Fixed Points of Rational Functions Satisfying the Carlitz Property

by

Kaitlyn Chubb

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of

Master of Science

in

Mathematics

Carleton University

Ottawa, Ontario

Abstract

Recent research within the field of cryptography has suggested that S-boxes should be chosen to contain few fixed points, motivating analysis of the fixed points of permutations. This thesis presents a novel means of obtaining fixed points for all functions satisfying a property put forth by L. Carlitz. We introduce an algorithm which cyclically generates fixed points for three such classes of functions, the most renowned of which are Rédei rational functions. Further, we provide an explicit expression for the fixed points of all Rédei functions over $\mathbb{F}_q$.

Acknowledgements

I would first like to acknowledge my thesis supervisors, Daniel Panario and Steven Wang, of the School of Mathematics and Statistics at Carleton University. Thank you both for your invaluable ideas, comments, and support. With your help, there was never an obstacle too large to overcome.

I must express my profound gratitude to my boyfriend, Phil, whose unfailing support made this accomplishment possible. You will never know the true extent of my appreciation for all that you have done. Thank you for learning about finite fields for me!

Further, I would like to thank my parents for their continuous encouragement throughout the entirety of my academic career, and for inspiring me to delve into the world of mathematical research.

Finally, to the bun, thank you for being a worthy companion throughout the writing process. Tonight, you get a carrot.

Contents

List of Illustrations

List of Appendices

1 Introduction

In this thesis, we are interested in the fixed points of various functions over a finite field, particularly when those functions are permutations. Permutations are integral to the fields of both coding theory and cryptography, hence much research has been invested in the cycle structure of permutations over $\mathbb{F}_q$. A *fixed point* of a function F is any element ρ such that $F(\rho) = \rho$. Indeed, the fixed points of a function are the cycles of length one within that function's cycle structure. We restrict our analysis to the study of these cycles.

Recent advances within the field of cryptography have intimated a link between the fixed points of permutations and the suitability of those permutations for use within cryptosystems. To be precise, consider a system which integrates a particular permutation, π. The fewer fixed points that π has, the better the cryptographic properties that the system will exhibit. Inspired by these findings, Charpin, Mesnager, and Sarkar, in [8], propose various methods for eliminating fixed points of permutations. Some of these methods require knowledge of the exact position of a permutation's fixed points, and hence the ability to efficiently discover the fixed points of a permutation is a necessity.

We present a novel means of obtaining the fixed points for particular function classes. This is achieved by furthering the implications of the Carlitz property. The Carlitz property is an interesting result proposed by L. Carlitz in 1962. By observing a key consequence of this property, we present a method to algorithmically determine the fixed points of all functions satisfying it. These functions

fall into one of three classes, the most renowned of the three being Rédei rational functions. Rédei functions have been put to a myriad of uses since their discovery including, but by no means limited to, pseudorandom number generation [10], employment within various cryptosystems [3, 11, 13], solving the Pell equation [2], serving as turbo code interleavers [14], and functioning as permutation polynomials over finite fields. The sheer pervasiveness of these functions motivates analysis of their cycle structure. To this end, we provide an explicit representation for the fixed points of all Rédei rational functions over $\mathbb{F}_q$.

Chapter 2 will provide some useful background information regarding finite fields and permutations. Here, we will introduce the Carlitz property and all classes of functions satisfying it. In Chapter 3, we survey many of the results that have been put forth concerning the fixed points of particular permutations. We also elaborate on the connection between the fixed points of permutations and the cryptographic security of systems employing these permutations. In Chapter 4, we demonstrate our contribution to this line of research by detailing an algorithm which produces fixed points for all functions satisfying the Carlitz property. For Rédei functions, this algorithm is efficient and robust, yielding all of a given function's fixed points with relatively low overhead. The algorithm for Type-1 and Type-3 functions is also provided, along with an optimization of the algorithm. Depending on the function, it may be more efficient to use a factoring algorithm to the same effect. The final section in this chapter gives an explicit expression for the fixed points of all Rédei functions over $\mathbb{F}_q$. Finally, Chapter 5 includes ideas for future work, as well as some concluding remarks. The appendices found at the end of this work consist of data tables illustrating some explicit results derived from the algorithms herein.

2 Background Information

We assume some background knowledge on the part of the reader; in particular, a basic understanding of finite fields and elementary number theory is necessary. Many of the concepts involved are discussed in the following section yet, should one wish to know more, Chapters 1 and 2 of [12] are an excellent resource.

2.1 Finite Fields

2.1.1 Algebraic principles

Familiarity of algebraic principles, such as rings and fields, is assumed on the part of the reader. We recall the following which are of especial interest in this thesis.

Definition 1. *A* group homomorphism *from* $(G, *)$ *to* $(H, \circ)$ *is a function* $h : G \to H$ *such that for all* a, b *in* G*,*

$$h(a * b) = h(a) \circ h(b).$$

Definition 2. *The* kernel of h *is the set of elements in* G *which are mapped to the identity in* H*,*

$$\ker(h) = \{a \in G : h(a) = e_H\}.$$

With these definitions in mind, we recall the following lemma.

Lemma 1. *The homomorphism,* h*, is injective if and only if* $\ker(h) = e_G$*.*

Proof. Clearly, if h is injective, there is a unique element in the kernel. Now assume $\ker(h) = e_G$. Then, for some positive integers i, j,

$$\begin{aligned} h(g_i) &= h(g_j) \\ h(g_i) \circ h(g_j)^{-1} &= e_H \\ h(g_i * g_j^{-1}) &= e_H \\ g_i * g_j^{-1} &= e_G \\ g_i &= g_j, \end{aligned}$$

and hence, h is injective. □

We remind the reader of the following algebraic definitions and theorems, which will lead into our discussion of basic finite field principles in the next section. Note, the notation $(G, \circ, e)$ refers to a group G with operation $\circ$ and identity element e. Additionally, we use F^* to represent $F \setminus \{0\}$.

Definition 3. *The* general linear group *of degree n is the set of $n \times n$ invertible matrices, together with the operation of ordinary matrix multiplication. We denote the general linear group of degree n over $\mathbb{F}_q$ as $GL(n, q)$.*

Definition 4. *A multiplicative group, G, is* cyclic *if there exists an element $g \in G$ such that, for any element $h \in G$, there exists some integer i with $h = g^i$. Such an element g is a* generator *of a cyclic group.*

Theorem 1. (Lagrange's Theorem) *For any finite group G, the order (number of elements) of every subgroup H of G divides the order of G.*

Definition 5. *A ring, $(F, +, \circ)$, is a* field *if $(F, +, 0)$ and $(F^*, \circ, 1)$ are commutative groups and the law of distributivity holds. If the set F is finite, $(F, +, \circ)$ is a* finite field.

Definition 6. *If R is an arbitrary ring and there exists a positive integer n such that $nr = 0$ for every $r \in R$, then the least such positive integer n is the* characteristic *of R. If no such positive integer n exists, R has characteristic 0.*

Corollary 1. (Corollary 1.45, [12]) *A finite field has prime characteristic.*

2.1.2 Elementary definitions and concepts

Throughout this section, we use the following notation.

- The ring $\mathbb{Z}/p\mathbb{Z}$ is a field with p elements, which we denote $\mathbb{F}_p$.
- We define the ring of polynomials over $\mathbb{F}_p$ with $n \in \mathbb{N}$ as

$$\mathbb{F}_p[X] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_i \in \mathbb{F}_p\}.$$

Definition 7. *A polynomial $f \in \mathbb{F}_p[X]$ is* irreducible in $\mathbb{F}_p[X]$ *if f has positive degree and $f = bc$ with $b, c \in \mathbb{F}_p[X]$ implies that either b or c is a constant polynomial.*

Definition 8. *Let p be a prime and consider an irreducible polynomial, f, over $\mathbb{F}_p$ of degree n. The ring $\mathbb{F}_p[X]/(f)$ is a* finite field *with p^n elements.*

Theorem 2. (Theorem 2.8, [12]) *The multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ is cyclic.*

We expect the reader to have an intuitive understanding of the order of an element within a group or field. The following lemma is useful, should one wish to obtain an element with given order.

Lemma 2. *Let $\mathbb{F}_q$ be a finite field, d be a positive integer, and $\alpha \in \mathbb{F}_q^*$. Then,*

$$\mathrm{ord}(\alpha^d) = \frac{\mathrm{ord}(\alpha)}{\gcd(\mathrm{ord}(\alpha), d)}.$$

Definition 9. *A* polynomial basis *is a basis of a polynomial ring, viewed as a vector space over the field of coefficients.*

If $q = p^t$, one example of a common polynomial basis is the monomial basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. This basis is as follows,

$$\{1, x, x^2, \ldots, x^{t-1}\}.$$

Observe that the basis is a set of linearly independent elements, and that the entire field $\mathbb{F}_q$ may be generated by taking all linear combinations of the elements within.

We now briefly discuss permutations, cycles, and involutions. In this thesis, we consider permutation polynomials over $\mathbb{F}_q$.

Definition 10. *A* permutation polynomial *of* $\mathbb{F}_q$ *is a polynomial* $f \in \mathbb{F}_q[X]$ *such that the associated function* $c \to f(c)$ *is a permutation of the elements of* $\mathbb{F}_q$.

Definition 11. *An* involution *is a function,* f*, that is its own inverse. That is,*

$$f(f(x)) = x$$

for all x *in the domain of* f.

Note that every involution is a permutation, one whose cycle structure consists of only cycles of length one and two. We will be working with an iterative function, Ω_P, whose iterates form cycles of elements in $\mathbb{F}_q$. Of particular interest to us are the function's fixed points.

Definition 12. *A* fixed point *of a function* F *is any element* ρ *such that* $F(\rho) = \rho$.

Another way to understand a fixed point of an iterative function is as a 1-cycle, or a cycle of length one, within that function's cycle structure.

2.1.3 Finite field properties

We remind the reader of some important properties of finite fields, which we call upon within this thesis.

Lemma 3. (Lemma 2.3, [12]) *If $\mathbb{F}_q$ is a finite field with q elements, then every $a \in \mathbb{F}_q$ satisfies $a^q = a$.*

The following theorem is known as the Generalized Euler Criterion and is useful for determining whether or not a particular element, a, is a square.

Theorem 3. (Theorem 2, [1]) *Let $q = p^t$ for an odd prime p and an arbitrary integer $t > 1$, and let $a \in \mathbb{F}_q^*$. Then there exists an element $x \in \mathbb{F}_q^*$ such that $a = x^2$ if and only if*

$$a^{(q-1)/2} = 1.$$

Lemma 4. *Every element $a \in \mathbb{F}_q^*$, $\mathrm{char}(\mathbb{F}_q) \neq 2$, is a square in the extension field $\mathbb{F}_{q^2}^*$.*

Proof. Clearly, if $a \in \mathbb{F}_q^*$ is a square in $\mathbb{F}_q^*$, then it is also a square in $\mathbb{F}_{q^2}^*$. Now consider $a \in \mathbb{F}_q^*$ a non-square. Then, by the Generalized Euler Criterion, $a^{(q-1)/2} = -1$. To determine whether a is a square in $\mathbb{F}_{q^2}^*$, we compute

$$a^{\frac{(q^2-1)}{2}} = a^{\frac{(q-1)(q+1)}{2}} = -1^{(q+1)} = 1.$$

By the Generalized Euler Criterion applied on $\mathbb{F}_{q^2}^*$, a is a square. □

Lemma 5. *Every element $a \in \mathbb{F}_{2^t}$ is a square.*

Proof. For this proof, we refer to Section 2.1.1 which elaborates on the key algebraic principles involved. Consider the finite field $\mathbb{F}_{2^t}$ with 2^t elements. The multiplicative group of this field is of odd order, $2^t - 1$. By Lagrange's Theorem, therefore, no element in $\mathbb{F}_{2^t}$ has order two. Now, we consider the map $f : \mathbb{F}_{2^t}^* \to \mathbb{F}_{2^t}^*$

given by $f(x) = x^2$. This is a group homomorphism whose kernel consists of all elements in $\mathbb{F}_{2^t}^*$ with order two. We just observed that $\ker(f) = 1$. By Lemma 1, f is injective and, because it maps $\mathbb{F}_{2^t}^*$ to itself, therefore, surjective. This tells us that every element in $\mathbb{F}_{2^t}^*$ is a square. □

In this work, we often need to make clear whether an element a is a square or a non-square in $\mathbb{F}_q$. We introduce χ notation, reliant upon the Generalized Euler Criterion (Theorem 3), which will be used henceforth.

Definition 13. *We denote by $\chi(a)$ the value of $a^{\frac{(q-1)}{2}}$. If $\chi(a) = 1$, then a is a square or* quadratic residue *in $\mathbb{F}_q^*$. If $\chi(a) = -1$, then a is a non-square, or* quadratic non-residue.

2.2 Relevant Functions and Concepts

We recall the following statistical method for later use within this paper.

Definition 14. *A random variable X follows the* hypergeometric distribution *if its probability mass function (pmf) is given by*

$$P(X = k) = \frac{\binom{K}{k}\binom{N-k}{n-k}}{\binom{N}{n}},$$

where N is the population size, K is the number of success states in the population, n is the number of draws, k is the number of observed successes, and $\binom{n}{k}$ is a binomial coefficient.

The hypergeometric distribution describes the probability of k successes in n draws, without replacement, from a finite population of size N containing K objects with a specified "success" feature. This is an *exchangeable distribution*, that is, given a finite sequence of observations (realizations of the random variables),

any re-ordering of this sequence is equally likely to occur. Therefore, the probability of drawing an element with a success feature on the ith draw is

$$P(X_i) = \frac{K}{N}. \tag{2.1}$$

We now introduce the notion of a non-constant rational transformation, which is central to this work; see [6] for more information.

Let

$$R(x) = \frac{ax+b}{cx+d} \in \mathbb{F}_q(x), \quad c \neq 0,$$

be a *non-constant rational transformation*. Consider the permutation of $\mathbb{F}_q$,

$$F(x) = \begin{cases} R(x) & \text{if } x \neq \frac{-d}{c}, \\ \frac{a}{c} & \text{if } x = \frac{-d}{c}. \end{cases}$$

The matrix associated with R is

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

where $A \in \mathrm{GL}(2, q)$, the general linear group of 2×2 matrices. The associated *characteristic polynomial* for this matrix is $h(x) = x^2 - (a+d)x + (ad - bc)$.

One particular type of function which we will return to often is the linearized polynomial. We discuss this function and its properties, below.

Definition 15. *The function*

$$L(x) = \sum_{i=0}^{l} c_i x^{q^i}$$

is a linearized polynomial*, where l is any non-negative integer and each c_i is in $\mathbb{F}_{q^m}$ for some fixed positive integer m.*

Remark 1. *Note that if x is a fixed point for L, $-x$ is also a fixed point. This may be easily observed by evaluating $L(-x)$.*

Definition 16. *A* Dickson matrix *is an $m \times m$ matrix over $\mathbb{F}_{q^m}$ of the form*

$$\begin{pmatrix} c_0 & c_1 & \dots & c_{m-1} \\ c_{m-1}^q & c_0^q & \dots & c_{m-2}^q \\ \vdots & \vdots & & \vdots \\ c_1^{q^{m-1}} & c_2^{q^{m-1}} & \dots & c_0^{q^{m-1}} \end{pmatrix}.$$

Theorem 4. [19] *The linearized polynomial $L(x) = \sum_{i=0}^{m-1} c_i x^{q^i}$ is a permutation polynomial over $\mathbb{F}_{q^m}$ if and only if the Dickson matrix associated to it, i.e. the Dickson matrix with the coefficients $c_0, c_1, \dots, c_{m-1}$ as entries of the first row, is non-singular.*

In this paper, we work with linearized polynomials comprised of powers of p, where each c_i is in $\mathbb{F}_q$ with $q = p^t$.

2.3 The Carlitz Property

Let $\mathbb{F}_q$ be the finite field with q elements. In this thesis, we consider all functions over $\mathbb{F}_q$ that satisfy the Carlitz property, which we define below.

Definition 17. *Let x, y be indeterminates. A rational function, f, over $\mathbb{F}_q$ has the* Carlitz property *if there exists an $a \in \mathbb{F}_q$ such that*

$$f\left(\frac{xy+a}{x+y}\right) = \frac{f(x)f(y)+a}{f(x)+f(y)}.$$

There are precisely three classes of functions which satisfy this property. In [5], Carlitz detailed these functions in the following theorem.

Theorem 5. *Let f be a rational function with coefficients in $\mathbb{F}_q$ that satisfies the property above, where a is a fixed number of $\mathbb{F}_q$ and x, y are indeterminates.*

If $a = 0$ and $q = p^t$, then

$$f(x) = \left(\sum_{i=0}^{l} c_i x^{-p^i} \right)^{-1}, \tag{2.2}$$

where the c_i are arbitrary numbers of $\mathbb{F}_q$ and l is some integer.

If $a \neq 0$ and q is odd, then

$$f(x) = \Phi \frac{(x+\Phi)^n + (x-\Phi)^n}{(x+\Phi)^n - (x-\Phi)^n}, \tag{2.3}$$

where $a = \Phi^2$ and $\Phi \in \mathbb{F}_{q^2}$. Therefore, f coincides with Rédei's function (Definition 18) for some n.

If $a \neq 0$ and $q = 2^t$, then

$$f(x) = \Phi + \left(\sum_{i=0}^{l} c_i (x+\Phi)^{-2^i} \right)^{-1}, \tag{2.4}$$

where $a = \Phi^2$, the c_i are arbitrary numbers of $\mathbb{F}_q$, and l is some integer.

Classes (2.2) and (2.4) will henceforth be referred to as Type-1 and Type-3 functions. Of particular interest is class (2.3), which represents all Rédei functions.

2.3.1 Rédei functions

Definition 18. *Consider the binomial expansion*

$$(x + \sqrt{y})^n = N(x,y) + D(x,y)\sqrt{y}.$$

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* $R_n(x,a) = \frac{N(x,a)}{D(x,a)}$.

The following are some important properties of Rédei functions.

Theorem 6. (Theorem 6, [5]) *Assume* $\mathrm{char}(\mathbb{F}_q) \neq 2$ *and* $a \in \mathbb{F}_q^*$. *The Rédei function* R_n *is a permutation function if and only if* $\gcd(n, q - \chi(a)) = 1$.

Theorem 7. (Corollary 4.8, [15]) *The number of fixed points of* $R_n(x, a)$ *over* $\mathbb{P}^1(\mathbb{F}_q)$ *is given by the formula*

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

Here, we present this simple result for Rédei functions which alludes to the symmetry of their fixed points.

Lemma 6. *Let* $R_n(x, a)$ *be a Rédei function defined over* $\mathbb{F}_q$ *with* $\mathrm{char}(\mathbb{F}_q) \neq 2$. *Then* $R_n(-x, a) = -R_n(x, a)$.

Proof. The result is clear by evaluating $R_n(-x, a)$ using Carlitz's representation of the Rédei function, as seen in (2.3). □

Corollary 2. *Let* $R_n(x, a)$ *be a Rédei function defined over* $\mathbb{F}_q$ *with* $\mathrm{char}(\mathbb{F}_q) \neq 2$. *If* x *in* $\mathbb{F}_q$ *is a fixed point for* R_n, *then* $-x$ *is as well.*

3 Previous Work in Fixed Points of Permutations over $\mathbb{F}_q$

It is only within the past few decades that mathematicians have begun to recognize the fixed points of permutations as important cryptographic criteria. In 1996, the connection between a permutation's suitability for S-box creation and its fixed points was put forth by A. M. Youssef, S. E. Tavares, and H. M. Heyes [20]. This discovery subsequently spurred finite field research on the fixed points of permutations and involutions. In this chapter, we present this connection in more detail and discuss precisely which permutations have had their fixed points unearthed to date.

3.1 Fixed Points and Cryptographic Security

The discovery occurred while Youssef, Tavares, and Heyes were in pursuit of a novel cryptographic scheme. In their paper "A New Class of Substitution-Permutation Networks", the authors present a substitution-permutation network, or SPN, which is more resource efficient than its predecessors. Indeed, SPNs employ permutations as a method of data obfuscation. Found within block cipher algorithms, SPNs incorporate S-boxes which are created using permutations. One of the chief drawbacks of SPNs is that two different modules are required for the encryption and decryption operations. In particular, this means that the inverse

S-boxes, and indeed, the inverse permutations for these S-boxes, must also be stored in the encryption hardware. This was historically resource intensive, leading the authors to search for a more efficient means of implementing the SPN structure. Their solution was to create S-boxes which leveraged involutions. The authors observed that by employing involutions as the permutations which define the S-boxes, they effectively eliminate the need to store the inverse S-boxes in hardware. This is because involutions are their own inverse, and as such, an S-box constructed using involutions serves as its own inverse.

While such an SPN has the distinct advantage of being more resource efficient than its ancestors, it is prudent to analyze the effect that S-boxes created with involutions will have on the overall security of the system. The authors observe that, given that the cycle structure of involutions consists of only 1-cycles and 2-cycles, the expected number of fixed points for an involution is higher than that of a random permutation. In order to determine whether this observation was detrimental to the security of the system, they ran experiments and gauged various cryptographic properties in relation to the number of fixed points that a given function possessed. The authors conclude that "the graphs clearly indicate a strong correlation between the cryptographic properties and the number of fixed points and suggest that the S-boxes should be chosen to contain few fixed points" [20].

Because this connection is fairly recent, there is yet to be an extensive body of research concerning cryptanalysis of systems through fixed point exploitation. One system for which such work has been done is the *reflection cipher* [4]. A reflection cipher is a cryptographic system in which the set of encryption functions is identical to the set of decryption functions. This implies that the encryption function is an involution. To be precise, let E_k be the encryption function for the cipher, where k is the chosen key. In a reflection cipher, there exists some

permutation P of the key space such that, for any key k,

$$(E_k)^{-1} = E_{P(k)}.$$

Here, P is called the *coupling permutation*. The authors of [4] observe that a coupling permutation should be an involution with no fixed points. Fixed points of P correspond to weak keys for the cipher because the corresponding encryption function is involutive. In fact, in [17], the authors successfully attack such ciphers by exploiting the fixed points of the involutions. They leverage self-similarity properties to determine classes of weak keys. Crucially, a probabilistic relation on the middle rounds of the cipher allows for an attack on the system when classes of fixed points exist in intermediate rounds. These attacks require known plaintext only.

Inspired by these findings, Charpin, Mesnagar, and Sarkar in [8] provide various methods for reducing the number of fixed points that a given permutation possesses, so that the permutation (or involution) may be used for cryptographic purposes. Indeed, one such method involves swapping the image of two fixed points, thereby eradicating the fixed points while maintaining the structure of the permutation. This method is as follows.

Theorem 8. (Theorem 31, [8]) *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an involution. Let α and β be two nonzero distinct elements of $\mathbb{F}_{2^n}$. Define $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ as follows:*

$$G(x) = \begin{cases} F(x) & \text{for all } x \notin \{\alpha, \beta\} \\ F(\alpha) & \text{if } x = \beta \\ F(\beta) & \text{if } x = \alpha. \end{cases}$$

Then G is an involution if and only if $\{\alpha, \beta\}$ is stable under F, that is,

$$\begin{cases} F(\alpha) = \alpha \\ F(\beta) = \beta \end{cases} \quad or \quad \begin{cases} F(\alpha) = \beta \\ F(\beta) = \alpha. \end{cases}$$

Corollary 3. *If α and β are two fixed points of an involution F, then G is an involution and α, β are not fixed points of G.*

This is one method of reducing pairs of fixed points of an involution over $\mathbb{F}_{2^n}$ and creating an involution with fewer fixed points than the original. The authors provide several more methods for reducing the number of fixed points of a permutation. We encourage the interested reader to refer to [8].

3.2 Permutations with Known Fixed Points

Thus far, we have established the importance of employing permutations with few fixed points in particular cryptosystems. Should one wish to deplete the number of fixed points that a given permutation or involution has, one such method includes that given in Theorem 8. Clearly, one must know what the fixed points of F are in order to use this method.

To date, there has been little activity in the realm of determining the fixed points for particular permutations. There do exist some results for well-known permutations such as Dickson involutions and monomial involutions.

Definition 19. *The* Dickson polynomial *of the first kind of degree k in indeterminate x and with parameter $a \in \mathbb{F}_{2^n}^*$ is defined by*

$$D_k(x, a) = \sum_{i=0}^{\lfloor k/2 \rfloor} \frac{k}{k-i} \binom{k-i}{i} a^k x^{k-2i}, \quad k \geq 2,$$

where $\lfloor k/2 \rfloor$ denotes the largest integer less than or equal to $k/2$.

Definition 20. *A* monomial *is a function of the form x^i, where i is some non-negative integer.*

In [7], the authors provide an explicit expression for all fixed points of Dickson involutions of the first kind over $\mathbb{F}_{2^m}$. These points are detailed as follows.

Theorem 9. *Consider an involution D_k on $\mathbb{F}_{2^m}$, where $1 \leq k \leq 2^n - 1$, $n = 2m$ with $m \geq 2$. Let T_n be described by*

$$T_n = \{u \quad | \quad 1 \leq u \leq 2^n - 2, \quad u^2 \equiv 1 \pmod{2^n - 1}\}.$$

Such an involution will have $k \in T_n$. We assume that D_k is not the identity modulo $(x^{2^m} + x)$, i.e. $k \notin \{\pm 1, \pm 2^m\}$. Let α be a primitive root of $\mathbb{F}_{2^n}$. Then $2^m - 1 = r_1 r_2$ and $2^m + 1 = s_1 s_2$. Moreover, the fixed points of D_k is the set of $\gamma + \gamma^{-1}$ where

$$\gamma \in \left\{ \begin{matrix} \alpha^{ir_2(2^m+1)}, 0 \leq i \leq (r_1 - 1)/2, & \alpha^{jr_1(2^m+1)}, 0 \leq j \leq (r_2 - 1)/2 \\ \alpha^{ls_2(2^m-1)}, 0 \leq l \leq (s_1 - 1)/2, & \alpha^{ts_1(2^m-1)}, 0 \leq t \leq (s_2 - 1)/2 \end{matrix} \right\}.$$

Monomials are another such example of permutation polynomials in common use. In [16], the authors provide an explicit expression for all fixed points of monomial involutions over $\mathbb{F}_q$, as seen below.

Theorem 10. *Let $q - 1 = 2^e p_1^{e_1} \dots p_r^{e_r}$, $d = 2^f p_1^{k_1} \dots p_r^{k_r}$, $f \leq e$, $k_j \in \{0, e_j\}$. Let α be a primitive root of $\mathbb{F}_q$. The fixed points of the monomial x^i over $\mathbb{F}_q$ are of the form 0 and α^j, for $j = \frac{q-1}{d} l$, $l = 1, \dots, d$.*

Finally, in [18], Qiang Wang discusses an algorithmic method for determining the number of fixed points of cyclotomic mapping permutation polynomials over $\mathbb{F}_q$. In fact, this algorithm can be modified to produce the fixed points themselves.

Such an algorithm is useful in the construction of cyclotomic mapping permutation polynomials which are involutions with few fixed points.

3.3 Research Question

The results for the functions above have some limitations regarding the field and the type of function. Indeed, for Dickson polynomials, we have results for the fixed points of involutions over $\mathbb{F}_{2^m}$ and for monomials, we have results for the fixed points of involutions over $\mathbb{F}_q$. In this thesis, we provide an algorithmic method of determining all fixed points of functions over $\mathbb{F}_q$ satisfying the Carlitz property. Further, we provide an explicit expression for the fixed points of all Rédei functions, permutation or otherwise, over $\mathbb{F}_q$.

4 Fixed Points of Functions Satisfying the Carlitz Property

4.1 Designing the Fixed Point Algorithm

We begin with an observation concerning the Carlitz property which will provide insight into the problem of determining the fixed points of functions satisfying this property. Throughout this work, we assume that each function f satisfying the Carlitz property is defined in relation to some chosen element $a \in \mathbb{F}_q$. By convention, we assume $\Phi \in \mathbb{F}_{q^2}$, where $a = \Phi^2$.

Lemma 7. *Let $x, y \in \mathbb{F}_q, x + y \neq 0$ be two fixed points of some function f which satisfies the Carlitz property. Then $\frac{xy+a}{x+y}$ is another fixed point for that function.*

Proof. Since $f(x) = x$ and $f(y) = y$, by the Carlitz property,

$$f\left(\frac{xy+a}{x+y}\right) = \frac{f(x)f(y)+a}{f(x)+f(y)} = \frac{xy+a}{x+y}.$$

Therefore, $\frac{xy+a}{x+y}$ is a fixed point for f. □

Suppose that we have obtained one non-zero fixed point, $P \neq \Phi$, of some function f which satisfies the Carlitz property. We can use this point to generate further fixed points for f by setting $x = P$ in the relation defined in Lemma 7 and

iteratively applying

$$y_{i+1} = \omega_P(y_i) \coloneqq \frac{Py_i + a}{P + y_i}, \qquad y_0 = P.$$

Definition 21. *Let $P \neq \Phi$ be a non-zero fixed point of some function f satisfying the Carlitz property. We define the iterative function Ω_P as follows:*

$$y_{i+1} = \Omega_P(y_i) \coloneqq \begin{cases} \omega_P(y_i) & \text{if } y_i \neq -P, \\ P & \text{if } y_i = -P. \end{cases}$$

Proposition 1. *Assume $a \in \mathbb{F}_q$ and $\Phi \in \mathbb{F}_{q^2}$. Let $a = \Phi^2$ and $P \in \mathbb{F}_q$, with $P \neq \Phi$, be a chosen non-zero fixed point of some function f satisfying the Carlitz property. The relation Ω_P induces cycles of fixed points for f whenever y_0 is a fixed point. In particular, setting $y_0 = P$ produces the first cycle.*

Proof. Let a be defined as in Theorem 5, according to the chosen function f. We observe that if $y_i \neq y_j$ in $\mathbb{F}_q$ for some positive integers i, j, then $\Omega_P(y_i) \neq \Omega_P(y_j)$ unless $P^2 = a$. To see this, we prove the contrapositive. Suppose, $y_i, y_j \neq -P$ so, in order to derive a contradiction, we suppose that $\omega_P(y_i) = \omega_P(y_j)$. Then,

$$\begin{aligned} \frac{Py_i + a}{P + y_i} &= \frac{Py_j + a}{P + y_j} \\ P^2y_i + ay_j &= P^2y_j + ay_i \\ y_i(P^2 - a) &= y_j(P^2 - a) \\ y_i &= y_j. \end{aligned}$$

Now, suppose $y_i \neq -P = y_j$. We determine when $\omega_P(y_i) = P$.

$$\omega_P(y_i) = \frac{Py_i + a}{P + y_i} = P \quad \text{implies} \quad P^2 = a.$$

Hence, as long as we choose a $P \neq \Phi$, no two iterations of Ω_P will yield the same result. That is, each iteration will produce a unique fixed point. By Lemma 7, since P is a fixed point, setting $y_0 = P$ will yield a cycle of fixed points. □

Lemma 8. *Let Ω_P be defined as in Definition 21, with $P \neq \Phi$ a non-zero fixed point of some function f satisfying the Carlitz property. Then, for $y_i, y_j \in \mathbb{F}_q$,*

$$\Omega_P(y_i) = y_j \quad \textit{if and only if} \quad \Omega_P(-y_j) = -y_i.$$

Proof. Suppose $\Omega_P(y_i) = y_j$. By definition, if $y_i = -P$, we have $P = y_j$. Evaluating, we find

$$\Omega_P(-y_j) = \Omega_P(-P) = P = -y_i.$$

Now suppose $y_i \neq -P$. Then we have $\omega_P(y_i) = \frac{Py_i+a}{P+y_i} = y_j$. We evaluate $\Omega_P(-y_j)$. Because, $y_i \neq -P$, $y_j \neq P$, hence $\Omega_P(-y_j) = \omega_P(-y_j)$.

$$\omega_P(-y_j) = \frac{-P\left(\frac{Py_i+a}{P+y_i}\right) + a}{P - \frac{Py_i+a}{P+y_i}} = \frac{-P^2y_i + ay_i}{P^2 - a} = \left(\frac{-P^2 + a}{P^2 - a}\right) y_i = -y_i.$$

The proof for the other direction is much the same. □

Lemma 8 lends some insight into the cycle structure of Ω_P. In particular, if an element y_i is not within the same cycle of Ω_P as its additive inverse, there must exist a symmetric cycle which contains $-y_i$ as well as the inverses of all elements in the same cycle as y_i. We will return to this property in Section 4.1.3.

4.1.1 The cycle structure of Ω_P

Let $P \neq 0, \Phi$ be a fixed point of some function f satisfying the Carlitz property. The function Ω_P is a non-constant rational transformation over $\mathbb{F}_q$ with matrix

$A \in \mathrm{GL}(2, q)$, the linear group of 2×2 matrices in $\mathbb{F}_q$, as follows

$$A = \begin{pmatrix} P & a \\ 1 & P \end{pmatrix}$$

and characteristic polynomial $h(x) = x^2 - 2Px + (P^2 - a)$. We can study the cycle structure of rational transformations to understand how Ω_P behaves. In particular, from [6], we have the following theorem, slightly modified to suit this paper.

Theorem 11. *Let $q = p^t$ and let $P \neq \Phi$ be a non-zero fixed point of some function f satisfying the Carlitz property. Define Ω_P as the permutation in Definition 21, and let h be the characteristic polynomial of the matrix A associated with Ω_P. Let $\alpha, \beta \in \mathbb{F}_{q^2}$ be the roots of h. There are three possible cases for the cycle structure of Ω_P.*

1. *Suppose h is irreducible. If $k = \mathrm{ord}(\frac{\alpha}{\beta}) = \frac{q+1}{v}, 1 \leq v < \frac{q+1}{2}$, then Ω_P has $v - 1$ cycles of length k and one cycle of length $k - 1$. In particular, Ω_P is a full cycle if $v = 1$.*

2. *Suppose $\alpha, \beta \in \mathbb{F}_q$ and $\alpha \neq \beta$. If $k = \mathrm{ord}(\frac{\alpha}{\beta}) = \frac{q-1}{v}, v \geq 1$, then Ω_P has $v-1$ cycles of length k, one cycle of length $k - 1$, and two cycles of length 1.*

3. *Suppose $h(x) = (x - \alpha)^2, \alpha \in \mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$, then Ω_P has $p^{t-1} - 1$ cycles of length p, one cycle of length $p - 1$, and one cycle of length 1.*

Remark 2. *In Cases 1 and 2, the cycle containing $y_0 = P$ is of length $k - 1$, while in Case 3, the cycle containing $y_0 = P$ is of length $p - 1$; see the proof of Theorem 2 in* [6]. *In particular, by Proposition 1, this tells us that the cycles of length $k - 1$ and $p - 1$ are cycles of fixed points.*

There are three classes of functions in $\mathbb{F}_q$ which satisfy the Carlitz property. Here, we examine the cycle structure of each class separately.

Lemma 9. *Let $a = 0$, $q = p^t$, and consider a Type-1 function,*

$$f(x) = \left(\sum_{i=0}^{l} c_i x^{-p^i} \right)^{-1},$$

where the c_i are arbitrary numbers of $\mathbb{F}_q$ and l is some integer. Let $P \neq \Phi$ be a non-zero fixed point of f. The cycle structure of Ω_P for f corresponds to Case 3 in Theorem 11, that is, Ω_P has $p^{t-1} - 1$ cycles of length p, one cycle of length $p - 1$, and one cycle of length 1.

Proof. The characteristic polynomial h for the matrix associated with Ω_P is

$$\begin{aligned} h(x) &= x^2 - 2Px + (P^2 - a) = x^2 - 2Px + P^2 \\ &= (x - P)^2 \end{aligned}$$

and therefore corresponds to Case 3. □

Lemma 10. *Let $a \neq 0$ be an element in $\mathbb{F}_q$ with q odd, and consider the class of functions coinciding with Rédei's function for some n, namely,*

$$f(x) = \Phi \frac{(x + \Phi)^n + (x - \Phi)^n}{(x + \Phi)^n - (x - \Phi)^n},$$

where $a = \Phi^2$ and $\Phi \in \mathbb{F}_{q^2}$. Let $P \neq \Phi$ be a non-zero fixed point of f. If $\chi(a) = -1$, the cycle structure of Ω_P for f corresponds with Case 1 in Theorem 11, that is, if $k = \mathrm{ord}(\frac{\alpha}{\beta}) = \frac{q+1}{v}, 1 \leq v < \frac{q+1}{2}$, then Ω_P has $v - 1$ cycles of length k and one cycle of length $k - 1$. If $\chi(a) = 1$, the cycle structure corresponds to Case 2, that is, if $k = \mathrm{ord}(\frac{\alpha}{\beta}) = \frac{q-1}{v}, v \geq 1$, then Ω_P has $v - 1$ cycles of length k, one cycle of length $k - 1$, and two cycles of length 1.

Proof. We consider the number of 1-cycles of Ω_P. Assuming that we have chosen $P \neq \Phi$, then $\Omega_P(y_l) = y_l$ for some positive l if and only if $y_l = \Phi$. This may

be seen as follows. Suppose $\Omega_P(y_l) = y_l$. Clearly, $y_l \neq -P$. Hence, we evaluate $\omega_P(y_l) = y_l$.

$$\omega_P(y_l) = \frac{Py_l + a}{P + y_l} = y_l \quad \text{implies} \quad y_l^2 = a \quad \text{and hence,} \quad y_l = \Phi.$$

Now, suppose $y_l = \Phi$. Then,

$$\Omega_P(y_l) = \omega_P(\Phi) = \frac{P\Phi + \Phi^2}{P + \Phi} = \Phi = y_l.$$

Having established the only two possible 1-cycles for this function, namely the square roots of a, we continue. Suppose $\chi(a) = -1$. In this case, $\Phi \notin \mathbb{F}_q$ and hence $y_l \neq \Phi$ for any l. Therefore, the cycle structure of Ω_P does not contain any 1-cycles. This means we are in Case 1. Suppose $\chi(a) = 1$. Then $\Phi \in \mathbb{F}_q$ and the cycle structure of Ω_P includes precisely two 1-cycles. This structure corresponds to Case 2. □

Lemma 11. *Let $a \neq 0$ with $q = 2^t$, and consider a Type-3 function,*

$$f(x) = \Phi + \left(\sum_{i=0}^{l} c_i (x + \Phi)^{-2^i} \right)^{-1},$$

where $a = \Phi^2$, the c_i are arbitrary numbers of $\mathbb{F}_q$ and l is some integer. Let $P \neq \Phi$ be a non-zero fixed point of f. The cycle structure of Ω_P for f corresponds to Case 3 in Theorem 11, that is, Ω_P has $2^{t-1} - 1$ cycles of length 2, and two cycles of length 1.

Proof. Because we are working in $\mathbb{F}_{2^t}$, every element is a square (Lemma 5) and, in particular, so is a; therefore, $\chi(a) = 1$. The characteristic polynomial h for the

matrix associated with Ω_P is then

$$h(x) = x^2 - 2Px + (P^2 - a) = x^2 + (P^2 + a)$$
$$= x^2 + (P + \Phi)^2 = [x + (P + \Phi)]^2.$$

This form of characteristic polynomial corresponds to Case 3. □

4.1.2 Producing fixed points for Rédei functions

This section provides a method for obtaining fixed points for Rédei functions, detailed in the fixed point algorithm given in Section 4.2.1.

Lemma 12. *Let* $\mathrm{char}(\mathbb{F}_q) \neq 2$, $P \neq \Phi$ *be a non-zero fixed point of* $R_n(x, a)$, *and let* $\alpha, \beta \in \mathbb{F}_{q^2}$ *be the roots of the characteristic polynomial of the matrix associated with* Ω_P. *The number of cycles of* Ω_P *containing fixed points for* $R_n(x, a)$ *is* $\frac{d}{k} + (1 + \chi(a))$, *where* $d = \gcd(n - 1, q - \chi(a))$ *and* $k = \mathrm{ord}(\frac{\alpha}{\beta})$.

Proof. From Theorem 7, the total number of fixed points for R_n in $\mathbb{F}_q$ is

$$N = \gcd(n - 1, q - \chi(a)) + (1 + \chi(a)) - 1 = (d - 1) + (1 + \chi(a)).$$

The cycles produced by Ω_P are of length k, except for one cycle of length $k - 1$ which happens to be a cycle of fixed points, as given by Remark 2. Depending on $\chi(a)$, there is also the possibility of two 1-cycles, as indicated by $(1 + \chi(a))$. The number of cycles entirely comprised of fixed points, including that of length $k-1$, is then

$$\frac{(d - 1) - (k - 1)}{k} + (1 + \chi(a)) + 1 = d/k + (1 + \chi(a)).$$

□

Evidently, setting $k = \gcd(n - 1, q - \chi(a))$ will concentrate the fixed points of

R_n into one cycle, in addition to the two 1-cycles containing $\pm\Phi$ when $\chi(a) = 1$. By choosing a suitable P to define Ω_P, we can ensure that all of the fixed points for R_n, except $\pm\Phi$, are in the same cycle.

Theorem 12. *Let* $\mathrm{char}(\mathbb{F}_q) \neq 2$ *and* $\Phi \in \mathbb{F}_{q^2}$. *A suitable fixed point* P *of* $R_n(x, a)$ *with which to define* Ω_P *is such that* $P = \Phi\left(\frac{1+\gamma}{1-\gamma}\right)$, *where* $a = \Phi^2$, $\mathrm{ord}(\gamma) = \gcd(n-1, q-\chi(a)) = k$ *and*

$$\gamma \in \begin{cases} \mathbb{F}_q & \text{if } \chi(a) = 1, \\ \mathbb{F}_{q^2} & \text{if } \chi(a) = -1. \end{cases}$$

Proof. From Theorem 11, we have $k = \mathrm{ord}(\frac{\alpha}{\beta})$, where $\alpha, \beta \in \mathbb{F}_{q^2}$ or $\mathbb{F}_q$, depending on $\chi(a)$. Set $\gamma = \frac{\alpha}{\beta}$. Then we must obtain an element γ with $\mathrm{ord}(\gamma) = k = \gcd(n-1, q-\chi(a))$. One way of doing so is by obtaining a generator element, g, for the field in question and relying on the identity $\mathrm{ord}(a^b) = \frac{\mathrm{ord}(a)}{\gcd(\mathrm{ord}(a),b)}$. To be clear, if $\chi(a) = 1$, we find g in $\mathbb{F}_q^*$ and determine $\gamma = g^b$ as follows

$$\begin{aligned} \mathrm{ord}(g^b) &= \frac{\mathrm{ord}(g)}{\gcd(\mathrm{ord}(g), b)} \\ k &= \frac{q-1}{\gcd(q-1, b)} \\ \gcd(q-1, b) &= \frac{q-1}{k}. \end{aligned}$$

One such solution for b is $\frac{q-1}{k}$. Therefore, we set $\gamma = g^{\frac{q-1}{k}}$. If $\chi(a) = -1$, find g in $\mathbb{F}_{q^2}^*$ and a very similar process yields $\gamma = g^{\frac{q^2-1}{k}}$.

Let α, β be the roots of $h(x) = x^2 - 2Px + (P^2 - a)$. From this, we derive the following system of equations:

$$\begin{aligned} \alpha - \gamma\beta &= 0 \\ \alpha + \beta &= 2P \\ \alpha\beta &= P^2 - a. \end{aligned}$$

Using the first two linear equations, we obtain the following matrix

$$\begin{bmatrix} 1 & -\gamma \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 0 \\ 2P \end{bmatrix}.$$

Solving for α, β, we get $\alpha = \gamma(\frac{2P}{1+\gamma})$ and $\beta = \frac{2P}{1+\gamma}$. Finally, using the third equation, we have

$$\begin{aligned} \gamma \left(\frac{2P}{1+\gamma} \right)^2 &= P^2 - a \\ a &= P^2 - \gamma \left[\frac{4P^2}{(1+\gamma)^2} \right] \\ a &= P^2 \left(\frac{1-\gamma}{1+\gamma} \right)^2 \\ P &= \pm \Phi \left(\frac{1+\gamma}{1-\gamma} \right). \end{aligned}$$

We can choose $P = \Phi\left(\frac{1+\gamma}{1-\gamma}\right)$. Defining Ω_P and setting $y_0 = P$ produces a cycle of points with length equal to the number of fixed points for R_n. To ensure that this cycle is a cycle of fixed points, we must show that $P \in \mathbb{F}_q$ and that P is itself a fixed point.

We show that $P = \Phi\left(\frac{1+\gamma}{1-\gamma}\right)$ is in $\mathbb{F}_q$ by proving that $P^q = P$. If $\chi(a) = 1$, clearly $P \in \mathbb{F}_q$. If $\chi(a) = -1$, observe that, since $\text{ord}(\gamma) = k$ and $k|(q+1)$, we have that $\gamma^q = \gamma^{-1}$. Similarly, note that, since a is non-square, by the Generalized Euler Criterion, $a^{(q-1)/2} = -1$, hence $\Phi^q = -\Phi$. Without loss of generality, we take Φ to be positive.

$$P^q = \left[\Phi \left(\frac{1+\gamma}{1-\gamma} \right) \right]^q = -\Phi \left(\frac{1+\gamma^q}{1-\gamma^q} \right) = -\Phi \left(\frac{\gamma+1}{\gamma-1} \right) = P.$$

Finally, we prove that P is a fixed point by evaluating $R_n(P, a)$ using equation

(2.3) and observing that $\text{ord}(\gamma)|(n-1)$ so $\gamma^n = \gamma$.

$$\begin{aligned}
R_n(P,a) &= \Phi\frac{(P+\Phi)^n + (P-\Phi)^n}{(P+\Phi)^n - (P-\Phi)^n} = \Phi\frac{\left[\Phi\left(\frac{1+\gamma}{1-\gamma}\right)+\Phi\right]^n + \left[\Phi\left(\frac{1+\gamma}{1-\gamma}\right)-\Phi\right]^n}{\left[\Phi\left(\frac{1+\gamma}{1-\gamma}\right)+\Phi\right]^n - \left[\Phi\left(\frac{1+\gamma}{1-\gamma}\right)-\Phi\right]^n} \\
&= \Phi\frac{\left[\Phi\left(\frac{2}{1-\gamma}\right)\right]^n + \left[\Phi\left(\frac{2\gamma}{1-\gamma}\right)\right]^n}{\left[\Phi\left(\frac{2}{1-\gamma}\right)\right]^n - \left[\Phi\left(\frac{2\gamma}{1-\gamma}\right)\right]^n} = \Phi\frac{\Phi^n\left[\frac{2^n}{(1-\gamma)^n} + \frac{2^n\gamma^n}{(1-\gamma)^n}\right]}{\Phi^n\left[\frac{2^n}{(1-\gamma)^n} - \frac{2^n\gamma^n}{(1-\gamma)^n}\right]} \\
&= \Phi\left(\frac{2^n + 2^n\gamma^n}{2^n - 2^n\gamma^n}\right) = \Phi\left(\frac{1+\gamma^n}{1-\gamma^n}\right) \\
&= P.
\end{aligned}$$

Then P is a fixed point for R_n and hence produces a single cycle consisting of all the fixed points for R_n. □

4.1.3 Producing fixed points for Type-1 and Type-3 functions

Because of the cycle structure of Ω_P, we are limited as to the number of fixed points that we can obtain for Type-1 and Type-3 functions without further effort. Unlike the Rédei fixed point algorithm, an algorithm for these functions is unable to induce a single cycle of Ω_P containing all fixed points for the function in question. We consider this problem below.

The number of fixed points for Type-1 and Type-3 functions

Lemma 13. *Both Type-1 and Type-3 functions have the same number of fixed points as the linearized polynomial* $L(x) = \sum_{i=0}^{l} c_i x^{p^i}$.

Proof. Set $L(x) = \sum_{i=0}^{l} c_i x^{p^i}$ and consider f a Type-1 function. Then f may be represented as the composition $f(x) = x^{-1} \circ L(x) \circ x^{-1}$. To evaluate the fixed

points of f, we set $x = f(x)$ as follows

$$\begin{aligned} x &= x^{-1} \circ L(x) \circ x^{-1} \\ x \circ x \circ x &= (x \circ x^{-1}) \circ L(x) \circ (x^{-1} \circ x) \\ x &= L(x). \end{aligned}$$

Now, consider f a Type-3 function. Then $f(x) = (\Phi + x) \circ x^{-1} \circ L(x) \circ (x + \Phi)^{-1}$. Proceeding in the same manner as above, set $x = f(x)$ and observe

$$\begin{aligned} x &= (\Phi + x) \circ x^{-1} \circ L(x) \circ (x + \Phi)^{-1} \\ x \circ (x + \Phi) &= (\Phi + x) \circ x^{-1} \circ L(x) \circ [(x + \Phi)^{-1} \circ (x + \Phi)] \\ (\Phi + x)^{-1} \circ (x + \Phi) &= [(\Phi + x)^{-1} \circ (\Phi + x)] \circ x^{-1} \circ L(x) \\ x \circ \mathrm{id}_{\mathbb{F}_q} &= (x \circ x^{-1}) \circ L(x) \\ x &= L(x). \end{aligned}$$

Thus, we again find that f has the same number of fixed points as L. □

Indeed, the number of fixed points for L is the number of distinct roots of

$$L^*(x) = \sum_{i=1}^{l} c_i x^{p^i} + (c_0 - 1)x = \sum_{i=1}^{l} d_i x^{p^i}.$$

From [12], we have the following result, adapted to suit this paper.

Theorem 13. *Let F be a finite extension of $\mathbb{F}_q$, $\{\beta_1, \ldots, \beta_s\}$ be a basis of F over $\mathbb{F}_p$, and let*

$$L(\beta_j) = \sum_{k=1}^{s} b_{jk}\beta_k \qquad \text{for } 1 \le j \le s,$$

where $b_{jk} \in \mathbb{F}_p$ for $1 \le j, k \le s$. The number of roots of L in the finite extension F is p^{s-r}, where r is the rank of the $s \times s$ matrix, B, over $\mathbb{F}_p$ whose (j, k) entry

is b_{jk}.

We immediately have the following corollary for the number of fixed points of Type-1 and Type-3 functions.

Theorem 14. *Let* $q = p^t$ *and consider a Type-1 or Type-3 function* f *defined over* $\mathbb{F}_q$. *The number of fixed points for* f *is* p^{t-r}, *where* r *is the rank of the* $t \times t$ *matrix* B *as described in Theorem 13.*

Proof. By Theorem 13, the number of roots of L^* in $\mathbb{F}_q$ is p^{t-r} where r is the rank of the $t \times t$ matrix B obtained by evaluating $L^*(\beta_j) = \sum_{k=1}^{t} b_{jk}\beta_k$ for $1 \leq j \leq t$. This corresponds with the number of fixed points for f. □

An algorithmic method for determining fixed points

Let $P \neq \Phi$ be a non-zero fixed point for f a Type-1 or Type-3 function. As per Lemmas 9 and 11, the fixed points are distributed across $p^{t-r-1}-1$ cycles of length p in the cycle structure of Ω_P, in addition to the cycle of length $p-1$ (by Remark 2), and a single 1-cycle.

Lemma 14. *Let* $a = \Phi^2$ *and let* $P \neq \Phi$ *be a non-zero fixed point for* f *a chosen Type-1 or Type-3 function. The cycle structure of* Ω_P *for the function* f *contains a 1-cycle consisting of the fixed point* Φ.

Proof. Clearly, Φ is a fixed point for Type-1 and Type-3 functions. To see that it is the element in the 1-cycle, observe that when $y_i = \Phi$,

$$y_{i+1} = \omega_P(\Phi) = \frac{P\Phi + \Phi^2}{P + \Phi} = \Phi.$$

□

Remark 3. *Note that* Φ *differs according to which function class we are working with. For Type-1 functions,* $q = p^t$ *with* $a = 0$ *and hence,* $\Phi = 0$. *For Type-3*

functions, $q = 2^t$ *and* $a \neq 0$*. In this case,* Φ *is the unique element such that* $a = \Phi^2$*.*

Lemma 15. *Let* f *be a chosen Type-1 function and let* $P \neq \Phi$ *be a non-zero fixed point for* f*. If* $\mathrm{char}(\mathbb{F}_q) \neq 2$ *and* $q = p^t$*, the fixed point cycles of length* p *in the cycle structure of* Ω_P *do not contain the additive inverse of any element within that cycle.*

Proof. By Lemma 8, should one element belong to the same cycle as its additive inverse, then all elements within that cycle have an additive inverse in that cycle. Because the field has odd characteristic and zero is contained in a 1-cycle (Lemma 14), this is a contradiction, therefore, no cycle of length p contains any of its elements' additive inverses. □

We may now build an algorithmic method for finding fixed points for f a Type-1 or Type-3 function over $\mathbb{F}_q$, $q = p^t$.

1. Compute the number of fixed points for f as $N = p^{t-r}$, where r is as in Theorem 13.
2. By Lemma 14, the first fixed point is Φ.
3. Perform a brute force search for a non-zero fixed point $P \neq \Phi$ to define Ω_P.
4. Set $y_0 = P$ and iteratively apply Ω_P to produce $p - 1$ fixed points (Remark 2).
5. Perform a brute force search for a fixed point, Q, which has not yet appeared in any cycle. Set $y_0 = Q$ and iteratively apply Ω_P to produce a cycle of p fixed points.
6. Repeat Step 5 until all N fixed points have been discovered.

Remark 4 (Optional Speed-Up)**.** *When* f *is a Type-1 function with* $\mathrm{char}(\mathbb{F}_q) \neq 2$*, then by Remark 1, Lemma 8, and Lemma 15, one may obtain two cycles of length* p *during Step 5, namely a cycle of unique fixed points and a second cycle containing*

the additive inverses of these points. To do so, record each fixed point found, as well as its additive inverse. This will decrease run-time by a factor of two.

If f is a Type-1 function with $\text{char}(\mathbb{F}_q) \neq 2$, then taking the above speed-up into account, one must perform $\frac{p^{t-r-1}+1}{2}$ brute force searches in order to determine all of the fixed points for f. If f is a Type-3 function or a Type-1 function with $\text{char}(\mathbb{F}_q) = 2$, one must perform 2^{t-r-1} brute force searches, as the speed-up does not apply.

Optimizing the Algorithm

Here, we recall Lemma 7, in which we denoted the mechanism for attaining new fixed points for f. If $x, y \in \mathbb{F}_q$ are two fixed points for f and $a = \Phi^2$, then

$$\frac{xy + a}{x + y} \tag{4.1}$$

is an additional fixed point for that function, not equal to x or y. Below, we apply this idea to create an analogous relation to Ω_P.

Lemma 16. *Suppose that we have found two cycles of fixed points, S and T, of length p within the cycle structure of Ω_P. Let the elements within those cycles be denoted s_i and t_j, respectively, where $i, j \in \{0, 1, \ldots, p-1\}$. Now, let $x = s_i$ and $y = t_j$ in Equation (4.1). The resulting elements obtained by applying (4.1) for varying $i, j \geq 0$ will all belong to some cycle $V \neq S, T$.*

Proof. Fix an element in S, say s_0. We want to prove that $\frac{s_0 t_j + a}{s_0 + t_j} \in V$ for all j.

Suppose we find that $\frac{s_0 t_0 + a}{s_0 + t_0} \in V$ for some cycle V and element $t_0 \in T$. We show that $\frac{s_0 t_1 + a}{s_0 + t_1} \in V$. Recall that these are cycles of Ω_P hence, $t_{j+1} = \frac{P t_j + a}{P + t_j}$. Then,

$$\frac{s_0 t_1 + a}{s_0 + t_1} = \frac{s_0 \left(\frac{P t_0 + a}{P + t_0}\right) + a}{s_0 + \frac{P t_0 + a}{P + t_0}} = \frac{P s_0 t_0 + P a + s_0 a + t_0 a}{P s_0 + P t_0 + s_0 t_0 + a} = \frac{P \left(\frac{s_0 t_0 + a}{s_0 + t_0}\right) + a}{P + \frac{s_0 t_0 + a}{s_0 + t_0}} \in V.$$

By induction, we have that $\frac{s_0 t_j + a}{s_0 + t_j} \in V$ for all j. By Proposition 1, each choice of t_j, where $j \in \{0, 1, \ldots, p-1\}$, produces a unique element in V. Therefore, this process will produce the entire cycle, V. Because s_i and t_j are interchangeable in (4.1), we also have that $\frac{s_i t_0 + a}{s_i + t_0} \in V$ for all i and some element t_0. Therefore, $\frac{s_i t_j + a}{s_i + t_j} \in V$ for any choice of $i, j \geq 0$.

We must now show that $V \neq S, T$. Suppose, in order to derive a contradiction, that $\frac{s_0 t_j + a}{s_0 + t_j} \in S$. Then, for some choice of j, we have $\frac{s_0 t_j + a}{s_0 + t_j} = s_0$. However, this implies that $a = s_0^2$, or $s_0 = \Phi$. By Lemma 14, Φ is not in any p-cycle. Then we must have $V \neq S, T$. □

Remark 5. *By Lemma 16, we may choose a representative element for each p-cycle of Ω_P. Let $s \in S$ be the representative for the p-cycle, S, within the cycle structure of Ω_P. Then,*

$$y_{i+1} = \omega_s(y_i) \coloneqq \frac{s y_i + a}{s + y_i}.$$

Definition 22. *Let $P \neq \Phi$ be a non-zero fixed point of f, with which we define Ω_P. Let s be the representative for the p-cycle, S, in the cycle structure of Ω_P. We define the iterative function Ω_s as follows:*

$$y_{i+1} = \Omega_s(y_i) \coloneqq \begin{cases} \omega_s(y_i) & \text{if } y_i \neq -s, \\ s & \text{if } y_i = -s. \end{cases}$$

Again, let S and T be cycles of Ω_P. Below, we define the two-step process $S \oplus T$, which will allow us to produce p-cycles of Ω_P.

Definition 23. *Let a be the usual element which defines f and let P be a fixed point of f. Let s, t, v be the representatives of p-cycles S, T and V in the Ω_P cycle structure. Suppose we have already obtained cycles S and T. The following two-step process, $S \oplus T$, produces a p-cycle, V.*

1. *Compute $\Omega_s(t)$ to obtain some element $v \in V$.*

2. Set $y_0 = v$ and iteratively apply $\Omega_P(y_i)$ to produce the cycle V.

Then, $S \oplus T = V$.

Iteratively applying $S \oplus T$ creates cycles formed of p-cycles of Ω_P. Indeed, let C_i be any given p-cycle. Then

$$C_{j+1} = S \oplus C_j \qquad \text{for } j \leq p.$$

By Remark 5, the cycle structure created by the iterative application of $S \oplus T$ mirrors that of Ω_P for f. Recall that the fixed points for f a Type-1 or Type-3 function are distributed across $p^{t-r-1} - 1$ cycles of length p in the cycle structure of Ω_P, in addition to one cycle of length $p - 1$ and a single 1-cycle consisting of Φ. The iterative application of $S \oplus T$ clusters p-cycles of Ω_P into a single cycle. Rather than cycles of elements of $\mathbb{F}_q$, these are cycles of p-cycles of Ω_P.

Here, we illustrate how the iterative application of $S \oplus T$ mirrors the cycle structure of Ω_P. First, observe that, by Remark 2, $S \oplus S$ produces a $(p-1)$-cycle of p-cycles of Ω_P, just as applying Ω_P with $y_0 = P$ created a $(p-1)$-cycle of elements. Additionally, iteratively applying $S \oplus T$, for any $T \neq S$ a p-cycle of Ω_P, will produce a cycle of length p formed of p-cycles of Ω_P. Note that, because this approach only generates p-cycles of Ω_P, we must be sure to first obtain the fixed points in the 1-cycle, namely Φ, as well as the $(p-1)$-cycle of Ω_P. See Figure 4.1 for an example implementation of this method.

What follows is an optimized algorithmic method for finding fixed points for f a Type-1 or Type-3 function over $\mathbb{F}_q$, $q = p^t$.

1. Compute the number of fixed points for f as $N = p^{t-r}$, where r is as in Theorem 13.

2. By Lemma 14, the first fixed point is Φ.

Example Implementation for f a Type-1 Function

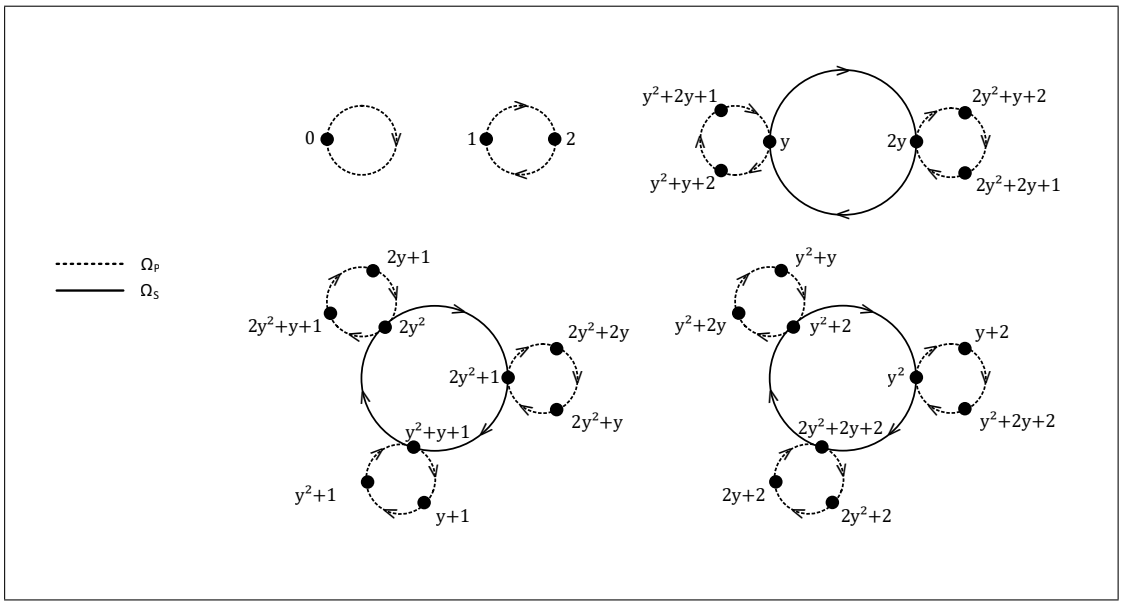

Figure 4.1: Each node is a fixed point for $f(x) = x$ over $\mathbb{F}_{3^3}$, where y is a root of the irreducible polynomial $x^3 + 2x + 1$.

3. Perform a brute force search for a non-zero fixed point $P \neq \Phi$ to define Ω_P.

4. Set $y_0 = P$ and iteratively apply Ω_P to yield $p - 1$ fixed points, by Remark 2.

5. Perform a brute force search for a fixed point, $s \neq \Phi$, which does not exist in the cycle of length $p - 1$. Define Ω_s.

6. Iteratively apply $C_{j+1} = S \oplus C_j$ with $C_0 = S$. This will create a $(p-1)$-cycle consisting of p-cycles of Ω_P.

7. Perform a brute force search for a fixed point which has not yet appeared in any cycle. Call this element t in some fixed point cycle, T.

8. Iteratively apply $C_{j+1} = S \oplus C_j$ with $C_0 = T$. This will produce a cycle of length p consisting of p-cycles of Ω_P. If $\text{char}(\mathbb{F}_q) \neq 2$, then the additive inverse of each fixed point obtained is also a fixed point.

9. Repeat Steps 7 and 8 until all points are found.

For Type-1 functions with $\mathrm{char}(\mathbb{F}_q) \neq 2$, this method requires $\frac{p^{t-r-2}+3}{2}$ brute forces. For Type-3 functions or Type-1 with $\mathrm{char}(\mathbb{F}_q) = 2$, this method requires $2^{t-r-2} + 1$ brute forces. We have improved the previous algorithm by a factor of p.

A word on brute force searches

Each brute force search takes time and resources, so it is prudent to understand how quickly one may perform them. An initial brute force search over the field is necessary to obtain a fixed point $P \neq \Phi$ with which to define Ω_P. The probability of obtaining such a point may be mapped by the hypergeometric distribution. In this case, a "success" state is denoted by an element in $\mathbb{F}_q$ being a fixed point. Note that, because P must be non-zero, we remove zero from our population. Hence, setting $N = p^t - 1$ and $K = p^{t-r} - 1$, we wish to determine the probability of obtaining a fixed point in the first few tries.

For a Type-1 function, we are working in $\mathbb{F}_q$ with $q = p^t$ and $a = 0$. Then, by (2.1), the probability of drawing a fixed point on the ith draw is

$$P(X_i) = \frac{K}{N} = \frac{p^{t-r} - 1}{p^t - 1} \approx p^{-r} \quad \text{for all } i.$$

For a Type-3 function, we are in the field $\mathbb{F}_q$ with $q = 2^t$ and $a \neq 0$. Therefore, there exists precisely one element $\Phi \in \mathbb{F}_q$ such that $a = \Phi^2$. Because Φ is not a valid element to set as P, we remove it from the population. Then with $N = 2^t - 2$ and $K = 2^{t-r} - 2$, we have

$$P(X_i) = \frac{K}{N} = \frac{2^{t-r} - 2}{2^t - 2} = \frac{2^{t-r-1} - 1}{2^{t-1} - 1} \approx 2^{-r} \quad \text{for all } i.$$

Clearly, the size of r is integral to the efficiency of the algorithm. If both r and

p are small, the probability of obtaining a fixed point at any given draw is high and we can find P with relatively little effort. Once this is done, we can apply Ω_P to determine $p-1$ fixed points for the function. Further fixed points must be obtained by additional brute force. These searches may again be mapped by the hypergeometric distribution, decreasing the search space each time a search is performed by removing those elements which have already been deemed a non-fixed point, as well as all cycles of fixed points obtained. When r is large, this process is slow and cumbersome. In this case, the efficient approach to obtaining fixed points for either of these classes is to use a factoring algorithm to determine the roots of

$$L^*(x) = \sum_{i=1}^{l} c_i x^{p^i} + (c_0 - 1)x = \sum_{i=1}^{l} d_i x^{p^i}.$$

For more information regarding the factorization of polynomials over finite fields, please refer to [9].

4.2 The Fixed Point Algorithm

Let $q = p^t$, $a \in \mathbb{F}_q$, and $\Phi \in \mathbb{F}_{q^2}$, with $a = \Phi^2$. An algorithm for producing all of the fixed points in $\mathbb{F}_q$ for a function f satisfying the Carlitz property is as follows.

4.2.1 f is a Rédei function

Algorithm 1: Print the fixed points for $R_n(x, a)$ over $\mathbb{F}_q$, where $a = \Phi^2$

Data: q odd; $a \neq 0$; $n > 0$; g a generator element in $\mathbb{F}_q^*$ if $\chi(a) = 1$, or $\mathbb{F}_{q^2}^*$ if $\chi(a) = -1$
Result: N fixed points for $R_n(x, a)$
$N \leftarrow \gcd(n-1, q-\chi(a)) + (1+\chi(a)) - 1$
$k \leftarrow \gcd(n-1, q-\chi(a))$
if $\chi(a) = 1$ **then** // find γ such that $\mathrm{ord}(\gamma) = k$
  print$(\pm\Phi)$
  $\gamma \leftarrow g^{\frac{q-1}{k}}$
else // $\chi(a) = -1$
  $\gamma \leftarrow g^{\frac{q^2-1}{k}}$
end
$P \leftarrow \Phi\left(\frac{1+\gamma}{1-\gamma}\right)$
$y \leftarrow P$
repeat // gives a cycle of length N
  if $y = -P$ **then**
    $y \leftarrow P$
  else
    $y \leftarrow \frac{Py+a}{P+y}$
  end
  print(y)
until $y = P$

4.2.2 f is a Type-1 or Type-3 function

Algorithm 2: Print the fixed points for f a Type-1 or Type-3 function over $\mathbb{F}_q$, where $q = p^t$ and $a = \Phi^2$

Data: r the rank of the $t \times t$ matrix B in Theorem 13
Result: p^{t-r} fixed points for f
$N \leftarrow p^{t-r}$
print(Φ)
perform a brute force search for a fixed point $P \neq 0, \Phi$
$y \leftarrow P$
repeat `// gives cycle of length` $p-1$
  if $y = -P$ **then**
    $y \leftarrow P$
  else
    $y \leftarrow \frac{Py+a}{P+y}$
  end
  print(y)
until $y = P$
fixedpointcounter $\leftarrow p$
while fixedpointcounter $< N$ **do**
  perform a brute force search for a fixed point Q not yet observed in any cycle
  $y \leftarrow Q$
  for $i \leftarrow 1$ **to** p **do**
    $y \leftarrow \frac{Py+a}{P+y}$
    print(y)
    if $\mathrm{char}(\mathbb{F}_q) \neq 2$ **then**
      print$(-y)$ `// additive inverses are fixed points`
    end
  end
  if $\mathrm{char}(\mathbb{F}_q) \neq 2$ **then**
    fixedpointcounter $\leftarrow$ fixedpointcounter $+2p$
  else
    fixedpointcounter $\leftarrow$ fixedpointcounter $+p$
  end
end

4.2.3 f is a Type-1 or Type-3 function, optimized

Algorithm 3: Print the fixed points for f a Type-1 or Type-3 function over $\mathbb{F}_q$, where $q = p^t$ and $a = \Phi^2$

Data: r the rank of the $t \times t$ matrix B in Theorem 13
Result: p^{t-r} fixed points for f
$N \leftarrow p^{t-r}$
Function `OmegaP(`y`):` `// produces p-cycles of fixed points`
  for $i \leftarrow 1$ **to** p **do**
    $y \leftarrow \frac{Py+a}{P+y}$
    print(y)
    if $\mathrm{char}(\mathbb{F}_q) \neq 2$ **and** Sflag $=$ *false* **then**
      print$(-y)$ `// additive inverses are fixed points`
      fixedpointcounter $\leftarrow$ fixedpointcounter $+2$
    else
      fixedpointcounter $\leftarrow$ fixedpointcounter $+1$
  if fixedpointcounter $= N$ **then**
    exit
  return y
Function `OmegaS(`y`):` `// produces cycles of cycles`
  if $y = S$ **then**
    numberofloops $= p - 1$
    Sflag $=$ *true*
  else
    numberofloops $= p$
    Sflag $=$ *false*
  for $i \leftarrow 1$ **to** numberofloops **do**
    if $y = -S$ **then**
      $y \leftarrow S$
    else
      $y \leftarrow \frac{Sy+a}{S+y}$
    $y \leftarrow$ `OmegaP(`y`)`
print(Φ)
perform a brute force search for a fixed point $P \neq 0, \Phi$
$y \leftarrow P$
repeat `// gives cycle of length` $p - 1$
  if $y = -P$ **then**
    $y \leftarrow P$
  else
    $y \leftarrow \frac{Py+a}{P+y}$
  print(y)
until $y = P$
fixedpointcounter $\leftarrow p$
if fixedpointcounter $= N$ **then**
  exit;
perform a brute force search for a fixed point S not yet obtained in any cycle
`OmegaS(`S`)`
while fixedpointcounter $< N$ **do**
  perform a brute force search for a fixed point V not yet obtained in any cycle
  `OmegaS(`V`)`

4.3 An Explicit Expression for the Fixed Points of Rédei Functions

The algorithm given in Chapter 4.2.1 alludes to an explicit representation for the fixed points of Rédei functions over $\mathbb{F}_q$, with $\text{char}(\mathbb{F}_q) \neq 2$.

Lemma 17. *Let $P = \Phi\left(\frac{1+\gamma}{1-\gamma}\right)$ be a non-zero fixed point for $R_n(x, a)$. The iterative generating function Ω_P for R_n may be redefined as*

$$y_{i+1} = \Omega_P(y_i) \coloneqq \begin{cases} \omega_P(y_i) & \text{if } y_i \neq -\Phi\left(\frac{1+\gamma}{1-\gamma}\right), \\ \Phi\left(\frac{1+\gamma}{1-\gamma}\right) & \text{if } y_i = -\Phi\left(\frac{1+\gamma}{1-\gamma}\right), \end{cases}$$

where $\omega_P(y_i) = \frac{Py_i+\Phi^2}{P+y_i} = \Phi\left[\frac{(y_i+\Phi)+\gamma(y_i-\Phi)}{(y_i+\Phi)-\gamma(y_i-\Phi)}\right]$.

Theorem 15. *Consider the Rédei function $R_n(x, a)$ with $a = \Phi^2$, where $a \in \mathbb{F}_q$ and $\Phi \in \mathbb{F}_{q^2}$. The fixed points for $R_n(x, a)$ are:*

$$P_i = \Phi\left(\frac{1+\gamma^i}{1-\gamma^i}\right)$$

where $k = \gcd(n-1, q-\chi(a))$, $i \in 1, 2, \ldots, k-1$, and γ is an arbitrary element such that $\text{ord}(\gamma) = k$ and

$$\gamma \in \begin{cases} \mathbb{F}_q & \text{if } \chi(a) = 1, \\ \mathbb{F}_{q^2} & \text{if } \chi(a) = -1. \end{cases}$$

Additionally, if $\chi(a) = 1$, $x = \pm\Phi$ are two further fixed points for $R_n(x, a)$.

Proof. From the definition of the Rédei function given in (2.3), clearly, if $\chi(a) = 1$ (that is, $\Phi \in \mathbb{F}_q$), then $\pm\Phi$ are two fixed points for $R_n(x, a)$.

We show that all P_i are fixed points of R_n by using an inductive argument.

Base case: We proved in Theorem 12 that $P_1 = \Phi\left(\frac{1+\gamma}{1-\gamma}\right)$ is a fixed point.

Inductive step: Assume P_j is a fixed point for some positive integer $j \neq 0$. We show that P_{j+1} is also a fixed point.

Using the representation of Ω_P in Lemma 17,

$$\Omega_P(P_j) = \Phi\left[\frac{\frac{2}{1-\gamma^j} + \gamma\left(\frac{2\gamma^j}{1-\gamma^j}\right)}{\frac{2}{1-\gamma^j} - \gamma\left(\frac{2\gamma^j}{1-\gamma^j}\right)}\right] = \Phi\left(\frac{1+\gamma^{j+1}}{1-\gamma^{j+1}}\right) = P_{j+1}.$$

Hence, by the principle of induction, P_i is a fixed point for any i. Since we are working in $\mathbb{F}_q$ and because $P_k = \infty$, we take $i \in 1, 2, \ldots, k-1$.

Observe that we have obtained all of the fixed points for the Rédei function since the total number of fixed points for $R_n(x, a)$ in $\mathbb{F}_q$ is

$$N = \gcd(n-1, q-\chi(a)) + (1+\chi(a)) - 1 = (k-1) + (1+\chi(a)).$$

If $\chi(a) = -1$, we have discovered all $k-1$ points. If $\chi(a) = 1$, we have found $k-1$ fixed points and simply include the two additional points $\pm\Phi$. □

The following examples illustrate this method for determining all fixed points for a given Rédei function. Note that the order in which the fixed points are obtained differs according to the user's choice of γ.

Example 1. *We wish to determine all of the fixed points for* $R_5(x, 3)$ *in* $\mathbb{F}_{13}$. *Here,* $\chi(a) = 1$ *and* $\Phi = \pm 4$. *We have* $k = \gcd(4, 12) = 4$ *and hence* $i \in 1, 2, 3$. *We must find an element* $\gamma \in \mathbb{F}_{13}$ *such that* $\mathrm{ord}(\gamma) = 4$. *We choose* $\gamma = 5$. *Then the fixed points for* $R_5(x, 3)$ *are*

$$\left\{P_i : P_i = 4\left(\frac{1+5^i}{1-5^i}\right), i = 1, 2, 3\right\} = \{7, 0, 6\},$$

with the two additional fixed points $\pm\Phi = \{4, 9\}$.

Example 2. *We wish to determine all of the fixed points for* $R_7(x, 2)$ *in* $\mathbb{F}_{29}$. *Here,* $\chi(a) = -1$ *and hence, we will need to choose a construction of* $\mathbb{F}_{29^2}$*:* $\mathbb{F}_{29^2} = \mathbb{F}_{29}[X]/(x^2 + 23x + 6)$. *Then* $\Phi = \pm(7x + 8)$. *We also have* $k = \gcd(6, 30) = 6$, *hence,* $i \in 1, 2, \ldots, 5$ *and we must find an element* $\gamma \in \mathbb{F}_{29^2}$ *such that* $\mathrm{ord}(\gamma) = 6$. *We choose* $\gamma = 6x + 26$. *Then the fixed points for* $R_7(x, 2)$ *are*

$$\left\{ P_i : P_i = (7x + 8)\left(\frac{1 + (6x + 26)^i}{1 - (6x + 26)^i}\right), i = 1, \ldots, 5 \right\} = \{20, 26, 0, 3, 9\}.$$

5 Conclusion

In an increasingly digital world, cryptographic security must be achieved alongside features such as speed, efficiency, and smaller hardware components. A recent surge of interest in involutions has sought to address these issues within certain cryptosystems, such as the reflection cipher. As it became known that the number of fixed points of such involutions is an important cryptographic criterion, methods for the reduction of fixed points began to surface, some of which necessitated knowledge of the precise location of these points. The ability to pinpoint and subsequently eliminate fixed points of permutations allows for the development of systems with good cryptographic properties.

In this thesis, we have introduced an algorithm which determines the fixed points of all rational functions over $\mathbb{F}_q$ satisfying the Carlitz property. When applied to a Rédei function, this algorithm efficiently generates all of the function's fixed points over $\mathbb{F}_q$. Further, we have provided an explicit expression for these points. For Type-1 and Type-3 functions, we provide a method for algorithmically determining their fixed points, along with an optimization of this method. Previous to this contribution, the only permutations whose fixed points had been discovered to date were those of Dickson involutions of the first kind over $\mathbb{F}_{2^t}$ and monomial involutions over $\mathbb{F}_q$.

Combining the efficiency of involutions with the security of a permutation with few fixed points is a useful angle to research. It would be of interest to determine precisely how the involution properties of Rédei functions interact with a

restriction on the number of fixed points for that function. In [16], the authors present explicit formulas for all the involutions of $\mathbb{F}_q$ that are given by monomials, a result which seamlessly translates to Rédei functions. The study of classes of Rédei involutions with a minimal set of fixed points would complement the same result for Dickson involutions given in [7].

6 References

[1] Aabrandt, A. and Hansen, V.L. (2016). *A note on powers in finite fields.* International Journal of Mathematical Education in Science and Technology, 47(6), 987-991.

[2] Barbero, S., Cerruti, U., and Murru, N. (2010). *Solving the Pell equation via Rédei rational functions.* The Fibonacci Quarterly, 48(4), 348-357.

[3] Bellini, E. and Murru, N. (2016). *An efficient and secure RSA-like cryptosystem exploiting Rédei rational functions over conics.* Finite Fields and Their Applications, 39, 179-194.

[4] Boura, C., Canteaut, A., Knudsen, L. R., and Leander, G. (2015). *Reflection ciphers.* Designs, Codes and Cryptography, 82(1-2), 3-25.

[5] Carlitz, L. (1962). *A note on permutation functions over a finite field.* Duke Mathematical Journal, 29(2), 325-332.

[6] Cesmelioglu, A., Meidl, W., and Topuzoglu, A. (2008). *On the cycle structure of permutation polynomials.* Finite Fields and Their Applications, 14(3), 593-614.

[7] Charpin, P., Mesnager, S., and Sarkar, S. (2016). *Dickson polynomials that are involutions.* In Contemporary Developments in Finite Fields and Applications, 22-47. Singapore: World Scientific Publishing Co. Pte. Ltd.

[8] Charpin, P., Mesnager, S., and Sarkar, S. (2016). *Involutions over the Galois field* $\mathbb{F}_{2^n}$. IEEE Transactions on Information Theory, 62(4), 2266-2276.

[9] von zur Gathen, J. and Panario, D. (2001). *Factoring Polynomials Over Finite Fields: A Survey.* Journal of Symbolic Computation, 31(1-2), 3-17.

[10] Gutierrez, J. and Winterhof, A. (2008). *Exponential sums of non-linear congruential pseudorandom number generators with Rédei functions.* Finite Fields and Their Applications, 14(2), 410-416.

[11] Kameswari, P. A. and Kumari, R. C. (2012). *Cryptosystem with Rédei rational functions via Pell conics.* International Journal of Computer Applications, 54(15), 1-6.

[12] Lidl, R. and Niederreiter, H. (1997). Finite Fields (2nd ed). Cambridge: Cambridge University Press.

[13] Nobauer, R. (1984). *Cryptanalysis of the Rédei scheme.* In Contributions to General Algebra, Vol. 3, Teubner, Vienna. 255-264.

[14] Panario, D., Sadeghi, M., and Sakzad, A. (2012). *Cycle structure of permutation functions over finite fields and their applications.* Advances in Mathematics of Communications, 6(3), 347-361.

[15] Qureshi, C. and Panario, D. (2015). *Rédei actions on finite fields and multiplication map in cyclic group.* SIAM Journal on Discrete Mathematics, 29(3), 1486-1503.

[16] Rubio, I., Pacheco-Tallaj, N., Corrada-Bravo, C., and Castro, F. (2017). *Explicit formulas for monomial involutions over finite fields.* Advances in Mathematics of Communications, 11(2), 301-306.

[17] Soleimany, H., Blondeau, C., Yu, X., Wu, W., Nyberg, K., Zhang, H., Zhang, L., and Wang, Y. (2013). *Reflection cryptanalysis of PRINCE-like ciphers*. Journal of Cryptology, 28(3), 718-744.

[18] Wang, Q. (2017). *A note on inverses of cyclotomic mapping permutation polynomials over finite fields*. Finite Fields and Their Applications, 45, 422-427.

[19] Wu, B. and Liu, Z. (2013). *Linearized polynomials over finite fields revisited*. Finite Fields and Their Applications, 22, 79-100.

[20] Youssef, A., Tavares, S., and Heys, H. (1996). *A new class of substitution-permutation networks*. Proceedings of Selected Areas in Cryptography, SAC-96, 132-147.

7 Appendices

Sample Fixed Points for Type-1 Functions

$\mathbb{F}_q$	$f(x)$	Φ	N	Fixed Points
$\mathbb{F}_{3^2}$ [a]	$\left(\frac{y}{x} + \frac{2y+1}{x^3}\right)^{-1}$	0	3	$[0,\ 1,\ 2]$
	$\left(\frac{2y+2}{x} + \frac{2}{x^3} + \frac{y}{x^{3^2}} + \frac{y+2}{x^{3^3}}\right)^{-1}$	0	3	$[0,\ y+2,\ 2y+1]$
$\mathbb{F}_{3^3}$ [b]	$\left(\frac{y^2+2}{x} + \frac{y}{x^3} + \frac{y^2+y+2}{x^{3^2}}\right)^{-1}$	0	1	$[0]$
	$\left(\frac{y^2+2y+2}{x} + \frac{y+1}{x^3} + \frac{2y^2+2y}{x^{3^2}}\right)^{-1}$	0	3	$[0,\ y^2+2y+1,$ $2y^2+y+2]$
$\mathbb{F}_{5^2}$ [c]	$\left(\frac{3y}{x} + \frac{3}{x^5} + \frac{3y+4}{x^{5^2}}\right)^{-1}$	0	5	$[0,\ y,\ 2y,\ 3y,\ 4y]$
	$\left(\frac{y+2}{x} + \frac{y}{x^5} + \frac{4}{x^{5^2}}\right)^{-1}$	0	5	$[0,\ y+2,\ 2y+4,$ $3y+1,\ 4y+3]$
$\mathbb{F}_{5^3}$ [d]	$\left(\frac{2y^2+4y+3}{x} + \frac{3y+3}{x^5}\right)^{-1}$	0	5	$[0,\ y^2+4y+1,$ $2y^2+3y+2,$ $3y^2+2y+3,$ $4y^2+y+4]$
	$\left(\frac{y^2+2y+1}{x} + \frac{4y+3}{x^5} + \frac{2y^2+y+3}{x^{5^2}}\right)^{-1}$	0	5	$[0,\ y^2+3y,\ 2y^2+y,$ $3y^2+4y,\ 4y^2+2y]$
$\mathbb{F}_7$	$\left(\frac{4}{x^7} + \frac{6}{x^{7^2}} + \frac{5}{x^{7^3}}\right)^{-1}$	0	7	$[0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6]$
$\mathbb{F}_{7^2}$ [e]	$\left(\frac{2y+4}{x} + \frac{6y+6}{x^7} + \frac{y+1}{x^{7^2}}\right)^{-1}$	0	1	$[0]$
	$\left(\frac{3y+6}{x} + \frac{5y+4}{x^7} + \frac{6}{x^{7^2}}\right)^{-1}$	0	7	$[0,\ y+2,\ 2y+4,$ $3y+6,\ 4y+1,$ $5y+3,\ 6y+5]$

Table 7.1: List of the N fixed points for f a Type-1 function with $a = 0$ and $q = p^t$.

[a] $y \in \mathbb{F}_{3^2}$ and a root of the primitive polynomial $x^2 + 2x + 2$.
[b] $y \in \mathbb{F}_{3^3}$ and a root of the primitive polynomial $x^3 + 2x + 1$.
[c] $y \in \mathbb{F}_{5^2}$ and a root of the primitive polynomial $x^2 + 4x + 2$.
[d] $y \in \mathbb{F}_{5^3}$ and a root of the primitive polynomial $x^3 + 3x + 3$.
[e] $y \in \mathbb{F}_{7^2}$ and a root of the primitive polynomial $x^2 + 6x + 3$.

Sample Fixed Points for Rédei Functions

$\mathbb{F}_q$	$R_n(x,a)$	$\chi(a)$	γ	N	Fixed Points
$\mathbb{F}_3$	$R_1(x,1)$	1	2	3	[1, 2, 0]
	$R_2(x,1)$	1	1	2	[1, 2]
	$R_3(x,1)$	1	2	3	[1, 2, 0]
$\mathbb{F}_{3^2}$ [a]	$R_1(x,2)$	1	y	9	$[y+1, 2y+2, y, 2,$ $y+2, 0, 2y+1, 1, 2y]$
	$R_2(x,2)$	1	1	2	$[y+1, 2y+2]$
	$R_3(x,2y+2)$	1	2	3	$[2y+1, y+2, 0]$
	$R_4(x,y+1)$	1	1	2	$[y, 2y]$
	$R_5(x,2)$	1	$y+1$	5	$[y+1, 2y+2, 2, 0, 1]$
	$R_6(x,2y+2)$	1	1	2	$[2y+1, y+2]$
	$R_7(x,y+1)$	1	2	3	$[y, 2y, 0]$
	$R_8(x,1)$	1	1	2	[2, 1]
	$R_9(x,1)$	1	y	9	$[2, 1, 2y+1, 2y+2,$ $y, 0, 2y, y+1, y+2]$
$\mathbb{F}_5$	$R_1(x,1)$	1	2	5	$[1, 4, 2, 0, 3]$
	$R_2(x,1)$	1	1	2	$[1, 4]$
	$R_3(x,1)$	1	4	3	$[1, 4, 0]$
	$R_4(x,4)$	1	1	2	$[2, 3]$
	$R_5(x,1)$	1	2	5	$[1, 4, 2, 0, 3]$
$\mathbb{F}_7$	$R_1(x,4)$	1	3	7	$[2, 5, 3, 1, 0, 6, 4]$
	$R_2(x,1)$	1	1	2	$[1, 6]$
	$R_3(x,1)$	1	6	3	$[1, 6, 0]$
	$R_4(x,2)$	1	2	4	$[3, 4, 5, 2]$
	$R_5(x,2)$	1	6	3	$[3, 4, 0]$
	$R_6(x,2)$	1	1	2	$[3, 4]$
	$R_7(x,1)$	1	3	7	$[1, 6, 5, 4, 0, 3, 2]$
$\mathbb{F}_{11}$	$R_1(x,3)$	1	2	11	$[5, 6, 7, 10, 3, 9, 0, 2, 8, 1, 4]$
	$R_2(x,3)$	1	1	2	$[5, 6]$
	$R_3(x,1)$	1	10	3	$[1, 10, 0]$
	$R_4(x,3)$	1	1	2	$[5, 6]$
	$R_5(x,3)$	1	10	3	$[5, 6, 0]$
	$R_6(x,1)$	1	4	6	$[1, 10, 2, 4, 7, 9]$
	$R_7(x,1)$	1	10	3	$[1, 10, 0]$
	$R_8(x,9)$	1	1	2	$[3, 8]$
	$R_9(x,1)$	1	10	3	$[1, 10, 0]$
	$R_{10}(x,4)$	1	1	2	$[2, 9]$
	$R_{11}(x,3)$	1	2	11	$[5, 6, 7, 10, 3, 9, 0, 2, 8, 1, 4]$

Table 7.2: List of the N fixed points for sample Rédei functions with a square.

[a] $y \in \mathbb{F}_{3^2}$ and a root of the primitive polynomial $x^2 + 2x + 2$.

$\mathbb{F}_q$	$R_n(x,a)$	$\chi(a)$	γ	N	Fixed Points
$\mathbb{F}_3$ [a]	$R_1(x,2)$	-1	$b+1$	3	$[2,0,1]$
	$R_2(x,2)$	-1	1	0	[]
	$R_3(x,2)$	-1	2	1	[0]
$\mathbb{F}_{3^2}$ [b]	$R_1(x,2y)$	-1	b^2+b+2	9	$[2b^3+2b^2+2, 2, b^3+b^2+2,$ $2b^3+2b^2, 0, b^3+b^2,$ $2b^3+2b^2+1, 1, b^3+b^2+1]$
	$R_2(x,y+2)$	-1	1	0	[]
	$R_3(x,2y)$	-1	2	1	[0]
	$R_4(x,2y+1)$	-1	1	0	[]
	$R_5(x,2y)$	-1	2	1	[0]
	$R_6(x,y)$	-1	$2b^2+b+2$	4	$[2b^3+2b^2+2, b^3+b^2+2,$ $2b^3+2b^2+1, b^3+b^2+1]$
	$R_7(x,y)$	-1	2	1	[0]
	$R_8(x,2y+1)$	-1	1	0	[]
	$R_9(x,2y)$	-1	2	1	[0]
$\mathbb{F}_5$ [c]	$R_1(x,2)$	-1	$2b+2$	5	$[3,4,0,1,2]$
	$R_2(x,3)$	-1	1	0	[]
	$R_3(x,2)$	-1	4	1	[0]
	$R_4(x,3)$	-1	$2b+1$	2	$[3,2]$
	$R_5(x,3)$	-1	4	1	[0]
$\mathbb{F}_7$ [d]	$R_1(x,3)$	-1	$2b+4$	7	$[6,2,4,0,3,5,1]$
	$R_2(x,6)$	-1	1	0	[]
	$R_3(x,5)$	-1	6	1	[0]
	$R_4(x,3)$	-1	1	0	[]
	$R_5(x,6)$	-1	$6b+4$	3	$[6,0,1]$
	$R_6(x,6)$	-1	1	0	[]
	$R_7(x,5)$	-1	6	1	[0]
$\mathbb{F}_{11}$ [e]	$R_1(x,7)$	-1	$9b+7$	11	$[5,10,9,4,3,0,8,7,2,1,6]$
	$R_2(x,2)$	-1	1	0	[]
	$R_3(x,6)$	-1	10	1	[0]
	$R_4(x,7)$	-1	$10b+7$	2	$[4,7]$
	$R_5(x,2)$	-1	$7b+8$	3	$[3,0,8]$
	$R_6(x,6)$	-1	1	0	[]
	$R_7(x,6)$	-1	$10b+8$	5	$[9,3,0,8,2]$
	$R_8(x,8)$	-1	1	0	[]
	$R_9(x,6)$	-1	$7b+8$	3	$[4,0,7]$
	$R_{10}(x,6)$	-1	$10b+7$	2	$[3,8]$
	$R_{11}(x,6)$	-1	10	1	[0]

Table 7.3: List of the N fixed points for sample Rédei functions with a non-square. The fixed points are represented in $\mathbb{F}_{q^2}$ but exist in $\mathbb{F}_q$.

[a] $b \in \mathbb{F}_{3^2}$ and a root of the irreducible polynomial x^2+2x+2.
[b] $y \in \mathbb{F}_{3^2}$ a root of x^2+2x+2 and $b \in \mathbb{F}_{3^4}$ a root of x^4+2x^3+2.
[c] $b \in \mathbb{F}_{5^2}$ a root of the irreducible polynomial x^2+4x+2.
[d] $b \in \mathbb{F}_{7^2}$ a root of the irreducible polynomial x^2+6x+3.
[e] $b \in \mathbb{F}_{11^2}$ a root of the irreducible polynomial x^2+7x+2.

Sample Fixed Points for Type-3 Functions

$\mathbb{F}_q$	$f(x)$	Φ	N	Fixed Points
$\mathbb{F}_2$	$\Phi + \left(\frac{1}{x+\Phi}\right)^{-1}$	1	2	[0, 1]
$\mathbb{F}_{2^2}$ [a]	$\Phi + \left(\frac{y+1}{x+\Phi}\right)^{-1}$	y	1	[y]
	$\Phi + \left(\frac{y+1}{(x+\Phi)^2}\right)^{-1}$	1	2	[1, y]
	$\Phi + \left(\frac{y+1}{(x+\Phi)^2} + \frac{y+1}{(x+\Phi)^{2^2}}\right)^{-1}$	1	2	[1, $y+1$]
$\mathbb{F}_{2^3}$ [b]	$\Phi + \left(\frac{y}{x+\Phi} + \frac{1}{(x+\Phi)^2}\right)^{-1}$	y^2+y+1	2	[1, y^2+y+1]
	$\Phi + \left(\frac{y^2+y+1}{x+\Phi} + \frac{1}{(x+\Phi)^2}\right)^{-1}$	y^2+1	2	[y^2+1, y^2+y]
	$\Phi + \left(\frac{y+1}{x+\Phi} + \frac{y^2+1}{(x+\Phi)^{2^2}}\right)^{-1}$	y^2+y	2	[0, y^2+y]
$\mathbb{F}_{2^4}$ [c]	$\Phi + \left(\frac{y+1}{x+\Phi}\right)^{-1}$	y^2+y	1	[y^2+y]
	$\Phi + \left(\frac{y^3+y^2}{(x+\Phi)^2}\right)^{-1}$	y^3+1	2	[y^2+1, y^3+1]
	$\Phi + \left(\frac{y^2+1}{(x+\Phi)^2} + \frac{y^2+1}{(x+\Phi)^{2^2}}\right)^{-1}$	y^3+y	1	[y^3+y]
$\mathbb{F}_{2^5}$ [d]	$\Phi + \left(\frac{y^4+y^3+y^2}{x+\Phi}\right)^{-1}$	y^2+y+1	1	[y^2+y+1]
	$\Phi + \left(\frac{y^4+1}{x+\Phi} + \frac{y^4+y^2}{(x+\Phi)^2}\right)^{-1}$	y^4+1	2	[y^4+1, y^4+y^3+1]
	$\Phi + \left(\frac{y^3+1}{x+\Phi} + \frac{y^2+1}{(x+\Phi)^{2^2}}\right)^{-1}$	y^3	2	[y^3, y^3+y^2+y+1]
$\mathbb{F}_{2^6}$ [e]	$\Phi + \left(\frac{y^3+y^2+y}{x+\Phi}\right)^{-1}$	y^4+y^2	1	[y^4+y^2]
	$\Phi + \left(\frac{y^5+y^4+y^3+y^2+1}{(x+\Phi)^2} + \frac{y^5+y^3+y^2}{(x+\Phi)^{2^2}}\right)^{-1}$	y^5+y^4	1	[y^5+y^4]
	$\Phi + \left(\frac{y^5+y^4+y^2+y}{(x+\Phi)^2} + \frac{y^5+y^4+y^3+y^2}{(x+\Phi)^{2^2}}\right)^{-1}$	y^3+y^2+y	4	[y^2+y, y^3+y^2+y, y^4+y^2, y^5+y^3+y]

Table 7.4: List of the N fixed points for f a Type-3 function with $a \neq 0$ and $q = 2^t$.

[a] $y \in \mathbb{F}_{2^2}$ and a root of the primitive polynomial $x^2 + x + 1$.
[b] $y \in \mathbb{F}_{2^3}$ and a root of the primitive polynomial $x^3 + x + 1$.
[c] $y \in \mathbb{F}_{2^4}$ and a root of the primitive polynomial $x^4 + x + 1$.
[d] $y \in \mathbb{F}_{2^5}$ and a root of the primitive polynomial $x^5 + x^2 + 1$.
[e] $y \in \mathbb{F}_{2^6}$ and a root of the primitive polynomial $x^6 + x^4 + x^3 + x + 1$.