\mathrm{CT}(g) = \mathrm{CT}(f)$, and
  - g is a strong complete mapping.

Theorem 1

Let $d, n \in \mathbb{N}^+$ and $1 > \epsilon > 0$. For all prime powers $q \geq q_1(d, n, \epsilon)$ with $q \equiv 1 \pmod{d}$ and all $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$:

First main result (Long cycles)

- f: first-order cyclotomic permutation (FOCP) of $\mathbb{F}_q$.
- Ass.: All cycles $\neq (0)$ of f are long and q is large enough.
- Then there ex. FOCP g of $\mathbb{F}_q$ s.t.:
  - $\mathrm{CT}(g) = \mathrm{CT}(f)$, and
  - g is a strong complete mapping.

Theorem 1

Let $d, n \in \mathbb{N}^+$ and $1 > \epsilon > 0$. For all prime powers $q \geq q_1(d, n, \epsilon)$ with $q \equiv 1 \pmod{d}$ and all $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$: If f is an FOCP of index d of $\mathbb{F}_q$ s.t. all cycles $\neq (0)$ of f have length $\geq \epsilon q$, then there ex. index d FOCP g of $\mathbb{F}_q$ s.t.

First main result (Long cycles)

- f: first-order cyclotomic permutation (FOCP) of $\mathbb{F}_q$.
- Ass.: All cycles $\neq (0)$ of f are long and q is large enough.
- Then there ex. FOCP g of $\mathbb{F}_q$ s.t.:
  - $\mathrm{CT}(g) = \mathrm{CT}(f)$, and
  - g is a strong complete mapping.

Theorem 1

Let $d, n \in \mathbb{N}^+$ and $1 > \epsilon > 0$. For all prime powers $q \geq q_1(d, n, \epsilon)$ with $q \equiv 1 \pmod{d}$ and all $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$: If f is an FOCP of index d of $\mathbb{F}_q$ s.t. all cycles $\neq (0)$ of f have length $\geq \epsilon q$, then there ex. index d FOCP g of $\mathbb{F}_q$ s.t.

1. $\mathrm{CT}(g) = \mathrm{CT}(f)$.

First main result (Long cycles)

- f: first-order cyclotomic permutation (FOCP) of $\mathbb{F}_q$.
- Ass.: All cycles $\neq (0)$ of f are long and q is large enough.
- Then there ex. FOCP g of $\mathbb{F}_q$ s.t.:
  - $\mathrm{CT}(g) = \mathrm{CT}(f)$, and
  - g is a strong complete mapping.

Theorem 1

Let $d, n \in \mathbb{N}^+$ and $1 > \epsilon > 0$. For all prime powers $q \geq q_1(d, n, \epsilon)$ with $q \equiv 1 \pmod{d}$ and all $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$: If f is an FOCP of index d of $\mathbb{F}_q$ s.t. all cycles $\neq (0)$ of f have length $\geq \epsilon q$, then there ex. index d FOCP g of $\mathbb{F}_q$ s.t.

1. $\mathrm{CT}(g) = \mathrm{CT}(f)$.
2. $g + c_i\,\mathrm{id}$ is a permutation of $\mathbb{F}_q$ for $i = 1, 2, \ldots, n$.

First main result (Long cycles)

- f: first-order cyclotomic permutation (FOCP) of $\mathbb{F}_q$.
- Ass.: All cycles $\neq (0)$ of f are long and q is large enough.
- Then there ex. FOCP g of $\mathbb{F}_q$ s.t.:
  - $\mathrm{CT}(g) = \mathrm{CT}(f)$, and
  - g is a strong complete mapping.

Theorem 1

Let $d, n \in \mathbb{N}^+$ and $1 > \epsilon > 0$. For all prime powers $q \geq q_1(d, n, \epsilon)$ with $q \equiv 1 \pmod{d}$ and all $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$: If f is an FOCP of index d of $\mathbb{F}_q$ s.t. all cycles $\neq (0)$ of f have length $\geq \epsilon q$, then there ex. index d FOCP g of $\mathbb{F}_q$ s.t.

1. $\mathrm{CT}(g) = \mathrm{CT}(f)$.
2. $g + c_i\,\mathrm{id}$ is a permutation of $\mathbb{F}_q$ for $i = 1, 2, \ldots, n$.

For $d = 1$: Theorem of Carlitz (see loc. cit.).

Second main result (Cosets)

Second main result (Cosets)

- f: index d FOCM of $\mathbb{F}_q$, $f(x) = a_i x$ for $x \in C_i = \omega^i C$.

Second main result (Cosets)

- f: index d FOCM of $\mathbb{F}_q$, $f(x) = a_i x$ for $x \in C_i = \omega^i C$.
- If $a_i \neq 0$, then $f(C_i)$ is a coset.

Second main result (Cosets)

- f: index d FOCM of $\mathbb{F}_q$, $f(x) = a_i x$ for $x \in C_i = \omega^i C$.
- If $a_i \neq 0$, then $f(C_i)$ is a coset.
- If q is large enough: complete control over how $f + c_j\,\mathrm{id}$ for $j = 1, \ldots, n$ map cosets, where f is suitable index d FOCM of $\mathbb{F}_q$.

Second main result (Cosets)

- f: index d FOCM of $\mathbb{F}_q$, $f(x) = a_i x$ for $x \in C_i = \omega^i C$.
- If $a_i \neq 0$, then $f(C_i)$ is a coset.
- If q is large enough: complete control over how $f + c_j \,\mathrm{id}$ for $j = 1, \ldots, n$ map cosets, where f is suitable index d FOCM of $\mathbb{F}_q$.

Theorem 2

Let $d, n \in \mathbb{N}^+$. For all prime powers $q \geq q_2(d, n)$ with $q \equiv 1 \pmod{d}$:

Second main result (Cosets)

- f: index d FOCM of $\mathbb{F}_q$, $f(x) = a_i x$ for $x \in C_i = \omega^i C$.
- If $a_i \neq 0$, then $f(C_i)$ is a coset.
- If q is large enough: complete control over how $f + c_j \mathrm{id}$ for $j = 1, \ldots, n$ map cosets, where f is suitable index d FOCM of $\mathbb{F}_q$.

Theorem 2

Let $d, n \in \mathbb{N}^+$. For all prime powers $q \geq q_2(d, n)$ with $q \equiv 1 \pmod{d}$: Let $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$, pairwise distinct, and choose functions

$$s_1, s_2, \ldots, s_n : \{0, 1, \ldots, d-1\} \to \{0, 1, \ldots, d-1\}.$$

Second main result (Cosets)

- f: index d FOCM of $\mathbb{F}_q$, $f(x) = a_i x$ for $x \in C_i = \omega^i C$.
- If $a_i \neq 0$, then $f(C_i)$ is a coset.
- If q is large enough: complete control over how $f + c_j \,\mathrm{id}$ for $j = 1, \ldots, n$ map cosets, where f is suitable index d FOCM of $\mathbb{F}_q$.

Theorem 2

Let $d, n \in \mathbb{N}^+$. For all prime powers $q \geq q_2(d, n)$ with $q \equiv 1 \pmod{d}$: Let $c_1, c_2, \ldots, c_n \in \mathbb{F}_q$, pairwise distinct, and choose functions

$$s_1, s_2, \ldots, s_n : \{0, 1, \ldots, d-1\} \to \{0, 1, \ldots, d-1\}.$$

There ex. index d FOCM f of $\mathbb{F}_q$ such that

$$(f + c_j \,\mathrm{id})(C_i) = C_{s_j(i)}$$

for $0 \leq i \leq d-1$ and $1 \leq j \leq n$.

Third main result (Simultaneous long cycles)

[13] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Third main result (Simultaneous long cycles)

- Controlling the $\mathrm{CT}(f + c_j\,\mathrm{id})$ is much harder.

[13] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Third main result (Simultaneous long cycles)

- Controlling the $\mathrm{CT}(f + c_j\,\mathrm{id})$ is much harder.
- By a theorem of Carlitz, [13], if q is large enough, there ex. prim. root ω of $\mathbb{F}_q$ s.t. $\omega + 1$ is also prim. root.

[13] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Third main result (Simultaneous long cycles)

- Controlling the $\mathrm{CT}(f + c_j\,\mathrm{id})$ is much harder.
- By a theorem of Carlitz, [13], if q is large enough, there ex. prim. root ω of $\mathbb{F}_q$ s.t. $\omega + 1$ is also prim. root.
- Then $f : x \mapsto \omega x$, and $f + \mathrm{id} : x \mapsto (\omega + 1)x$ are both $(q-1)$-regular, and FOCMs of index $d = 1$.

[13] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Third main result (Simultaneous long cycles)

- Controlling the $\mathrm{CT}(f + c_j \,\mathrm{id})$ is much harder.
- By a theorem of Carlitz, [13], if q is large enough, there ex. prim. root ω of $\mathbb{F}_q$ s.t. $\omega + 1$ is also prim. root.
- Then $f : x \mapsto \omega x$, and $f + \mathrm{id} : x \mapsto (\omega + 1)x$ are both $(q-1)$-regular, and FOCMs of index $d = 1$.
- Theorem 3 extends this to $d > 1$.

[13] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Third main result (Simultaneous long cycles)

- Controlling the $\mathrm{CT}(f + c_j \,\mathrm{id})$ is much harder.
- By a theorem of Carlitz, [13], if q is large enough, there ex. prim. root ω of $\mathbb{F}_q$ s.t. $\omega + 1$ is also prim. root.
- Then $f : x \mapsto \omega x$, and $f + \mathrm{id} : x \mapsto (\omega + 1)x$ are both $(q-1)$-regular, and FOCMs of index $d = 1$.
- Theorem 3 extends this to $d > 1$.

Theorem 3

Let $\underline{d \in \mathbb{N}^+}$. For all prime powers $q \geq q_3(d)$ with $q \equiv 1 \pmod{d}$, there ex. FOCM f of $\mathbb{F}_q$ of smallest index d s.t.:

[13] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Third main result (Simultaneous long cycles)

- Controlling the $\mathrm{CT}(f + c_j\,\mathrm{id})$ is much harder.
- By a theorem of Carlitz, [13], if q is large enough, there ex. prim. root ω of $\mathbb{F}_q$ s.t. $\omega + 1$ is also prim. root.
- Then $f : x \mapsto \omega x$, and $f + \mathrm{id} : x \mapsto (\omega + 1)x$ are both $(q-1)$-regular, and FOCMs of index $d = 1$.
- Theorem 3 extends this to $d > 1$.

Theorem 3

Let $\underline{d \in \mathbb{N}^+}$. For all prime powers $q \geq q_3(d)$ with $q \equiv 1 \pmod{d}$, there ex. FOCM f of $\mathbb{F}_q$ of smallest index d s.t.:

1. f is compl. map. of $\mathbb{F}_q$.

[13] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Third main result (Simultaneous long cycles)

- Controlling the $\mathrm{CT}(f + c_j \,\mathrm{id})$ is much harder.
- By a theorem of Carlitz, [13], if q is large enough, there ex. prim. root ω of $\mathbb{F}_q$ s.t. $\omega + 1$ is also prim. root.
- Then $f : x \mapsto \omega x$, and $f + \mathrm{id} : x \mapsto (\omega + 1)x$ are both $(q-1)$-regular, and FOCMs of index $d = 1$.
- Theorem 3 extends this to $d > 1$.

Theorem 3

Let $\underline{d \in \mathbb{N}^+}$. For all prime powers $q \geq q_3(d)$ with $q \equiv 1 \pmod{d}$, there ex. FOCM f of $\mathbb{F}_q$ of smallest index d s.t.:

1. f is compl. map. of $\mathbb{F}_q$.
2. f and $f + \mathrm{id}$ are $(q-1)$-regular.

[13] L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956. Theorem 1.

Cycle types: Formal definition and background

[14] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

Cycle types: Formal definition and background

- Ω: fin. set, $\sigma \in \mathrm{Sym}(\Omega)$. For $\ell = 1, 2, \ldots, |\Omega|$:
  k_ℓ: number of length ℓ cycles of σ.

[14] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

Cycle types: Formal definition and background

- Ω: fin. set, $\sigma \in \mathrm{Sym}(\Omega)$. For $\ell = 1, 2, \ldots, |\Omega|$:
  k_ℓ: number of length ℓ cycles of σ. Set

$$\mathrm{CT}(\sigma) := x_1^{k_1} x_2^{k_2} \cdots x_{|\Omega|}^{k_{|\Omega|}} \in \mathbb{Q}[x_n : n \in \mathbb{N}^+].$$

[14] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

Cycle types: Formal definition and background

- Ω: fin. set, $\sigma \in \mathrm{Sym}(\Omega)$. For $\ell = 1, 2, \ldots, |\Omega|$:
  k_ℓ: number of length ℓ cycles of σ. Set

$$\mathrm{CT}(\sigma) := x_1^{k_1} x_2^{k_2} \cdots x_{|\Omega|}^{k_{|\Omega|}} \in \mathbb{Q}[x_n : n \in \mathbb{N}^+].$$

- Pólya[14]: original def.; also def. *cycle index* ("average CT") of perm. gp.

[14] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

Cycle types: Formal definition and background

- Ω: fin. set, $\sigma \in \mathrm{Sym}(\Omega)$. For $\ell = 1, 2, \ldots, |\Omega|$: k_ℓ: number of length ℓ cycles of σ. Set

$$\mathrm{CT}(\sigma) := x_1^{k_1} x_2^{k_2} \cdots x_{|\Omega|}^{k_{|\Omega|}} \in \mathbb{Q}[x_n : n \in \mathbb{N}^+].$$

- Pólya[14]: original def.; also def. *cycle index* ("average CT") of perm. gp.
- Cycle indices studied by many authors, e.g. [2], [11], [12] and [32].

[14] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

Cycle types: Formal definition and background

- Ω: fin. set, $\sigma \in \mathrm{Sym}(\Omega)$. For $\ell = 1, 2, \ldots, |\Omega|$:
  k_ℓ: number of length ℓ cycles of σ. Set

$$\mathrm{CT}(\sigma) := x_1^{k_1} x_2^{k_2} \cdots x_{|\Omega|}^{k_{|\Omega|}} \in \mathbb{Q}[x_n : n \in \mathbb{N}^+].$$

- Pólya[14]: original def.; also def. *cycle index* ("average CT") of perm. gp.
- Cycle indices studied by many authors, e.g. [2], [11], [12] and [32].
- $\ell \in \mathbb{N}^+$: BU_ℓ (ℓ-*th blow-up function*) is the $\mathbb{Q}$-algebra end. of $\mathbb{Q}[x_n : n \in \mathbb{N}^+]$ with $\mathrm{BU}_\ell(x_n) = x_{\ell n}$ for all $n \in \mathbb{N}^+$.

[14] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

Fourth main result (Recursive construction): Notation 1

[15] L. Reis and Q. Wang, The additive index of polynomials over finite fields, preprint (2021), `https://arxiv.org/abs/2105.02374`.

Fourth main result (Recursive construction): Notation 1

- K: field, V: K-vector space, W: K-subspace of V.

[15] L. Reis and Q. Wang, The additive index of polynomials over finite fields, preprint (2021), `https://arxiv.org/abs/2105.02374`.

Fourth main result (Recursive construction): Notation 1

- K: field, V: K-vector space, W: K-subspace of V.
- $f: V \to V$ is *W-coset-wise K-affine* if $f(x) = \varphi_C(x) + v_C$ for all $x \in C$ (coset of W), and

[15] L. Reis and Q. Wang, The additive index of polynomials over finite fields, preprint (2021), `https://arxiv.org/abs/2105.02374`.

Fourth main result (Recursive construction): Notation 1

- K: field, V: K-vector space, W: K-subspace of V.
- $f: V \to V$ is *W-coset-wise K-affine* if $f(x) = \varphi_C(x) + v_C$ for all $x \in C$ (coset of W), and
  1. $\varphi_C \ldots K$-end. of V with $\varphi_C(W) \subseteq W$;

[15] L. Reis and Q. Wang, The additive index of polynomials over finite fields, preprint (2021), https://arxiv.org/abs/2105.02374.

Fourth main result (Recursive construction): Notation 1

- K: field, V: K-vector space, W: K-subspace of V.
- $f: V \to V$ is *W-coset-wise K-affine* if $f(x) = \varphi_C(x) + v_C$ for all $x \in C$ (coset of W), and
  1. $\varphi_C \ldots K$-end. of V with $\varphi_C(W) \subseteq W$;
  2. $v_C \in V$.

[15] L. Reis and Q. Wang, The additive index of polynomials over finite fields, preprint (2021), https://arxiv.org/abs/2105.02374.

Fourth main result (Recursive construction): Notation 1

- K: field, V: K-vector space, W: K-subspace of V.
- $f : V \to V$ is *W-coset-wise K-affine* if $f(x) = \varphi_C(x) + v_C$ for all $x \in C$ (coset of W), and
  1. $\varphi_C \ldots K$-end. of V with $\varphi_C(W) \subseteq W$;
  2. $v_C \in V$.
- Case $\varphi_C = \varphi$ for all C recently studied by Reis and Wang[15].

[15] L. Reis and Q. Wang, The additive index of polynomials over finite fields, preprint (2021), https://arxiv.org/abs/2105.02374.

Fourth main result (Recursive construction): Notation 1

- K: field, V: K-vector space, W: K-subspace of V.
- $f: V \to V$ is *W-coset-wise K-affine* if $f(x) = \varphi_C(x) + v_C$ for all $x \in C$ (coset of W), and
  1. $\varphi_C \ldots K$-end. of V with $\varphi_C(W) \subseteq W$;
  2. $v_C \in V$.
- Case $\varphi_C = \varphi$ for all C recently studied by Reis and Wang[15].
- $\mathrm{GL}_d(p)$: group of invertible $(d \times d)$-mat. over $\mathbb{F}_p$.

[15] L. Reis and Q. Wang, The additive index of polynomials over finite fields, preprint (2021), `https://arxiv.org/abs/2105.02374`.

Fourth main result (Recursive construction): Notation 1

- K: field, V: K-vector space, W: K-subspace of V.
- $f : V \to V$ is *W-coset-wise K-affine* if $f(x) = \varphi_C(x) + v_C$ for all $x \in C$ (coset of W), and
  1. $\varphi_C \ldots K$-end. of V with $\varphi_C(W) \subseteq W$;
  2. $v_C \in V$.
- Case $\varphi_C = \varphi$ for all C recently studied by Reis and Wang[15].
- $\mathrm{GL}_d(p)$: group of invertible $(d \times d)$-mat. over $\mathbb{F}_p$.
- $\mathrm{CGL}_d(p)$: subset of $M \in \mathrm{GL}_d(p)$ with $\det(M+1) \neq 0$ (complete linear mappings).

[15] L. Reis and Q. Wang, The additive index of polynomials over finite fields, preprint (2021), `https://arxiv.org/abs/2105.02374`.

Fourth main result (Recursive construction): Notation 1

- K: field, V: K-vector space, W: K-subspace of V.
- $f: V \to V$ is *W-coset-wise K-affine* if $f(x) = \varphi_C(x) + v_C$ for all $x \in C$ (coset of W), and
  1. $\varphi_C \ldots K$-end. of V with $\varphi_C(W) \subseteq W$;
  2. $v_C \in V$.
- Case $\varphi_C = \varphi$ for all C recently studied by Reis and Wang[15].
- $\mathrm{GL}_d(p)$: group of invertible $(d \times d)$-mat. over $\mathbb{F}_p$.
- $\mathrm{CGL}_d(p)$: subset of $M \in \mathrm{GL}_d(p)$ with $\det(M+1) \neq 0$ (complete linear mappings).
- $M \in \mathrm{GL}_d(p)$, $v \in \mathbb{F}_p^d$: $x \mapsto xM + v$ is denot. by $\lambda(M, v)$ (aff. perm.).

[15] L. Reis and Q. Wang, The additive index of polynomials over finite fields, preprint (2021), https://arxiv.org/abs/2105.02374.

Fourth main result (Recursive construction): Notation 1

- K: field, V: K-vector space, W: K-subspace of V.
- $f : V \to V$ is *W-coset-wise K-affine* if $f(x) = \varphi_C(x) + v_C$ for all $x \in C$ (coset of W), and
  1. $\varphi_C \ldots K$-end. of V with $\varphi_C(W) \subseteq W$;
  2. $v_C \in V$.
- Case $\varphi_C = \varphi$ for all C recently studied by Reis and Wang[15].
- $\mathrm{GL}_d(p)$: group of invertible $(d \times d)$-mat. over $\mathbb{F}_p$.
- $\mathrm{CGL}_d(p)$: subset of $M \in \mathrm{GL}_d(p)$ with $\det(M + 1) \neq 0$ (complete linear mappings).
- $M \in \mathrm{GL}_d(p)$, $v \in \mathbb{F}_p^d$: $x \mapsto xM + v$ is denot. by $\lambda(M, v)$ (aff. perm.).
- On next slide, we give a technical def. of a set $\Gamma(d, p, \ell)$ of CTs of aff. permutations.

[15] L. Reis and Q. Wang, The additive index of polynomials over finite fields, preprint (2021), https://arxiv.org/abs/2105.02374.

Fourth main result (Recursive construction): Notation 2

- If $\ell = 1$, set

$$\Gamma(d,p,\ell) := \{\mathrm{CT}(\lambda(M,v)) : M \in \mathrm{CGL}_d(p), v \in \mathbb{F}_p^d\}.$$

Fourth main result (Recursive construction): Notation 2

- If $\ell = 1$, set

$$\Gamma(d,p,\ell) := \{\mathrm{CT}(\lambda(M,v)) : M \in \mathrm{CGL}_d(p), v \in \mathbb{F}_p^d\}.$$

- If $\ell \geq 2$ and $(d,p) \neq (1,2),(1,3),(2,2)$, set

$$\Gamma(d,p,\ell) := \{\mathrm{CT}(\lambda(M,v)) : M \in \mathrm{GL}_d(p), v \in \mathbb{F}_p^d\}.$$

Fourth main result (Recursive construction): Notation 2

- If $\ell = 1$, set

$$\Gamma(d,p,\ell) := \{\mathrm{CT}(\lambda(M,v)) : M \in \mathrm{CGL}_d(p), v \in \mathbb{F}_p^d\}.$$

- If $\ell \geq 2$ and $(d,p) \neq (1,2),(1,3),(2,2)$, set

$$\Gamma(d,p,\ell) := \{\mathrm{CT}(\lambda(M,v)) : M \in \mathrm{GL}_d(p), v \in \mathbb{F}_p^d\}.$$

- If $\ell \geq 2$ and $(d,p) = (1,2)$, set $\Gamma(d,p,\ell) := \emptyset$.
- If $\ell \geq 2$ and $(d,p) = (1,3)$, set $\Gamma(d,p,\ell) := \{x_1^3, x_3\}$.
- If $\ell \geq 2$ and $(d,p) = (2,2)$, set $\Gamma(d,p,\ell) := \{x_1^4, x_2^2, x_1x_3\}$.

Fourth main result (Recursive construction)

Theorem 4

Let $d, t \in \mathbb{N}^+$, p a prime.

Fourth main result (Recursive construction)

Theorem 4

Let $d, t \in \mathbb{N}^+$, p a prime.

- Assume that $x_1^{k_1} x_2^{k_2} \cdots x_{p^t}^{k_{p^t}} = \mathrm{CT}(f)$ for some compl. map. f of $\mathbb{F}_p^t$.

Fourth main result (Recursive construction)

Theorem 4

Let $d, t \in \mathbb{N}^+$, p a prime.

- Assume that $x_1^{k_1} x_2^{k_2} \cdots x_{p^t}^{k_{p^t}} = \mathrm{CT}(f)$ for some compl. map. f of $\mathbb{F}_p^t$.
- For $\ell = 1, 2, \ldots, p^t$ and $i = 1, 2, \ldots, k_\ell$, fix $\gamma_{\ell,i} \in \Gamma(d, p, \ell)$.

Fourth main result (Recursive construction)

Theorem 4

Let $d, t \in \mathbb{N}^+$, p a prime.

- Assume that $x_1^{k_1} x_2^{k_2} \cdots x_{p^t}^{k_{p^t}} = \mathrm{CT}(f)$ for some compl. map. f of $\mathbb{F}_p^t$.
- For $\ell = 1, 2, \ldots, p^t$ and $i = 1, 2, \ldots, k_\ell$, fix $\gamma_{\ell,i} \in \Gamma(d, p, \ell)$.

Then for each d-dim. $\mathbb{F}_p$-subsp. W of $\mathbb{F}_p^{d+t}$, there ex. W-coset-wise $\mathbb{F}_p$-affine compl. map. of $\mathbb{F}_p^{d+t}$ of cycle type

$$\prod_{\ell=1}^{p^t} \prod_{i=1}^{k_\ell} \mathrm{BU}_\ell(\gamma_{\ell,i}).$$

Fourth main result (Recursive construction)

Theorem 4

Let $d, t \in \mathbb{N}^+$, p a prime.

- Assume that $x_1^{k_1} x_2^{k_2} \cdots x_{p^t}^{k_{p^t}} = \mathrm{CT}(f)$ for some compl. map. f of $\mathbb{F}_p^t$.
- For $\ell = 1, 2, \ldots, p^t$ and $i = 1, 2, \ldots, k_\ell$, fix $\gamma_{\ell,i} \in \Gamma(d, p, \ell)$.

Then for each d-dim. $\mathbb{F}_p$-subsp. W of $\mathbb{F}_p^{d+t}$, there ex. W-coset-wise $\mathbb{F}_p$-affine compl. map. of $\mathbb{F}_p^{d+t}$ of cycle type

$$\prod_{\ell=1}^{p^t} \prod_{i=1}^{k_\ell} \mathrm{BU}_\ell(\gamma_{\ell,i}).$$

Corollary

$q = p^k$: odd prime power, S: Sylow p-subgroup of $\mathrm{Sym}(q)$.

Fourth main result (Recursive construction)

Theorem 4

Let $d, t \in \mathbb{N}^+$, p a prime.

- Assume that $x_1^{k_1} x_2^{k_2} \cdots x_{p^t}^{k_{p^t}} = \mathrm{CT}(f)$ for some compl. map. f of $\mathbb{F}_p^t$.
- For $\ell = 1, 2, \ldots, p^t$ and $i = 1, 2, \ldots, k_\ell$, fix $\gamma_{\ell,i} \in \Gamma(d, p, \ell)$.

Then for each d-dim. $\mathbb{F}_p$-subsp. W of $\mathbb{F}_p^{d+t}$, there ex. W-coset-wise $\mathbb{F}_p$-affine compl. map. of $\mathbb{F}_p^{d+t}$ of cycle type

$$\prod_{\ell=1}^{p^t} \prod_{i=1}^{k_\ell} \mathrm{BU}_\ell(\gamma_{\ell,i}).$$

Corollary

$q = p^k$: odd prime power, S: Sylow p-subgroup of $\mathrm{Sym}(q)$. Then for all $\sigma \in S$: $\mathrm{CT}(\sigma) = \mathrm{CT}(f)$ for some compl. map. f of $\mathbb{F}_q$.

Current section

1. Introduction: Complete mappings and cycle types
2. Our main results
3. Proof sketch of Theorem 4
4. References

Wreath products

Definition (Imprimitive permutational wreath product)

$\underline{G \leq \mathrm{Sym}(\Omega)}$, $\underline{P \leq \mathrm{Sym}(\Lambda)}$.

Wreath products

Definition (Imprimitive permutational wreath product)

$\underline{G \leq \mathrm{Sym}(\Omega)}$, $\underline{P \leq \mathrm{Sym}(\Lambda)}$. $G \wr_{\mathrm{imp}} P \leq \mathrm{Sym}(\Omega \times \Lambda)$ has elements

Wreath products

Definition (Imprimitive permutational wreath product)

$\underline{G \leq \mathrm{Sym}(\Omega)}$, $\underline{P \leq \mathrm{Sym}(\Lambda)}$. $G \wr_{\mathrm{imp}} P \leq \mathrm{Sym}(\Omega \times \Lambda)$ has elements

$$(\sigma, (g_{\lambda'})_{\lambda' \in \Lambda}) : (\omega, \lambda) \mapsto (g_{\sigma(\lambda)}(\omega), \sigma(\lambda))$$

for $\sigma \in P$ and $g_{\lambda'} \in G$.

Wreath products

Definition (Imprimitive permutational wreath product)

$G \leq \mathrm{Sym}(\Omega)$, $P \leq \mathrm{Sym}(\Lambda)$. $G \wr_{\mathrm{imp}} P \leq \mathrm{Sym}(\Omega \times \Lambda)$ has elements

$$(\sigma, (g_{\lambda'})_{\lambda' \in \Lambda}) : (\omega, \lambda) \mapsto (g_{\sigma(\lambda)}(\omega), \sigma(\lambda))$$

for $\sigma \in P$ and $g_{\lambda'} \in G$.

Intuition:

- $\Omega \times \Lambda = \bigsqcup_{\lambda \in \Lambda} \Omega_\lambda$ where $\Omega_\lambda := \Omega \times \{\lambda\}$ (copy of Ω).

Wreath products

Definition (Imprimitive permutational wreath product)

$\underline{G \leq \mathrm{Sym}(\Omega)}$, $\underline{P \leq \mathrm{Sym}(\Lambda)}$. $G \wr_{\mathrm{imp}} P \leq \mathrm{Sym}(\Omega \times \Lambda)$ has elements

$$(\sigma, (g_{\lambda'})_{\lambda' \in \Lambda}) : (\omega, \lambda) \mapsto (g_{\sigma(\lambda)}(\omega), \sigma(\lambda))$$

for $\sigma \in P$ and $g_{\lambda'} \in G$.

Intuition:

- $\Omega \times \Lambda = \bigsqcup_{\lambda \in \Lambda} \Omega_\lambda$ where $\Omega_\lambda := \Omega \times \{\lambda\}$ (copy of Ω).
- $(\sigma, (g_{\lambda'})_{\lambda' \in \Lambda})$ acts on $\Omega \times \Lambda$ by

Wreath products

Definition (Imprimitive permutational wreath product)

$G \leq \mathrm{Sym}(\Omega)$, $P \leq \mathrm{Sym}(\Lambda)$. $G \wr_{\mathrm{imp}} P \leq \mathrm{Sym}(\Omega \times \Lambda)$ has elements

$$(\sigma, (g_{\lambda'})_{\lambda' \in \Lambda}) : (\omega, \lambda) \mapsto (g_{\sigma(\lambda)}(\omega), \sigma(\lambda))$$

for $\sigma \in P$ and $g_{\lambda'} \in G$.

Intuition:

- $\Omega \times \Lambda = \bigsqcup_{\lambda \in \Lambda} \Omega_\lambda$ where $\Omega_\lambda := \Omega \times \{\lambda\}$ (copy of Ω).
- $(\sigma, (g_{\lambda'})_{\lambda' \in \Lambda})$ acts on $\Omega \times \Lambda$ by
  - first permuting the copies Ω_λ acc. to σ: $(\omega, \lambda) \mapsto (\omega, \sigma(\lambda))$, and then

Wreath products

Definition (Imprimitive permutational wreath product)

$G \leq \mathrm{Sym}(\Omega)$, $P \leq \mathrm{Sym}(\Lambda)$. $G \wr_{\mathrm{imp}} P \leq \mathrm{Sym}(\Omega \times \Lambda)$ has elements

$$(\sigma, (g_{\lambda'})_{\lambda' \in \Lambda}) : (\omega, \lambda) \mapsto (g_{\sigma(\lambda)}(\omega), \sigma(\lambda))$$

for $\sigma \in P$ and $g_{\lambda'} \in G$.

Intuition:

- $\Omega \times \Lambda = \bigsqcup_{\lambda \in \Lambda} \Omega_\lambda$ where $\Omega_\lambda := \Omega \times \{\lambda\}$ (copy of Ω).
- $(\sigma, (g_{\lambda'})_{\lambda' \in \Lambda})$ acts on $\Omega \times \Lambda$ by
  - first permuting the copies Ω_λ acc. to σ: $(\omega, \lambda) \mapsto (\omega, \sigma(\lambda))$, and then
  - permuting each copy $\Omega_{\lambda'}$ acc. to $g_{\lambda'}$: $(\omega, \sigma(\lambda)) \mapsto (g_{\sigma(\lambda)}(\omega), \sigma(\lambda))$.

Coset-wise affine permutations as a wreath product

Coset-wise affine permutations as a wreath product

- $G \leq \mathrm{Sym}(\Omega)$, $H \leq \mathrm{Sym}(\Sigma)$. An *isomorphism of perm. gps.* $G \to H$ is a bijection $\beta : \Omega \to \Sigma$ s.t. H is im. of

$$G \to \mathrm{Sym}(\Sigma), g \mapsto \beta \circ g \circ \beta^{-1}.$$

Coset-wise affine permutations as a wreath product

- $G \leq \mathrm{Sym}(\Omega)$, $H \leq \mathrm{Sym}(\Sigma)$. An *isomorphism of perm. gps.* $G \to H$ is a bijection $\beta : \Omega \to \Sigma$ s.t. H is im. of

$$G \to \mathrm{Sym}(\Sigma), g \mapsto \beta \circ g \circ \beta^{-1}.$$

- K: field, V: K-vector space, W: K-subspace of V.

Coset-wise affine permutations as a wreath product

- $G \leq \mathrm{Sym}(\Omega)$, $H \leq \mathrm{Sym}(\Sigma)$. An *isomorphism of perm. gps.* $G \to H$ is a bijection $\beta : \Omega \to \Sigma$ s.t. H is im. of

$$G \to \mathrm{Sym}(\Sigma), g \mapsto \beta \circ g \circ \beta^{-1}.$$

- K: field, V: K-vector space, W: K-subspace of V. $\mathrm{CAff}_K(V, W)$: perm. gp. of W-coset-wise K-aff. perm. of V.

Coset-wise affine permutations as a wreath product

- $G \le \mathrm{Sym}(\Omega)$, $H \le \mathrm{Sym}(\Sigma)$. An *isomorphism of perm. gps.* $G \to H$ is a bijection $\beta : \Omega \to \Sigma$ s.t. H is im. of

$$G \to \mathrm{Sym}(\Sigma), g \mapsto \beta \circ g \circ \beta^{-1}.$$

- K: field, V: K-vector space, W: K-subspace of V. $\mathrm{CAff}_K(V, W)$: perm. gp. of W-coset-wise K-aff. perm. of V. It is iso. to

$$\mathrm{Aff}_K(W) \wr_{\mathrm{imp}} \mathrm{Sym}(V/W),$$

where $\mathrm{Aff}_K(W)$: gp. of K-aff. perm. $x \mapsto xM + w$ of W.

Coset-wise affine permutations as a wreath product

- $G \leq \mathrm{Sym}(\Omega)$, $H \leq \mathrm{Sym}(\Sigma)$. An *isomorphism of perm. gps.* $G \to H$ is a bijection $\beta : \Omega \to \Sigma$ s.t. H is im. of

$$G \to \mathrm{Sym}(\Sigma), g \mapsto \beta \circ g \circ \beta^{-1}.$$

- K: field, V: K-vector space, W: K-subspace of V. $\mathrm{CAff}_K(V, W)$: perm. gp. of W-coset-wise K-aff. perm. of V. It is iso. to

$$\mathrm{Aff}_K(W) \wr_{\mathrm{imp}} \mathrm{Sym}(V/W),$$

where $\mathrm{Aff}_K(W)$: gp. of K-aff. perm. $x \mapsto xM + w$ of W.
- There ex. iso.

$$\mathrm{CAff}_K(V, W) \to \mathrm{Aff}_K(W) \wr_{\mathrm{imp}} \mathrm{Sym}(V/W)$$

Coset-wise affine permutations as a wreath product

- $G \leq \mathrm{Sym}(\Omega)$, $H \leq \mathrm{Sym}(\Sigma)$. An *isomorphism of perm. gps.* $G \to H$ is a bijection $\beta : \Omega \to \Sigma$ s.t. H is im. of

$$G \to \mathrm{Sym}(\Sigma), g \mapsto \beta \circ g \circ \beta^{-1}.$$

- K: field, V: K-vector space, W: K-subspace of V. $\mathrm{CAff}_K(V, W)$: perm. gp. of W-coset-wise K-aff. perm. of V. It is iso. to

$$\mathrm{Aff}_K(W) \wr_{\mathrm{imp}} \mathrm{Sym}(V/W),$$

where $\mathrm{Aff}_K(W)$: gp. of K-aff. perm. $x \mapsto xM + w$ of W.

- There ex. iso.

$$\mathrm{CAff}_K(V, W) \to \mathrm{Aff}_K(W) \wr_{\mathrm{imp}} \mathrm{Sym}(V/W)$$

s.t. compl. map. in $\mathrm{CAff}_K(V, W)$ corr. to the el. $(\sigma, (A_u)_{u \in V/W})$ with σ and each A_u compl. map. (of V/W resp. W).

Cycle types of wreath product elements

- Goal: Determine all possible $\mathrm{CT}((\sigma,(A_u)_{u\in V/W}))$ with σ and A_u compl. map.

[16] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

Cycle types of wreath product elements

- Goal: Determine all possible $\mathrm{CT}((\sigma, (A_u)_{u \in V/W}))$ with σ and A_u compl. map.
- To compute these cycle types, follow Pólya[16]:

[16] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

Cycle types of wreath product elements

- Goal: Determine all possible $\mathrm{CT}((\sigma, (A_u)_{u \in V/W}))$ with σ and A_u compl. map.
- To compute these cycle types, follow Pólya[16]:
  - For each cycle $\zeta = (u_1, u_2, \ldots, u_\ell)$ of σ, form $A_{u_1} A_{u_2} \cdots A_{u_\ell} \in \mathrm{Aff}_K(W)$.

[16] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

Cycle types of wreath product elements

- Goal: Determine all possible $\mathrm{CT}((\sigma,(A_u)_{u\in V/W}))$ with σ and A_u compl. map.
- To compute these cycle types, follow Pólya[16]:
  - For each cycle $\zeta=(u_1,u_2,\ldots,u_\ell)$ of σ, form $A_{u_1}A_{u_2}\cdots A_{u_\ell}\in\mathrm{Aff}_K(W)$.
  - Then form the blow-up $\mathrm{BU}_\ell(\mathrm{CT}(A_{u_1}A_{u_2}\cdots A_{u_\ell}))$.

[16] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

Cycle types of wreath product elements

- Goal: Determine all possible $\mathrm{CT}((\sigma, (A_u)_{u \in V/W}))$ with σ and A_u compl. map.
- To compute these cycle types, follow Pólya[16]:
  - For each cycle $\zeta = (u_1, u_2, \ldots, u_\ell)$ of σ, form $A_{u_1} A_{u_2} \cdots A_{u_\ell} \in \mathrm{Aff}_K(W)$.
  - Then form the blow-up $\mathrm{BU}_\ell(\mathrm{CT}(A_{u_1} A_{u_2} \cdots A_{u_\ell}))$.
  - Finally, multiply those blow-ups together:

$$\mathrm{CT}((\sigma, (A_u)_{u \in V/W})) = \prod_{\text{cycles } \zeta=(u_1,\ldots,u_\ell) \text{ of } \sigma} \mathrm{BU}_\ell(\mathrm{CT}(A_{u_1} \cdots A_{u_\ell})).$$

[16] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

Products of complete affine mappings

Our case: $K = \mathbb{F}_p$, σ and each A_u arbitrary compl. map.

Products of complete affine mappings

Our case: $K = \mathbb{F}_p$, σ and each A_u arbitrary compl. map.

Question

For given ℓ, which elements of $\mathrm{Aff}_{\mathbb{F}_p}(\mathbb{F}_p^d) = \mathrm{AGL}_d(p)$ are a product of ℓ compl. map. in $\mathrm{AGL}_d(p)$?

Products of complete affine mappings

Our case: $K = \mathbb{F}_p$, σ and each A_u arbitrary compl. map.

Question

For given ℓ, which elements of $\mathrm{Aff}_{\mathbb{F}_p}(\mathbb{F}_p^d) = \mathrm{AGL}_d(p)$ are a product of ℓ compl. map. in $\mathrm{AGL}_d(p)$?

Proposition

$d, \ell \in \mathbb{N}^+$, p prime.
$M(d, p, \ell)$: set of products of ℓ compl. map. in $\mathrm{AGL}_d(p)$. Then

Products of complete affine mappings

Our case: $K = \mathbb{F}_p$, σ and each A_u arbitrary compl. map.

Question

For given ℓ, which elements of $\mathrm{Aff}_{\mathbb{F}_p}(\mathbb{F}_p^d) = \mathrm{AGL}_d(p)$ are a product of ℓ compl. map. in $\mathrm{AGL}_d(p)$?

Proposition

$d, \ell \in \mathbb{N}^+$, p prime.
$M(d,p,\ell)$: set of products of ℓ compl. map. in $\mathrm{AGL}_d(p)$. Then

1. $M(d,p,1) = \{\lambda(M,v) : M \in \mathrm{CGL}_d(p), v \in \mathbb{F}_p^d\}$.

Products of complete affine mappings

Our case: $K = \mathbb{F}_p$, σ and each A_u arbitrary compl. map.

Question

For given ℓ, which elements of $\mathrm{Aff}_{\mathbb{F}_p}(\mathbb{F}_p^d) = \mathrm{AGL}_d(p)$ are a product of ℓ compl. map. in $\mathrm{AGL}_d(p)$?

Proposition

$d, \ell \in \mathbb{N}^+$, p prime.
$M(d,p,\ell)$: set of products of ℓ compl. map. in $\mathrm{AGL}_d(p)$. Then

1. $M(d,p,1) = \{\lambda(M,v) : M \in \mathrm{CGL}_d(p), v \in \mathbb{F}_p^d\}$.
2. If $\ell \geq 2$: $M(d,p,\ell) = \mathrm{AGL}_d(p)$ unless $(d,p) \in \{(1,2),(1,3),(2,2)\}$.

Products of complete affine mappings

Our case: $K = \mathbb{F}_p$, σ and each A_u arbitrary compl. map.

Question

For given ℓ, which elements of $\mathrm{Aff}_{\mathbb{F}_p}(\mathbb{F}_p^d) = \mathrm{AGL}_d(p)$ are a product of ℓ compl. map. in $\mathrm{AGL}_d(p)$?

Proposition

$d, \ell \in \mathbb{N}^+$, p prime.
$M(d,p,\ell)$: set of products of ℓ compl. map. in $\mathrm{AGL}_d(p)$. Then

1. $M(d,p,1) = \{\lambda(M,v) : M \in \mathrm{CGL}_d(p), v \in \mathbb{F}_p^d\}$.
2. If $\ell \geq 2$: $M(d,p,\ell) = \mathrm{AGL}_d(p)$ unless $(d,p) \in \{(1,2),(1,3),(2,2)\}$.
3. If $\ell \geq 2$, $(d,p) = (1,2)$: $M(d,p,\ell) = \emptyset$.
4. If $\ell \geq 2$, $(d,p) = (1,3)$: $M(d,p,\ell) = \{(1)\}$.
5. If $\ell \geq 2$, $(d,p) = (2,2)$: $M(d,p,\ell) = \langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \rangle$.

Concluding the proof of Theorem 4

Concluding the proof of Theorem 4

- Consequence:

$$\Gamma(d,p,\ell)=\{\mathrm{CT}(B_1B_2\cdots B_\ell):B_i\in\mathrm{AGL}_d(p),B_i\text{ is complete}\}.$$

Concluding the proof of Theorem 4

- Consequence:

$$\Gamma(d,p,\ell) = \{\mathrm{CT}(B_1 B_2 \cdots B_\ell) : B_i \in \mathrm{AGL}_d(p), B_i \text{ is complete}\}.$$

- Choosing the A_u suitably, we can get

$$\mathrm{CT}((\sigma,(A_u)_{u\in V/W})) = \prod_{\text{cycles } \zeta \text{ of } \sigma} \mathrm{BU}_\ell(\gamma_\zeta)$$

for arbitrary el. $\gamma_\zeta \in \Gamma(\dim_{\mathbb{F}_p}(W), p, \ell(\zeta))$.

Concluding the proof of Theorem 4

- Consequence:

$$\Gamma(d,p,\ell)=\{\mathrm{CT}(B_1B_2\cdots B_\ell): B_i\in \mathrm{AGL}_d(p), B_i \text{ is complete}\}.$$

- Choosing the A_u suitably, we can get

$$\mathrm{CT}((\sigma,(A_u)_{u\in V/W}))=\prod_{\text{cycles } \zeta \text{ of } \sigma}\mathrm{BU}_\ell(\gamma_\zeta)$$

  for arbitrary el. $\gamma_\zeta\in\Gamma(\dim_{\mathbb{F}_p}(W),p,\ell(\zeta))$.
- If we
  - set $t:=\dim_{\mathbb{F}_p}(V/W)$ and $d:=\dim_{\mathbb{F}_p}(W)$,

Concluding the proof of Theorem 4

- Consequence:

$$\Gamma(d,p,\ell) = \{\mathrm{CT}(B_1 B_2 \cdots B_\ell) : B_i \in \mathrm{AGL}_d(p), B_i \text{ is complete}\}.$$

- Choosing the A_u suitably, we can get

$$\mathrm{CT}((\sigma,(A_u)_{u\in V/W})) = \prod_{\text{cycles } \zeta \text{ of } \sigma} \mathrm{BU}_\ell(\gamma_\zeta)$$

for arbitrary el. $\gamma_\zeta \in \Gamma(\dim_{\mathbb{F}_p}(W), p, \ell(\zeta))$.

- If we
  - set $t := \dim_{\mathbb{F}_p}(V/W)$ and $d := \dim_{\mathbb{F}_p}(W)$,
  - write $\mathrm{CT}(\sigma) = x_1^{k_1} x_2^{k_2} \cdots x_{p^t}^{k_{p^t}}$,

Concluding the proof of Theorem 4

- Consequence:

$$\Gamma(d,p,\ell) = \{\mathrm{CT}(B_1 B_2 \cdots B_\ell) : B_i \in \mathrm{AGL}_d(p), B_i \text{ is complete}\}.$$

- Choosing the A_u suitably, we can get

$$\mathrm{CT}((\sigma,(A_u)_{u\in V/W})) = \prod_{\text{cycles } \zeta \text{ of } \sigma} \mathrm{BU}_\ell(\gamma_\zeta)$$

  for arbitrary el. $\gamma_\zeta \in \Gamma(\dim_{\mathbb{F}_p}(W), p, \ell(\zeta))$.
- If we
  - set $t := \dim_{\mathbb{F}_p}(V/W)$ and $d := \dim_{\mathbb{F}_p}(W)$,
  - write $\mathrm{CT}(\sigma) = x_1^{k_1} x_2^{k_2} \cdots x_{p^t}^{k_{p^t}}$,
  - enumerate ℓ-cycles of σ as $\zeta_{\ell,i}$ for $i = 1,2,\ldots,k_\ell$, and

Concluding the proof of Theorem 4

- Consequence:

$$\Gamma(d,p,\ell)=\{\mathrm{CT}(B_1B_2\cdots B_\ell): B_i\in \mathrm{AGL}_d(p), B_i \text{ is complete}\}.$$

- Choosing the A_u suitably, we can get

$$\mathrm{CT}((\sigma,(A_u)_{u\in V/W}))=\prod_{\text{cycles } \zeta \text{ of } \sigma}\mathrm{BU}_\ell(\gamma_\zeta)$$

  for arbitrary el. $\gamma_\zeta\in\Gamma(\dim_{\mathbb{F}_p}(W),p,\ell(\zeta))$.

- If we
  - set $t:=\dim_{\mathbb{F}_p}(V/W)$ and $d:=\dim_{\mathbb{F}_p}(W)$,
  - write $\mathrm{CT}(\sigma)=x_1^{k_1}x_2^{k_2}\cdots x_{p^t}^{k_{p^t}}$,
  - enumerate ℓ-cycles of σ as $\zeta_{\ell,i}$ for $i=1,2,\ldots,k_\ell$, and
  - write $\gamma_{\ell,i}$ instead of $\gamma_{\zeta_{\ell,i}}$,

Concluding the proof of Theorem 4

- Consequence:

$$\Gamma(d,p,\ell) = \{\mathrm{CT}(B_1 B_2 \cdots B_\ell) : B_i \in \mathrm{AGL}_d(p), B_i \text{ is complete}\}.$$

- Choosing the A_u suitably, we can get

$$\mathrm{CT}((\sigma, (A_u)_{u \in V/W})) = \prod_{\text{cycles } \zeta \text{ of } \sigma} \mathrm{BU}_\ell(\gamma_\zeta)$$

for arbitrary el. $\gamma_\zeta \in \Gamma(\dim_{\mathbb{F}_p}(W), p, \ell(\zeta))$.

- If we
  - set $t := \dim_{\mathbb{F}_p}(V/W)$ and $d := \dim_{\mathbb{F}_p}(W)$,
  - write $\mathrm{CT}(\sigma) = x_1^{k_1} x_2^{k_2} \cdots x_{p^t}^{k_{p^t}}$,
  - enumerate ℓ-cycles of σ as $\zeta_{\ell,i}$ for $i = 1, 2, \ldots, k_\ell$, and
  - write $\gamma_{\ell,i}$ instead of $\gamma_{\zeta_{\ell,i}}$,

this becomes the statement of Theorem 4.

Current section

1. Introduction: Complete mappings and cycle types
2. Our main results
3. Proof sketch of Theorem 4
4. References

References

1. J. Bell, Cyclotomic orthomorphisms of finite fields, *Discrete Appl. Math.* **161**(1–2): 294–300, 2013.
2. A. Bors and Q. Wang, Generalized cyclotomic mappings: Switching between polynomial, cyclotomic, and wreath product form, to appear in *Commun. Math. Res.*, digital version available under `https://doc.global-sci.org/uploads/online_news/CMR/a399f07452983bc3e4a1841da72b5780.pdf`.
3. A. Bors and Q. Wang, Cycle types of complete mappings of finite fields, to appear in *J. Algebra*, preprint available under `https://arxiv.org/abs/2105.00140`.
4. A. Bors and Q. Wang, Coset-wise affine functions and cycle types of complete mappings, preprint (2021), `https://arxiv.org/abs/2109.03922`.
5. L. Carlitz, Sets of primitive roots, *Compositio Math.* **13**: 65–70, 1956.
6. A. Çeşmelioğlu, W. Meidl and A. Topuzoğlu, On the cycle structure of permutation polynomials, *Finite Fields Appl.* **14**: 593–614, 2008.

References cont.

7. P. Charpin, S. Mesnager and S. Sarkar, Involutions over the Galois field $\mathbb{F}_{2^n}$, *IEEE Trans. Inform. Theory* **62**(4): 2266–2276, 2016.
8. Y. Chen, L. Wang and S. Zhu, On the constructions of n-cycle permutations, *Finite Fields Appl.* **73**: 101847, 2017.
9. A.B. Evans, Applications of complete mappings and orthomorphisms of finite groups, *Quasigroups Related Systems* **23**: 5–30, 2015.
10. A.B. Evans, *Orthogonal Latin Squares Based on Groups*, Springer (Developments in Mathematics, 57), Cham, 2018.
11. H. Fripertinger, Cycle indices of linear, affine, and projective groups, *Linear Algebra Appl.* **263**: 133–156, 1997.
12. J. Fulman, Cycle indices for the finite classical groups, *J. Group Theory* **2**: 251–289, 1999.
13. D. Gerike and G.M. Kyureghan, Permutations on finite fields with invariant cycle structure on lines, *Des. Codes Cryptogr.* **88**: 1723–1740, 2020.

References cont.

14. S.W. Golomb, G. Gong and L. Mittenthal, Constructions of orthomorphisms of $\mathbb{Z}_2^n$, in: D. Jungnickel and H. Niederreiter (eds.), *Finite Fields and Applications. Proceedings of the Fifth International Conference on Finite Fields and Applications Fq5, held at the University of Augsburg, Germany, August 2–6, 1999*, Springer, Berlin-Heidelberg, 2001, pp. 178–195.
15. L. Işik, A. Topuzoğlu and A. Winterhof, Complete mappings and Carlitz rank, *Des. Codes Cryptogr.* **85**: 121–128, 2017.
16. H.B. Mann, The construction of orthogonal Latin squares, *Ann. Math. Statistics* **13**: 418–423, 1942.
17. L. Mittenthal, Block substitutions using orthomorphic mappings, *Adv. Appl. Math.* **16**(10): 59–71, 1995.
18. L. Mittenthal, Nonlinear dynamic substitution devices and methods for block substitutions employing coset decompositions and direct geometric generation, US Patent 5647001, 1997.

References cont.

19. A. Muratović-Ribić and E. Pasalic, A note on complete polynomials over finite fields and their applications in crpytography, *Finite Fields Appl.* **25**: 306–315, 2014.
20. H. Niederreiter, *Random number generation and quasi-Monte Carlo Methods*, SIAM (CBMS-NSF Regional Conference Series in Applied Mathematics, 63), Philadelphia, 1992.
21. H. Niederreiter and K.H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* **33**(2): 197–212, 1984.
22. H. Niederreiter and A. Winterhof, Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields, *Discrete Math.* **295**(1–3): 161–171, 2005.
23. T. Niu, K. Li, L. Qu and Q. Wang, New constructions of involutions over finite fields, *Cryptogr. Commun.* **12**: 165–185, 2020.
24. G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68**(1): 145–254, 1937.

References cont.

25. L. Reis and Q. Wang, The additive index of polynomials over finite fields, preprint (2021), `https://arxiv.org/abs/2105.02374`.
26. I.M. Rubio, G.L. Mullen, C. Corrada and F.N. Castro, Dickson permutation polynomials that decompose in cycles of the same length, in: G.L. Mullen et al. (eds.), *Finite Fields and Applications. Eighth International Conference on Finite Fields and Applications. July 9–13, 2007. Melbourne, Australia*, American Mathematical Society (Contemporary Mathematics, vol. 461), Providence, 2008, pp. 229–240.
27. A. Sakzad, M.-R. Sadeghi and D. Panario, Cycle structure of permutation functions over finite fields and their applications, *Adv. Math. Commun.* **6**(3): 347–361, 2012.
28. R.H. Schulz, On check digit systems using anti-symmetric mappings, in: I. Althöfer et al. (eds.), *Numbers, information and complexity*, Kluwer, Boston, 2000, pp. 295–310.

References cont.

29. Z. Tu, X. Zeng and L. Hu, Several classes of complete permutation polynomials, *Finite Fields Appl.* **25**: 182–193, 2014.
30. Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, in: S.W. Golomb et al. (eds.), *Sequences, Subsequences, and Consequences*, Springer (Lecture Notes in Comput. Sci., vol. 4893), Berlin, 2007, pp. 119–128.
31. Q. Wang, Cyclotomy and permutation polynomials of large indices, *Finite Fields Appl.* **22**: 57–69, 2013.
32. W.-D. Wei, X.-H. Gao and B.-F. Yang, Equivalence relation on the set of subsets of Z_v and enumeration of the equivalence classes (Research Announcement), *Adv. Math.* **17**: 326–327, 1988.
33. A. Winterhof, Generalizations of complete mappings of finite fields and some applications, *J. Symbolic Comput.* **64**: 42–52, 2014.
34. G. Wu, N. Li, T. Helleseth and Y. Zhang, Some classes of monomial complete permutation polynomials over finite fields of characteristic two, *Finite Fields Appl.* **28**: 148–165, 2014.

References cont.

35. G. Xu and X. Cao, Complete permutation polynomials over finite fields of odd characteristic, *Finite Fields Appl.* **31**: 228–240, 2015.
36. Z. Zha, L. Hu and X. Cao, Constructing permutations and complete permutations over finite fields via subfield-valued polynomials, *Finite Fields Appl.* **31**: 162–177, 2015.
37. Y. Zheng, Y. Yu, Y. Zhang and D. Pei, Piecewise constructions of inverses of cyclotomic mapping permutation polynomials, *Finite Fields Appl.* **40**: 1–9, 2016.
38. M. Wu, C. Li and Z. Wang, Characterizations and constructions of triple-cycle permutations of the form $x^r h(x^s)$, *Des. Codes Cryptogr.* **88**(10): 2119–2132, 2020.