Rédei Permutations with Cycles of the Same Length

Juliane Capaverde[2], Ariane Masuda[1], and Virgínia Rodrigues[2]

[1] Department of Mathematics, New York City College of Technology

[2] Departamento de Matemática Pura e Aplicada, Universidade Federal do Rio Grande do Sul

Abstract

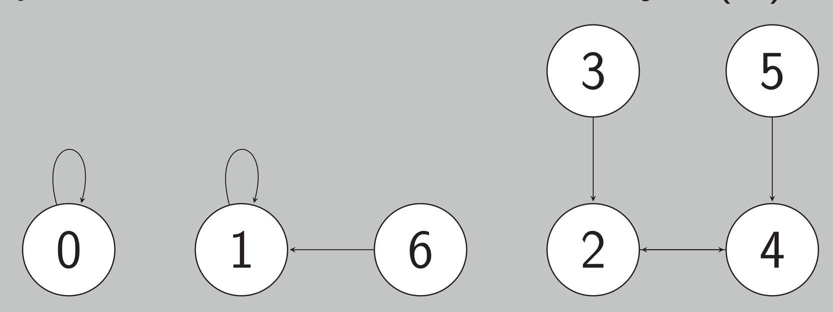
Let $\mathbb{F}_q$ be a finite field of odd characteristic. We study Rédei functions that induce permutations over $\mathbb{P}^1(\mathbb{F}_q)$ whose cycle decomposition contains only cycles of length 1 and j, for an integer $j \geq 2$. When j is a prime number, we give necessary and sufficient conditions for a Rédei permutation of this type to exist over $\mathbb{P}^1(\mathbb{F}_q)$, characterize Rédei permutations consisting of 1- and j-cycles, and determine their total number. We also present explicit formulas for Rédei involutions based on the number of fixed points.

Functional Graphs

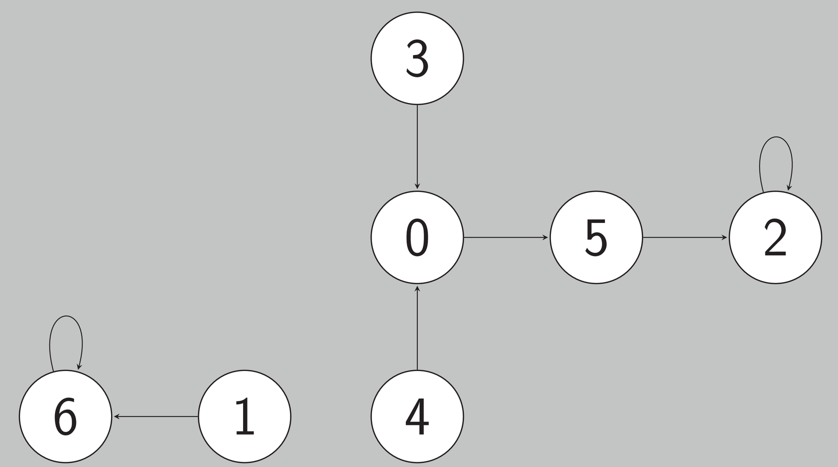
- Let S be a finite set and $f : S \to S$ be a mapping.
- The **functional graph associated to f** is a directed graph where the vertices are labelled by the elements of S, and a directed edge connects a vertex a with a vertex b if and only if $b = f(a)$.
- Let $\mathbb{F}_q$ be the finite field of order q.

Example

▷ The functional graph of $f : \mathbb{F}_7 \to \mathbb{F}_7$ defined by $f(x) = x^2$ is



▷ The functional graph of $g : \mathbb{F}_7 \to \mathbb{F}_7$ defined by $g(x) = x^2 + 5$ is



The functional graphs of x^2 and $x^2 + 5$ are not isomorphic.

Rédei Function

- 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 a positive integer m and $a \in \mathbb{F}_q$, the **Rédei function** is $R_{m,a} : P^1(\mathbb{F}_q) \to P^1(\mathbb{F}_q)$ where

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

The Isomorphism Problem

- We denote the functional graph of $R_{m,a}$ over $\mathbb{P}^1(\mathbb{F}_q)$ by $\mathcal{G}(m, a, q)$.
- **Problem**: Find conditions on m, n, a, b, q such that $\mathcal{G}(m, a, q)$ is isomorphic to $\mathcal{G}(n, b, q)$.
- Our goal is to characterize permutation $R_{m,a}$ with 1- and j-cycles for a prime j.

The Graph Structure

- $\chi(a) = 1$ if a is a square in $\mathbb{F}_q^*$, and -1 otherwise.

Theorem (Qureshi and Panario [2])

The Rédei function $R_{m,a}$ induces a permutation of $\mathbb{P}^1(\mathbb{F}_q)$ if and only if $\gcd(m, q - \chi(a)) = 1$. In this case, we have the following decomposition in disjoint cycles:

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

where ϕ is the Euler's totient function, $o_d(m)$ is the order of m modulo d, and $Cyc(c)$ denotes a c-cycle.

Main Results

Theorem (Capaverde, M., and Rodrigues [1], 2020)

Let p be an odd prime. There exists a Rédei permutation over $\mathbb{P}^1(\mathbb{F}_q)$ with cycles of length 1 and p if and only if $q - 1$ or $q + 1$ has a prime factor of the form $pk + 1$ or is divisible by p^2.

Theorem (Capaverde, M., and Rodrigues [1], 2020)

Let p be an odd prime and M be the number of Rédei permutations over $\mathbb{P}^1(\mathbb{F}_q)$ with cycles of length 1 and p with fixed parameter a. Then

$$M = \begin{cases} p^r - 1 & \text{if } p^2 \nmid q - \chi(a) \\ p^{r+1} - 1 & \text{if } p^2 \mid q - \chi(a), \end{cases}$$

where $r = |\{p' \text{ prime} \colon p' \equiv 1 \pmod{p}, p' \mid q - \chi(a)\}|$.

Theorem (Capaverde, M., and Rodrigues [1], 2020)

Let $\nu_p(z)$ be the p-adic valuation of z. A Rédei permutation $R_{m,a}$ over $\mathbb{P}^1(\mathbb{F}_q)$ is an involution with $d + \chi(a) + 1$ fixed points if and only if d is even, $\nu_2(d) \in \{1, \nu_2(q - \chi(a)) - 1, \nu_2(q - \chi(a))\}$, and $\gcd(d, (q - \chi(a))/d) \mid 2$. In this case, $m \equiv k(q - \chi(a))/d - 1 \pmod{q - \chi(a)}$, where k reduced modulo d equals

$$\begin{cases} 2\left(\frac{q-\chi(a)}{d}\right)^{\varphi(d)-1} & \text{if } \nu_2(d) = \nu_2(q - \chi(a)) \\ \left(\frac{q-\chi}{2d}\right)^{\varphi(d)-1} + \frac{d}{2} & \text{if } \nu_2(d) = \nu_2(q - \chi(a)) - 1 \geq 1 \\ \left(\frac{q-\chi(a)}{2d}\right)^{\varphi(d)-1}, \left(\frac{q-\chi(a)}{2d}\right)^{\varphi(d)-1} + \frac{d}{2} & \text{if } \nu_2(d) = 1, \nu_2(q - \chi(a)) \geq 3 \end{cases}$$

Remarks

- The type of function under investigation is of interest in the construction of interleavers for turbo codes. In addition, involutions have cryptographic applications such as the design of S-boxes.
- In our paper, we also give procedures to construct Rédei permutations with a prescribed number of fixed points and j-cycles for $j \in \{3, 4, 5\}$.
- Our results allow us to find all Rédei functions whose functional graphs consist of fixed points and j-cycles where j is any prime number, without the aid of a computer, depending on the factorization of $q \pm 1$.

Example

Let $R_{m,a}$ be a Rédei permutation over $\mathbb{F}_{125}$. The following are **all Rédei permutations with 1- and j-cycles over $\mathbb{P}^1(\mathbb{F}_{125})$, where j is prime**.

▷ when $\chi(a) = 1$: $R_{123,a}$ has 4 fixed points and 61 2-cycles; $R_{61,a}$ has 6 fixed points and 60 2-cycles; $R_{63,a}$ has 64 fixed points and 31 2-cycles; $R_{m,a}$ has 6 fixed points and 40 3-cycles when $m \in \{5, 25\}$; $R_{m,a}$ has 6 fixed points and 24 5-cycles when $m \in \{33, 97, 101, 109\}$.

▷ when $\chi(a) = -1$: $R_{125,a}$ has 2 fixed points and 62 2-cycles; $R_{71,a}$ has 14 fixed points and 56 2-cycles; $R_{55,a}$ has 18 fixed points and 54 2-cycles; $R_{m,a}$ has 6 fixed points and 40 3-cycles when $m \in \{25, 67, 79, 121\}$; $R_{m,a}$ has 18 fixed points and 36 3-cycles when $m \in \{37, 109\}$; $R_{m,a}$ has 42 fixed points and 28 3-cycles when $m \in \{43, 85\}$.

Open Problems

- Find all Rédei permutations with 1- and j-cycles when j is not prime
- Obtain closed formulas for m such that $R_{m,a}$ is a Rédei permutation with 1- and j-cycles, $j \neq 2$.

References

[1] J. Capaverde, A. M. Masuda, and V. M. Rodrigues, Rédei permutations with cycles of the same length. Des. Codes Cryptogr. 88, 2561–2579 (2020).

[2] C. Qureshi and D. Panario, Rédei actions on finite fields and multiplication map in cyclic group, SIAM J. Discrete Math. 29(3), 1486–1503 (2015).

Acknowledgement. The second author received support for this project provided by a PSC-CUNY Grant.