Rédei permutations with the same cycle structure

Juliane Capaverde[1] and Ariane Masuda[2]

[1]Universidade Federal do Rio Grande do Sul
[2]New York City College of Technology, CUNY

(joint work with Virgínia Rodrigues[1])

Finite Fields eSeminar
October 20, 2021

Rédei functions

- Let $\mathbb{P}^1(\mathbb{F}_q) := \mathbb{F}_q \cup \{\infty\}$.
- Write $(x + \sqrt{y})^m$ as $N(x, y) + D(x, y)\sqrt{y}$.
- For $m \in \mathbb{N}$ and $a \in \mathbb{F}_q$, the *Rédei function* is $R_{m,a} : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$ where

$$R_{m,a}(x) = \begin{cases} \dfrac{N(x,a)}{D(x,a)} & \text{if } D(x,a) \neq 0, x \neq \infty \\ \infty & \text{otherwise.} \end{cases}$$

- When $a \neq 0$ and q is odd, Carlitz showed that

$$R_{m,a}(x) = \sqrt{a}\frac{(x + \sqrt{a})^m + (x - \sqrt{a})^m}{(x + \sqrt{a})^m - (x - \sqrt{a})^m}.$$

Rédei functions

$$R_{1,a}(x) = x$$
$$R_{2,a}(x) = \frac{x^2 + a}{2x}$$
$$R_{3,a}(x) = \frac{x^3 + 3ax}{3x^2 + a}$$
$$R_{4,a}(x) = \frac{x^4 + 6ax^2 + a^2}{4x^3 + 4ax}$$
$$R_{5,a}(x) = \frac{x^5 + 10ax^3 + 5a^2x}{5x^4 + 10ax^2 + a^2}$$
$$R_{6,a}(x) = \frac{x^6 + 15ax^4 + 15a^2x^2 + a^3}{6x^5 + 20ax^3 + 6a^2x}$$
$$R_{7,a}(x) = \frac{x^7 + 21ax^5 + 35a^2x^3 + 7a^3x}{7x^6 + 35ax^4 + 21a^2x^2 + a^3}$$

Rédei functions

- From now on, q is odd.
- Let $\chi(a)$ be the quadratic character of $a \in \mathbb{F}_q^*$, that is,

$$\chi(a) = \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbb{F}_q^* \\ -1 & \text{otherwise.} \end{cases}$$

- $R_{m,a}$ and $R_{n,a}$ induce the same function if and only if $m \equiv n \pmod{q - \chi(a)}$.

Rédei permutations

- For $a \neq 0$, $R_{m,a}$ induces a permutation of $\mathbb{P}^1(\mathbb{F}_q)$ if and only if $\gcd(m, q - \chi(a)) = 1$.
- If q is odd, then m is odd.

The cycle structure of a Rédei permutation

Proposition (Qureshi and Panario, 2015)

(a) *The decomposition of the Rédei permutation* $R_{m,a}$ *into cycles is*

$$\bigoplus_{d \mid q-\chi(a)} \left\{ \frac{\varphi(d)}{o_d(m)} \times Cyc(o_d(m)) \right\} \oplus (\chi(a)+1) \times \{\bullet\}$$

where $Cyc(c)$ *denotes a* c*-cycle.*

(b) *The number of fixed points of* $R_{m,a}$ *is* $\gcd(m-1, q-\chi(a)) + \chi(a) + 1$.

Main question

When do $R_{m,a}$ and $R_{n,b}$ have the same cycle structure?

$\star$ Recall: The decomposition of the Rédei permutation $R_{m,a}$ into cycles is

$$\bigoplus_{d \mid q-\chi(a)} \left\{ \frac{\varphi(d)}{o_d(m)} \times Cyc(o_d(m)) \right\} \oplus (\chi(a)+1) \times \{\bullet\}$$

where $Cyc(c)$ denotes a c-cycle.

A general criterion

Proposition (Deng, 2013)

Let X_1 and X_2 be finite sets, and $f_1 \colon X_1 \to X_1$ and $f_2 \colon X_2 \to X_2$ be permutations. Then f_1 and f_2 have the same cycle structure if and only if f_1^r and f_2^r have the same number of fixed points for every positive integer r.

The number of fixed points of $R_{m,a}^r$

⋆ Recall: $R_{m,a}$ has $\gcd(m-1, q-\chi(a))+\chi(a)+1$ fixed points.

- $R_{m,a} \circ R_{n,a} = R_{mn,a}$
- $\underbrace{R_{m,a} \circ \cdots \circ R_{m,a}}_{r \text{ times}} = R_{m^r,a}$
- The number of fixed points in the r^{th} iterate of $R_{m,a}$ is

$$\gcd(m^r-1, q-\chi(a))+\chi(a)+1.$$

A criterion for Rédei permutations

Proposition

The Rédei permutations $R_{m,a}$ and $R_{n,b}$ have the same cycle structure if and only if

$$\gcd(m^r - 1, q - \chi(a)) + \chi(a) = \gcd(n^r - 1, q - \chi(b)) + \chi(b)$$

for all positive integers r.

- In this talk, we focus on the case $\chi(a) = \chi(b) = \chi$. We need

$$\gcd(m^r - 1, q - \chi) = \gcd(n^r - 1, q - \chi)$$

  for all positive integers r.
- Work in progress: the case $\chi(a) \neq \chi(b)$.

Example: $\mathbb{P}^1(\mathbb{F}_{49})$

[3, 13, 17, 23, 27, 33, 37, 47]
[7, 43]
[9, 19, 29, 39]
[11, 21, 31, 41]

(a) $\chi = -1$

[5, 29]
[7, 31]
[11, 35]
[13, 37]
[19, 43]
[23, 47]

(b) $\chi = 1$

Lists with values of m and n for which $R_{m,a}$ and $R_{n,b}$ have the same cycle structure when $\chi(a) = \chi(b) = \chi$ over $\mathbb{P}^1(\mathbb{F}_{49})$.

- $\chi = -1$; Pattern: $+10$, $+10$, $+10$, $+10$

[**3**, 13, 17, 23, 27, 33, 37, 47]	numbers in symmetric positions add up to 50
[**7**, 43]	numbers in symmetric positions add up to 50
[**9**, 19, 29, 39]	numbers in symmetric positions add up to 48
[**11**, 21, 31, 41]	numbers in symmetric positions add up to 52, the above list $+2$

- $\chi = 1$; Pattern: $+24$, $+24$, $+24$, $+24$, $+24$, $+24$

[**5**, 29]	
[**7**, 31]	the above list $+2$
[**11**, 35]	the above list $+4$
[**13**, 37]	the above list $+2$
[**19**, 43]	the above list $+6$
[**23**, 47]	the above list $+4$

Question 1

Can we find families of Rédei permutations with the same cycle structure?

Families of Rédei permutations with the same cycle structure

q	m	n	Conditions
p^k	p^{ℓ_1}	p^{ℓ_2}	$1 \leq \ell_1, \ell_2 < k$, $\gcd(\ell_1, k) = \gcd(\ell_2, k)$ If $\chi = -1$, then $\nu_2(\ell_1), \nu_2(\ell_2)$ is either $>$ or $\leq \nu_2(k)$.
p^{2k}	p	$p^{2k} - p + 1$	$\chi = -1$
$\chi \pmod 8$	$\dfrac{q-\chi}{4} + 1$	$\dfrac{3(q-\chi)}{4} + 1$	None
$\chi \pm 2 \pmod 8$	$\dfrac{q-\chi \pm 2}{4}$	$\dfrac{q-\chi \pm 4}{2}$	None

The cycle structure of the families

χ	q	m	n	Cycle Structure
-1	p^k k odd prime	p^{ℓ_1} $1 \leq \ell_1 < k$ ℓ_1 odd	p^{ℓ_2} $1 \leq \ell_2 < k$ ℓ_2 odd	$(2 \times \{\bullet\}) \oplus \left(\frac{p-1}{2} \times \mathrm{Cyc}(2)\right) \oplus \left(\frac{p^k - p}{2k} \times \mathrm{Cyc}(2k)\right)$
-1	p^k k odd prime	p^{ℓ_1} $1 \leq \ell_1 < k$ ℓ_1 even	p^{ℓ_2} $1 \leq \ell_2 < k$ ℓ_2 even	$((p+1) \times \{\bullet\}) \oplus \left(\frac{p^k - p}{k} \times \mathrm{Cyc}(k)\right)$
1	p^k k prime	p^{ℓ_1} $1 \leq \ell_1 < k$	p^{ℓ_2} $1 \leq \ell_2 < k$	$((p+1) \times \{\bullet\}) \oplus \left(\frac{p^k - p}{k} \times \mathrm{Cyc}(k)\right)$
-1	p^{2k}	p	$p^{2k} - p + 1$	$(2 \times \{\bullet\}) \oplus \bigoplus_{\substack{d \mid 2k \\ \nu_2(d) = \nu_2(2k)}} (N_{2d} \times \mathrm{Cyc}(2d))$ where $2dN_{2d} = p^d + 1 - \sum_{\substack{s \mid 2d \\ \nu_2(s) = \nu_2(2d)}} 2sN_{2s} - 2$
χ	$\chi \pmod 8$	$\frac{q-\chi}{4} + 1$	$\frac{3(q-\chi)}{4} + 1$	$\begin{cases} \left(\left(\frac{q-\chi}{4} + \chi + 1\right) \times \{\bullet\}\right) \oplus \left(\frac{3(q-\chi)}{8} \times \mathrm{Cyc}(2)\right) & \text{if } \frac{q-\chi}{8} \text{ is odd} \\ \left(\left(\frac{q-\chi}{4} + \chi + 1\right) \times \{\bullet\}\right) \oplus \left(\frac{q-\chi}{8} \times \mathrm{Cyc}(2)\right) \oplus \left(\frac{q-\chi}{8} \times \mathrm{Cyc}(4)\right) & \text{if } \frac{q-\chi}{8} \text{ is even} \end{cases}$

Example: $\mathbb{P}^1(\mathbb{F}_{3^{60}})$

$R_{3,a}$ and $R_{3^{60}-2,b}$ have the same cycle structure on $\mathbb{P}^1\left(\mathbb{F}_{3^{60}}\right)$ when $\chi(a) = \chi(b) = -1$. To obtain the number of cycles and their corresponding lengths, we consider every positive divisor d of $2k = 60$ with $\nu_2(d) = \nu_2(60) = 2$.

- For $d = 4$, we get $N_8 = \left(3^4 + 1 - 2\right)/8$, so $N_8 = 10$.
- For $d = 12$, we get $N_{24} = \left(3^{12} + 1 - 8N_8 - 2\right)/24$, so $N_{24} = 22,140$
- For $d = 20$, we get $N_{40} = \left(3^{20} + 1 - 8N_8 - 2\right)/40$, so $N_{40} = 87,169,608$.
- For $d = 60$, we get $N_{120} = \left(3^{60} + 1 - 8N_8 - 24N_{24} - 40N_{40} - 2\right)/120$, so

$$N_{120} = 353,259,652,293,468,362,590,059,312.$$

Hence the cycle structure is

$$\begin{aligned} & (2 \times \{\bullet\}) \oplus (10 \times \mathrm{Cyc}(8)) \oplus (22,140 \times \mathrm{Cyc}(24)) \oplus (87,169,608 \times \mathrm{Cyc}(40)) \\ \oplus \quad & (353,259,652,293,468,362,590,059,312 \times \mathrm{Cyc}(120)). \end{aligned}$$

Example: $\mathbb{P}^1(\mathbb{F}_{49})$

[3, 13, 17, 23, 27, 33, 37, 47]
[7, 43]
[9, 19, 29, 39]
[11, 21, 31, 41]

initial families

(a) $\chi = -1$

[5, 29]
[7, 31]
[11, 35]
[13, 37]
[19, 43]
[23, 47]

initial families

(b) $\chi = 1$

Lists with values of m and n for which $R_{m,a}$ and $R_{n,b}$ have the same cycle structure when $\chi(a) = \chi(b) = \chi$ over $\mathbb{P}^1(\mathbb{F}_{49})$.

χ	q	m	n	Cycle Structure
-1	p^k k odd prime	p^{ℓ_1} $1 \leq \ell_1 < k$ ℓ_1 odd	p^{ℓ_2} $1 \leq \ell_2 < k$ ℓ_2 odd	$(2 \times \{\bullet\}) \oplus \left(\frac{p-1}{2} \times \mathrm{Cyc}(2)\right) \oplus \left(\frac{p^k - p}{2k} \times \mathrm{Cyc}(2k)\right)$
-1	p^k k odd prime	p^{ℓ_1} $1 \leq \ell_1 < k$ ℓ_1 even	p^{ℓ_2} $1 \leq \ell_2 < k$ ℓ_2 even	$((p+1) \times \{\bullet\}) \oplus \left(\frac{p^k - p}{k} \times \mathrm{Cyc}(k)\right)$
1	p^k k prime	p^{ℓ_1} $1 \leq \ell_1 < k$	p^{ℓ_2} $1 \leq \ell_2 < k$	$((p+1) \times \{\bullet\}) \oplus \left(\frac{p^k - p}{k} \times \mathrm{Cyc}(k)\right)$
-1	p^{2k}	p	$p^{2k} - p + 1$	$(2 \times \{\bullet\}) \oplus \bigoplus_{\substack{d \mid 2k \\ \nu_2(d) = \nu_2(2k)}} (N_{2d} \times \mathrm{Cyc}(2d))$ where $2dN_{2d} = p^d + 1 - \sum_{\substack{s \mid 2d \\ \nu_2(s) = \nu_2(2d)}} 2sN_{2s} - 2$
χ	$\chi \pmod 8$	$\frac{q-\chi}{4} + 1$	$\frac{3(q-\chi)}{4} + 1$	$\begin{cases} \left(\left(\frac{q-\chi}{4} + \chi + 1\right) \times \{\bullet\}\right) \oplus \left(\frac{3(q-\chi)}{8} \times \mathrm{Cyc}(2)\right) & \text{if } \frac{q-\chi}{8} \text{ is odd} \\ \left(\left(\frac{q-\chi}{4} + \chi + 1\right) \times \{\bullet\}\right) \oplus \left(\frac{q-\chi}{8} \times \mathrm{Cyc}(2)\right) \oplus \left(\frac{q-\chi}{8} \times \mathrm{Cyc}(4)\right) & \text{if } \frac{q-\chi}{8} \text{ is even} \end{cases}$

Question 2

Can we describe the Rédei permutations that decompose into 1- and j-cycles?

1- and j-cycles

⋆ Recall: The j^{th} iterate of $R_{m,a}$ has $\gcd(m^j - 1, q - \chi(a)) + \chi(a) + 1$ fixed points.

- If $R_{m,a}$ decomposes into 1- and j-cycles, then

$$\gcd(m^j - 1, q - \chi(a)) + \chi(a) + 1 = q + 1.$$

(q, χ, j)-admissible integers

⋆ Recall: $R_{m,a}$ has $\gcd(m-1, q-\chi(a)) + \chi(a) + 1$ fixed points.

Definition

An integer d is (q, χ, j)-admissible if there exists an $R_{m,a}$ that decomposes into 1- and j-cycles with $d + \chi + 1$ fixed points and $\chi(a) = \chi$.

- $d = \gcd(m-1, q-\chi)$

When $j = p$ is prime

Proposition

Let p be a prime, $q - \chi = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and $d = p_1^{\beta_1} \cdots p_r^{\beta_r}$ with $0 \leq \beta_i \leq \alpha_i$. Then d is (q, χ, p)-admissible if and only if

$$\beta_i = \begin{cases} \alpha_i - 1 \text{ or } \alpha_i & \text{if } p_i = p > 2 \text{ and } \alpha_i \geq 2 \\ 1,\ \alpha_i - 1 \text{ or } \alpha_i & \text{if } p_i = p = 2 \text{ and } \alpha_i \geq 2 \\ 0 \text{ or } \alpha_i & \text{if } p_i \equiv 1 \pmod{p} \\ \alpha_i & \text{otherwise} \end{cases}$$

for each $i \in \{1, \ldots, r\}$.

An existence condition

- Case $p = 2$: Rédei involutions always exist.

Corollary

Let p be an odd prime. There exists a Rédei permutation with 1- and p-cycles if and only if $q - 1$ or $q + 1$ has a prime factor of the form $pk + 1$ or is divisible by p^2.

A characterization of Rédei permutations with 1- and p-cycles

Theorem

Let p be a prime and d be a (q, χ, p)-admissible integer. The Rédei permutation $R_{m,a}$ has $d + \chi + 1$ fixed points and p-cycles if and only if

(i) *m is a solution to*

$$\begin{cases} m \equiv 1 & \pmod{d} \\ m^{p-1} + m^{p-2} + \cdots + m + 1 \equiv 0 & \pmod{(q-\chi)/d} \end{cases}$$

(ii) $p^{\nu_p(q-\chi)} \nmid m - 1$, *if* $\nu_p(d) = \nu_p(q - \chi) - 1$.

Counting

Proposition

Let p be an odd prime and d be (q, χ, p)-admissible. Let M_d be the number of Rédei permutations with fixed parameter a, $d + \chi + 1$ fixed points, and p-cycles. Then

$$M_d = \begin{cases} (p-1)^u & \text{if } \nu_p(d) = \nu_p(q - \chi) \\ (p-1)^{u+1} & \text{if } \nu_p(d) = \nu_p(q - \chi) - 1, \end{cases}$$

where $u = |\{p' \text{ prime} \colon p' \equiv 1 \pmod{p}, p' \mid q - \chi \text{ and } p' \nmid d\}|$.

Rédei involutions

Theorem

Let $q-\chi = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the prime factorization of $q-\chi$, and $d = 2^{\beta_0} p_1^{\beta_1} \cdots p_r^{\beta_r}$ be a proper divisor of $q-\chi$. Then there exists a Rédei involution $R_{m,a}$ with $d+\chi+1$ fixed points over $\mathbb{P}^1(\mathbb{F}_q)$ if and only if $\beta_i \in \{0, \alpha_i\}$ for $1 \le i \le r$ and one of the following situations occurs:

(i) $\beta_0 \in \{\alpha_0 - 1, \alpha_0\}$ *and* $\beta_0 \ge 1$. *In this case, $R_{m,a}$ has a unique cycle structure and* $m \equiv k(q-\chi)/d - 1 \pmod{q-\chi}$ *for*

$$k = \begin{cases} \left(\dfrac{q-\chi}{2d}\right)^{\varphi(d)-1} + \dfrac{d}{2} & \text{if } \beta_0 = \alpha_0 - 1 \\ 2\left(\dfrac{q-\chi}{d}\right)^{\varphi(d)-1} & \text{if } \beta_0 = \alpha_0 \end{cases}$$

with k reduced modulo d.

(ii) $\alpha_0 \geq 3$ and $\beta_0 = 1$. In this case, $R_{m,a}$ and $R_{n,b}$ have the same cycle structure, where m or $n \equiv k(q-\chi)/d - 1 \pmod{q-\chi}$ for

$$k = \left(\frac{q-\chi}{2d}\right)^{\varphi(d)-1}$$

with k reduced modulo d, and $m \equiv n + (q-\chi)/2 \pmod{q-\chi}$.

Example: $\mathbb{P}^1(\mathbb{F}_{125})$

- $\chi(a) = 1$: $q - 1 = 2^2 \cdot 31$

j	prime $jk+1$, $jk+1 \mid q-1$?	$j^2 \mid q-1$?	d	M_d	m	# fixed points	# j-cycles
2	N/A		2	1	123	4	61
			4	1	61	6	60
			62	1	63	64	31
3	yes, 31	no	4	2	$5, 25$	6	40
4	no	N/A					
5	yes, 31	no	4	4	$33, 97, 101, 109$	6	24
prime ≥ 7	no	no					

Example: $\mathbb{P}^1(\mathbb{F}_{125})$

- $\chi(a) = -1$: $q + 1 = 2 \cdot 3^2 \cdot 7$

j	prime $jk+1$, $jk+1 \mid q+1$?	$j^2 \mid q+1$?	d	M_d	m	# fixed points	# j-cycles
2	N/A		2	1	125	2	62
			14	1	71	14	56
			18	1	55	18	54
3	yes, 7	yes	6	4	$25, 67, 79, 121$	6	40
			18	2	$37, 109$	18	36
			42	2	$43, 85$	42	28
4	no	N/A					
prime ≥ 5	no	no					

Example: $\mathbb{P}^1(\mathbb{F}_{49})$

[3, 13, 17, 23, 27, 33, 37, 47]	
[7, 43]	initial families
[9, 19, 29, 39]	
[11, 21, 31, 41]	1-and 5-cycles

(a) $\chi = -1$

[5, 29]	
[7, 31]	
[11, 35]	
[13, 37]	initial families
[19, 43]	
[23, 47]	involutions

(b) $\chi = 1$

Lists with values of m and n for which $R_{m,a}$ and $R_{n,b}$ have the same cycle structure when $\chi(a) = \chi(b) = \chi$ over $\mathbb{P}^1(\mathbb{F}_{49})$.

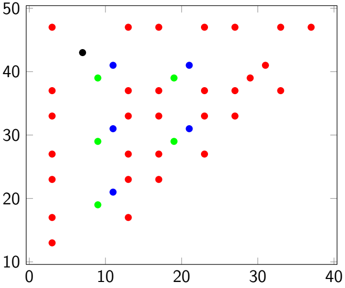
Back to the main question

When do $R_{m,a}$ and $R_{n,b}$ have the same cycle structure?

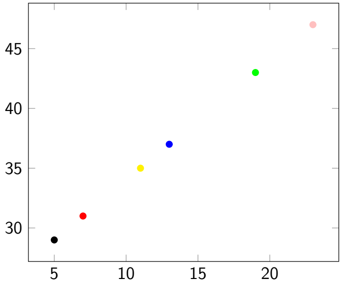
The set S_χ^q

- $\mathcal{S}_\chi^q = \{(m,n) \in \mathbb{N}^2 \colon R_{m,a}$ and $R_{n,b}$ are Rédei permutations with the same cycle structure for some $a, b \in \mathbb{F}_q$ with $\chi(a) = \chi(b) = \chi\}$.
- Clearly, $(m,n) \in S_\chi^q$ if and only if $(n,m) \in S_\chi^q$.

Plotting the points in S_χ^{49}



(a) $\chi = -1$



(b) $\chi = 1$

Pairs $(m, n) \in S_\chi^{49}$ with $1 < m < n < 49 - \chi$, color-coded by their cycle structures.

The distribution of the points in S_{-1}^{49} over lines

Equation of the line	Pairs (m, n) lying on the line
$y = x + 4$	$(13, 17)$, $(23, 27)$, $(33, 37)$
$y = x + 6$	$(17, 23)$, $(27, 33)$
$y = x + 10$	$(3, 13)$, $(9, 19)$, $(11, 21)$, $(13, 23)$, $(17, 27)$, $(19, 29)$, $(21, 31)$, $(23, 33)$, $(27, 37)$, $(29, 39)$, $(31, 41)$, $(37, 47)$
$y = x + 14$	$(3, 17)$, $(13, 27)$, $(23, 37)$, $(33, 47)$
$y = x + 16$	$(17, 33)$
$y = x + 20$	$(3, 23)$, $(9, 29)$, $(11, 31)$, $(13, 33)$, $(17, 37)$, $(19, 39)$, $(21, 41)$, $(27, 47)$
$y = x + 24$	$(3, 27)$, $(13, 37)$, $(23, 47)$
$y = x + 30$	$(3, 33)$, $(9, 39)$, $(11, 41)$, $(17, 47)$
$y = x + 34$	$(3, 37)$, $(13, 47)$
$y = x + 36$	$(7, 43)$
$y = x + 44$	$(3, 47)$

The distribution of the pairs $(m, n) \in S_{-1}^{49}$ over eleven lines.

A complete characterization of S_χ^q

Theorem

Suppose $q-\chi = p_1^{\alpha_1}\cdots p_t^{\alpha_t}$ *is the prime factorization of* $q-\chi$, *m is coprime with* $q-\chi$, *and* $\theta_i = o_{p_i}(m)$. *Then* $(m,n)\in S_\chi^q$ *if and only if* $n = m + k(q-\chi)/d$, *where d is a proper divisor of* $q-\chi$ *and k is an integer, and for each* p_i *that divides d the following conditions hold:*

(i) $p_i \nmid n$ *and* $o_{p_i}(n) = \theta_i$,

(ii) $\gcd(m^{\theta_i}-1, p_i^{\alpha_i}) = \gcd(n^{\theta_i}-1, p_i^{\alpha_i})$.

(iii) *If* $p_i = 2$, $\alpha_i > 1$ *and* $\nu_2(m-1) = 1$, *then* $\gcd(m^2-1, 2^{\alpha_i}) = \gcd(n^2-1, 2^{\alpha_i})$.

Idea of the proof

- Recall: $(m,n) \in S_\chi^q$ if and only if $\gcd(m^r-1, q-\chi) = \gcd(n^r-1, q-\chi)$ for all positive integers r.
- $q-\chi = p_1^{\alpha_1}\cdots p_t^{\alpha_t} \quad \Longrightarrow \quad \gcd(m^r-1, q-\chi) = \prod_{i=1}^{t} \gcd(m^r-1, p_i^{\alpha_i})$
- If p is odd and $\theta = o_p(m)$, then $\nu_p(m^r-1) = \begin{cases} 0 & \text{if } \theta \nmid r \\ \nu_p(m^\theta-1)+\nu_p(t) & \text{if } r = t\theta \end{cases}$
- If $p=2$, then $\nu_2(m^r-1) = \begin{cases} \nu_2(m-1) & \text{if } r \text{ is odd} \\ \nu_2(m^2-1)+\nu_2(r)-1 & \text{if } r \text{ is even} \end{cases}$

Symmetries in S_χ^q

Proposition

Suppose $q-\chi = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ *is the prime factorization of* $q-\chi$ *and* d *is a proper divisor of* $q-\chi$*. If* $(m,n)\in S_\chi^q$*, then* $(m+k(q-\chi)/d, n+k(q-\chi)/d)\in S_\chi^q$ *if and only if for each* p_i *that divides* d *the following conditions hold:*

(i) $p_i \nmid m+k(q-\chi)/d, n+k(q-\chi)/d$ *and* $\theta_i := o_{p_i}(m+k(q-\chi)/d) = o_{p_i}(n+k(q-\chi)/d)$,

(ii) $\gcd((m+k(q-\chi)/d)^{\theta_i}-1, p_i^{\alpha_i}) = \gcd((n+k(q-\chi)/d)^{\theta_i}-1, p_i^{\alpha_i})$.

(iii) *If* $p_i=2$, $\alpha_i>1$ *and* $\nu_2((m+k(q-\chi)/d)-1)=1$*, then* $\gcd((m+k(q-\chi)/d)^2-1, 2^{\alpha_i}) = \gcd((n+k(q-\chi)/d)^2-1, 2^{\alpha_i})$.

Equation of the line	Generator (m, n)	d	$(m + k \cdot 50/d, n + k \cdot 50/d)$, $(n + k \cdot 50/d, m + k \cdot 50/d)$ in $\mathbb{Z}_{50}^2$
$y = x + 4$	$(13, 17)$	5	$(23, 27)$, $(33, 37)$
$y = x + 44$ $y = x + 6$	$(3, 47)$	5	$(17, 23)$, $(27, 33)$
$y = x + 10$	$(3, 13)$	25	$(9, 19)$, $(11, 21)$, $(13, 23)$, $(17, 27)$, $(19, 29)$, $(21, 31)$, $(23, 33)$, $(27, 37)$, $(29, 39)$, $(31, 41)$, $(37, 47)$
$y = x + 14$ $y = x + 36$	$(3, 17)$	5	$(13, 27)$, $(23, 37)$, $(33, 47)$ $(7, 43)$
$y = x + 34$ $y = x + 16$	$(3, 37)$	5	$(13, 47)$ $(17, 33)$
$y = x + 20$	$(3, 23)$	25	$(9, 29)$, $(11, 31)$, $(13, 33)$, $(17, 37)$, $(19, 39)$, $(21, 41)$, $(27, 47)$
$y = x + 24$	$(3,27)$	5	$(13, 37)$, $(23, 47)$
$y = x + 30$	$(3, 33)$	25	$(9, 39)$, $(11, 41)$, $(17, 47)$

The distribution of the points over eleven lines and their corresponding generators.

All Rédei permutations $R_{m,a}$ over $\mathbb{P}^1(\mathbb{F}_{49})$, with $1 \leq m < 49 - \chi(a)$

$\chi(a)$	m	Cycle Structure
-1	1	$50 \times \{\bullet\}$
-1	$3, 13, 17, 23, 27, 33, 37, 47$	$(2 \times \{\bullet\}) \oplus (2 \times \mathrm{Cyc}(4)) \oplus (2 \times \mathrm{Cyc}(20))$
-1	$7, 43$	$(2 \times \{\bullet\}) \oplus (12 \times \mathrm{Cyc}(4))$
-1	$9, 19, 29, 39$	$(2 \times \{\bullet\}) \oplus (4 \times \mathrm{Cyc}(2)) \oplus (4 \times \mathrm{Cyc}(10))$
-1	$11, 21, 31, 41$	$(10 \times \{\bullet\}) \oplus (8 \times \mathrm{Cyc}(5))$
-1	49	$(2 \times \{\bullet\}) \oplus (24 \times \mathrm{Cyc}(2))$
1	1	$50 \times \{\bullet\}$
1	$5, 29$	$(6 \times \{\bullet\}) \oplus (10 \times \mathrm{Cyc}(2)) \oplus (6 \times \mathrm{Cyc}(4))$
1	$7, 31$	$(8 \times \{\bullet\}) \oplus (21 \times \mathrm{Cyc}(2))$
1	$11, 35$	$(4 \times \{\bullet\}) \oplus (11 \times \mathrm{Cyc}(2)) \oplus (6 \times \mathrm{Cyc}(4))$
1	$13, 37$	$(14 \times \{\bullet\}) \oplus (6 \times \mathrm{Cyc}(2)) \oplus (6 \times \mathrm{Cyc}(4))$
1	17	$(18 \times \{\bullet\}) \oplus (16 \times \mathrm{Cyc}(2))$
1	$19, 43$	$(8 \times \{\bullet\}) \oplus (9 \times \mathrm{Cyc}(2)) \oplus (6 \times \mathrm{Cyc}(4))$
1	$23, 47$	$(4 \times \{\bullet\}) \oplus (23 \times \mathrm{Cyc}(2))$
1	25	$(26 \times \{\bullet\}) \oplus (12 \times \mathrm{Cyc}(2))$
1	41	$(10 \times \{\bullet\}) \oplus (20 \times \mathrm{Cyc}(2))$

Theorem

The only isolated Rédei permutations are the isolated Rédei involutions.

- Idea of the proof:
  If $R_{m,a}$ is not an involution, then $\rho := o_{q-\chi}(m) > 2$. In this case, the pair $(m, m^{\rho-1})$ is in S_χ^q.

Final remark

The mappings

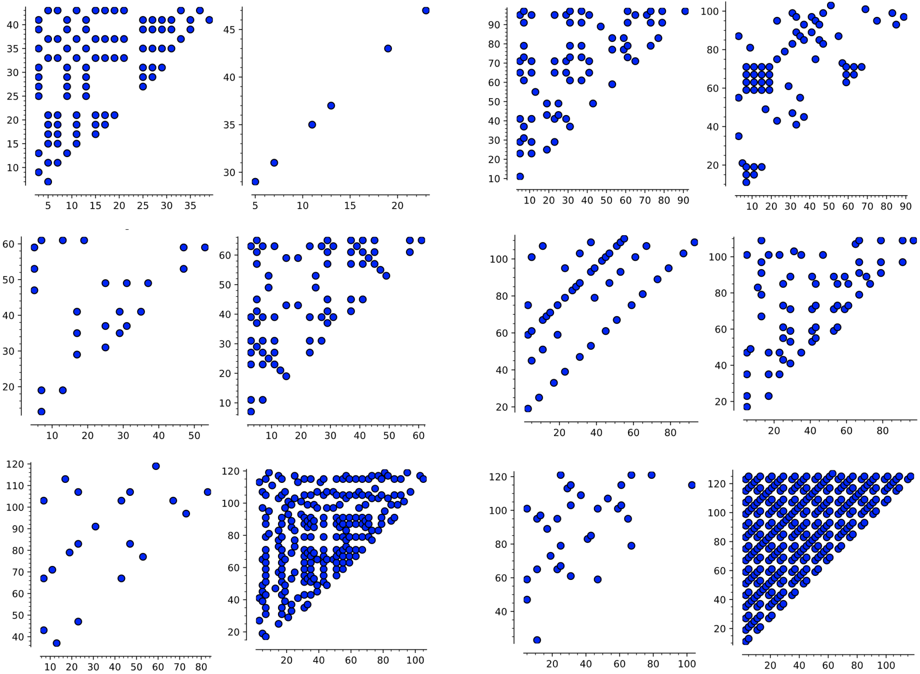
$$
\begin{aligned}
&R_{m,a} \colon \mathbb{D}_q \to \mathbb{D}_q \\
&f_m \colon \mathbb{Z}_{q-\chi} \to \mathbb{Z}_{q-\chi}, \quad x \mapsto mx \\
&g_m \colon \mathbb{C}_q \to \mathbb{C}_q, \qquad\quad x \mapsto x^m
\end{aligned}
$$

have the same cycle structure, where

$$
\mathbb{D}_q = \begin{cases} \mathbb{P}^1(\mathbb{F}_q) & \text{if } \chi(a) = -1 \\ \mathbb{P}^1(\mathbb{F}_q) \setminus \{\pm\sqrt{a}\} & \text{if } \chi(a) = 1, \end{cases} \qquad \mathbb{C}_q = \begin{cases} U_{q+1} & \text{if } \chi(a) = -1 \\ \mathbb{F}_q^* & \text{if } \chi(a) = 1, \end{cases}
$$

and U_{q+1} is the subgroup of order $q+1$ in $\mathbb{F}_{q^2}$.

Thank you!



40 35 30 25 20 15 10
5 10 15 20 25 30 35
45 40 35 30
5 10 15 20
90 80 70 60 50 40 30 20 10
10 20 30 40 50 60 70 80 90
100 80 60 40 20
10 20 30 40 50 60 70 80 90
60 50 40 30 20
10 20 30 40 50
60 50 40 30 20 10
10 20 30 40 50 60
100 80 60 40 20
20 40 60 80
100 80 60 40 20
20 40 60 80
120 110 100 90 80 70 60 50 40
10 20 30 40 50 60 70 80
120 100 80 60 40 20
20 40 60 80 100
120 100 80 60 40
20 40 60 80 100
120 100 80 60 40 20
20 40 60 80 100