On Reflexible Polynomials

Aleksander Malnič
University of Ljubljana and University of Primorska

Joint work with
Boštjan Kuzman and Primož Potočnik

Graphs, groups, and more:
celebrating Brian Alspach's 80th and Dragan Maruščč's 65th birthdays
Koper, Slovenia

May 28 – June 1, 2018

Reflexible polynomials

Reflexible polynomials

$f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{F}[x]$ is **reflexible** if

$$\text{type (1)} \quad \exists\, \lambda \in \mathbb{F}^* \ \ \forall\, i : \quad \lambda a_{k-i} = a_i \tag{1}$$

$$\text{type (2)} \quad \exists\, \lambda \in \mathbb{F}^* \ \ \forall\, i : \quad \lambda a_{k-i} = (-1)^i a_i \tag{2}$$

Reflexible polynomials

$f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{F}[x]$ is **reflexible** if

$$\begin{array}{lllll} \text{type (1)} & \exists\,\lambda \in \mathbb{F}^* \;\; \forall\, i: & \lambda a_{k-i} & = & a_i \\ \text{type (2)} & \exists\,\lambda \in \mathbb{F}^* \;\; \forall\, i: & \lambda a_{k-i} & = & (-1)^i a_i \end{array} \qquad \begin{array}{r}(1)\\(2)\end{array}$$

type (1) $\Rightarrow \lambda = \pm 1$

Reflexible polynomials

$f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{F}[x]$ is **reflexible** if

$$\text{type (1)} \quad \exists\, \lambda \in \mathbb{F}^* \quad \forall\, i : \quad \lambda a_{k-i} = a_i \tag{1}$$

$$\text{type (2)} \quad \exists\, \lambda \in \mathbb{F}^* \quad \forall\, i : \quad \lambda a_{k-i} = (-1)^i a_i \tag{2}$$

$$\textbf{type (1)} \Rightarrow \lambda = \pm 1$$

$$4 + 2x + 3x^2 + x^3 \in \mathbb{Z}_5[x] \qquad \lambda = -1, \quad \text{type (1)}$$

Reflexible polynomials

$f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{F}[x]$ is **reflexible** if

$$\begin{array}{lllcll} \text{type (1)} & \exists\,\lambda \in \mathbb{F}^* & \forall\, i: & \lambda a_{k-i} & = & a_i \end{array} \qquad (1)$$

$$\begin{array}{lllcll} \text{type (2)} & \exists\,\lambda \in \mathbb{F}^* & \forall\, i: & \lambda a_{k-i} & = & (-1)^i a_i \end{array} \qquad (2)$$

type (1) $\Rightarrow \lambda = \pm 1$

$4 + 2x + 3x^2 + x^3 \in \mathbb{Z}_5[x] \quad \lambda = -1, \quad$ type (1)

$\lambda = 1$ self-reciprocal, palindromic, Gorenstein polynomials

Reflexible polynomials

$f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{F}[x]$ is **reflexible** if

$$\begin{array}{lllll} \text{type (1)} & \exists\, \lambda \in \mathbb{F}^* \;\; \forall\, i: & \lambda a_{k-i} & = & a_i \end{array} \quad (1)$$

$$\begin{array}{lllll} \text{type (2)} & \exists\, \lambda \in \mathbb{F}^* \;\; \forall\, i: & \lambda a_{k-i} & = & (-1)^i a_i \end{array} \quad (2)$$

type (1) $\Rightarrow \lambda = \pm 1$

$4 + 2x + 3x^2 + x^3 \in \mathbb{Z}_5[x] \quad \lambda = -1, \quad$ type (1)

$\lambda = 1$ self-reciprocal, palindromic, Gorenstein polynomials

Reflexible polynomials

$f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{F}[x]$ is **reflexible** if

$$\begin{array}{llrcl} \text{type (1)} & \exists\,\lambda \in \mathbb{F}^* \ \ \forall\, i : & \lambda a_{k-i} & = & a_i \qquad (1) \\ \text{type (2)} & \exists\,\lambda \in \mathbb{F}^* \ \ \forall\, i : & \lambda a_{k-i} & = & (-1)^i a_i \qquad (2) \end{array}$$

type (1) $\Rightarrow \lambda = \pm 1$

$4 + 2x + 3x^2 + x^3 \in \mathbb{Z}_5[x] \quad \lambda = -1,$ type (1)

$\lambda = 1$ self-reciprocal, palindromic, Gorenstein polynomials

over $\mathbb{Z}_p$: criptography, sequences, subfields in alg. closures

Reflexible polynomials

$f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{F}[x]$ is **reflexible** if

$$\begin{array}{llll} \text{type (1)} & \exists\, \lambda \in \mathbb{F}^* \;\; \forall\, i: & \lambda a_{k-i} = a_i & (1) \\ \text{type (2)} & \exists\, \lambda \in \mathbb{F}^* \;\; \forall\, i: & \lambda a_{k-i} = (-1)^i a_i & (2) \end{array}$$

type (1) $\Rightarrow \lambda = \pm 1$

$4 + 2x + 3x^2 + x^3 \in \mathbb{Z}_5[x] \quad \lambda = -1, \quad$ type (1)

$\lambda = 1$ self-reciprocal, palindromic, Gorenstein polynomials

over $\mathbb{Z}_p$: criptography, sequences, subfields in alg. closures

over $\mathbb{Q}, \mathbb{C}$: cyclotomic polynomials are self-reciprocal

Reflexible polynomials

$f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{F}[x]$ is **reflexible** if

$$\begin{array}{lllll} \text{type (1)} & \exists\,\lambda \in \mathbb{F}^* & \forall\, i: & \lambda a_{k-i} & = & a_i \qquad (1) \\ \text{type (2)} & \exists\,\lambda \in \mathbb{F}^* & \forall\, i: & \lambda a_{k-i} & = & (-1)^i a_i \qquad (2) \end{array}$$

type (1) $\Rightarrow \lambda = \pm 1$

$4 + 2x + 3x^2 + x^3 \in \mathbb{Z}_5[x] \quad \lambda = -1,$ type (1)

$\lambda = 1$ self-reciprocal, palindromic, Gorenstein polynomials

over	$\mathbb{Z}_p$	:	criptography, sequences, subfields in alg. closures
over	$\mathbb{Q}, \mathbb{C}$	:	cyclotomic polynomials are self-reciprocal
irr. over	$\mathbb{Q}/\mathbb{Z}$	:	char. poly. of auto. of certain unimodular latices

Reflexible polynomials

$f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{F}[x]$ is **reflexible** if

$$\begin{array}{llll} \text{type (1)} & \exists\, \lambda \in \mathbb{F}^* \quad \forall\, i: & \lambda a_{k-i} = a_i & (1) \\ \text{type (2)} & \exists\, \lambda \in \mathbb{F}^* \quad \forall\, i: & \lambda a_{k-i} = (-1)^i a_i & (2) \end{array}$$

$$\textbf{type (1)} \Rightarrow \lambda = \pm 1$$

$$4 + 2x + 3x^2 + x^3 \in \mathbb{Z}_5[x] \qquad \lambda = -1, \quad \text{type (1)}$$

$\lambda = 1$ self-reciprocal, palindromic, Gorenstein polynomials

over	$\mathbb{Z}_p$	:	criptography, sequences, subfields in alg. closures
over	$\mathbb{Q}, \mathbb{C}$	:	cyclotomic polynomials are self-reciprocal
irr. over	$\mathbb{Q}/\mathbb{Z}$	:	char. poly. of auto. of certain unimodular latices

$$\textbf{type (2)} \Rightarrow \lambda^2 = (-1)^k$$

k even : $\lambda = \pm 1$, $\quad k$ odd : $\lambda^2 = -1$ and $\mathbb{F} = \mathbb{Z}_p$, $p \equiv 1 \mod 4$

Reflexible polynomials

$f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{F}[x]$ is **reflexible** if

$$\begin{array}{lllll} \text{type (1)} & \exists\,\lambda \in \mathbb{F}^* \ \ \forall\, i: & \lambda a_{k-i} & = & a_i \\ \text{type (2)} & \exists\,\lambda \in \mathbb{F}^* \ \ \forall\, i: & \lambda a_{k-i} & = & (-1)^i a_i \end{array} \qquad \begin{array}{l} (1) \\ (2) \end{array}$$

type (1) $\Rightarrow \lambda = \pm 1$

$4 + 2x + 3x^2 + x^3 \in \mathbb{Z}_5[x] \quad \lambda = -1, \quad$ type (1)

$\lambda = 1$ self-reciprocal, palindromic, Gorenstein polynomials

over	$\mathbb{Z}_p$	:	criptography, sequences, subfields in alg. closures
over	$\mathbb{Q}, \mathbb{C}$	:	cyclotomic polynomials are self-reciprocal
irr. over	$\mathbb{Q}/\mathbb{Z}$	:	char. poly. of auto. of certain unimodular latices

type (2) $\Rightarrow \lambda^2 = (-1)^k$

k even : $\lambda = \pm 1, \quad k$ odd : $\lambda^2 = -1$ and $\mathbb{F} = \mathbb{Z}_p,\ p \equiv 1 \mod 4$

$3 + 4x + 2x^2 + x^3 \in \mathbb{Z}_5[x], \quad \lambda = 3, \quad$ type (2)

Our motivation: symmetries of arc-transitive graphs

Our motivation: symmetries of arc-transitive graphs

4-val graphs with arc-transitive $G \leq \mathrm{Aut}(\Gamma)$, not semi-simple

4-val graphs with arc-transitive $G \leq \mathrm{Aut}(\Gamma)$, not semi-simple

first systematic approach by Gardiner and Praeger, 94

Praeger's normal reduction
Recursive factorization by N min $\triangleleft$ G

4-val graphs with arc-transitive $G \leq \mathrm{Aut}(\Gamma)$, not semi-simple

first systematic approach by Gardiner and Praeger, 94

Praeger's normal reduction
Recursive factorization by N min $\triangleleft$ G

Classify Γ when $\Gamma/\mathbb{Z}_p^r = K_1, K_2, C_n$

Our motivation: symmetries of arc-transitive graphs

4-val graphs with arc-transitive $G \leq \mathrm{Aut}(\Gamma)$, not semi-simple

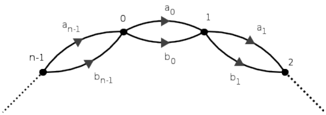
first systematic approach by Gardiner and Praeger, 94

Praeger's normal reduction
Recursive factorization by N min $\lhd$ G

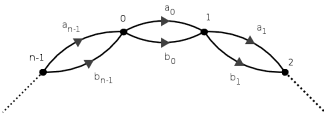
Classify Γ when $\Gamma/\mathbb{Z}_p^r = K_1, K_2, C_n$

Completely solved, except for $\Gamma/\mathbb{Z}_p^r = C_n$ and p odd

Minimal $\mathbb{Z}_p^r$-coverings $\Gamma \to C_n^{(2)}$

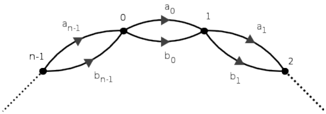


Minimal $\mathbb{Z}_p^r$-coverings $\Gamma \to C_n^{(2)}$



Classify minimal VT and ET elementary abelian covers of $C_n^{(2)}$

Minimal $\mathbb{Z}_p^r$-coverings $\Gamma \to C_n^{(2)}$



Classify minimal VT and ET elementary abelian covers of $C_n^{(2)}$

M, Marušič, Potočnik, Elementary abelian covers, JACO, 2004.

Results: $\Gamma/\mathbb{Z}_p^r = C_n^{(2)}$, where $\mathbb{Z}_p^r$ min $\lhd H$: VT and ET

Results: $\Gamma/\mathbb{Z}_p^r = C_n^{(2)}$, where $\mathbb{Z}_p^r$ min $\lhd H$: VT and ET

Thm 1. All minimal graphs Γ arise from cyclic or negacyclic codes.

Thm 1. All minimal graphs Γ arise from cyclic or negacyclic codes.

$$M_{g(x)} = \begin{bmatrix} \alpha_0 & \dots & \alpha_m & 0 & \dots & & & \cdots & 0 \\ 0 & \alpha_0 & \dots & \alpha_m & \ddots & & & & \vdots \\ \vdots & \ddots & \ddots & & \ddots & & & & \\ & & & & & & & & \\ & & & & \ddots & & \ddots & \ddots & \vdots \\ \vdots & & & & \ddots & \alpha_0 & \dots & \alpha_m & 0 \\ 0 & \cdots & & & \cdots & 0 & \alpha_0 & \dots & \alpha_m \end{bmatrix} \in \mathbb{Z}_p^{r \times n}$$

matrix associated with a proper divisor $g(x) \mid x^n \pm 1$, $\deg(g(x)) = n - r$

Results: $\Gamma/\mathbb{Z}_p^r = C_n^{(2)}$, where $\mathbb{Z}_p^r$ min $\lhd H$: VT and ET

Thm 1. All minimal graphs Γ arise from cyclic or negacyclic codes.

$$M_{g(x)} = \begin{bmatrix} \alpha_0 & \dots & \alpha_m & 0 & \dots & & & \cdots & 0 \\ 0 & \alpha_0 & \dots & \alpha_m & \ddots & & & & \vdots \\ \vdots & \ddots & \ddots & & \ddots & & & & \\ & & & & & & & & \\ & & & & \ddots & & \ddots & \ddots & \vdots \\ \vdots & & & & \ddots & \alpha_0 & \dots & \alpha_m & 0 \\ 0 & \cdots & & & \cdots & 0 & \alpha_0 & \dots & \alpha_m \end{bmatrix} \in \mathbb{Z}_p^{r\times n}$$

matrix associated with a proper divisor $g(x) \mid x^n \pm 1$, $\deg(g(x)) = n - r$

$\Gamma = \Gamma_{g(x)}$ has vertex set $\mathbb{Z}_p^r \times \mathbb{Z}_n$ and $(\underline{v}, j) \sim (\underline{v} \pm \underline{u}_{j+1}, j+1)$

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 2. $\Gamma_{g(x)}$ is at least VT and ET.

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 2. $\Gamma_{g(x)}$ is at least VT and ET.

Lifted groups preserve the degree of symmetry (Djoković, 74)
$\Rightarrow$ Consider M – the largest group that lifts. **When is M AT?**

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 2. $\Gamma_{g(x)}$ is at least VT and ET.

Lifted groups preserve the degree of symmetry (Djoković, 74)
$\Rightarrow$ Consider M – the largest group that lifts. **When is M AT?**

d maximal: $g(x) = g_d(x^d)$ $g_d(x)$: **reduced polynomial**

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 2. $\Gamma_{g(x)}$ is at least VT and ET.

Lifted groups preserve the degree of symmetry (Djoković, 74)
$\Rightarrow$ Consider M – the largest group that lifts. **When is M AT?**

d maximal: $g(x) = g_d(x^d)$ $g_d(x)$: **reduced polynomial**

Lemma. $d|n$ and $d|r = \dim \mathbb{Z}_p^r$, and M acts on $V(C_n^{(2)})$ with kernel $\mathbb{Z}_2^d$.

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 2. $\Gamma_{g(x)}$ is at least VT and ET.

Lifted groups preserve the degree of symmetry (Djoković, 74)
$\Rightarrow$ Consider M – the largest group that lifts. **When is M AT?**

d maximal: $g(x) = g_d(x^d)$ $g_d(x)$: **reduced polynomial**

Lemma. $d|n$ and $d|r = \dim \mathbb{Z}_p^r$, and M acts on $V(C_n^{(2)})$ with kernel $\mathbb{Z}_2^d$.

Thm 3. M, the largest group that lifts is AT $\Leftrightarrow$ $g_d(x)$ is reflexible.

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 2. $\Gamma_{g(x)}$ is at least VT and ET.

Lifted groups preserve the degree of symmetry (Djoković, 74)
$\Rightarrow$ Consider M – the largest group that lifts. **When is M AT?**

d maximal: $g(x) = g_d(x^d)$ $g_d(x)$: **reduced polynomial**

Lemma. $d|n$ and $d|r = \dim \mathbb{Z}_p^r$, and M acts on $V(C_n^{(2)})$ with kernel $\mathbb{Z}_2^d$.

Thm 3. M, the largest group that lifts is AT $\Leftrightarrow$ $g_d(x)$ is reflexible.

Example.
$g(x) = (3 + 4x^2 + 2x^4 + x^6) \mid (x^8 - 1) \in \mathbb{Z}_5[x]$, not reflexible
$g_2(x) = (3 + 4x + 2x^2 + x^3) \mid (x^4 - 1) \in \mathbb{Z}_5[x]$, $\lambda = 3$, type 2

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 2. $\Gamma_{g(x)}$ is at least VT and ET.

Lifted groups preserve the degree of symmetry (Djoković, 74)
$\Rightarrow$ Consider M – the largest group that lifts. **When is M AT?**

d maximal: $g(x) = g_d(x^d)$ $g_d(x)$: **reduced polynomial**

Lemma. $d|n$ and $d|r = \dim \mathbb{Z}_p^r$, and M acts on $V(C_n^{(2)})$ with kernel $\mathbb{Z}_2^d$.

Thm 3. M, the largest group that lifts is AT $\Leftrightarrow$ $g_d(x)$ is reflexible.

Example.
$g(x) = (3 + 4x^2 + 2x^4 + x^6) \mid (x^8 - 1) \in \mathbb{Z}_5[x]$, not reflexible
$g_2(x) = (3 + 4x + 2x^2 + x^3) \mid (x^4 - 1) \in \mathbb{Z}_5[x]$, $\lambda = 3$, type 2

$\Gamma_{g(x)}$ is AT

$\Gamma_{g(x)} = C4[200, 22]$ in Potočnik-Wilson census

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 4. $\Gamma_{g(x)} \to C_n^{(2)}$ is minimal $\Leftrightarrow$

Thm 4. $\Gamma_{g(x)} \to C_n^{(2)}$ is minimal $\Leftrightarrow$

- $g_d(x)$ not reflexible:
  $g_d(x)$ is a maximal proper divisor of $x^{n/d} \pm 1$

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 4. $\Gamma_{g(x)} \to C_n^{(2)}$ is minimal $\Leftrightarrow$

- $g_d(x)$ not reflexible:
  $g_d(x)$ is a maximal proper divisor of $x^{n/d} \pm 1$
- $g_d(x)$ is reflexible:
  $g_d(x)$ is a maximal weakly reflexible proper divisor of $x^{n/d} \pm 1$

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 4. $\Gamma_{g(x)} \to C_n^{(2)}$ is minimal $\Leftrightarrow$

- $g_d(x)$ not reflexible:
  $g_d(x)$ is a maximal proper divisor of $x^{n/d} \pm 1$
- $g_d(x)$ is reflexible:
  $g_d(x)$ is a maximal weakly reflexible proper divisor of $x^{n/d} \pm 1$

Example.
$n = 3,\ p = 7, \quad x^3 - 1 = (x-1)(x-2)(x-4)$

Thm 4. $\Gamma_{g(x)} \to C_n^{(2)}$ is minimal $\Leftrightarrow$

- $g_d(x)$ not reflexible:
  $g_d(x)$ is a maximal proper divisor of $x^{n/d} \pm 1$
- $g_d(x)$ is reflexible:
  $g_d(x)$ is a maximal weakly reflexible proper divisor of $x^{n/d} \pm 1$

Example.
$n = 3,\ p = 7, \quad x^3 - 1 = (x-1)(x-2)(x-4)$

- $g(x) = g_1(x) = x^2 + 4x + 2 = (x-1)(x-2)$

Thm 4. $\Gamma_{g(x)} \to C_n^{(2)}$ is minimal $\Leftrightarrow$

- $g_d(x)$ not reflexible:
  $g_d(x)$ is a maximal proper divisor of $x^{n/d} \pm 1$
- $g_d(x)$ is reflexible:
  $g_d(x)$ is a maximal weakly reflexible proper divisor of $x^{n/d} \pm 1$

Example.
$n = 3,\ p = 7, \quad x^3 - 1 = (x-1)(x-2)(x-4)$

- $g(x) = g_1(x) = x^2 + 4x + 2 = (x-1)(x-2)$
  $g_1(x)$ not reflexible, cover is minimal, M is not AT.

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 4. $\Gamma_{g(x)} \to C_n^{(2)}$ is minimal $\Leftrightarrow$

- $g_d(x)$ not reflexible:
  $g_d(x)$ is a maximal proper divisor of $x^{n/d} \pm 1$
- $g_d(x)$ is reflexible:
  $g_d(x)$ is a maximal weakly reflexible proper divisor of $x^{n/d} \pm 1$

Example.
$n = 3,\ p = 7, \quad x^3 - 1 = (x-1)(x-2)(x-4)$

- $g(x) = g_1(x) = x^2 + 4x + 2 = (x-1)(x-2)$
  $g_1(x)$ not reflexible, cover is minimal, M is not AT.
  However, $\Gamma = C4[21, 2]$ is AT

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 4. $\Gamma_{g(x)} \to C_n^{(2)}$ is minimal $\Leftrightarrow$

- $g_d(x)$ not reflexible:
  $g_d(x)$ is a maximal proper divisor of $x^{n/d} \pm 1$
- $g_d(x)$ is reflexible:
  $g_d(x)$ is a maximal weakly reflexible proper divisor of $x^{n/d} \pm 1$

Example.
$n = 3,\ p = 7, \quad x^3 - 1 = (x-1)(x-2)(x-4)$

- $g(x) = g_1(x) = x^2 + 4x + 2 = (x-1)(x-2)$
  $g_1(x)$ not reflexible, cover is minimal, M is not AT.
  However, $\Gamma = C4[21, 2]$ is AT
- $g(x) = g_1(x) = x^2 + 2x + 4 = (x-1)(x-4)$

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 4. $\Gamma_{g(x)} \to C_n^{(2)}$ is minimal $\Leftrightarrow$

- $g_d(x)$ not reflexible:
  $g_d(x)$ is a maximal proper divisor of $x^{n/d} \pm 1$
- $g_d(x)$ is reflexible:
  $g_d(x)$ is a maximal weakly reflexible proper divisor of $x^{n/d} \pm 1$

Example.
$n = 3$, $p = 7$, $\quad x^3 - 1 = (x-1)(x-2)(x-4)$

- $g(x) = g_1(x) = x^2 + 4x + 2 = (x-1)(x-2)$
  $g_1(x)$ not reflexible, cover is minimal, M is not AT.
  However, $\Gamma = C4[21, 2]$ is AT
- $g(x) = g_1(x) = x^2 + 2x + 4 = (x-1)(x-4)$
  Same as above, $\Gamma = C4[21, 2]$.

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 4. $\Gamma_{g(x)} \to C_n^{(2)}$ is minimal $\Leftrightarrow$

- $g_d(x)$ not reflexible:
  $g_d(x)$ is a maximal proper divisor of $x^{n/d} \pm 1$
- $g_d(x)$ is reflexible:
  $g_d(x)$ is a maximal weakly reflexible proper divisor of $x^{n/d} \pm 1$

Example.
$n = 3$, $p = 7$, $\quad x^3 - 1 = (x-1)(x-2)(x-4)$

- $g(x) = g_1(x) = x^2 + 4x + 2 = (x-1)(x-2)$
  $g_1(x)$ not reflexible, cover is minimal, M is not AT.
  However, $\Gamma = C4[21, 2]$ is AT
- $g(x) = g_1(x) = x^2 + 2x + 4 = (x-1)(x-4)$
  Same as above, $\Gamma = C4[21, 2]$.
- $g(x) = g_1(x) = x - 1$

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 4. $\Gamma_{g(x)} \to C_n^{(2)}$ is minimal $\Leftrightarrow$

- $g_d(x)$ not reflexible:
  $g_d(x)$ is a maximal proper divisor of $x^{n/d} \pm 1$
- $g_d(x)$ is reflexible:
  $g_d(x)$ is a maximal weakly reflexible proper divisor of $x^{n/d} \pm 1$

Example.
$n = 3$, $p = 7$, $\quad x^3 - 1 = (x-1)(x-2)(x-4)$

- $g(x) = g_1(x) = x^2 + 4x + 2 = (x-1)(x-2)$
  $g_1(x)$ not reflexible, cover is minimal, M is not AT.
  However, $\Gamma = C4[21,2]$ is AT
- $g(x) = g_1(x) = x^2 + 2x + 4 = (x-1)(x-4)$
  Same as above, $\Gamma = C4[21,2]$.
- $g(x) = g_1(x) = x - 1$
  $g_1(x)$ is reflexible and maximal weakly reflexible
  since $x^2 + 4x + 2$ and $x^2 + 2x + 4$ not reflexible.

Starting with a proper divisor $g(x) \mid x^n \pm 1$

Thm 4. $\Gamma_{g(x)} \to C_n^{(2)}$ is minimal $\Leftrightarrow$

- $g_d(x)$ not reflexible:
  $g_d(x)$ is a maximal proper divisor of $x^{n/d} \pm 1$
- $g_d(x)$ is reflexible:
  $g_d(x)$ is a maximal weakly reflexible proper divisor of $x^{n/d} \pm 1$

Example.
$n = 3$, $p = 7$, $\quad x^3 - 1 = (x-1)(x-2)(x-4)$

- $g(x) = g_1(x) = x^2 + 4x + 2 = (x-1)(x-2)$
  $g_1(x)$ not reflexible, cover is minimal, M is not AT.
  However, $\Gamma = C4[21, 2]$ is AT
- $g(x) = g_1(x) = x^2 + 2x + 4 = (x-1)(x-4)$
  Same as above, $\Gamma = C4[21, 2]$.
- $g(x) = g_1(x) = x - 1$
  $g_1(x)$ is reflexible and maximal weakly reflexible
  since $x^2 + 4x + 2$ and $x^2 + 2x + 4$ not reflexible.
  So the cover is minimal and AT, $\Gamma = C4[147, 6]$.

Reflexible polynomials – further properties

Reflexible polynomials – further properties

$$
\begin{aligned}
x^k f(x^{-1}) &= \lambda f(x) && \text{type (1)} \\
x^k f(-x^{-1}) &= \lambda f(x) && \text{type (2)}
\end{aligned}
$$

Reflexible polynomials – further properties

$$\begin{aligned} x^k f(x^{-1}) &= \lambda f(x) \qquad \text{type (1)} \\ x^k f(-x^{-1}) &= \lambda f(x) \qquad \text{type (2)} \end{aligned}$$

Prop 1.

- $f(x)$, $h(x)$ reflexible, same type $\Rightarrow$ $f(x)h(x)$ reflexible, same type.
- $f(x)h(x)$, $f(x)$ reflexible, same type $\Rightarrow$ $h(x)$ reflexible, same type.

Reflexible polynomials – further properties

$$\begin{aligned} x^k f(x^{-1}) &= \lambda f(x) \qquad \text{type (1)} \\ x^k f(-x^{-1}) &= \lambda f(x) \qquad \text{type (2)} \end{aligned}$$

Prop 1.

- $f(x)$, $h(x)$ reflexible, same type $\Rightarrow f(x)h(x)$ reflexible, same type.
- $f(x)h(x)$, $f(x)$ reflexible, same type $\Rightarrow h(x)$ reflexible, same type.

$\Rightarrow$ Two semigroups, generated by **minimal reflexible** polynomials

$$
\begin{aligned}
x^k f(x^{-1}) &= \lambda f(x) \qquad \text{type (1)} \\
x^k f(-x^{-1}) &= \lambda f(x) \qquad \text{type (2)}
\end{aligned}
$$

Prop 1.

- $f(x)$, $h(x)$ reflexible, same type $\Rightarrow$ $f(x)h(x)$ reflexible, same type.
- $f(x)h(x)$, $f(x)$ reflexible, same type $\Rightarrow$ $h(x)$ reflexible, same type.

$\Rightarrow$ Two semigroups, generated by **minimal reflexible** polynomials

Prop 2.

- $f(x)$ reflexible type (1) $\Leftrightarrow$ $f(a) = 0$ iff $f(a^{-1}) = 0$, same multiplicity
- $f(x)$ reflexible type (2) $\Leftrightarrow$ $f(a) = 0$ iff $f(-a^{-1}) = 0$, same multiplic.

Reflexible polynomials – further properties

$$\begin{aligned} x^k f(x^{-1}) &= \lambda f(x) \quad \text{type (1)} \\ x^k f(-x^{-1}) &= \lambda f(x) \quad \text{type (2)} \end{aligned}$$

Prop 1.

- $f(x)$, $h(x)$ reflexible, same type $\Rightarrow$ $f(x)h(x)$ reflexible, same type.
- $f(x)h(x)$, $f(x)$ reflexible, same type $\Rightarrow$ $h(x)$ reflexible, same type.

$\Rightarrow$ Two semigroups, generated by **minimal reflexible** polynomials

Prop 2.

- $f(x)$ reflexible type (1) $\Leftrightarrow$ $f(a) = 0$ iff $f(a^{-1}) = 0$, same multiplicity
- $f(x)$ reflexible type (2) $\Leftrightarrow$ $f(a) = 0$ iff $f(-a^{-1}) = 0$, same multiplic.

Prop 3.

- type 1: $(x-1)^{k_1}(x+1)^{k_{-1}} \prod (x^2 - (a + a^{-1})x + 1)^{k_a}$
- type 2: $(x^2-1)^{k_{1,-1}} \prod (x^2 - (a - a^{-1})x - 1)^{k_a} (x-\theta)^{k_\theta}$
  $\theta^2 = -1$, $p \equiv 1 \mod 4$.

Extremal case: $d = r$ (lifted group has max stab)

Extremal case: $d = r$ (lifted group has max stab)

$dt = d\deg(g_d(x)) = \deg(g(x)) = n - r$. Let $s = n/d$. Then $t = s - 1$.

Extremal case: $d = r$ (lifted group has max stab)

$dt = d \deg(g_d(x)) = \deg(g(x)) = n - r$. Let $s = n/d$. Then $t = s - 1$.

- $s = 1$: $t = 0$, $d = r = n$, so $g(x) = g_d(x) = 1$. $\mathrm{Aut}(C_n^{(2)})$ lifts.

Extremal case: $d = r$ (lifted group has max stab)

$dt = d \deg(g_d(x)) = \deg(g(x)) = n - r$. Let $s = n/d$. Then $t = s - 1$.

- $s = 1$: $t = 0$, $d = r = n$, so $g(x) = g_d(x) = 1$. $\mathrm{Aut}(C_n^{(2)})$ lifts.
- $s > 1$: $g_d(x)$ generates a 1-dim code in $\mathbb{Z}_p^s$ with $g_d(x)$ reflexible

Extremal case: $d = r$ (lifted group has max stab)

$dt = d \deg(g_d(x)) = \deg(g(x)) = n - r$. Let $s = n/d$. Then $t = s - 1$.

- $s = 1$: $t = 0$, $d = r = n$, so $g(x) = g_d(x) = 1$. $\mathrm{Aut}(C_n^{(2)})$ lifts.
- $s > 1$: $g_d(x)$ generates a 1-dim code in $\mathbb{Z}_p^s$ with $g_d(x)$ reflexible

$$x^s \pm 1 = (x - \theta) g_d(x)$$

Extremal case: $d = r$ (lifted group has max stab)

$dt = d\deg(g_d(x)) = \deg(g(x)) = n - r$. Let $s = n/d$. Then $t = s - 1$.

- $s = 1$: $t = 0$, $d = r = n$, so $g(x) = g_d(x) = 1$. $\mathrm{Aut}(C_n^{(2)})$ lifts.
- $s > 1$: $g_d(x)$ generates a 1-dim code in $\mathbb{Z}_p^s$ with $g_d(x)$ reflexible

$$x^s \pm 1 = (x - \theta)g_d(x)$$

- $g_d(x)$ **type 1**: $\theta = \pm 1$

$$g_d(x) = 1 + x + \ldots + x^t \qquad \Gamma = C^{\pm 1}(p, sr, r)$$

Extremal case: $d = r$ (lifted group has max stab)

$dt = d\deg(g_d(x)) = \deg(g(x)) = n - r$. Let $s = n/d$. Then $t = s - 1$.

- $s = 1$: $t = 0$, $d = r = n$, so $g(x) = g_d(x) = 1$. $\mathrm{Aut}(C_n^{(2)})$ lifts.
- $s > 1$: $g_d(x)$ generates a 1-dim code in $\mathbb{Z}_p^s$ with $g_d(x)$ reflexible

$$x^s \pm 1 = (x - \theta)g_d(x)$$

- $g_d(x)$ **type 1**: $\theta = \pm 1$

$$g_d(x) = 1 + x + \ldots + x^t \qquad \Gamma = C^{\pm 1}(p, sr, r)$$

- $g_d(x)$ **type 2**: $s = 2q, \quad \theta^2 = -1, \quad p \equiv 1 \mod 4$

$$g_d(x) = \theta^t + \theta^{t-1}x + \ldots x^t, \qquad \Gamma = C^{\pm\theta}(p, 2qr, r)$$

Extremal case: $\mathbb{Z}_p^2$

Extremal case: $\mathbb{Z}_p^2$

$$\Rightarrow r = 2 \text{ and } d \big| r \Rightarrow d = 1$$

Extremal case: $\mathbb{Z}_p^2$

$$\Rightarrow r = 2 \text{ and } d | r \Rightarrow d = 1$$

$$x^n \pm 1 = (x^2 - \gamma x + \delta) g(x), \quad g(x) = g_d(x), \text{ maximal refleksible}$$

Extremal case: $\mathbb{Z}_p^2$

$$\Rightarrow r = 2 \text{ and } d \mid r \Rightarrow d = 1$$

$$x^n \pm 1 = (x^2 - \gamma x + \delta) g(x), \quad g(x) = g_d(x), \text{ maximal refleksible}$$

- $g(x)$ **type 1**: $\Rightarrow x^2 - \gamma x + \delta$ type 1 $\Rightarrow (x - a)(x - a^{-1})$

$$\Rightarrow r = 2 \text{ and } d | r \Rightarrow d = 1$$

$x^n \pm 1 = (x^2 - \gamma x + \delta) g(x)$, $\quad g(x) = g_d(x)$, maximal refleksible

- $g(x)$ **type 1**: $\Rightarrow x^2 - \gamma x + \delta$ type 1 $\Rightarrow (x - a)(x - a^{-1})$

  $a \notin \mathbb{Z}_p$, irreducible

  $a \in \mathbb{Z}_p$, $a^2 \neq \pm 1$

Extremal case: $\mathbb{Z}_p^2$

$$\Rightarrow r = 2 \text{ and } d | r \Rightarrow d = 1$$

$x^n \pm 1 = (x^2 - \gamma x + \delta) g(x)$, $\quad g(x) = g_d(x)$, maximal refleksible

- $g(x)$ **type 1**: $\Rightarrow x^2 - \gamma x + \delta$ type 1 $\Rightarrow (x - a)(x - a^{-1})$

  $a \notin \mathbb{Z}_p$, irreducible

  $a \in \mathbb{Z}_p$, $a^2 \neq \pm 1$

- $g(x)$ **type 2**:

Extremal case: $\mathbb{Z}_p^2$

$$\Rightarrow r = 2 \text{ and } d|r \Rightarrow d = 1$$

$x^n \pm 1 = (x^2 - \gamma x + \delta)g(x), \quad g(x) = g_d(x)$, maximal refleksible

- $g(x)$ **type 1**: $\Rightarrow x^2 - \gamma x + \delta$ type 1 $\Rightarrow (x - a)(x - a^{-1})$

  $a \notin \mathbb{Z}_p$, irreducible

  $a \in \mathbb{Z}_p$, $a^2 \neq \pm 1$

- $g(x)$ **type 2**:

  n **even**: $\Rightarrow x^2 - \gamma x + \delta = (x - a)(x + a^{-1})$ type 2

  $a \notin \mathbb{Z}_p$, irreducible

  $a \in \mathbb{Z}_p$, $a^2 \neq \pm 1$

Extremal case: $\mathbb{Z}_p^2$

$$\Rightarrow r = 2 \text{ and } d | r \Rightarrow d = 1$$

$x^n \pm 1 = (x^2 - \gamma x + \delta)g(x), \quad g(x) = g_d(x)$, maximal refleksible

- $g(x)$ **type 1**: $\Rightarrow x^2 - \gamma x + \delta$ type 1 $\Rightarrow (x - a)(x - a^{-1})$

  $a \notin \mathbb{Z}_p$, irreducible

  $a \in \mathbb{Z}_p$, $a^2 \neq \pm 1$

- $g(x)$ **type 2**:

  n **even**: $\Rightarrow x^2 - \gamma x + \delta = (x - a)(x + a^{-1})$ type 2

  $a \notin \mathbb{Z}_p$, irreducible

  $a \in \mathbb{Z}_p$, $a^2 \neq \pm 1$

  n **odd**: No.

Thank you!