Permutation automorphisms of cyclic codes

Henk D.L. Hollmann

Tartu, 9 Mai, 2022

University of Tartu, Taru, Estonia
Email: henk.hollmann@ut.ee

Content

Contents of this talk:

- Pre-introduction
- Introduction
- Three related problems
- List of examples
- Future work
- Conclusions

Pre-introduction

Automorphisms of cyclic codes is old research topic. Several classes of codes (BCH, Reed-Muller and GRM) have answers, but general answers are difficult.

- In 1998 Charpin suggested to investigate automorphisms of irreducible cyclic codes, minimal cyclic codes.
- Most of these codes have automorphism group generated by the cyclic shift and a permutation related to a Frobenius mapping, the standard ones that every such cyclic code has.
- But occasionally, there are more. We will call such codes non-standard irreducible cyclic codes or NSIC-codes. Most famous example: the Golay codes.

Problem: classify all the NSIC-codes.

This talk discusses some progress on this problem.

Setting in the paper

:

- $\mathbb{F}$ is a field [here a finite field $\mathbb{F}_q$ of order q];
- n is a positive integer with $\gcd(n, \mathrm{char}(\mathbb{F})) = 1$;
- $\mathbb{E}$ is the splitting field of $x^n - 1$ over $\mathbb{F}$,
  smallest extension of $\mathbb{F}$ that contains all n-th roots of unity over $\mathbb{F}$ (a Galois-extension);
- $m := [\mathbb{E} : \mathbb{F}]$
  Then $\mathcal{G} := \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ has size m.
- $\mathcal{U} = \mathcal{U}_{n,q}$ is the (unique!) group of order n in an extension of $\mathbb{F}$. Then $\mathcal{U}_{n,q}$ is contained in $\mathbb{E}$ and consists of the n-th roots of unity, the solutions of $x^n = 1$ in $\mathbb{E}$.

- If $\mathbb{E} = \mathbb{F}(\alpha)$ (if α has degree m over $\mathbb{F}$), then the minimal polynomial $f(x)$ of α over $\mathbb{F}$ is

$$f(x) = \prod_{\sigma \in \mathcal{G}} (x - \sigma(\alpha)).$$

- An $\mathbb{F}$-linear map on $\mathbb{E}$ has the form

$$L(x) = \sum_{\sigma \in \mathcal{G}} \lambda_\sigma \sigma(x)$$

  with $\lambda_\sigma \in \mathbb{E}$ for all $\sigma \in \mathcal{G}$.
- An $\mathbb{F}$-linear map $x \to \lambda\sigma(x)$ is called standard, the others are called non-standard.
- If $\mathbb{F} = \mathbb{F}_q$ is a finite field of size q, a power of a prime p, and $\mathbb{E} = \mathbb{F}_{q^m}$, then the maps

$$\sigma_i : x \to x^{q^i}$$

  $(i = 0, \ldots, m-1)$ make up the group $\mathcal{G} = \mathrm{Gal}(\mathbb{F}_{q^m}, \mathbb{F}_q)$.

Notation throughout this talk

- $\mathbb{F}_q$ a finite field
  (so $q = p^r$, a power of a prime p)
- n positive integer with $\gcd(n, q) = 1$
- $m = \mathrm{ord}_n(q)$ is the multiplicative order of q modulo n
  (smallest positive integer such that $n \mid q^m - 1$)
  Then $\mathbb{F}_{q^m}$ is splitting field of $x^n - 1$ over $\mathbb{F}_q$
- $U = U_{n,q}$: multiplicative group of order n in extension of $\mathbb{F}_q$
  n-th roots of unity over $\mathbb{F}_q$
  solutions of $x^n - 1 = 0$, hence smallest extension is $\mathbb{F}_{q^m}$.
  $\mathcal{U}_{n,q} = \langle \xi \rangle$ is cyclic
  $\xi \in \mathcal{U}_{n,q}$ primitive n-th root of unity, $\mathrm{ord}(\xi) = n$.
  minimal polynomial of ξ over $\mathbb{F}_q$ is

$$f(x) = (x - \xi)(x - \xi^q) \cdots (x - \xi^{q^{m-1}}),$$

  $\deg(f) = m$.

- $\mathrm{GL}(m, \mathbb{F}_q)$: group of invertible $\mathbb{F}_q$-linear maps on $\mathbb{F}_{q^m} \cong \mathbb{F}_q^m$
- **Recall** $x \to x^q$ and $x \to \alpha x$ ($\alpha \in \mathbb{F}_{q^m}$) are *linear* maps on $\mathbb{F}_{q^m}$. [NB: Elements of $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$.]
  In this talk: maps $x \to \alpha x^{q^i}$ are called *standard* in $\mathrm{GL}(m, \mathbb{F}_q)$
  (standard = boring)

- $\mathcal{S}_n$: group of all *permutations* on $\mathbb{Z}_n$
- Special permutations:
  - $\sigma : i \to i + 1 \pmod n$ (cyclic shift)
  - $\phi : i \to qi \pmod n$ (Frobenius permutation)
- Group $\langle \sigma, \phi \rangle$: standard permutations (order mn)
  (again: standard = boring)

The order (or *exponent*) of a polynomial $g(x) \in \mathbb{F}_q[x]$ is the smallest integer $k > 0$ for which $g(x) \mid x^k - 1$.

Introduction

Definition

$\mathcal{L}(n,q)$: *all* $\mathbb{F}_q$*-linear maps on* $\mathbb{F}_{q^m}$ *that fix* $\mathcal{U}_{n,q}$ set-wise.

Definition

$\mathcal{L}_{\mathrm{st}}(n,q)$: *the (boring)* standard *maps in* $\mathcal{L}(n,q)$:

maps $x \to \alpha x^{q^i}$ *with* $\alpha \in \mathcal{U}_{n,q}$ *and* $i = 0, 1, \ldots, m-1$.

Fix $\mathcal{U}_{n,q}$ since $\mathcal{U}_{n,q} = \langle \xi \rangle$ and $\mathrm{ord}(\xi^q) = n$.

NB: $\boxed{|\mathcal{L}_{\mathrm{st}}(n,q)| = nm}$.

Theorem

$\mathcal{L}(n,q)$ *is* subgroup *of* $\mathrm{GL}(m, \mathbb{F}_q)$.

Proof: $L \in \mathcal{L}(n,q)$ is *invertible*: ξ is generator of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ and image $L(\mathcal{U}_{n,q})$ contains ξ. $\square$

Usually, $\mathcal{L}(n,q) = \mathcal{L}_{\mathrm{st}}(n,q)$

But occasionally, there exist non-standard maps fixing $\mathcal{U}_{n,q}$ set-wise.

Definition

If $|\mathcal{L}(n,q)| > nm$, then the pair $(n, \mathbb{F}_q)$ is called non-standard.

Example

Let $n = q^m - 1$. Then $\mathcal{U}_{n,q} = \mathbb{F}_{q^m} \setminus \{0\}$, hence

$$\mathcal{L}(n = q^m - 1, q) = \mathrm{GL}(m, \mathbb{F}_q).$$

Counting $\rightarrow$ the pair $(n = q^m - 1, \mathbb{F}_q)$ is non-standard if and only if $m > 2$ or $m = 2, q > 2$. $\square$

Relations with other research fields

1. Non-standard linear recurring sequence subgroups

Let $f(x) = f_m x^m + f_{m-1} x^{m-1} + \cdots + f_1 x + f_0 \in \mathbb{F}_q[x]$ with $f_m \neq 0 \neq f_0$ be fixed.

Definition

A sequence $\mathbf{s} = (s_i)_{i \geq 0}$ *in* $\overline{\mathbb{F}}_p$ *satisfying the m-th order recurrence relation*

$$f_m s_i + f_{m-1} s_{i-1} + \cdots + f_1 s_{i-m+1} + f_0 s_{i-m} = 0 \qquad (0.1)$$

for all integers $i \geq m$ *will be referred to as an f-sequence. Such a sequence is a linear recurring sequence.*

Definition

The subgroup $\mathcal{U} = \mathcal{U}_{n,q}$ of order n in $\mathbb{F}_{q^m}$ is called an f-subgroup if there exists an f-sequence $\mathbf{s} = (s_i)_{i \geq 0}$ in $\mathbb{F}_{q^m}$ with period n that represents $\mathcal{U}$, that is,

$$\mathcal{U} = \{s_0, s_1, \ldots, s_{n-1}\}.$$

Example: $\xi \in \mathbb{F}_{q^m}$, $\mathrm{ord}(\xi) = n$, $f(\xi) = 0$.

Then $\mathbf{s}$ with $s_i = \xi^i$ is f-sequence and represents $\langle \xi \rangle = \mathcal{U}_{n,q}$.

Such an f-sequence is called *cyclic*: $s_{i+1}/s_i = \alpha$, constant, for all i.

Here cyclic = standard = boring

Definition

An f-subgroup $\mathcal{U}$ is called non-standard if there exists a non-cyclic f-sequence that represents $\mathcal{U}$.

Studied by Brison and Noguiera in a sequence of papers.

Theorem

If f is irreducible over $\mathbb{F}_q$ with $\mathrm{ord}(f) = n$, then the only f-subgroup is $\mathcal{U}_{n,q}$.

Theorem

If f is irreducible over $\mathbb{F}_q$, then $\mathcal{U}_{n,q}$ is a non-standard f-subgroup if and only if the pair $(n, \mathbb{F}_q)$ is non-standard.

Proof: Idea: f-sequences **s** have the form

$$s_i = \ell_0 \xi^i + \ell_1 (\xi^q)^i + \cdots + \ell_{m-1} (\xi^{q^{m-1}})^i = L(\xi^i),$$

where $L(x) = \ell_0 x + \ell_1 x^q + \cdots + \ell_{m-1} x^{q^{m-1}} \in \mathrm{GL}(m, \mathbb{F}_q)$. □

2. Permutation automorphisms of irreducible cyclic codes

A linear code of length n and dimension k over $\mathbb{F}_q$ is just a k-dimensional subspace of $\mathbb{F}_q^n$.

The dual $C^\perp$ of a linear code $C \subseteq \mathbb{F}_q^n$ is

$$C^\perp = \{\boldsymbol{v} \in \mathbb{F}_q^n \mid (\boldsymbol{v}, \mathbf{c}) = 0 \text{ for all } \mathbf{c} \in C\}.$$

The elementary codes are $\{\mathbf{0}\}$, $\mathbb{F}_q^n$ (the trivial codes), and the repetition code $\{\lambda(1, 1, \ldots, 1) \mid \lambda \in \mathbb{F}_q^n\}$ and its dual.

Convention: label the coordinates with $\mathbb{Z}_n$.

A permutation $\pi \in \mathcal{S}_n$ acts on $\mathbb{F}^n$ as

$$\pi : \mathbf{c} \mapsto \mathbf{c}^\pi = (c_{\pi^{-1}(0)}, \ldots, c_{\pi^{-1}(n-1)}) \tag{0.2}$$

for every $\mathbf{c} \in \mathbb{F}^n$.

Define $C^\pi = \{\mathbf{c}^\pi \mid \mathbf{c} \in C\}$.

Definition

The group of permutation automorphisms of a code $C \subseteq \mathbb{F}_q^n$ is

$$\mathrm{PAut}(C) = \{\pi \in \mathcal{S}_n \mid C^\pi = C\}.$$

Theorem

$$\mathrm{PAut}(C^\perp) = \mathrm{PAut}(C).$$

Proof: Obvious. □

A cyclic code of length n over $\mathbb{F}_q$ is a *linear* code invariant under the cyclic shift $\sigma : i \to i+1 \pmod{n}$, so with $\sigma \in \mathrm{PAut}(C)$.

So a cyclic code is a linear code closed under the cyclic shift map

$$\sigma : \mathbf{c} = (c_0, \ldots, c_{n-1}) \mapsto \mathbf{c}^\sigma = (c_{n-1}, c_0, \ldots, c_{n-2}).$$

Convention: $\mathbf{c} \in \mathbb{F}_q^n$

$$\mathbf{c} = (c_0, \ldots, c_{n-1}) \leftrightarrow c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

$c(x) \in \mathcal{R}_{N,q} := \mathbb{F}_q[x] \bmod x^n - 1$.

Note that

$$c^\pi(x) = \sum_{i=0}^{n-1} c_i x^{\pi(i)}; \tag{0.3}$$

in particular, $\mathbf{c}^\sigma$ corresponds to $c^\sigma(x) = xc(x) \pmod{x^n - 1}$.

So a cyclic code of length n over $\mathbb{F}_q$ is closed under multiplication by x in ring $\mathcal{R}_{n,q} = \mathbb{F}_q[x] \bmod x^n - 1$; since a cyclic code over $\mathbb{F}_q$ is also $\mathbb{F}_q$-linear it is in fact an *ideal* in the ring $\mathcal{R}_{n,q}$,which is a principal ideal ring. As a consequence, every cyclic code C of length n over $\mathbb{F}_q$ is of the form

$$C = g\mathcal{R}_{n,q} := \{a(x)g(x) \bmod x^n - 1 \mid a(x) \in \mathbb{F}_q[x], \deg(a) < n - \deg(g)\} \tag{0.4}$$

for some uniquely determined monic divisor $g(x)$ of $x^n - 1$ in $\mathbb{F}_q[x]$, the generator (polynomial) of C.

Every cyclic code of lenth n over $\mathbb{F}_q$ is also invariant under the Frobenius map $\phi : i \to qi \bmod n$. Indeed, if $\mathbf{c} \in C$, then

$$\mathbf{c}^{\phi} \leftrightarrow c^{\phi}(x) = c(x^q) \equiv c(x)^q \bmod x^n - 1,$$

so $\mathbf{c}$ and $\mathbf{c}^{\phi}$ have the same zeros.

Theorem

Let $\mathrm{PAut}_{\mathrm{st}}(C) := \langle \sigma, \phi \rangle$. *Then* $\mathrm{PAut}_{\mathrm{st}}(C)$ *is a subgroup of* $\mathrm{PAut}(C)$, *of order* nm.

The permutations from $\mathrm{PAut}_{\mathrm{st}}(C)$ are called the standard permutation automorphisms of C.

An irreducible (or *minimal*) cyclic code of length n over $\mathbb{F}_q$ is a code with generator polynomial $(x^n - 1)/g(x)$ where $g(x)$ is irreducible over $\mathbb{F}_q$ and has order n.

(A maximal cyclic code of length n over $\mathbb{F}_q$ is a code with generator polynomial $g(x)$ where $g(x)$ is irreducible over $\mathbb{F}_q$ and has order n; dual codes!)

Usually, if C is an irreducible cyclic code, then $\mathrm{PAut}(C) = \mathrm{PAut}_{\mathrm{st}}(C)$.

Definition

If C is an irreducible cyclic code and C has a non-standard permutation automorphism, then we say that C is a non-standard irreducible cyclic code or NSIC-code.

Fix ξ of order n in $\mathbb{F}_{q^m}$, and let $f(x) \in \mathbb{F}_q[x]$ be its minimal polynomial over $\mathbb{F}_q$. Then $\mathcal{U}_{n,q} = \langle \xi \rangle$.

Definition

Define $\Psi : \mathcal{L}(n,q) \to \mathcal{S}_n$ as follows. If $L \in \mathcal{L}(n,q)$, then there is $\pi \in \mathcal{S}_n$ such that $L(\xi^i) = \xi^{\pi(i)}$; set $\Psi(L) = \pi$.

Easy to see: Ψ is a one-to-one homomorphism on $\mathcal{L}(n,q)$.

Theorem

Let $C = C_{\xi}, q$ be the irreducible cyclic code of length n over $\mathbb{F}_q$ with generator $(x^n - 1)/f(x)$. Then C is a NSIC-code if and only if the pair $(n, \mathbb{F}_q)$ is non-standard. Moreover,
$\mathrm{PAut}(C) = \mathrm{PAut}(C^{\perp}) = \Psi(\mathcal{L}(n,q))$ *and*
$\mathrm{PAut}_{\mathrm{st}}(C) = \mathrm{PAut}(C^{\perp}) = \Psi(\mathcal{L}_{\mathrm{st}}(n,q))$.

Proof: Proof is not too complicated. One side: If $\mathbf{c} \in C^{\perp}$, then $c(\xi) = 0$, hence $0 = L(c(\xi)) = c^{\pi}(\xi)$, so $c^{\pi} \in C^{\perp}$. $\square$

Known examples

(Some come from non-standard linear recurring sequence subgroups, some from coding theory.)

Example

The non-standard pair $(n = q^m - 1, \mathbb{F}_q)$ corresponds to the (dual of the) primitive BCH code of designed distance 2. If $q = 2$, this is the simplex code. □

Example

The binary and ternary Golay codes are both (duals of) irreducible cyclic codes, with a huge permutation automorphism group (M_{23} and $\mathrm{PSL}(2, 11)$, respectively). So these are both NSIC-codes, and the pairs $(n = 23, \mathbb{F}_2)$ and $(n = 11, \mathbb{F}_3)$ are both non-standard. □

Example

Every repetition code C of length n and its dual has $\mathrm{PAut}(C) = \mathcal{S}_n$. If $m = n - 1$ and $n \geq 5$ then the dual is a NSIC-code. □

Example

NSIC-codes of length kn from irreducible polynomials of the form $g(x^k)$ with $g(x) \in \mathbb{F}_q[x]$ of order n. These codes are (duals of) cyclic product codes of the form $\mathbb{F}_q \times C$ with C the cyclic code with generator $g(x)$. □

Example

NSIC-codes obtained from smaller NSIC-codes by a construction technique called *lifing and extension*. □

Theorem

The above list of examples is complete in the case where $m = 2$.

Proof: Proof uses the known subgroup structure of $\mathrm{PG}(2, q)$. $\square$

Future work

- Develop a more general notion of non-standard cyclic codes (started).
- Classification for dimensions $m = 3, 4, \ldots$.

Conclusions

- We have connected two research topics,
  - ▶ non-standard linear recurring sequence subgroups

  and
  - ▶ (permutation) automorphisms of (irreducible) cyclic codes,

  through the notion of $\mathcal{L}(n, q)$ and non-standard pairs $(n, \mathbb{F}_q)$.
- We have introduced the notion of NSIC-codes as irreducible cyclic codes having "extra", non-standard, permutation automorphisms.
- We have classified the NSIC-codes of dimension $m = 2$.