Automorphisms of cyclic codes (preceded by a brief research overview)

Henk Hollmann

Singapore, Nanyang Technological University, 29 Sept. 2010

Contents

Introduction

Background:
graduation (association schemes) & Ph.D. (modulation codes)
from Eindhoven Technical University, the Netherlands,
supervisor Jack van Lint (and Paul Siegel)

1982-1985:
CNET (Centre National d'Études des Télécommunications),
Issy-les-Moulineaux (Paris), France

Main work:
FFT (Fast Fourier Transforms)
NTT (Number Theoretic Transforms)

Co-inventor (with Pierre Duhamel) of split-radix FFT.

1985-2009:

Philips Research Laboratories, Eindhoven, the Netherlands
(1999-2009: Principal Scientist)

Responsible for Discrete Mathematics within Philips Research

Consultancy and research in Discrete Mathematics, Coding Theory, Cryptography, Information Theory, and Digital Signal Processing.

2010-:

- Eindhoven University of Technology, the Netherlands
- Own math consultancy firm

1. Recurrence relations, recurring sequences, and q-polynomials

$q = p^r$, p prime

$\sigma_0, \sigma_1, \ldots, \sigma_{m-1} \in \mathbf{F}_q$, $\sigma_0 \neq 0$

recurrence relation (of order m)

$$u_k = \sigma_{m-1} u_{k-1} + \cdots + \sigma_1 u_{k-m+1} + \sigma_0 u_{k-m} \tag{1}$$

with characteristic polynomial

$$f(x) = x^m - \sigma_{m-1} x^{m-1} - \cdots - \sigma_1 x - \sigma_0 \tag{2}$$

$u = u(u_0, u_1, \ldots, u_{m-1})$ sequence generated by (1) from $u_0, \ldots, u_{m-1}$.

The smallest period $\mathrm{per}(u)$ is smallest $M \geq 1$ for which $u_{M+k} = u_k \ \forall k$.

The order $\mathrm{ord}(f)$ is smallest $N \geq 1$ for which $f(x) | x^N - 1$.

Fact 1: $\mathrm{per}(u) | \mathrm{ord}(f)$

Fact 2: f irreducible over $\mathbf{F}_q$ with zeroes $\xi, \xi^q \ldots, \xi^{q^{m-1}} \in \mathbf{F}_{q^m}$, then

- $\mathrm{per}(u) = \mathrm{ord}(f)$ iff $(u_0, \ldots, u_{m-1}) \neq 0$;
- $u_k = L_0 \xi^k + L_1 \xi^{qk} \cdots + L_{m-1} \xi^{q^{m-1}k} = L(\xi^k)$ for all k

$L(x) = L_0 x + L_1 x^q \cdots + L_{m-1} x^{q^{m-1}}, \qquad L_1, \ldots, L_{m-1} \in \mathbf{F}_{q^m}$ will be referred to as a q-polynomial over $\mathbf{F}_{q^m}$ of q-degree m. (linearized polynomial).

Fact: 1-1 with $\mathbf{F}_q$-linear maps on $\mathbf{F}_{q^m}$.

Brison, Nogueira (2003)

A multiplicative subgroup $\mathbf{K} \subseteq \mathbf{F}^*$, with $\mathbf{F}_q \subseteq \mathbf{F}$, is called f-subgroup if $\exists u_0, \ldots, u_{m-1}$ such that

$$\mathbf{K} = \{u_0, u_1, \ldots, u_{n-1}\}, \qquad |K| = n = \mathrm{ord}(u)$$

- wlog $u_0 = 1$
- $\mathbf{F}^*$ *cyclic*, so $\mathbf{K}$ uniquely determined by $|\mathbf{K}|$
- ξ zero of f, then $\langle \xi \rangle$ is f-subgroup (take $u_i = \xi^i$)
- f irreducible over $\mathbf{F}_q$ with zero ξ, then $\langle \xi \rangle$ is only f-subgroup (since $\mathrm{ord}(u) = \mathrm{ord}(f) = \mathrm{ord}(\xi)$).

f not mentioned: $\mathbf{K}$ is linear recurring sequence subgroup

Question: Is an f-subgroup always of the form $\langle \xi \rangle$, for a zero ξ of f?

From now on, f is irreducible over $\mathbf{F}_q$, of degree m, with zero $\xi \in \mathbf{F}_{q^m}$

$\langle \xi \rangle$ is called non-standard f-subgroup if

$$\langle \xi \rangle = \{u_0 = 1, u_1, \ldots, u_{n-1}\}, \qquad n = |\langle \xi \rangle| = \mathrm{ord}(\xi)$$

with $(u_0, \ldots, u_{m-1}) \neq (1, \xi^{q^j}, \xi^{2q^j}, \ldots, \xi^{(m-1)q^j})$ for all j
(Brison and Nogueira)

- ξ is called non-standard, of degree m over $\mathbf{F}_q$ and order n, if its minimal polynomial f over $\mathbf{F}_q$ has degree m, with $\langle\xi\rangle$ non-standard f-subgroup, of order (size) n
- A q-polynomial $L(x) = L_0 x + L_1 x^q \cdots + L_{m-1} x^{q^{m-1}}$ is called non-standard, of q-degree m over $\mathbf{F}_{q^m}$, if $L_0, \ldots, L_{m-1} \in \mathbf{F}_{q^m}$ and $L(x) \neq c x^{q^j}$ for all $c \in \mathbf{F}_{q^m}$ and all $j = 0, \ldots, m-1$.

Consequence: ξ is non-standard of degree m over $\mathbf{F}_q$ if and only if there exists a non-standard q-polynomial L of q-degree m over $\mathbf{F}_{q^m}$ such that

$$L(\langle\xi\rangle) = \langle\xi\rangle.$$

ξ is called non-standard of degree m over $\mathbf{F}_q$ if

- $\mathbf{F}_{q^m}$ is smallest extension of $\mathbf{F}_q$ containing ξ, and
- if $\exists$ $\mathbf{F}_q$-linear map L on $\mathbf{F}_{q^m}$, not of the form $L(x) = cx^{q^j}$, for which $L(\langle\xi\rangle) = \langle\xi\rangle$.

2. Two basic non-standard examples

$\xi \in \mathbf{F}_{q^m}$, degree m over $\mathbf{F}_q$, order $n = \mathrm{ord}(\xi)$

Obviously no non-standard examples for $m = 1$. ($u_k = \sigma_0 u_{k-1}$, $u_0 = 1 \Longrightarrow u_k = {\sigma_0}^k$)

No non-standard examples with $n \leq 4$: If $m > 1$, then $n \geq 3$; if $n = 3$, then $\langle \xi \rangle = \{1, \xi, \xi^q\}$; if $n = 4$, then $\xi^2 = -1$ and $\xi^q = -\xi$.

Example 1: $n = q^m - 1$, that is, ξ primitive in $\mathbf{F}_{q^m}$, i.e., $\langle \xi \rangle = \mathbf{F}^*_{q^m}$. Then ξ non-standard iff $m \geq 2$ and $q^m > 4$ (i.e., $n > 4$).

Proof:

$m \times m$ $\mathbf{F}_q$-matrix $\mathcal{L} \leftrightarrow$ q-polynomial L of q-degree m over $\mathbf{F}_{q^m}$.

Straightforward counting of non-singular matrices $\Longrightarrow$ not all from standard q-polynomials cx^{q^j} if $m \geq 2$ and $q^m > 4$.

□

Example 2: ξ has minimal polynomial $f(x) = x^m - \eta$ over $\mathbf{F}_q$. Then ξ non-standard over $\mathbf{F}_q$ iff $m > 1$ and $n > 4$.

Proof: $\langle\xi\rangle = \langle\eta\rangle.\{1, \xi, \ldots, \xi^{m-1}\}$.

Hence for $i = 0, \ldots, m-1$:
$L(\xi^i) = \eta_i \xi^{\tau(i)}$,
with $\eta_i \in \langle\eta\rangle$, and τ permutation on $\{0, \ldots, m-1\}$.

$L(1) = 1$ iff $\eta_0 = 1$ and $\tau(0) = 0$.

Extend by $\mathbf{F}_q$-linearity $\Longrightarrow L(\langle\xi\rangle) \subseteq \langle\xi\rangle$ and non-singular on $\mathbf{F}_{q^m}$.

$e = \mathrm{ord}(\eta)$, then $e > 1$ (since $x^m - 1$ not irreducible for $m > 1$).

$\#$ choices $e^{m-1}(m-1)! > m$ ($= \#$ "forbidden" choices
$L(x) = x^{q^j}$)
iff ($e = 2$ and $m \geq 3$) or ($e \geq 3$ and $m \geq 2$), that is $[m, e > 1]$, iff
$n = me > 4$.

$\square$

$\Longrightarrow$ Examples with $m = 2$, $n = 2e \geq 6$, if both q, $(q-1)/e$ odd.

3. Permutation automorphisms of (linear) cyclic codes

$\boxed{(n, q) = 1}$

Cyclic code of length n over $\mathbf{F}_q$ is $\mathbf{F}_q$-subspace $C \subseteq \mathbf{F}_q^n$ such that

$c = (c_0, c_1, \ldots, c_{n-1}) \in C \Longrightarrow c^\sigma := (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C.$

Ideal in $\mathcal{R} = \mathbf{F}_q[x] \bmod x^n - 1$, hence if $n | q^m - 1$ $(m > 0)$, then
$\exists Z \subseteq \mathbf{F}_{q^m}^*$, all n-th roots of 1, such that
$C = \{c(x) \in \mathcal{R} \mid c(\beta) = 0 \;\; \forall \beta \in Z\}$.

Definition: $\pi \in S_n$ (permutations on $\{0, 1, , \ldots, n-1\}$), then

$$c^\pi = (c_{\pi(0)}, c_{\pi(1)}, \ldots, c_{\pi(n-1)}).$$

Permutation automorphisms $\mathrm{PermAut}(C)$:

All $\pi \in S_n$ such that $c \in C \Longrightarrow c^\pi \in C$.

- $\sigma \in \mathrm{PermAut}(C)$
- $\psi : i \mapsto qi \bmod n$, then $\psi \in \mathrm{PermAut}(C)$
  Frobenius automorphism, $c^\psi(x) = c(x^q)$.

So $< \sigma, \psi > \subseteq \mathrm{PermAut}(C)$.

Question: When is there more?

Theorem

C cyclic code, length n, over $\mathbf{F}_q$, with defining zero ξ, of degree m over $\mathbf{F}_q$, and of order n. Then C has more permutation automorphisms if and only if ξ non-standard over $\mathbf{F}_q$.

Proof:

a) Suppose L q-polynomial of q-degree m and

$$L(\xi^i) = \xi^{\pi(i)}, \qquad \pi \in S_n.$$

If $c \in C$, then

$$\begin{aligned} 0 = L(0) &= L(\sum_{i=0}^{n-1} c_i \xi^i) \\ &= \sum_{i=0}^{n-1} c_i L(\xi^i) \\ &= \sum_{i=0}^{n-1} c_i \xi^{\pi(i)} = \sum_{j=0}^{n-1} c_{\pi^{-1}(j)} \xi^j, \end{aligned}$$

hence $c^{\pi^{-1}(i)} \in C$. So $\pi^{-1} \in \mathrm{PermAut}(C)$.

b) Let $\pi^{-1} \in \mathrm{PermAut}(C)$. Define a q-polynomial L on $\mathbf{F}_{q^m}$ by

$$L(\xi^j) = \xi^{\pi(j)}, \qquad j = 0, \ldots, m-1, \tag{3}$$

and extend by $\mathbf{F}_q$-linearity.

For $j \geq m$, let

$$\xi^j = a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1}.$$

Then

$$c = (a_0, a_1, \ldots, a_{m-1}, 0, \ldots, 0, -1, 0, \ldots, 0) \in C,$$

(-1 in position j), hence also $c^{\pi^{-1}} \in C$, so that

$$\begin{aligned} 0 &= \sum_{i=0}^{n-1} c_i^{\pi^{-1}} \xi^i = \sum_{i=0}^{n-1} c_{\pi^{-1}}(i)\xi^i = \sum_{k=0}^{n-1} c_k \xi^{\pi(k)} \\ &= a_0\xi^{\pi(0)} + a_1\xi^{\pi(1)} + \cdots a_{m-1}\xi^{\pi(m-1)} - \xi^{\pi(j)} \\ &= L(\xi^j) - \xi^{\pi(j)}. \end{aligned}$$

So (3) holds for <u>all</u> j, that is, $L(\xi^i) = \xi^{\pi(i)}, \qquad \pi \in S_n$.

□

Fact: $\boxed{\sigma \leftrightarrow L(x) = \xi x \text{ and } \psi^{-1} \leftrightarrow L(x) = x^q.}$

So $\mathrm{PermAut}(C)$ is bigger than $< \sigma, \psi >$ iff there are non-standard L fixing $\langle \xi \rangle$.

Conclusion: full classification is a difficult problem!

New examples:

Example 3: (Binary Golay code) Let $q = 2$, $n = 23$, and $m = 11$; let α primitive in $\mathbf{F}_{2^{11}}$ and $\xi = \alpha^{(2^{11}-1)/23}$.
ξ is defining zero for the length-23 binary Golay code, and is non-standard of order $n = 23$ and degree $m = 11$ over $\mathbf{F}_2$.

Example 4: (Ternary Golay) Let $q = 3$, $n = 11$, and $m = 5$; let α primitive in $\mathbf{F}_{3^5}$ and $\xi = \alpha^{(2^5-1)/11}$.
ξ is defining zero for the length-11 ternary Golay code, and is non-standard of order $n = 1$ and degree $m = 5$ over $\mathbf{F}_3$.

Further examples rare: only "non-standard" binary QR- codes of length < 4000 are the $(7, 4, 3)$ Hamming and the binary Golay.

4. Extening and lifting

Important definition: q-order $\mathrm{ord}_q(\xi)$: smallest $d \geq 1$ for which $\xi^d \in \mathbf{F}_q$. (Restricted period of f.)

Lemma

(i) $d = \mathrm{ord}_q(\xi) = n/(n, q-1)$
(ii) $n = de$, *with* $e = (n, q-1)$ *and* $(d, \frac{q-1}{e}) = 1$

Proof: $e = (n, q-1)$, then
$\xi^d \in \mathbf{F}_q$ iff $\xi^{d(q-1)} = 1$ iff $n | d(q-1)$ iff $\frac{n}{e} | d$.
□

Theorem

$d = \mathrm{ord}_q(\xi)$, *then* $m \leq d$, $d | \frac{q^m-1}{q-1}$, *and* $m = d$ *iff* $f(x) = x^d - \xi^d$.

Proof: $\xi \in \mathbf{F}_{q^m} \Longrightarrow \xi^{\frac{q^m-1}{q-1}} \in \mathbf{F}_q$;
$f(x)$ minimal polynomial of ξ over $\mathbf{F}_q \Longrightarrow f(x) | x^d - \xi^d$.
□

Theorem (Extension)

Let ϕ non-standard of degree m over $\mathbf{F}_q$, with order $\mathrm{ord}(\phi) = n$ and q-order $d = \mathrm{ord}_q(\phi)$. If ξ in $\mathbf{F}_q^*\langle\phi\rangle$ with $\langle\phi\rangle \subseteq \langle\xi\rangle$, then ξ also non-standard of degree m over $\mathbf{F}_q$, with same q-order and same non-standard q-polynomials.

Proof:

Let $\langle\phi\rangle \subseteq \langle\xi\rangle \subseteq \mathbf{F}_q^*\langle\phi\rangle$.

- Obviously, ξ and ϕ have the same degree over $\mathbf{F}_q$.
- $\mathrm{ord}_q(\xi) = \mathrm{ord}_q(\phi) = d$:
  Let $e = (n, q-1)$ and write $f = (q-1)/e$.
  Then $n = de$, $(d, f) = 1$, and
  $|\mathbf{F}_q^*\langle\phi\rangle| = |\mathbf{F}_q^*\{1, \phi, \ldots, \phi^{d-1}\}| = (q-1)d = nf$.
  So $N = \mathrm{ord}(\langle\xi\rangle) = nk$ with $k|f$.
  Then $(N, q-1) = (dek, ef) = ek(d, f/k) = ek$, hence
  $\mathrm{ord}_q(\xi) = N/ek = d$.

- L q-polynomial of q-degree m over $\mathbf{F}_{q^m}$, L bijection on $\langle\phi\rangle$, then L also bijection on $\mathbf{F}_q^*\langle\phi\rangle$:

  $\alpha, \beta \in \mathbf{F}_q$ and $L(\alpha\phi^i) = L(\beta\phi^j) \Longrightarrow$
  $\alpha\beta^{-1} = L(\phi^j)/L(\phi^i) \in \langle\phi\rangle$ and $L(\alpha\beta^{-1}\phi^i) = L(\phi^j) \Longrightarrow$
  $\alpha\beta^{-1}\phi^i = \phi^j$, or $\alpha\phi^i = \beta\phi^j$.

Finally, $\langle\phi\rangle \subseteq \langle\xi\rangle \Longleftrightarrow \langle\xi\rangle = H\langle\phi\rangle$ with H subgroup of $\mathbf{F}_q^* \Longrightarrow$ $L(\langle\xi\rangle) \subseteq \langle\xi\rangle$, so L bijection on $\langle\xi\rangle$.

In fact, $H = \mathbf{F}_q \cap \langle\xi\rangle = \langle\xi^d\rangle$, of size ke since $\phi^d \in H$.

$\square$

Remark1: $\langle \phi \rangle \subseteq \langle \xi \rangle$ iff $n = \mathrm{ord}(\phi) | \mathrm{ord}(\xi)$.

Remark2: ϕ non-standard of degree m over $\mathbf{F}_q$,
$\xi \in \langle \phi \rangle$, and $\langle \xi \rangle = \langle \phi \rangle$, then ξ also non-standard.

Remark 3: Apllies to ternary Golay $\Longrightarrow$
non-standard element in $\mathbf{F}_{3^5}$, of of order 22 and degree 5 over $\mathbf{F}_3$.

Let $\boxed{q_0 = p^s \text{ and } q = q_0^t}$.

Theorem (Lifting)

ξ non-standard of degree m over $\mathbf{F}_{q_0}$ and $(m, t) = 1$, then ξ also non-standard of degree m over $\mathbf{F}_q$, with $\mathrm{ord}_q(\xi) = \mathrm{ord}_{q_0}(\xi)$.

Proof:

- q-order: $n | q_0^m - 1$, hence

$$(n, q - 1) = (n, q_0^m - 1, q_0^t - 1) = (n, q_0 - 1).$$

- degree and non-standard:

$$\xi, \xi^{q_0}, \ldots, \xi^{q_0^{m-1}} \text{ distinct}, \qquad \xi^{q_0^m} = \xi.$$

  Now $\boxed{\xi^{q_0^k} = \xi^{q_0^{k \bmod m}}}$ and
  $\{0, t, 2t, \ldots, (m-1)t\} \equiv \{0, 1, \ldots, m-1\} \bmod m$,
  so $\{\xi, \xi^q, \ldots, \xi^{q^{m-1}}\} = \{\xi, \xi^{q_0}, \ldots, \xi^{q_0^{m-1}}\}$, and
  same minimal polynomial & same recursion.

$\square$

Conclusion: If

- ϕ non-standard of degree m over $\mathbf{F}_{q_0}$, with order $n_0 = de_0$ and q_0-order d, so $e_0 | q_0 - 1$ and $(d, \frac{q_0-1}{e_0}) = 1$;
- $q = q_0^t$ with $(t, m) = 1$, then (first lift, then extend)

$\exists$ ξ non-standard of degree m over $\mathbf{F}_q$, with order $n = de$ and q-order d whenever

$$e_0 | e | q - 1.$$

Example 1 (primitive element) $\longrightarrow$ Example 1*, with

$$\boxed{d = \frac{q_0^m - 1}{q_0 - 1}, \qquad n = \frac{q_0^m - 1}{q_0 - 1} e, \qquad \text{with} \qquad q_0 - 1 |\, e \,| q - 1},$$

for $m \geq 2$ and $q_0^m > 4$.

"Classical" examples for $m = 2$, $f(x) = x^2 - \sigma_1 x - \sigma_0$ over $\mathbf{F}_q$:

- $\sigma_1 = 0$; q-order $d = m = 2$, well understood
- $\sigma_1 \neq 0$;
  - $d = 3$ not possible
  - $d = q_0 + 1$, $q = q_0^t$ with t odd, $q_0 > 2$, $n = (q_0 + 1)e$ with $q_0 - 1 \mid e \mid q - 1$ by extension and lifting a primitive element.

Aim: Show that we can reverse this construction.

So ξ non-standard of degree m and q-order d over $\mathbf{F}_q$, then

- First task: $d = q_0 + 1$, where $q = q_0^t$ with t odd;
- Then: ξ obtained from ϕ, with $\langle \phi \rangle = \langle \xi \rangle \cap \mathbf{F}_{q_0^2}$, by extension and lifting.
- Finally: show that ϕ primitive.

5. A subgroup in $\mathrm{PGL}(m, q)$

- $\xi \in \mathbf{F}_{q^m}$ non-standard of degree m over $\mathbf{F}_q$; order n, q-order d; put $\boxed{\eta = \xi^d}$.
- characteristic polynomial of ξ over $\mathbf{F}_q$ is

$$f(x) = x^m - \sigma_{m-1}x^{m-1} - \cdots - \sigma_1 x - \sigma_0.$$

$T : \xi^i \mapsto \xi^{i+1}$;
$L : \xi^i \mapsto \xi^{\pi(i)}$, $(\pi \in S_n)$.
Both $\mathbf{F}_q$-linear maps on $\mathbf{F}_{q^m}$ fixing set $\langle \xi \rangle$.

Note that $T^d = \xi^d I = \eta I$,

Consider T and L as maps on $\mathrm{PG}(m-1,q) \to \tilde{T}$ and $\tilde{L}$

So identify ξ and $\lambda\xi$ $\forall \lambda in \mathbf{F}_q^*$.

Consequence: $\tilde{T}$ has order d.

$\tilde{G} = \langle \tilde{T}, \tilde{L} \rangle$ subgroup of $\mathrm{PGL}(m,q)$ fixing set $C = \{1, \xi, \ldots, \xi^{d-1}\}$ of size d in $\mathrm{PG}(m-1,q)$.

6. The case $m = 2$: subgroups of $\mathrm{PGL}(2, q)$

From now on, $\boxed{m = 2}$, $\quad f(x) = x^2 - \sigma_1 x - \sigma_0$.

$$L(1) = 1, \qquad L(\xi) = \omega + \nu\xi.$$

$$L = \begin{pmatrix} 1 & \omega \\ 0 & \nu \end{pmatrix}, \qquad T = \begin{pmatrix} 0 & \sigma_0 \\ 1 & \sigma_1 \end{pmatrix}.$$

<u>normalisation</u>: $\lambda = \sigma_0/\sigma_1^2, \quad \tilde{\xi} = \xi/\sigma_1$ zero of $x^2 - x - \lambda$;
$\tilde{\omega} = \omega/\sigma_1$, $L(\tilde{\xi}) = \tilde{\omega} + \nu\tilde{\xi}$,

$$L \to \Gamma = \begin{pmatrix} 1 & \tilde{\omega} \\ 0 & \nu \end{pmatrix} \qquad T \to \Lambda = \begin{pmatrix} 0 & \lambda \\ 1 & 1 \end{pmatrix}.$$

w.r.t. basis $\langle 1, \tilde{\xi} \rangle$.

$\mathcal{O} = \{1, \Lambda(1) = \tilde{\xi}, \ldots, \Lambda^{d-1}(1)\} = \tilde{\xi}^{d-1}\} \subseteq \mathrm{PG}(1, q)$ is an orbit of subgroup $G = \langle \Lambda, \Gamma \rangle$ of $\mathrm{PGL}(2, q)$, of size d.

Theorem (Dickson, around 1900)

Let $q = p^r$ with p prime.
(i) If $g \neq \mathrm{id}$ in $\mathrm{PGL}(2, q)$ has order k, with f fixed points, then all orbits of size > 1 have size k, and one of:

$$f = 0, k | q + 1; \qquad f = 1, k = p; \qquad f = 2, k | q - 1.$$

Theorem (continued)

(ii) The <u>subgroups</u> of $\mathrm{PGL}(2,q)$ *are as follows:*

1. *<u>Cyclic</u> subgroups* C_k*, of order* $k = 2$ *(if* p *is odd), or of order* $k > 2$ *with* $k | q \pm 1$*.*
2. *<u>Dihedral</u> subgroups* D_{2k} *of order* $2k$*, with* $k = 2$ *(if* p *is odd), or with* $k > 2$ *and* $k | q \pm 1$*.*
3. *<u>Elementary abelian</u> subgroups* E_{p^k}*, of order* p^k $(0 \leq k \leq r)$*.*
4. *A <u>semidirect product</u>* $E_{p^k} \rtimes C_\ell$ *of an elementary subgroup* E_{p^k}*,* $1 \leq k \leq r$*, and a cyclic group* C_ℓ*, where* $\ell | q - 1$ *and* $\ell | p^k - 1$*.*
5. *Subgroups isomorphic to* $A_4 \cong \mathrm{PSL}(2,3)$*,* $S_4 \cong \mathrm{PGL}(2,3)$*, or* $A_5 \cong \mathrm{PSL}(2,4)$*.*
6. *One conjugacy class of subgroups isomorphic to* $\mathrm{PSL}(2,p^k)$*, where* $k | r$*.*
7. *One conjugacy class of subgroups isomorphic to* $\mathrm{PGL}(2,p^k)$*, where* $k | r$*.*

Analysis of Λ and Γ:

$\Lambda : \tilde{\xi}^i \mapsto \tilde{\xi}^{i+1}$ has order d and no fixed points, so $d | q+1$.

$$L(x) = x \qquad \Leftrightarrow \qquad \Gamma = I, \qquad \nu = 1, \qquad \tilde{\omega} = 0;$$

$$L(x) = x^q \qquad \Leftrightarrow \qquad \nu = -1, \qquad \tilde{\omega} = 1.$$

Theorem

The group $G = \langle \Lambda, \Gamma \rangle$ *is one of the following.*

- *A cyclic group, when* $L(x) = x$*;*
- *a dihedral group, when* $L(x) = x^q$*;*
- *a conjugate of* $\mathrm{PSL}(2, q_0)$ *or* $\mathrm{PGL}(2, q_0)$*, in the nonstandard case, with* $d = q_0 + 1 > 3$ *and* $q = q_0^t$*, with* t *odd.*

Proof:

1. G cyclic $\implies \Gamma\Lambda = \Lambda\Gamma \implies \Lambda = I$ (case $L(x) = x$);
2. G dihedral $\implies \Lambda^2 = (\Lambda\Gamma)^2 \implies \nu = -1, \tilde{\omega} = 1, L(x) = x^q$;
3. $G \neq E_{p^k}$ with $k \geq 2$: note $d|q+1$, so $(p,d) = 1$;
4. $G \neq E_{p^k} \rtimes C_\ell$, $\ell|q-1$, $\ell|p^k-1$;
   note $(d,p) = 1$, so $d|\ell$; then $d|q+1 \implies d|2$ (no, $d \geq 3$).
5. If $G \simeq A_4, S_4, A_5$, then $d \in \{3,4,5\}$.
   Separate argument:
   $d = 3$ impossible;
   $d = 4 \implies p = 3, \qquad d = 5 \implies p = 2$

6,7 $G \simeq \mathrm{PSL}(2,q_0), \mathrm{PGL}(2,q_0)$, with $q_0 = p^s$, $q = p^r$, $s|r$.
Orbitsizes $q_0 + 1$, $q_0^2 - q_0$, $q_0(q_0^2 - 1)$ and $(d,p) = 1$, so
$d = q_0 + 1 | q + 1$, hence $t = r/s$ odd.

$\square$

Theorem

$\lambda, \nu, \tilde{\omega} \in \mathbf{F}_{q_0}$, hence $G = \mathrm{PSL}(2, q_0)$ or $G = \mathrm{PGL}(2, q_0)$.

Proof:

Step 1: $M \in \mathrm{PGL}(2, q)$, $q = q_0^t$,
then $M \in \mathrm{PGL}(2, q_0)$ iff $M^{(q_0)} = \phi M \; \exists_{\phi \in \mathbf{F}_q^*}$, where

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{(q_0)} = \begin{pmatrix} a^{(q_0)} & b^{(q_0)} \\ c^{(q_0)} & d^{(q_0)} \end{pmatrix}.$$

[Idea: iff $x \mapsto \frac{ax+b}{cx+d}$ fixes $\mathbf{F}_{q_0}^+ := \mathbf{F}_{q_0} \cup \{\infty\}$ setwise,
so iff $\left(\frac{ax+b}{cx+d}\right)^{(q_0)} = \frac{ax+b}{cx+d} \; \forall x$
So second-degree polynomial in x is zero, so all coefficients are zero.]

Consequence: If $AMA^{-1} \in \mathrm{PGL}(2, q_0)$,
then $(AMA^{-1})^{(q_0)} = \phi AMA^{-1}$, so

$$\boxed{\det(M)^{q_0-1} = \phi^2, \qquad \mathrm{Tr}(M) = 0 \text{ or } \phi = \mathrm{Tr}(M)^{q_0-1}}.$$

Now $\det(\Lambda) = -\lambda, \qquad \mathrm{Tr}(\Lambda) = 1$, so
$\phi = 1, \qquad (-\lambda)^{q_0-1} = 1$, hence $\lambda \in \mathbf{F}_{q_0}^*$.

Step 2: $d = q_0 + 1$, so $\langle\Lambda\rangle(1) = \{1, \tilde{\xi}, \ldots, \tilde{\xi}^{q_0}\} = \mathrm{PG}(1, q_0)$,
hence Γ fixes $\mathrm{PG}(1, q_0)$, so $\nu, \tilde{\omega} \in \mathbf{F}_{q_0}$.

□

7. Reversing the construction

Theorem

If $d = q_0 + 1 \geq 4$, then $\xi \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ obtained from some $\phi \in \mathbf{F}_{q_0^2} \setminus \mathbf{F}_{q_0}$, with q_0-order $q_0 + 1$ again, by lifting and extension.

Proof:

We want $\langle\phi\rangle \subseteq \langle\xi\rangle \subseteq \mathbf{F}_q^*\langle\phi\rangle$ and $\langle\phi\rangle \subseteq \mathbf{F}_{q_0^2}^*$.

So consider

$$\langle\phi\rangle := \mathbf{F}_{q_0^2}^* \cap \langle\xi\rangle \qquad \text{(cyclic)}.$$

$L(1) = 1, \qquad L(\tilde{\xi}) = \nu\tilde{\xi} + \tilde{\omega}, \qquad \nu, \tilde{\omega} \in \mathbf{F}_{q_0};$

$\tilde{\xi} \in \mathbf{F}_{q_0^2} \setminus \mathbf{F}_{q_0}$ since zero of $x^2 - x - \lambda$ (irreducible), $\lambda \in \mathbf{F}_{q_0}^*$;

hence $L(\mathbf{F}_{q_0^2}) \subseteq \mathbf{F}_{q_0^2}$, so that

$\boxed{L \text{ bijection on } \langle\phi\rangle}$.

$n = \mathrm{ord}(\xi) = (q_0 + 1)e, \qquad e = (n, q-1), \qquad q = q_0^t \ (t \text{ odd}).$

By "definition", $\phi = \xi^{\delta_0}$, where

$$\delta_0 = n/(n, q_0^2 - 1)$$

is q_0^2-order of ξ.

Put $e_0 = (e, q_0 - 1)$; now $\boxed{\delta_0 = e/e_0}$, so
$n_0 = \mathrm{ord}(\phi) = (q_0 + 1)e_0$.

$d = q_0 + 1$: $\quad (d, \frac{q-1}{e}) = 1 \Leftrightarrow (q-1)/e$ odd $\implies (q_0 - 1)/e_0$ odd.

Hence q_0-order

$$\begin{aligned} d_0 &= n_0/(n_0, q_0 - 1) \\ &= (q_0 + 1)/(q_0 + 1, \frac{q_0 - 1}{e_0}), \end{aligned}$$

so $\boxed{d_0 = \mathrm{ord}_{q_0}(\phi) = q_0 + 1}$.

Last step: Done if

$$\boxed{\xi \in \mathbf{F}_q^* \langle \phi \rangle}.$$

Now $\eta = \xi^{q_0+1} \in \mathbf{F}_q, \qquad \phi = \xi^{e/e_0} \qquad$, so

$$\mathbb{F}_q^* \langle \phi \rangle \geq \langle \eta \rangle \langle \phi \rangle$$

contains all ξ^k with

$$k = i(q_0 + 1) + je/e_0 \bmod n = (q_0 + 1)e.$$

So ok if $\boxed{(q_0 + 1, e/e_0) = 1.}$

Follows from e/e_0 odd. (Details...)

8. Conclusions

ξ non-standard of degree 2 over $\mathbf{F}_q$, with $n = \mathrm{ord}(\xi)$ and q-order $d = \mathrm{ord}_q(\xi)$: either $\boxed{d = 2}$ (well-understood) or $d \geq 4$ of form $\boxed{d = q_0 + 1}$, where $q = q_0^t$, t odd, and obtainable from non-standard ϕ of degree 2 over $\mathbf{F}_{q_0}$ with q_0-order $q_0 + 1$ again, by first lifting ϕ to $\mathbf{F}_q$, nad then extension to ξ.

Now use theorem (Brison, Nogueira):

If ϕ non-standard of degree 2 over $\mathbf{F}_{q_0}$ with q_0-order $q_0 + 1$, then ϕ primitive.

9. Further problems

- $m \geq 3$? Subgroups of $\mathrm{PGL}(3, q)$?
- Other cyclic codes?