SIAM J. DISCRETE MATH.
Vol. 29, No. 3, pp. 1486–1503

RÉDEI ACTIONS ON FINITE FIELDS AND MULTIPLICATION MAP IN CYCLIC GROUP*

CLAUDIO QURESHI† AND DANIEL PANARIO‡

Abstract. We describe the functional graph of the multiplication-by-n map in a cycle group and use this to obtain the structure of the functional graph associated with a Rédei function over a nonbinary finite field $\mathbb{F}_q$. In particular, we obtain two descriptions of the tree attached to the cyclic nodes in these graphs and provide period and preperiod estimates for Rédei functions. We also extend characterizations of Rédei permutations by describing their decomposition into disjoint cycles. Finally, we obtain some results on the length of the cycles related to Rédei permutations and we give an algorithm to construct Rédei permutations with prescribed length cycles in a geometric progression.

Key words. dynamical systems over finite fields, Redei functions over finite fields, multiplication map in cyclic groups

AMS subject classifications. 12Y05, 11T99

DOI. 10.1137/140993338

1. Introduction.

The dynamics of iterations of polynomials and rational functions over finite fields have attracted much attention in recent years. This is in part due to their applications in cryptography and integer factorization methods like the *Pollard rho algorithm*; see, for example, [5, 9, 22] for some applications in elliptic curve cryptography

In general, let $\mathcal{F}_n$ be the set of functions or mappings from the set $[1..n]$ to itself. With any $\varphi \in \mathcal{F}_n$ there is associated a *functional graph* on n nodes with a directed edge from vertex u to vertex v if and only if $\varphi(u) = v$. Functional graphs of mappings are sets of connected components; the components are directed cycles of nodes and each of those nodes is the root of a tree.

We are interested here in functions over finite fields. Iterations of functions over finite fields have centered on studies such as

- period and preperiod of an element;
- (average) "rho length" (number of iterations until we cycle back);
- number of connected components;
- length of cycles (largest, smallest, average);
- number of fixed points and conditions to have a permutation;
- isomorphism of graphs; and so on.

Iterations of some functions over finite fields have strong symmetries that can be mathematically explained. In that sense, previous results for several quadratic functions are in [15, 17, 21]; iterations of $x + x^{-1}$ have been dealt with in [20] and iterations of Chebyshev polynomials over finite fields have been treated in [6]. An estimate for the number of nonisomorphic graphs of degree d polynomials is given in [11]; in [12] some results on the asymptotic behavior for the tail and cycle length of random

*Received by the editors October 28, 2014; accepted for publication (in revised form) May 27, 2015; published electronically August 18, 2015.
http://www.siam.org/journals/sidma/29-3/99333.html

†Institute of Mathematics, State University of Campinas, Brazil (cqureshi@gmail.com). This author was partially supported by FAPESP of Brazil under grants 2012/10600-2 and 2014/04096-5.

‡School of Mathematics and Statistics, Carleton University, Canada (daniel@math.carleton.ca). This author was partially funded by NSERC of Canada.

mappings with restricted preimages are provided. Algebraic dynamical systems generated by several rational functions on many variables over finite fields have also been considered; see section 10.5 of [10].

In this paper we study the action of *Rédei functions over nonbinary finite fields* via the action of the multiplication-by-n map over a cyclic group. These functional graphs present a strong type of symmetries. The cyclic decomposition and some properties related to the trees attached to cyclic nodes were studied in [19]. We extend the description of these functional graphs giving two different characterizations for its associated trees. In section 2 we introduce some important concepts for this paper, such as ν-series and their associated trees, which play an important role in the description of the nonperiodic part of some functional graphs that are studied in the following sections. In section 3 we focus our attention in the action of the multiplication-by-n map over the cyclic group $\mathbb{Z}_m$, describing its functional graph and relating its trees to the trees associated with ν-series. We also give in this section an alternative description of these trees. In section 4 we apply the previous results to the case of Rédei functions. We start this section with a review of Rédei functions over finite fields and we briefly comment on their main properties and applications. Next, we give the structure of the functional graph associated with a Rédei function, providing period and preperiod studies. As corollaries of our main structural theorem, we extend the characterization of Rédei permutations by describing their decomposition into disjoint cycles and use this to obtain a method for constructing Rédei functions with prescribed length cycles in certain geometric progression. Finally, in section 5 we list further interesting research problems related to map iterations over finite fields and in particular to Rédei iterations.

2. Preliminaries, definitions, and notation. In this section we introduce the concept of ν-series and a special type of tree associated with them that plays a crucial role in our results.

2.1. The ν-series.

DEFINITION 2.1. *Let $\nu > 1$ be an integer. A ν-series is a finite sequence of positive integers $V = (\nu_1, \nu_2, \ldots, \nu_D)$ such that*

(i) $\nu_{i+1} \mid \nu_i$ *for* $1 \le i \le D-1$;
(ii) $\nu_D > 1$;
(iii) $\nu = \prod_{i=1}^{D} \nu_i$.

By convention, for $\nu = 1$ we have only one ν-series that is denoted by (1). *The numbers ν_i for $1 \le i \le D$ are the components of V. For $V \neq (1)$ the number D is the depth of V and is denoted by depth(V) and for $V = (1)$ we define depth$(V) = 0$.*

Example 2.2. $V = (24, 24, 6, 2, 2)$ is a 13824-series with *depth*$(V) = 5$.

The radical of a positive integer n is the product of the distinct prime divisors of n and is denoted by $\mathrm{rad}(n)$; by convention $\mathrm{rad}(1) = 1$. If ν and n are positive integers with $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$, we have a particular way, to be given next, to construct ν-series in which each component is a divisor of n.

DEFINITION 2.3. *If $\nu > 1$ and n are positive integers with rad$(\nu) \mid$ rad(n) the ν-series generated by n, denoted by $\nu(n)$, is defined as*

$$\begin{cases} \nu_1 = \gcd(\nu, n), \\ \nu_{i+1} = \gcd\left(\frac{\nu}{\nu_1 \nu_2 \ldots \nu_i}, n\right) & \text{for } i \ge 1. \end{cases}$$

If $D = \max\{i \ge 1 : \nu_i > 1\}$, we define $\nu(n) = (\nu_1, \nu_2, \ldots, \nu_D)$. By convention, for $\nu = 1$ we define $\nu(n) = (1)$ for all n.

PROPOSITION 2.4. *The ν-series generated by n with $rad(\nu) \mid rad(n)$ is well defined. Moreover, if $D = \max\{\lceil e_p(\nu)/e_p(n)\rceil : p \mid n,\ p \text{ prime}\}$, where $e_p(n)$ denotes the exponent of the prime p in n, then D is the depth of $\nu(n)$.*

Proof. We observe first that if p is a prime number that does not divide n, then $e_p(\nu_i) = 0$ for all $i \geq 1$. On the other hand, if p is a prime divisor of n and $e_p(\nu) = qe_p(n) + r$ with $0 \leq r < e_p(n)$, one can prove by induction that

$$e_p(\nu_i) = \begin{cases} e_p(n) & \text{if } 1 \leq i \leq q, \\ r & \text{if } i = q+1, \\ 0 & \text{if } i > q+1. \end{cases}$$

From this, we have that $\nu(n)$ is a ν'-series with depth $D = \max\{\lceil e_p(\nu)/e_p(n)\rceil : p \mid n,$ p prime$\}$, where

$$\nu' = \prod_{i=1}^{D} \nu_i = \prod_{p|n} p^{e_p(\nu)}.$$

Now, as $\text{rad}(\nu) \mid \text{rad}(n)$ the last equation implies $\nu' = \nu$. ∎

We observe that with the notation as above

$$D = \min\{\lambda \in \mathbb{Z}^+ : \nu \mid n^\lambda\}.$$

Example 2.5. If we take $\nu = 360, n = 30$, the 360-series V associated with $n = 30$ is

$$\begin{cases} \nu_1 = \gcd(360, 30) = 30, & \nu/\nu_1 = 360/30 = 12; \\ \nu_2 = \gcd(12, 30) = 6, & \nu/(\nu_1\nu_2) = 12/6 = 2; \\ \nu_3 = \gcd(2, 30) = 2, & \nu/(\nu_1\nu_2\nu_3) = 2/2 = 1. \end{cases}$$

Therefore $V = 360(30) = (30, 6, 2)$. The depth of this 360-series is 3.

2.2. Trees associated with ν-series. Let $G = (V, E)$ be a directed graph and $G_i = (V_i, E_i)$ be subgraphs of G for $1 \leq i \leq m$. The notation $G = \bigoplus_{i=1}^m G_i$ means that $V = \biguplus_{i=1}^m V_i$, the disjoint union of the sets V_i, and $E = \biguplus_{i=1}^m E_i$, the disjoint union of the edges in E_i. We denote by $\bullet$ any graph consisting of a unique vertex and by $\simeq$ the isomorphism relation. If H denotes a directed graph (or the isomorphism class of some directed graph) and $n \in \mathbb{Z}^+$, then $G \simeq n \times H$ means $G = \bigoplus_{i=1}^n G_i$ with each $G_i \simeq H$. We also consider the graph $\emptyset$ as a graph without vertices and edges. As our goal is to describe some functional graph, it is convenient to introduce the following definition.

DEFINITION 2.6. *Let T be a rooted tree and $f \in \mathbb{Z}^+$. We denote by $Cyc(f, T)$ a directed graph with a unique cycle of length f such that each node in that cycle is the root of a tree isomorphic to T. When $T = \bullet$, that is, it consists of only one vertex, we denote $Cyc(f, \bullet)$ by $Cyc(f)$.*

Functional graphs associated with Rédei function have special symmetries: each connected component is of the form $Cyc(f, T)$ for some $f \in \mathbb{Z}^+$ and some rooted tree T (the same T for all connected components). Describing the trees T requires a bit of work, so we start by introducing some operations and notation on trees.

NOTATION 2.7. *If T is a rooted tree and x is a vertex (or node) in T, we denote by $\rho_T(x)$ the set of directed predecessors of x in T. In this way, $\#\rho_T(x) = indeg(x)$ is the in-degree of x. By definition each vertex in T has out-degree equal to 1 except*

for the root which has out-degree equal to 0. *The vertices* x *with* $\rho_T(x) = \emptyset$ *are called leaves; the set of all leaves in* T *is denoted by* $\mathcal{H}_T$. *We consider the empty graph* $\emptyset$ *as a rooted tree.*

DEFINITION 2.8. *Let* $T_1, T_2, \ldots, T_k$ *be rooted trees with roots* $t_1, t_2, \ldots, t_k$, *respectively. If* $G = \bigoplus_{i=1}^{k} T_i$ *is the graph whose connected components are the rooted trees* T_i *for* $1 \leq i \leq k$, *then* $\langle G \rangle$ *denotes a rooted tree where its root has directed predecessors* $t_1, t_2, \ldots, t_k$. *The empty graph verifies* $G \oplus \emptyset = G$ *for every graph* G *and* $\langle \emptyset \rangle = \bullet$ *(the tree consisting of a unique point).*

Now, we define a special type of trees associated with ν-series. These trees play an important role in the description of the Rédei functional graphs.

DEFINITION 2.9. *If* $V = (\nu_1, \nu_2, \ldots, \nu_D)$ *is a* ν*-series, we define recursively the tree* T_V *associated with* V *as follows:*

$$\begin{cases} T_V^0 = \bullet, \\ T_V^k = \langle \nu_k \times T_V^{k-1} \oplus \bigoplus_{i=1}^{k-1} (\nu_i - \nu_{i+1}) \times T_V^{i-1} \rangle \text{ for } 1 \leq i \leq D, \end{cases} \tag{2.1}$$

and

$$T_V = \left\langle (\nu_D - 1) \times T_V^{D-1} \oplus \bigoplus_{i=1}^{D-1} (\nu_i - \nu_{i+1}) \times T_V^{i-1} \right\rangle. \tag{2.2}$$

For $V = (1)$ *we define* $T_V = \bullet$.

Example 2.10. In Figure 1 we show the inductive construction of T_V when the ν-series $V = (\nu_1, \nu_2, \nu_3, \nu_4)$ has four components.

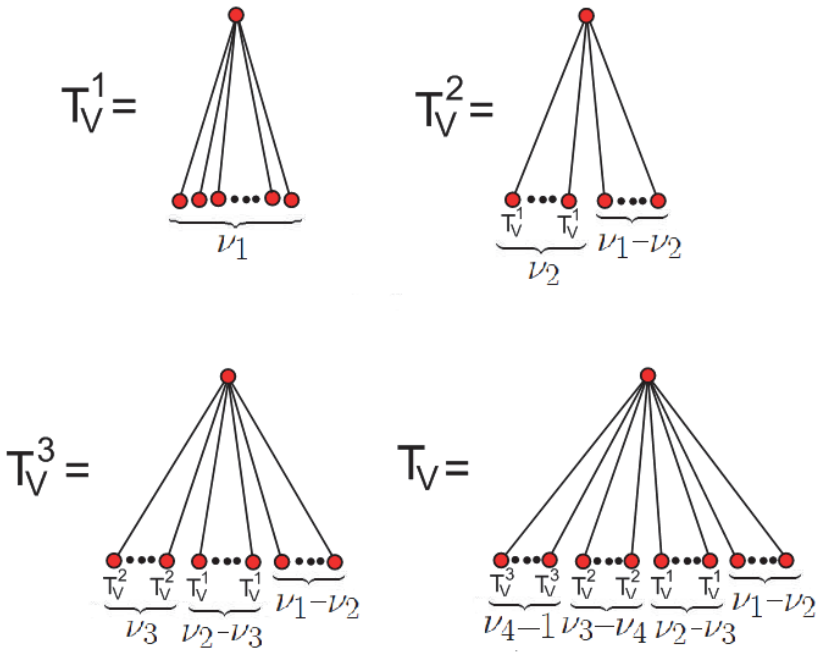

FIG. 1. *Inductive definition of* T_V *for* $V = (\nu_1, \nu_2, \nu_3, \nu_4)$.

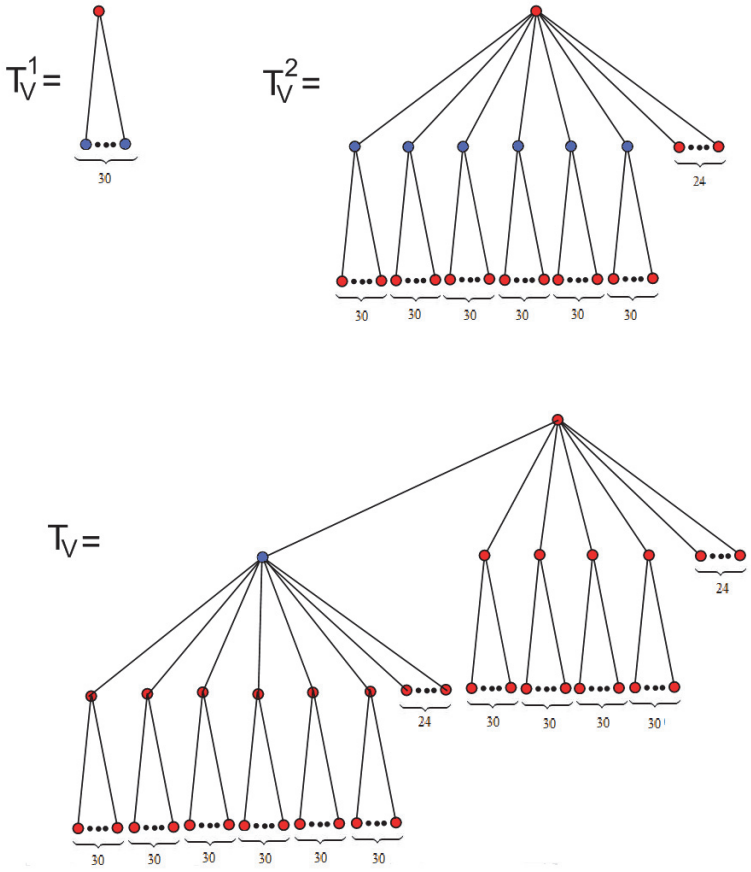

FIG. 2. *The tree associate with the* 360*-series* $V = 360(30)$.

Example 2.11. We consider the 360-series associated with 30, that is, $V = 360(30) = (30, 6, 2)$. In Figure 2 we show the inductive construction of T_V for this 360-series.

PROPOSITION 2.12. *If* $rad(\nu) \mid rad(n)$ *the tree associated with the* ν*-series generated by* n *has exactly* ν *vertices.*

Proof. If we denote by n_k the number of vertices of $T^k_{\nu(n)}$ for $0 \leq k \leq D$, the number of vertices of $T_{\nu(n)}$ is $n_D - n_{D-1}$, where the sequence $(n_k)_{0 \leq k \leq D}$ verifies

$$\begin{cases} n_0 = 1, \\ n_k = \nu_k n_{k-1} + \sum_{i=1}^{k-1} (\nu_i - \nu_{i+1}) n_{i-1} + 1 \text{ for } 1 \leq k \leq D. \end{cases}$$

We can rewrite this last recurrence relation as

$$n_k = \sum_{i=2}^{k} (n_{i-1} - n_{i-2}) \nu_i + \nu_1 n_0 + 1 \text{ for } 1 \leq k \leq D.$$

Clearly, $n_k - n_{k-1} = \nu_k (n_{k-1} - n_{k-2})$ for $2 \leq k \leq D$, which implies that the number of vertices of $T_{\nu(n)}$ is $n_D - n_{D-1} = \prod_{j=1}^{D} \nu_j = \nu$. ∎

The proof of the following lemma is immediate.

LEMMA 2.13. *If* $T = \langle T_1 \oplus T_2 \oplus \ldots \oplus T_k \rangle$, *then*

$$depth(T) = \max_{1 \le i \le k} depth(T_i) + 1.$$

PROPOSITION 2.14. *If* $T_{\nu(n)}$ *is the tree associated with* $\nu(n)$, *then*

$$depth(T_{\nu(n)}) = depth(\nu(n))$$

Proof. Let $D = depth(\nu(n))$. Using (2.1) and Lemma 2.13, we can prove by induction that $depth(T^k_{\nu(n)}) = k$. Using again Lemma 2.13 and (2.2) we have

$$depth(T_{\nu(n)}) = depth(T^{D-1}_{\nu(n)}) + 1 = (D-1) + 1 = D = depth(\nu(n)). \quad \square$$

DEFINITION 2.15. *Let* $n \ge 2$ *and* $f \ge 1$ *be integers and* $\lambda \in \mathbb{R}$ *such that* $n^\lambda = \nu \in \mathbb{Z}^+$. *We define*

$$H_n(f, \lambda) = Cyc(f, T_{\nu(n)}).$$

Remark 2.16. The following are some properties of the parameter λ that are not difficult to check:

- $H_n(f, \lambda)$ is a cycle if and only if $\lambda = 0$.
- When $\lambda \in \mathbb{N}$ this parameter represents the depth of the tree attached to the cyclic points in $H_n(f, \lambda)$.
- In general, the depth of the tree is given by the number of components of the ν-series $\nu(n)$ which is the least integer D such that $\nu \mid n^D$.
- $H_n(f, \lambda)$ has exactly fn^λ vertices.

3. Functional graph associated with the *n*-map. If m and n are positive integers we can consider the factorization $m = \nu\omega$ with $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$ and $\gcd(n, \omega) = 1$. The n-map in $\mathbb{Z}_m$ is the application $x \mapsto nx$, which we also denote by n. The main goal of this section is to describe the functional graph of this map. Part of this was done in [19], where it is proved that each connected component is of the form $Cyc(f, T)$; see also [4]. An explicit expression for the periodic part (that is, the length of the cycles and how many of them) and properties of the tree T are also given in [19]. In this section we give another characterization of T (and therefore of the functional graph) in terms of trees associated with ν-series and in terms of certain operators c_r that are defined below. We start by introducing some general notation and definitions.

DEFINITION 3.1. *Let* $g : A \to A$ *be a function defined over a finite set* A. *If* $\pi \ge 1$ *and* $\rho \ge 0$ *are the least integers such that* $g^{\pi+\rho}(u) = g^\rho(u)$, *then* u *has* period $\pi = \mathrm{per}(u)$ *and* preperiod $\rho = \mathrm{pper}(u)$ *(with respect to* g*). Moreover,* u *is a* periodic point *when* $\mathrm{pper}(u) = 0$ *and* strictly preperiodic *otherwise.*

NOTATION 3.2. *If* $g : A \to A$ *is a function defined over some finite set* A *and* $B \subseteq A$ *is such that* $g(B) \subseteq B$, *we denote by* $\mathcal{G}(g/B)$ *the functional graph of the restriction* $g|_B : B \to B$. *We also denote by* $Per(g/B) = \{x \in B : x \text{ is a periodic point}\}$. *In particular, when* $B = Per(g/A)$ *we denote by* $\mathcal{G}^{per}(g/A) = \mathcal{G}(g/B)$. *If* $x \in Per(g/A)$ *we denote by* $T_x(g/A)$ *the tree attached to* x *in the functional graph* $\mathcal{G}(g/A)$. *Sometimes when* $Per(g/A) = \{x\}$ *or the isomorphism class of* $T_x(g/A)$ *does not depend on* x *we denote* $T_x(g/A)$ *by* $T(g/A)$. *As usual, we denote by* $o_n(d)$ *the order of* d *modulo* n.

LEMMA 3.3. *Let* d *be a divisor of* ω. *If* $x \in \nu\mathbb{Z}_{\nu\omega}$ *with* $\gcd(\omega, x) = \omega/d$, *then* x *is a periodic point in* $\mathcal{G}(n/\mathbb{Z}_{\nu\omega})$ *and* $per(x) = o_n(d)$.

Proof. If $x \in \nu\mathbb{Z}_{\nu\omega}$ with $\gcd(\omega, x) = \omega/d$ we have

$$n^\pi x \equiv x \,(\mathrm{mod}\ \nu\omega) \Leftrightarrow n^\pi x \equiv x \,(\mathrm{mod}\ \omega) \Leftrightarrow n^\pi \equiv 1 \,(\mathrm{mod}\ d) \Leftrightarrow \pi \equiv 0 \,(\mathrm{mod}\ o_n(d)).$$

Then x is a periodic point in $\mathcal{G}(n/\mathbb{Z}_{\nu\omega})$ and $\mathrm{per}(x) = o_n(d)$. ∎

PROPOSITION 3.4. *We have that* $Per(n/\mathbb{Z}_{\nu\omega}) = \nu\mathbb{Z}_{\nu\omega}$ *and the following isomorphism holds:*

$$\mathcal{G}^{per}(n/\mathbb{Z}_{\nu\omega}) \simeq \bigoplus_{d|\omega} \left\{ \frac{\varphi(d)}{o_d(n)} \times Cyc(o_d(n)) \right\}.$$

Proof. By Lemma 3.3 we have $\mathrm{Per}(n/\mathbb{Z}_{\nu\omega}) \supseteq \nu\mathbb{Z}_{\nu\omega}$. For the other inclusion we observe that if there exists $\pi \geq 1$ such that $n^\pi x \equiv x \pmod{\nu\omega}$, then $(n^\pi - 1)x \equiv 0 \pmod{\nu}$. Therefore $x \equiv 0 \pmod{\nu}$ since $\gcd(n^\pi - 1, \nu) = 1$ (because $\mathrm{rad}(\nu) \mid \mathrm{rad}(n)$). This proves the first part.

For the second part we consider the partition $\nu\mathbb{Z}_{\nu\omega} = \biguplus_{d|\omega} A(d)$, where $A(d) = \{x \in \nu\mathbb{Z}_{\nu\omega} : \gcd(\omega, x) = \omega/d\}$. As $\gcd(\omega, n) = 1$ we have $nA(d) = A(d)$, and therefore

$$\mathcal{G}^{\mathrm{per}}(n/\mathbb{Z}_{\nu\omega}) = \mathcal{G}(n/\nu\mathbb{Z}_{\nu\omega}) = \bigoplus_{d|\omega} \mathcal{G}(n/A(d)). \tag{3.1}$$

By Lemma 3.3, all points in $A(d)$ have period $o_n(d)$. Hence, the graph $\mathcal{G}(n/A(d))$ is the union of $\#A(d)/o_n(d)$ cycles of length $o_n(d)$.

Finally we observe that $x \in A(d)$ if and only if $x \equiv \nu \cdot \frac{\omega}{d} \cdot u$ with $\gcd(u, d) = 1$, and for different choices of u we have different values of x. Then $\#A(d) = \varphi(d)$ and

$$\mathcal{G}(n/A(d)) \simeq \frac{\varphi(d)}{o_n(d)} \times Cyc(o_n(d)).$$

Substituting this equation into (3.1) we have the desired isomorphism. ∎

NOTATION 3.5. *For* $x \in \mathbb{Z}$ *we denote by* $\eta(x) = \min\{k \geq 0 : n^k x \equiv 0 \pmod{\nu}\}$.

Remark 3.6. We observe that $\eta(x) = depth(\nu(x))$, the depth of the ν-series generated by x.

PROPOSITION 3.7. *If* $T_a(n/\mathbb{Z}_{\nu\omega})$ *denotes the tree attached to the periodic point* a *in* $\mathcal{G}(n/\mathbb{Z}_{\nu\omega})$*, we have the following:*

(i) *The vertices of* $T_a(n/\mathbb{Z}_{\nu\omega})$ *are the elements* $b \in \mathbb{Z}_{\nu\omega}$ *such that* $b \equiv w_0^{\eta(b)} a \pmod{\omega}$*, where* $nw_0 \equiv 1 \pmod{\omega}$.

(ii) *We have the isomorphism*

$$T_a(n/\mathbb{Z}_{\nu\omega}) \simeq T_0(n/\mathbb{Z}_\nu),$$

where $T_0(n/\mathbb{Z}_\nu)$ *denotes the tree attached to* 0 *in* $\mathcal{G}(n/\mathbb{Z}_\nu)$.

Proof. (i) If $b \in T_a(n/\mathbb{Z}_{\nu\omega})$, then $a = n^k b$, where k is the least exponent such that $n^k b$ is a periodic point. By Proposition 3.4, this least exponent has to be equal to $\eta(b)$, therefore $n^{\eta(b)} b = a$. In particular $n^{\eta(b)} b \equiv a \pmod{\omega}$, and so $b \equiv w_0^{\eta(b)} a \pmod{\omega}$.

(ii) For a periodic point $a \in \mathbb{Z}_{\nu\omega}$ we consider

$$V_a = \{b \in \mathbb{Z}_{\nu\omega} : b \equiv w_0^{\eta(b)} a \pmod{\omega}\}$$

and the function $g : V_a \to V_a$ defined by

$$g(x) = \begin{cases} nx & \text{if } x \neq a, \\ a & \text{if } x = a. \end{cases}$$

We observe that the graph $\mathcal{G}(g/V_a)$ is composed of the tree $T_a(n/\mathbb{Z}_{\nu\omega})$ together with a loop in a. On the other hand, using Proposition 3.4 we have that the graph $\mathcal{G}(n/\mathbb{Z}_\nu)$ is composed of the tree $T_0(n/\mathbb{Z}_\nu)$ and a loop in 0. Therefore, it is sufficient to prove that $\mathcal{G}(g/V_a) \simeq \mathcal{G}(n/\mathbb{Z}_\nu)$. To prove this last assertion suffices to prove that the function $\pi : V_a \to \mathbb{Z}_\nu$ is a bijection and $\pi \circ g = n \circ \pi$.

The equation $\pi \circ g = n \circ \pi$ can be directly checked. To prove that π is a bijection we observe that for each $\alpha \in \mathbb{Z}_\nu$, by the Chinese remainder theorem, there exists a unique $b \in \mathbb{Z}_{\nu\omega}$ such that $b \equiv \alpha \pmod{\nu}$ and $b \equiv w_0^{\eta(\alpha)} a \pmod{\omega}$. ∎

COROLLARY 3.8. *There exists a tree $T = T(n/\mathbb{Z}_{\nu\omega})$ such that*

$$\mathcal{G}(n/\mathbb{Z}_{\nu\omega}) \simeq \bigoplus_{d|\omega} \left\{ \frac{\varphi(d)}{o_d(n)} \times Cyc(o_d(n), T) \right\}.$$

Moreover, this tree T can be obtained from the graph $\mathcal{G}(n/\mathbb{Z}_\nu)$ by deleting the loop in 0.

COROLLARY 3.9. *Let $T_0(n/\mathbb{Z}_\nu)$ be the tree attached to 0 in $\mathcal{G}(n/\mathbb{Z}_\nu)$. The isomorphism class of $T(n/\mathbb{Z}_{\nu\omega})$ does not depend on ω and $T_0(n/\mathbb{Z}_\nu)$ is a representative for this isomorphism class.*

The next objective is to prove that $T_0(n/\mathbb{Z}_\nu) = T_{\nu(n)}$. This requires a new operator on trees that we define next.

DEFINITION 3.10. *Let d and m be positive integers such that $d \mid m$ and T a rooted tree with vertices $\mathbb{Z}_m$ and root 0. We denote by $\mathcal{H}_T$ the set of leaves (vertices of in-degree 0) except for the root in the case that the tree consists only of one vertex. We say that T is a (d, m)-tree if it verifies the following conditions:*

(i) *indeg$(0) \in \{0, d-1\}$,*
(ii) *indeg$(x) = d$ if $x \notin \mathcal{H}_T, x \neq 0$,*
(iii) *$\#\mathcal{H}_T = m - \frac{m}{d}$.*

We denote by Tree(d, m) the set of all (d, m)-trees.

DEFINITION 3.11. *Let $d, m \in \mathbb{Z}^+$ with $d \mid m$ and $r = sd$ with $s \in \mathbb{Z}^+$. We define an operator*

$$c_r : Tree(d, m) \to Tree(sd, rm)$$

as follows. For $T \in Tree(d, m)$ we consider a pair $(\mathcal{P}, f)$, where $\mathcal{P}$ is a partition of $\mathbb{Z}_{rm}$ of the form $\mathcal{P} = \{D_x : x \in \mathbb{Z}_m\} \cup \{H_x : x \in \mathcal{H}_T\}$, where $\#D_x = s$ and $\#H_x = sd$ (we observe that $s \cdot \#\mathbb{Z}_m + sd \cdot \#\mathcal{H}_T = sm + sd(m - \frac{m}{d}) = rm$). The set D_x is called the set of duplicates of x and the set H_x is the set of new predecessors of x. The function $f : \mathbb{Z}_m \to \mathbb{Z}_{rm}$ satisfies $f(0) = 0$ and $f(x) \in D_x$ for all $x \in \mathbb{Z}_m$.

If $\rho_T(x)$ denotes the set of predecessors of x in T, we define the rooted tree $c_r(T) = \widetilde{T}$ whose vertices are $\mathbb{Z}_{rm}$, the root is 0, the set of leaves is $\mathcal{H}_{\widetilde{T}} = \mathbb{Z}_{rm} \setminus Im(f)$, and for the other vertices we have

$$\begin{aligned} \rho_{\widetilde{T}}(0) &= \biguplus_{y \in \rho_T(0)} D_y \uplus (D_0 \setminus \{0\}), \\ \rho_{\widetilde{T}}(f(x)) &= \biguplus_{y \in \rho_T(x)} D_y && \text{if } x \notin \mathcal{H}_T, x \neq 0, \\ \rho_{\widetilde{T}}(f(x)) &= H_x && \text{if } x \in \mathcal{H}_T, x \neq 0. \end{aligned}$$

Remark 3.12. Informally, if $T \in \text{Tree}(d, m)$ and $r = sd$ we obtain $c_r(T)$ attaching $d(s-1)$ new directed predecessors to each nonleaf vertex of T and attaching r new directed predecessors to each leaf of T.

PROPOSITION 3.13. *If $T \in Tree(d, m)$ with $d \mid m$ and $\widetilde{T} = c_r(T)$, where $r = sd$ with $s \in \mathbb{Z}^+$ (for some choice of pair $(\mathcal{P}, f)$ as in Definition 3.11), we have*

(i) $\widetilde{T} \in \mathit{Tree}(sd, rm)$;
(ii) *the function* $f : \mathbb{Z}_m \to \mathbb{Z}_{rm}$ *induce an injective homomorphism between* T *and* $\widetilde{T}$;
(iii) *the isomorphism class of* $c_r(t) = \widetilde{T}$ *does not depend on the choice of the pair* $(\mathcal{P}, f)$.

Proof. i) If $m = 1$, then $d = 1$ and $r = s \in \mathbb{Z}^+$. In this case, by construction, we have $\mathcal{H}_{\widetilde{T}} = \mathbb{Z}_r \setminus \{0\}$, which implies $\mathrm{indeg}(0) = r - 1$ and $\#\mathcal{H}_{\widetilde{T}} = r - 1 = r - \frac{r}{s}$, therefore $\widetilde{T} \in \mathrm{Tree}(s, r)$.

For $m > 1$ we have

$$\mathrm{indeg}(0) = \#\rho_{\widetilde{T}}(0) = s \cdot \#\rho_T(0) + s - 1 = s(d-1) + s - 1 = sd - 1.$$

For $x \notin \mathcal{H}_T, x \neq 0$ we have

$$\mathrm{indeg}(f(x)) = \#\rho_{\widetilde{T}}(f(x)) = s \cdot \#\rho_T(x) = sd.$$

For $x \in \mathcal{H}_T, x \neq 0$ we have

$$\mathrm{indeg}(f(x)) = \#H_x = sd.$$

With respect to the leaves, $\#\mathcal{H}_{\widetilde{T}} = rm - \#\mathrm{Im}(f) = rm - m = rm - \frac{rm}{sd}$, and therefore $\widetilde{T} \in \mathrm{Tree}(s, r)$.

(ii) The fact that f is injective follows from the fact that $\mathcal{P}$ is a partition. On the other hand, by construction we have $D_y \subseteq \rho_{\widetilde{T}}(f(x))$ for all $y \in \rho_T(x)$. Hence, $y \in \rho_T(x)$ implies $f(y) \in D_y \subseteq \rho_{\widetilde{T}}(f(x))$, which proves that f is a homomorphism between T and $\widetilde{T}$.

(iii) We consider $\widetilde{T}_1$ and $\widetilde{T}_2$ two constructions of $c_r(T)$, using the pairs $(\mathcal{P}_1, f_1)$ and $(\mathcal{P}_2, f_2)$, respectively. The partitions are of the form

$$\mathcal{P}_i = \{D_x^i : x \in \mathbb{Z}_m\} \cup \{H_x^i : x \in \mathcal{H}_T\} \quad \text{for } i = 1, 2.$$

Let $F : \mathbb{Z}_{rm} \to \mathbb{Z}_{rm}$ be a bijection that satisfies
(1) $F(f_1(x)) = f_2(x)$ for all $x \in \mathbb{Z}_m$,
(2) $F(D_x^1) = D_x^2$ for all $x \in \mathbb{Z}_m$,
(3) $F(H_x^1) = H_x^2$ for all $x \in \mathcal{H}_T$.

We prove next that F is an isomorphism between $\widetilde{T}_1$ and $\widetilde{T}_2$.

First, we observe that $F(\mathcal{H}_{\widetilde{T}_1}) = \mathbb{Z}_{rm} \setminus F(\mathrm{Im}(f_1)) = \mathbb{Z}_{rm} \setminus \mathrm{Im}(f_2) = \mathcal{H}_{\widetilde{T}_2}$, that is, F maps leaves into leaves. Moreover, it follows from (1), (2), and (3) that $F(\rho_{\widetilde{T}_1}(f_1(x))) = \rho_{\widetilde{T}_2}(F(f_1(x)))$ for all $x \in \mathbb{Z}_m$, which prove that F is an isomorphism, and then $\widetilde{T}_1$ and $\widetilde{T}_2$ are isomorphic. ∎

Now, we can obtain a new characterization of the trees T_V, where V is a ν-series.

LEMMA 3.14. *If* $V = (\nu_1, \nu_2, \ldots, \nu_D)$ *is a* ν*-series, then*

$$T_V = c_{\nu_1} \circ c_{\nu_2} \circ \cdots \circ c_{\nu_D}(\bullet),$$

where $\bullet$ *denotes the tree with one vertex* $0 \in \mathbb{Z}_1$.

Proof (sketch of the proof). If T is a tree, the *defoliate* of T is another tree T' obtained from T by removing all its leaves. Since $T_1 \simeq T_2$ implies that $T_1' \simeq T_2'$, the defoliate is well defined on isomorphism classes of trees. Other important properties of the defoliate are $(T_1 \oplus T_2)' = T_1' \oplus T_2'$, $(n \times T)' = n \times T'$, and $\langle T_1, T_2, \ldots, T_k \rangle' = \langle T_1', T_2', \ldots, T_k' \rangle$ if at least one of the T_i is nonempty (by convention $\emptyset' = \emptyset$). Using

the recursive definition of T_V we have that $T'_V \simeq T_{V'}$, where $V' = (\nu_2, \dots, \nu_D)$ is a ν'-series, where $\nu' = \frac{\nu}{\nu_1}$.

As above, $\rho_T(x)$ denotes the set of predecessors of x in T, $\mathcal{H}_T$ denotes the set of leaves in T, and we define $\rho_T^h(x) = \rho_T(x) \cap \mathcal{H}_T$ and $\text{indeg}^h(x) = \#\rho_T^h(x)$.

We can choose T a representative of T_V and T_0 a representative of $T_{V'}$ with vertices $\mathbb{Z}_\nu$ and $\mathbb{Z}_{\nu'}$, respectively, and root $0 \in \mathbb{Z}_\nu$ and $0 \in \mathbb{Z}_{\nu'}$, respectively. Since $T'_V = T_{V'}$ we can define an injective homomorphism of trees $f : T_0 \to T$. Counting predecessors in T, we obtain $\text{indeg}(0) = \frac{\nu_1}{\nu_2} \cdot \text{indeg}^h(0) + \frac{\nu_1}{\nu_2} - 1$ and

- $\text{indeg}(f(x)) = \frac{\nu_1}{\nu_2} \cdot \text{indeg}^h(f(x))$ for $x \notin \mathcal{H}_{T_0}, x \neq 0$,
- $\text{indeg}(f(x)) = \nu_1$ for $x \in \mathcal{H}_{T_0}, x \neq 0$.

This property allows us to define a partition $\mathcal{P}$ as in Definition 3.11 and we obtain that $T = c_{\nu_1}(T_0)$. Applying this several times we obtain the equivalence between both definitions of T_V. ∎

LEMMA 3.15. *Let n and ν be integers such that rad(ν) | rad(n). We denote by $\nu_1 = \gcd(n, \nu)$ and by $\nu' = \frac{\nu}{\nu_1}$. We have that $T_0(n/\mathbb{Z}_\nu) \in Tree(\nu_1, \nu)$ and $T_0(n/\mathbb{Z}_\nu) = c_{\nu_1}(T_0(n/\mathbb{Z}_{\nu'}))$.*

Proof. For $\nu = 1$ we have $T_0(n/\mathbb{Z}_\nu) = \bullet$ the tree with only one vertex and it is clear that this tree belongs to Tree$(1, 1)$. If $\nu > 1$, then $\nu' < \nu$ (because $\text{rad}(\nu) \mid \text{rad}(n)$), and by Proposition 3.13 it is sufficient to prove that $T_0(n/\mathbb{Z}_\nu) = c_{\nu_1}(T_0(n/\mathbb{Z}_{\nu'}))$ assuming $T_0(n/\mathbb{Z}_{\nu'}) \in \text{Tree}(\nu_2, \nu')$, where $\nu_2 = \gcd(n, \nu')$.

Hence, we can assume $\nu > 1$ and if we denote by $T = T_0(n/\mathbb{Z}_\nu)$ and $T' = T_0(n/\mathbb{Z}_{\nu'})$ we prove that $T = C_{\nu_1}(T')$ from some adequate choice of $(\mathcal{P}, f)$.

We define the function $f : \mathbb{Z}_{\nu'} \to \mathbb{Z}_\nu$ as $f(x) = \nu_1 x \pmod{\nu}$. This function is well defined because $\nu/\nu_1 = \nu'$. We also define the partition $\mathcal{P} = \{D_t : t \in \mathbb{Z}_{\nu'}\} \cup \{H_t : t \in \mathcal{H}_{T'}\}$, where

$$D_t = \left\{ \nu_1 t + k\nu' : 0 \leq k < \frac{\nu_1}{\nu_2} \right\} \qquad \text{for } t \in \mathbb{Z}_{\nu'},$$
$$H_t = \{\omega_0 t + k\nu' : 0 \leq k < \nu_1\} \qquad \text{for } t \in \mathcal{H}_{T'},$$

and where ω_0 is such that $\omega_0 \cdot (\frac{n}{\nu_1}) \equiv 1 \pmod{\nu'}$.

To prove that the sets D_t are disjoint and $\#D_t = \nu_1/\nu_2$ suffices to prove that for $t_1, t_2 \in \mathbb{Z}_{\nu'}$ and $0 \leq k_1, k_2 < \nu_1/\nu_2$, the congruence $\nu_1 t_1 + k_1\nu' \equiv \nu_1 t_2 + k_2\nu' \pmod{\nu}$ implies $k_1 = k_2$ and $t_1 = t_2$. We have that $\nu_1 t_1 + k_1\nu' \equiv \nu_1 t_2 + k_2\nu' \pmod{\nu}$ implies $k_1\nu' \equiv k_2\nu' \pmod{\nu_1}$, that is, $k_1 \equiv k_2 \pmod{\frac{\nu_1}{\nu_2}}$ (since $\gcd(\nu_1, \nu') = \nu_2$) and so $k_1 = k_2$. Now, $\nu_1 t_1 \equiv \nu_1 t_2 \pmod{\nu}$ implies $t_1 \equiv t_2 \pmod{\nu'}$, and so $t_1 = t_2$.

To prove that the sets H_t are disjoint and $\#H_t = \nu_1$ suffices to prove that for $t_1, t_2 \in \mathcal{H}_{T'}$ and $0 \leq k_1, k_2 < \nu_1$, the congruence $\omega_0 t_1 + k_1\nu' \equiv \omega_0 t_2 + k_2\nu' \pmod{\nu}$ implies $t_1 = t_2$ and $k_1 = k_2$. We have that $\omega_0 t_1 + k_1\nu' \equiv \omega_0 t_2 + k_2\nu' \pmod{\nu}$ implies $t_1 \equiv t_2 \pmod{\nu'}$ (because $\gcd(\omega_0, \nu') = 1$) and so $t_1 = t_2$. Now, $k_1\nu' \equiv k_2\nu' \pmod{\nu}$ implies $k_1 \equiv k_2 \pmod{\nu_1}$, and so $k_1 = k_2$.

As $D_t \subset \nu_2\mathbb{Z}_\nu$ for all $t \in \mathbb{Z}_{\nu'}$ and $H_t \cap \nu_2\mathbb{Z}_\nu = \emptyset$ for all $t \in \mathcal{H}_{T'}$ (because $t \in \mathcal{H}_{T'}$ implies $t \not\equiv 0 \pmod{\nu_2}$) we have that the sets in $\mathcal{P}$ are disjoint. Computing cardinalities we can conclude that $\mathcal{P}$ is a partition. It is immediate to check that $f(t) = \nu_1 t \in D_t$ for all $t \in \mathbb{Z}_{\nu'}$ and so we have $T = c_{\nu_1}(T')$. ∎

THEOREM 3.16. *Let n and ν be integers such that rad(ν) | rad(n); then*

$$T(n/\mathbb{Z}_\nu) = T_{\nu(n)}.$$

Proof. If $\nu(n) = (\nu_1, \nu_2, \dots, \nu_D)$, applying several times Lemma 3.15 we have

$$\begin{aligned} T(n/\mathbb{Z}_\nu) &= c_{\nu_1}(T(n/\mathbb{Z}_{\frac{\nu}{\nu_1}}) = c_{\nu_1} \circ c_{\nu_2}(T(n/\mathbb{Z}_{\frac{\nu}{\nu_1\nu_2}})) = \cdots \\ &= c_{\nu_1} \circ c_{\nu_2} \circ \cdots \circ c_{\nu_D}(T(n/\mathbb{Z}_1)) = T_{\nu(n)}, \end{aligned}$$

where in the last equation we use $T(n/\mathbb{Z}_1) = \bullet$ and Lemma 3.14. ∎

4. Application to Rédei functions. In this section we show how to translate dynamic properties of the n-map to the case of Rédei functions. Using results of the previous section we can obtain a complete description of the functional graph of Rédei function and a formula for the period and preperiod of points. We obtain a more explicit description for a special case and use it to obtain Rédei functions with prescribed cycles with length in a geometric progression that extends results obtained in [18].

We start this section by introducing some preliminaries about Rédei functions.

4.1. Background on Rédei functions. There are several equivalent definitions for Rédei function. The classical definition considers the binomial expansion $(x + \sqrt{y})^n = N(x, y) + D(x, y)\sqrt{y}$. Then, the *Rédei function* $R_n(x, a)$ defined over $\mathbb{P}^1(\mathbb{F}_q) := \mathbb{F}_q \cup \{\infty\}$ for $a \in \mathbb{F}_q$ is $R_n(x, a) = \frac{N(x,a)}{D(x,a)}$. Table 1 gives the first few Rédei functions for $a \in \mathbb{F}_q$.

TABLE 1
First few Rédei functions $R_n(x, a)$ for $a \in \mathbb{F}_q$.

$R_1(x, a)$	$= x$
$R_2(x, a)$	$= (x^2 + a)/2x$
$R_3(x, a)$	$= (x^3 + 3ax)/(3x^2 + a)$
$R_4(x, a)$	$= (x^4 + 6ax^2 + a^2)/(4x^3 + 4ax)$
$R_5(x, a)$	$= (x^5 + 10ax^3 + 5a^2x)/(5x^4 + 10ax^2 + a^2)$
$R_6(x, a)$	$= (x^6 + 15ax^4 + 15a^2x^2 + a^3)/(6x^5 + 20ax^3 + 6a^2x)$
$R_7(x, a)$	$= (x^7 + 21ax^5 + 35a^2x^3 + 7a^3x)/(7x^6 + 35ax^4 + 21a^2x^2 + a^3)$

The most convenient way of writing Rédei functions for us is due to Carlitz [3]. For a fixed $a \in \mathbb{F}_q^*$ we define

$$R_n(x, a) = \sqrt{a}\, \frac{(x + \sqrt{a})^n + (x - \sqrt{a})^n}{(x + \sqrt{a})^n - (x - \sqrt{a})^n} \quad \text{if } \operatorname{char}(\mathbb{F}_q) \neq 2.$$

In this section, we consider the Möbius function over finite fields defined as $\gamma(u) = \frac{u+\sqrt{a}}{u-\sqrt{a}}$ for $u \in \mathbb{P}^1(\mathbb{F}_q)$, with $\gamma(u) = \infty$ if $u = \sqrt{a}$. Then we can write

$$R_n(x, a) = \sqrt{a}\, \frac{\gamma(x)^n + 1}{\gamma(x)^n - 1}, \tag{4.1}$$

where we use the standard rules when $\gamma(x) = \infty$, that is, $\infty^n = \infty$, $\frac{\infty}{\infty} = 1$, and $\infty \pm 1 = \infty$. If we define $R_n(x, a) = \infty$ when the denominator vanishes, we have a mapping $R_n : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$. We are interested in understanding the functional graph of this mapping.

One important property of Rédei functions that we use in this section is that $R_n \circ R_m = R_{nm}$ for fixed $a \in \mathbb{F}_q^*$ and n, m positive integers; see [16].

Another classical result that we use is that the Rédei function $R_n(x,a)$ induces a permutation function on $\mathbb{P}^1(\mathbb{F}_q)$ if and only if $\gcd(n, q-\chi(a)) = 1$, where χ is the quadratic character in $\mathbb{F}_q^*$ (that is, $\chi(a) = 1$ if a is a square in $\mathbb{F}_q^*$, and -1 otherwise). This is a well-known fact about Rédei functions; see, for example, [3, 16]. Partial results giving the description in disjoint cycles of Rédei functions are presented in [18].

Rédei functions have been applied in many areas such as in pseudorandom number generators [7, 8, 13], in cryptography [14], to solve Pell equations [1], for interleavers in turbo codes [18], and to solve a conjecture about permutation trinomials [23].

4.2. The functional graph of Rédei functions.

LEMMA 4.1. *Let $a \in \mathbb{F}_q^*$ be a nonsquare element in a nonbinary finite field; then we have $\gamma(\mathbb{P}^1(\mathbb{F}_q)) = U$, the multiplicative subgroup of order $q+1$ of $\mathbb{F}_{q^2}$.*

Proof. Since $\chi(a) = -1$ we have $\gamma(\mathbb{P}^1(\mathbb{F}_q)) \subseteq \mathbb{F}_{q^2}$. Let $x, y \in \mathbb{P}^1(\mathbb{F}_q)$. We need to prove that $\gamma(x)\gamma(y) \in \gamma(\mathbb{P}^1(\mathbb{F}_q))$. If $x = \infty$ or $y = \infty$, the assertion is clear. Otherwise we have

$$\gamma(x)\gamma(y) = \frac{x+\sqrt{a}}{x-\sqrt{a}} \cdot \frac{y+\sqrt{a}}{y-\sqrt{a}} = \frac{xy+a+(x+y)\sqrt{a}}{xy+a-(x+y)\sqrt{a}}$$
$$= \begin{cases} 1 = \gamma(\infty) & \text{if } x+y = 0, \\ \gamma\left(\frac{xy+a}{x+y}\right) & \text{if } x+y \neq 0. \end{cases}$$

In both cases we have $\gamma(x)\gamma(y) \in \gamma(\mathbb{P}^1(\mathbb{F}_q))$. ∎

When a is a square over $\mathbb{F}_q^*$ we restrict the domain of $R_n(x,a)$ to the set $\mathbb{D}_q = \mathbb{P}^1(\mathbb{F}_q)\backslash\{\pm\sqrt{a}\}$. Since in this case $\sqrt{a}$ and $-\sqrt{a}$ are isolated fixed point, the functional graphs of the Rédei function over $\mathbb{P}^1(\mathbb{F}_q)$ and $\mathbb{D}_q$ are essentially the same. When $a \in \mathbb{F}_q^*$ is a nonsquare element we define $\mathbb{D}_q = \mathbb{P}^1(\mathbb{F}_q)$.

From here we denote $\mathcal{G}(n,a,q)$ by $\mathcal{G}(R_n(x,a)/\mathbb{D}_q)$ and we denote $\mathcal{G}^{\mathrm{per}}(n,a,q)$ by $\mathcal{G}^{\mathrm{per}}(R_n(x,a)/\mathbb{D}_q)$. The function γ is injective and $\gamma(\mathbb{D}_q) = U_{q+1}$ the multiplicative subgroup of order $q+1$ of $\mathbb{F}_{q^2}$ when $\chi(a) = -1$ (Lemma 4.1) or $\gamma(\mathbb{D}_q) = \mathbb{F}_q^*$ when $\chi(a) = 1$. If $R_n(x) = R_n(x,a)$ we have by direct calculation that in both cases $\gamma \circ R_n(x) = x^n \circ \gamma(x)$ for all $x \in \mathbb{D}_q$ and therefore the following diagram commutes:

$$\text{if } \chi(a) = -1: \quad \begin{array}{ccc} \mathbb{D}_q & \xrightarrow{R_n} & \mathbb{D}_q \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\gamma} \\ U_{q+1} & \xrightarrow{x^n} & U_{q+1} \end{array} \qquad \text{if } \chi(a) = 1: \quad \begin{array}{ccc} \mathbb{D}_q & \xrightarrow{R_n} & \mathbb{D}_q \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\gamma} \\ \mathbb{F}_q^* & \xrightarrow{x^n} & \mathbb{F}_q^* \end{array}$$

We observe that if G is a multiplicative cyclic group of order m, then $x^n : G \to G$ is conjugate to $n : \mathbb{Z}_m \to \mathbb{Z}_m$ (multiplication by m) via any isomorphism $\varphi : G \to \mathbb{Z}_m$ and so $\mathcal{G}(x^n/G) \simeq \mathcal{G}(n/\mathbb{Z}_m)$. Since both U_{q+1} and $\mathbb{F}_q^*$ are multiplicative cyclic groups we have the following proposition.

PROPOSITION 4.2. *Let $n \in \mathbb{Z}^+$ and $\mathbb{F}_q$ be a finite field and $a \in \mathbb{F}_q^*$. We have*

- $\mathcal{G}(n,a,q) \simeq \mathcal{G}(x^n/U_{q+1}) \simeq \mathcal{G}(n/\mathbb{Z}_{q+1})$ *if* $\chi(a) = -1$,
- $\mathcal{G}(n,a,q) \simeq \mathcal{G}(x^n/\mathbb{F}_q^*) \simeq \mathcal{G}(n/\mathbb{Z}_{q-1})$ *if* $\chi(a) = 1$.

If $q-\chi(a)=\nu\omega$ with $\mathrm{rad}(\nu)|\mathrm{rad}(n)$ and $\gcd(\omega,n)=1$, we have in both cases $\mathcal{G}(n,a,q)\simeq\mathcal{G}(n/\mathbb{Z}_{\nu\omega})\simeq\mathcal{G}(n/\mathbb{Z}_\nu\times\mathbb{Z}_\omega)$, where the last isomorphism is via the remainder Chinese theorem since $\gcd(\nu,\omega)=1$.

We denote by $\{\bullet\}$ any graph consisting of a unique vertex v with a loop (v,v). If we apply the above observations together Definition 2.15, Corollary 3.8, and Theorem 3.16 we obtain the following proposition.

THEOREM 4.3. *Let $n\in\mathbb{Z}^+$, $a\in\mathbb{F}_q^*$ and $\mathcal{G}(n,a,q)$ the functional graph of the Rédei function $R_n(x,a)$ as a map over $\mathbb{P}^1(\mathbb{F}_q)$. We express $q-\chi(a)=\nu\omega$ with $rad(\nu)\mid rad(n)$ and $\gcd(n,\omega)=1$. If $\lambda\in\mathbb{R}$ is such that $n^\lambda=\nu$, then*

$$\mathcal{G}(n,a,q)\simeq\bigoplus_{d|\omega}\left\{\frac{\varphi(d)}{o_d(n)}\times H_n(o_d(n),\lambda)\right\}\oplus(1+\chi(a))\times\{\bullet\}.$$

Example 4.4. Let us describe the structure of the functional graph associated with $R_3(x,1)=\frac{x^3+3x}{3x^2+1}$ over $P^1(\mathbb{F}_{37})$. First, we have $q-\chi(a)=36=3^2\cdot2^2$, and so $n=3$, $\lambda=2$, and $\omega=4$. Using Theorem 4.3 we get (see Figure 3)

$$\begin{aligned}\mathcal{G}(3,1,37)&\simeq\bigoplus_{d|4}\left\{\frac{\varphi(d)}{o_d(3)}\times H_3(o_d(3),2)\right\}\oplus\{\bullet,\bullet\}\\&\simeq 2\times H_3(1,2)\oplus H_3(2,2)\oplus\{\bullet,\bullet\}.\end{aligned}$$

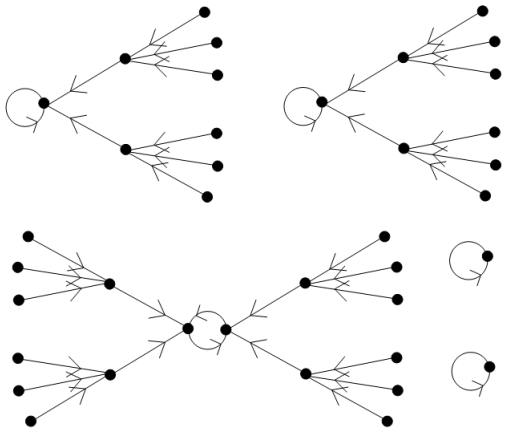

FIG. 3. *Structure of the functional graph associated with $R_3(x,1)=\frac{x^3+3x}{3x^2+1}$ over $P^1(\mathbb{F}_{37})$.*

An important consequence of Theorem 4.3 is that it allows us to obtain a formula for the period and preperiod of Rédei functions.

PROPOSITION 4.5. *Let $\mathcal{G}(n,a,q)$ be the functional graph of the Rédei function $R_n(x,a)$ as a map over $\mathbb{P}^1(\mathbb{F}_q)$ and $q-\chi(a)=\nu\omega$ with $rad(\nu)\mid rad(n)$ and $\gcd(n,\omega)=1$. If $u\in\mathbb{P}^1(\mathbb{F}_q)$ and we express the multiplicative order over $\mathbb{F}_{q^2}$ as $\mathrm{ord}(\gamma(u))=\nu_u d$ with $rad(\nu_u)\mid rad(n)$ and $\gcd(n,d)=1$ (by convention $\mathrm{ord}(\infty)=\mathrm{ord}(0)=1$) we have that $\nu_u\mid\nu$, $d\mid\omega$ and*

- $\mathrm{per}(u)=\mathrm{ord}_d(n)$,
- $\mathrm{pper}(u)=depth(\nu_u(n))=\min\{t\in\mathbb{Z}^+:\nu_u\mid n^t\}$.

There is a special case of interest when $\omega=p^\alpha$ or $\omega=2p^\alpha$, where p is an odd prime and α is a positive integer. In this case it is possible to obtain a more explicit

representation of the functional graph. We recall that ω is such that $q-\chi(a)=\nu\omega$ with $\mathrm{rad}(\nu)\mid\mathrm{rad}(n)$ and $\gcd(n,\omega)=1$.

THEOREM 4.6. *Let n,a,q,λ, and ω be as in Theorem 4.3 with the additional condition $\omega=p^\alpha$ if n is even or $\omega=2p^\alpha$ if n is odd, where p is an odd prime. Let $\eta=\frac{\varphi(\omega)}{o_\omega(n)}=p^h\kappa$ with $p\nmid\kappa$ and $f=\frac{p-1}{\kappa}$. We have the following isomorphism for the functional graph associated with the Rédei function $R_n(x,a)$ over $\mathbb{P}^1(\mathbb{F}_q)$.*

For n even,

$$\mathcal{G}(n,a,q)\simeq H_n(1,\lambda)\oplus\frac{p^{h+1}-1}{f}\times H_n(f,\lambda)\oplus\bigoplus_{i=h+2}^{\alpha}\{\kappa p^h\times H_n(fp^{i-h-1},\lambda)\}\oplus(1+\chi(a))\times\{\bullet\},$$

and for n odd,

$$\mathcal{G}(n,a,q)\simeq 2\times H_n(1,\lambda)\oplus\frac{2(p^{h+1}-1)}{f}\times H_n(f,\lambda)\oplus\bigoplus_{i=h+2}^{\alpha}\{2\kappa p^h\times H_n(fp^{i-h-1},\lambda)\}\oplus(1+\chi(a))\times\{\bullet\}.$$

Proof. We observe first that

$$\eta=\frac{\varphi(\omega)}{o_\omega(n)}=\frac{p^{\alpha-1}(p-1)}{o_\omega(n)}=p^h\kappa \tag{4.2}$$

with $0\le h\le\alpha-1$ and $\kappa\mid p-1$.

Let r be a primitive root modulo ω (and therefore a primitive root modulo d, for all $d\mid\omega$). As $\gcd(n,\omega)=1$, then $n\equiv r^t \pmod{\omega}$ for some integer t, $1\le t\le\varphi(\omega)$. Changing r for another primitive root if it is necessary, we can suppose that $t\mid\varphi(\omega)$ and in this case we have

$$o_\omega(n)=o_\omega(r^t)=\frac{o_\omega(r)}{\gcd(t,\varphi(\omega))}=\frac{\varphi(\omega)}{t}.$$

Comparing with (4.2) we conclude that $t=\eta$ and $n\equiv r^\eta \pmod{\omega}$.

For $d\mid\omega$ of the form $d=p^i$ or $d=2p^i$ with $1\le i\le\alpha$ we have

$$o_d(n)=o_d(r^\eta)=\frac{o_d(r)}{\gcd(o_d(r),\eta)}=\frac{\varphi(d)}{\gcd(\varphi(d),\eta)}=\frac{p^{i-1}(p-1)}{\gcd(p^{i-1}(p-1),p^h\kappa)}$$
$$=\frac{p^{i-1}(p-1)}{p^{\min(i-1,h)}\kappa}=p^{\max(i-1-h,0)}f=\begin{cases}f & \text{if } i\le h+1,\\ p^{i-h-1}f & \text{if } h+1<i\le\alpha.\end{cases}$$

Then, we can rewrite Theorem 4.3 in the following way. For n even,

$$\mathcal{G}(n,a,q)=\frac{\varphi(1)}{o_1(n)}\times H_n(1,\lambda)\oplus\left(\sum_{i=1}^{h+1}\frac{\varphi(p^i)}{o_{p^i}(n)}\right)\times H_n(f,\lambda)\oplus\bigoplus_{i=h+2}^{\alpha}\left\{\frac{\varphi(p^i)}{o_{p^i}(n)}\times H_n(fp^{i-h-1},\lambda)\right\}\oplus(1+\chi(a))\times\{\bullet\}.$$

For n odd,

$$\mathcal{G}(n,a,q) = \left(\frac{\varphi(1)}{o_1(n)} + \frac{\varphi(2)}{o_2(n)}\right) \times H_n(1,\lambda) \oplus \left(\sum_{i=1}^{h+1} \frac{\varphi(p^i)}{o_{p^i}(n)} + \frac{\varphi(2p^i)}{o_{2p^i}(n)}\right) \times H_n(f,\lambda)$$
$$\oplus \bigoplus_{i=h+2}^{\alpha} \left\{ \left(\frac{\varphi(p^i)}{o_{p^i}(n)} + \frac{\varphi(2p^i)}{o_{2p^i}(n)}\right) \times H_n(fp^{i-h-1},\lambda) \right\} \oplus (1+\chi(a)) \times \{\bullet\}.$$

Note that for n odd and $i \geq 1$ we have $\varphi(p^i) = \varphi(2p^i)$ and $o_{p^i}(n) = o_{2p^i}(n)$, therefore $\frac{\varphi(p^i)}{o_{p^i}(n)} + \frac{\varphi(2p^i)}{o_{2p^i}(n)} = 2\frac{\varphi(p^i)}{o_{p^i}(n)}$.

We conclude the proof observing that in both cases we have

$$\sum_{i=1}^{h+1} \frac{\varphi(p^i)}{o_{p^i}(n)} = \sum_{i=1}^{h+1} \frac{p^{i-1}(p-1)}{f} = \kappa \sum_{i=1}^{h+1} p^{i-1} = \kappa \cdot \frac{p^{h+1}-1}{p-1} = \frac{p^{h+1}-1}{f},$$

and for $h+1 < i \leq \alpha$, we have

$$\frac{\varphi(p^i)}{o_{p^i}(n)} = \frac{p^{i-1}(p-1)}{p^{i-1-h}f} = \kappa p^h. \qquad \square$$

4.3. Rédei permutations and their cycle decomposition. Here we give other corollaries than can be obtained from Theorem 4.3 related to the cycle decomposition. In particular we give a way to construct Rédei functions whose length cycles are in arithmetic progression that extend results obtained in [18].

COROLLARY 4.7. *The Rédei function $R_n(x,a)$ induces a permutation of $\mathbb{P}^1(\mathbb{F}_q)$ if and only if* $\gcd(n, q-\chi(a)) = 1$. *In this case we have the following decomposition in disjoint cycles:*

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

where $Cyc(c)$ denotes a directed cycle of length c.

Proof. As a consequence of Theorem 4.3 it is easy to conclude that $R_n(x,a)$ induces a permutation if and only if $\lambda = 0$ (Remark 2.16). This is equivalent to $\gcd(n, q-\chi(a)) = 1$. In this case each $H_n\left(o_d(n),\lambda\right) = Cyc\left(o_d(n)\right)$, and so it is a directed cycle of length $o_d(n)$. $\square$

COROLLARY 4.8. *The number of fixed points of $R_n(x,a)$ over $\mathbb{P}^1(\mathbb{F}_q)$ is given by the formula*

$$\gcd\left(n-1, q-\chi(a)\right) + \left(1+\chi(a)\right).$$

This corollary can be seen as a consequence of the following more general result (by taking $k=1$).

COROLLARY 4.9. *Let k be a positive integer. The number of points of $R_n(x,a)$ over $\mathbb{P}^1(\mathbb{F}_q)$ whose period divide k is given by the formula*

$$\gcd\left(n^k-1, q-\chi(a)\right) + \left(1+\chi(a)\right).$$

Proof. We consider the set $P_k = \{x \in \mathbb{P}^1(\mathbb{F}_q) : \mathrm{per}(x) \mid k\}$. If $x \in P_k$, x belongs to a connected component $H_n(o_d(n),\lambda)$ with $o_d(n) \mid k$. Now, $o_d(n) \mid k$ if and only if $n^k \equiv 1 \pmod{d}$ if and only if $d \mid n^k - 1$.

On the other hand, each component $H_n(o_d(n), \lambda)$ with $d \mid n^k - 1$ has exactly $o_d(n)$ points in P_k, so

$$\begin{aligned}\#P_k &= \sum_{d|\omega, d|n^k-1} \left\{ \frac{\varphi(d)}{o_d(n)} \cdot o_d(n) \right\} + (1 + \chi(a)) \\ &= \sum_{d|\gcd(n^k-1,\omega)} \varphi(d) + (1 + \chi(a)) = \gcd(n^k - 1, \omega) + (1 + \chi(a)) \\ &= \gcd(n^k - 1, q - \chi(a)) + (1 + \chi(a)). \quad \square\end{aligned}$$

Remark 4.10. Corollary 4.9 gives an alternative way to prove Theorem 3.14 of [18]. If we denote by N_j the number of cycles of length j, we obtain

$$jN_j + \sum_{i|j, i<j} iN_i = \gcd(n^j - 1, q - \chi(a)) + (1 + \chi(a)).$$

In particular, when $\chi(a) = -1$ the ∞ point is an isolated fixed point and we can consider $R_n(x, a) : \mathbb{F}_q \to \mathbb{F}_q$. In this case we have

$$jN_j + \sum_{i|j, i<j} iN_i = \gcd(n^j - 1, q - \chi(a)) - 1$$

as stated in Theorem 3.14 of [4].

The following corollary that characterizes Rédei permutations with cycles of length 1 and j (where j is an integer greater than 1) appears in [18] and can be seen as a direct consequence of Theorem 4.3.

COROLLARY 4.11 (Theorem 3.15 of [18]). *If* $\gcd(n, q + 1) = 1$ *and* $\chi(a) = -1$, *then the Rédei permutation* $R_n(x, a)$ *has all its cycles of length* 1 *or* j *if and only if for every divisor* d *of* $q + 1$ *we have* $n \equiv 1 \pmod d$ *or* $j = \mathrm{ord}_d(n)$.

Proof. The length of the cycles is given by $o_d(n) = \mathrm{ord}_d(n)$, where d runs over the divisors of $q + 1$ and $\mathrm{ord}_d(n) = 1$ if and only if $n \equiv 1 \pmod d$. $\square$

A naive generalization of the above corollary is given next. It can be proved in the same way as above.

COROLLARY 4.12. *If* $\gcd(n, q+1) = 1$ *and* $\chi(a) = -1$, *then the Rédei permutation* $R_n(x, a)$ *has all its cycles of length belonging to a set* $S = \{1, j_1, \ldots, j_t\}$ *if and only if for every divisor* d *of* $q + 1$ *we have* $\mathrm{ord}_d(n) \in S$.

COROLLARY 4.13. *The length of the largest cycle in* $\mathcal{G}(n, a, q)$ *is* $m = \mathrm{ord}_\omega(n)$, *where* $q - \chi(a) = n^\lambda \omega$ *and* $n \nmid \omega$ *as in Theorem* 4.3.

Proof. The lengths of the cycles are given by $o_d(n)$, where d runs over the divisors of ω. If d is a divisor of ω we have $n^m \equiv 1 \pmod \omega$ if and only if $n^m \equiv 1 \pmod d$ if and only if $o_d(n) \mid m$ and thus $m \geq o_d(n)$. $\square$

Theorem 4.6 allows us to construct special types of Rédei functions.

Despite the fact that we have the above characterizations, it is not clear how to construct Rédei functions where all the nontrivial cycles (that is, cycles of length greater than one) have length j. We show next a method to construct such Rédei functions. Moreover, given an integer $j \geq 2$ and an integer $t \geq 1$, the method allows us to construct Rédei functions whose nontrivial cycles have length $j, jp, jp^2, \ldots, jp^{t-1}$ for some prime number p (when $t = 1$ we obtain a Rédei function whose nontrivial cycles have length j).

Remark 4.14. Let j and t be positive integers with $j \geq 2$ and p be a prime number such that $p \equiv 1 \pmod j$. Let us suppose that we want to construct a Rédei function

$R_n(x,a)$ defined over a finite field $\mathbb{F}_q$ with exactly t different lengths for the nontrivial cycles following the geometric progression $j, jp, jp^2, \ldots, jp^{t-1}$. We can apply the next steps:

1. Pick a number $\alpha \geq t$ such that $2p^\alpha - 1 = q$ is a power of prime.
2. Pick a nonsquare element in $\mathbb{Z}_{q+1}$.
3. Choose a primitive root r modulo $\mathbb{Z}_{q+1}$.
4. Compute $n \equiv r^{p^{\alpha-t}\left(\frac{p-1}{j}\right)} \pmod{q+1}$.

Then, the Rédei function $R_n(x,a)$ defined over $\mathbb{F}_q$ has nontrivial cycles of length $j, jp, jp^2, \ldots, jp^{t-1}$ as required. Indeed, we have that $\chi(a) = -1$ and $\gcd(n, q+1) = 1$. With the notation used in Theorem 4.6, $\omega = q+1, \nu = 1, o_\omega(n) = j = f$, and n is odd (because $q+1$ is even). We obtain that $\nu = p^h\kappa$, where $h = \alpha - t$ and $\kappa = \frac{p-1}{j}$. By Theorem 4.6 we have, the largest cycle in $\mathcal{G}(n,a,q)$ has length $fp^{\alpha-h-1} = jp^{t-1}$, which appear exactly $\kappa p^h = \frac{(p-1)p^h}{j}$ times. The other length cycles are $1, j, \ldots, jp^{t-2}$ and their multiplicities can be obtained from Theorem 4.6.

5. Conclusion. In this paper we characterize the functional graph of Rédei functions, using the dynamics of the n-map over cyclic groups. We derive results about the cycle decomposition of Rédei permutations and give estimates for the period and preperiod of points. We also propose a method to construct Rédei function with prescribed cycles.

Next, we comment on potential further problems related to this work. In [2] a generalization of the Rédei function is given. It may be possible to explain the dynamics of such generalization. In particular one could characterize when they give a permutation and in this case describe its decomposition into disjoint cycles. One could also attempt to extend the characterization of the functional graph associated with the n-map in cyclic groups to more general endomorphism over finite abelian groups. Another natural question is to understand when two functional graphs associated with Rédei functions are isomorphic. A partial answer can be obtained using the results in [4] and our observations in section 4.2 for the case when the second parameters of the Rédei functions are congruent modulo a square. It could be interesting to obtain conditions when the functional graphs associated with $R_n(x,a)$ and $R_m(x,b)$ are isomorphic for the case $\chi(a) \neq \chi(b)$ (over the domain $\mathbb{P}^1(\mathbb{F}_q)$).

Finally, as in [6], we could define tower of field extensions related to Rédei functions to then study how primes decompose in such tower of field extensions.

Acknowledgments. Parts of this paper were written during a pleasant stay by the first author at Carleton University. He wishes to thank Carleton University for its hospitality. We thank an anonymous referee for several helpful comments.

REFERENCES

[1] S. Barbero, U. Cerruti, and N. Murru, *Solving the Pell equation via Rédei rational functions*, Fibonacci Quart., 48 (2010), pp. 348–357.
[2] S. Barbero, U. Cerruti, and N. Murru, *Generalized Redei rational functions and rational approximations over conics*, Int. J. Pure Appl. Math., 64 (2010), pp. 305–317.
[3] L. Carlitz, *A note on permutation functions over a finite field*, Duke Math. J., 29 (1962), pp. 325–332.
[4] G. Deng, *Isomorphic digraphs from affine maps of finite cyclic groups*, ISRN Combin. 2013 (2013), 398641.
[5] R. Gallant, R. Lambert, and S. Vanstone, *Improving the parallelized Pollard lambda search on anomalous binary curves*, Math. Comp., 69 (2000), pp. 1699–1705.

[6] T. Gassert, *Chebyshev action on finite fields*, Discrete Math., 315 (2014) pp. 83–94.
[7] D. Gomez and A. Winterhof, *Multiplicative character sums of recurring sequences with Rédei functions*, in Sequences and Their Applications—SETA 2008. Springer, Berlin, 2008, pp. 175–181.
[8] J. Gutierrez and A. Winterhof, *Exponential sums of nonlinear congruential pseudorandom number generators with Rédei functions*, Finite Fields Appl., 14 (2008), pp. 410–416.
[9] D. Johnson, A. Menezes, and S. Vanstone, *The elliptic curve digital signature algorithm*, Internat. J. Information Security, 1 (2001), pp. 36–63.
[10] G. Mullen and D. Panario, *Handbook of Finite Fields*, CRC Press, Boca Raton, FL, 2013.
[11] S. V. Konyagin et al., *Functional Graphs of Polynomials over Finite Fields*, preprint, arXiv:1307.2718, 2013.
[12] A. MacFie and D. Panario, *Random mappings with restricted preimages*, in Progress in Cryptology—LATINCRYPT 2012, Springer, Berlin, 2012, pp. 254–270.
[13] W. Meidl and Arne Winterhof, *On the linear complexity profile of nonlinear congruential pseudorandom number generators with Rédei functions*, Finite Fields Appl., 13 (2007), pp. 628–634.
[14] R. Nobauer, *Cryptanalysis of the Rédei scheme*, Contrib. General Algebra, 3 (1984), pp. 255–264.
[15] A. Peinado, F. Montoya, J. Muñoz, and A. Yuste, Maximal periods of $x^2 + c$ in $\mathbb{F}_q$, in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Comput. Sci. 2227, Springer, Berlin, 2001, pp. 219–228.
[16] L. Rédei, *Über eindeutig umkehrbare polynome in endlichen körpen*, Acta Sci. Math. Szeged, 11 (1946), pp. 85–92.
[17] T. Rogers, *The graph of the square mapping on the prime fields*, Discrete Math., 148 (1996), pp. 317–324.
[18] A. Sakzad, M. Sadeghi, and D. Panario, *Cycle structure of permutation functions over finite fields and their applications*, Adv. Math. Commun., 6 (2012), pp. 347–361.
[19] M. Sha, *Digraphs from endomorphisms of finite cyclic groups*, J. Combin. Math. Combin. Comput., 83 (2012), pp. 105–120.
[20] S. Ugolini, *On the iterations of certain maps $X \mapsto K \cdot (X + X^{-1})$ over finite fields of odd characteristic*, J. Number Theory, 142 (2014), pp. 274–297.
[21] T. Vasiga and J. Shallit, *On the iteration of certain quadratic maps over GF(p)*, Discrete Math. 227 (2004), pp. 219–240.
[22] M. Wiener and R. Zuccherato, *Faster attacks on elliptic curve cryptosystems*, in Proceedings of Selected Areas in Cryptography, Lecture Notes in Comput. Sci. 1556, Springer, Berlin, 1998, pp. 190–200.
[23] M. Zieve, *Permutation polynomials on $\mathbb{F}_q$ induced from Rédei function bijections on subgroups of $\mathbb{F}_q^*$*, Monatsh. Math., to appear.