UNIVERSITY OF PUERTO RICO
RIO PIEDRAS CAMPUS
FACULTY OF NATURAL SCIENCES
DEPARTMENT OF MATHEMATICS

Involutions of Finite Fields Obtained From Binomials of the Form $x^m(x^{\frac{q-1}{2}} + a)$

Lillian González Albino

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE IN MATHEMATICS
AT THE UNIVERSITY OF PUERTO RICO

March 11th, 2022

APPROVED BY THE MASTER OF SCIENCE ADVISORY COMMITTEE

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF SCIENCE IN MATHEMATICS

AT THE UNIVERSITY OF PUERTO RICO

ADVISOR: _____

Ivelisse Rubio, Ph.D.

University of Puerto Rico, Río Piedras

Department of Computer Science

READERS: _____

Ariane Masuda, Ph.D.

New York City College of Technology

Department of Mathematics

_____

Luis A. Medina, Ph.D.

University of Puerto Rico, Río Piedras

Department of Mathematics

Abstract

Permutations of finite fields $\mathbb{F}_q$ have many applications ranging from cryptography and combinatorics to the theory of computation. In many of these applications, a permutation and its inverse are stored in memory. A good option to reduce the memory footprint is to generate the permutation with a polynomial at the time of implementation. A better option is to use a permutation polynomial that is its own inverse; in this case, the permutation is called an involution. In applications to cryptography, the number of fixed points is correlated with its cryptographic properties.

In 2018, Zheng et al. characterized involutions of the form $x^m h(x^s)$ over $\mathbb{F}_q$, and, in 2017, Castro et al. gave explicit formulas for monomial involutions of $\mathbb{F}_q$ and their fixed points. The next simplest polynomials to study would be the binomials.

In this work we characterize involutions of $\mathbb{F}_q$ of the form $x^m(x^{\frac{q-1}{2}} + a)$ in terms of the number of fixed points. We present explicit formulas for obtaining these involutions and formulas for their fixed points. Additionally, we give an improvement of Zheng et al.'s result for polynomial involutions of $\mathbb{F}_q$ of the form $x^m h(x^{\frac{q-1}{2}})$.

Dedication

I dedicate this work to my dad, Roberto González Cruz, whose unwavering love and support got me to where I am today and will surely take me to where I need to be tomorrow.

Acknowledgements

I would first like to thank Dr. Ivelisse Rubio whom I have had the privilege to call my mentor since 2015. This has been a long and unconventional journey throughout which she has countless times encouraged me to push past my own expectations. I also want to thank Dr. Ariane Masuda for suggesting we continue this problem for this thesis and for her invaluable guidance throughout its completion. I am immensely grateful to both of them for all their help, guidance and friendship.

I want to give special thanks to my parents, sister, life partner, and closest friends; through all the ups and downs, they have given me the love and support that I could not have done without.

Thank you to Dr. Luis A. Medina for being part of my thesis committee and for his feedback on this work. Finally, I would like to thank the PRLSAMP that helped make this collaboration possible.

Contents

Introduction

Permutations of finite fields $\mathbb{F}_q$ have been extensively studied, in part due to their wide range of applications. In many applications such as the design of block ciphers, a permutation and its inverse are stored in memory, a burden for environments with limited resources such as Radio-Frequency Identification (RFID) tags. Instead of using two permutations, we can reduce the memory footprint by using permutations that are their own inverses, called involutions [3, 6, 8]. There have been studies that show that involutions are good candidates against linear and differential attacks on block ciphers. Moreover, these studies suggest that the number of fixed points is negatively correlated to the cryptographic properties of block ciphers [16, 4]. Another application that benefits from the use of involutions is the construction of deterministic interleavers for turbo codes, where usually permutations with few fixed elements have good dispersion properties [12, 14, 13].

In 2017, Castro et al. not only characterized monomial involutions of $\mathbb{F}_q$, they also gave explicit formulas to construct all monomial involutions given the size of the field and the number of fixed points [2]. To follow the work done by Castro et al., a natural next step is to study binomials involutions that are linear combinations of monomial involutions. This leads us to the study of the binomial $x^{q-2} + ax^{\frac{q-3}{2}}$, a linear combination of two well studied monomial involutions [12]. Involutions of this form were characterized by Cáceres and Colón in [5]; note that we can write this binomial as $x^{\frac{q-3}{2}}(x^{\frac{q-1}{2}} + a)$. To generalize these results, we study a more general family of binomials, namely binomials of the form $x^m(x^{\frac{q-1}{2}} + a)$ over $\mathbb{F}_q$. In 2019, a characterization of involutions of a family of polynomials over

$\mathbb{F}_q$ that encompasses $x^m(x^{\frac{q-1}{2}}+a)$ was given by Zheng et al. in [17].

In this work we continue the work on monomial involutions in [2] by giving both explicit formulas for involutions of the form $x^m(x^{\frac{q-1}{2}}+a)$ of $\mathbb{F}_q$ with a prescribed number of fixed points and explicit formulas for calculating their fixed points. We also give an improvement of the work done by Zheng et al. in [17] for polynomial involutions of $\mathbb{F}_q$ of the form $x^m h(x^{\frac{q-1}{2}})$.

2 Preliminaries

In this chapter we present the necessary definitions and results for the development of our work.

2.1 Finite Fields

We work over finite fields throughout this thesis. This section provides basic definitions and properties of finite fields.

Definition 2.1. A set F is a **field** if the following hold

1. F is a commutative group under addition,
2. $F \setminus \{0\}$ is a commutative group under multiplication,
3. $a(b+c) = ab + ac$, for all $a, b, c \in F$.

Definition 2.2. A **finite field** is a field that contains a finite number of elements. A finite field with q elements is denoted by $\mathbb{F}_q$. The multiplicative group of $\mathbb{F}_q$ is denoted by ${\mathbb{F}_q}^*$.

Proposition 2.3 ([7], Proposition 7.1.3)**.** *The number of elements in a finite field is a power of a prime.*

Proposition 2.4 ([7], Theorem 7.2.3)**.** *Let $n \geq 1$ be an integer and p be a prime. Then there exists a finite field with p^n elements.*

Proposition 2.5 ([7], Theorem 7.1.1)**.** *The multiplicative group of a finite field, ${\mathbb{F}_q}^*$, is cyclic.*

Since ${\mathbb{F}_q}^*$ is cyclic, there exists a non-zero element of the field that generates ${\mathbb{F}_q}^*$; we call this element a primitive element of the field.

Definition 2.6. Let $\alpha \in \mathbb{F}_q$. Then α is a **primitive element** of $\mathbb{F}_q$ if the powers of α generate all the elements of ${\mathbb{F}_q}^*$. That is ${\mathbb{F}_q}^* = \langle\alpha\rangle = \{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{q-2}\}$.

Primitive elements are useful because we can describe any non-zero element of the field as a specific power of α.

Example 2.7. Let $q = 13$. Note that

$$\begin{aligned}
2^0 &\equiv 1 \pmod{13}, & 2^4 &\equiv 3 \pmod{13}, & 2^8 &\equiv 9 \pmod{13},\\
2^1 &\equiv 2 \pmod{13}, & 2^5 &\equiv 6 \pmod{13}, & 2^9 &\equiv 5 \pmod{13},\\
2^2 &\equiv 4 \pmod{13}, & 2^6 &\equiv 12 \pmod{13}, & 2^{10} &\equiv 10 \pmod{13},\\
2^3 &\equiv 8 \pmod{13}, & 2^7 &\equiv 11 \pmod{13}, & 2^{11} &\equiv 7 \pmod{13}.
\end{aligned}$$

Hence, 2 is a primitive element of $\mathbb{F}_{13}$, i.e. $\mathbb{F}_{13}^* = \langle 2\rangle$.

$\diamond$

Proposition 2.8. Let q be odd. If α is a primitive element of $\mathbb{F}_q$, then $\alpha^{\frac{q-1}{2}} = -1$.

Proof. By the definition of a primitive element of $\mathbb{F}_q$, $q-1$ is the smallest integer such that $\alpha^{q-1} = 1$. Then $\alpha^{q-1} - 1 = 0$. Since $q-1$ is even, $\frac{q-1}{2} \in \mathbb{Z}$. Now,

$$\begin{aligned}
&(\alpha^{\frac{q-1}{2}})^2 - 1 = 0\\
\iff\ &(\alpha^{\frac{q-1}{2}} - 1)(\alpha^{\frac{q-1}{2}} + 1) = 0\\
\iff\ &\alpha^{\frac{q-1}{2}} = \pm 1.
\end{aligned}$$

But since $\frac{q-1}{2} < q-1$, then $\alpha^{\frac{q-1}{2}} = -1$.

$\square$

Definition 2.9. Let $r \in \mathbb{N}$. An r^{th} **root of unity** in $\mathbb{F}_q$ is an element $z \in \mathbb{F}_q$ that satisfies $z^r = 1$.

2.2 Elementary Number Theory

Number Theory is a branch of mathematics that studies integers. Its origin dates back to the ancient Greeks and since then various branches of mathematics have stemmed from Number Theory. Elementary Number Theory uses elementary methods to solve equations with integers. In this section we provide definitions and results from this field that aid us in working with fixed points and involutions. We use these concepts often in Chapters 3 and 4, therefore we provide various examples in this section to familiarize ourselves with them.

Definition 2.10. Let $a \in \mathbb{F}_q$. We say that a is a **square** in $\mathbb{F}_q$ if there exists $x \in \mathbb{F}_q$ such that $x^2 = a$ in $\mathbb{F}_q$. If a is not a square in $\mathbb{F}_q$ then we say it is a **non-square** in $\mathbb{F}_q$.

Example 2.11. Let $q = 13$. Then,

$$\begin{aligned}
0^2 &\equiv 0 \pmod{13}, & 5^2 &\equiv 12 \pmod{13}, & 9^2 &\equiv 3 \pmod{13},\\
1^2 &\equiv 1 \pmod{13}, & 6^2 &\equiv 10 \pmod{13}, & 10^2 &\equiv 9 \pmod{13},\\
2^2 &\equiv 4 \pmod{13}, & 7^2 &\equiv 10 \pmod{13}, & 11^2 &\equiv 4 \pmod{13},\\
3^2 &\equiv 9 \pmod{13}, & 8^2 &\equiv 12 \pmod{13}, & 12^2 &\equiv 1 \pmod{13}.\\
4^2 &\equiv 3 \pmod{13}, & & & &
\end{aligned}$$

Therefore, $0, 1, 3, 4, 9, 10, 12$ are squares and $2, 5, 6, 7, 8, 11$ are non-squares in $\mathbb{F}_{13}$.

$\diamond$

Definition 2.12. Let q be odd. The **quadratic character** of $\mathbb{F}_q$ is the function $\eta : \mathbb{F}_q \to \{0, 1, -1\}$ defined by

$$\eta(a) = \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if } a \text{ is a square in } {\mathbb{F}_q}^*, \\ -1 & \text{if } a \text{ is a non-square in } \mathbb{F}_q. \end{cases}$$

Proposition 2.13. Let q be odd and $a \in \mathbb{F}_q$, then $\eta(a) = a^{\frac{q-1}{2}}$.

Proof. If $a = 0$, then $\eta(0) = 0^{\frac{q-1}{2}} = 0$. Let α be a primitive element of $\mathbb{F}_q$ and $a \in \mathbb{F}_q{}^*$. Then $a = \alpha^i$ for some $i \in \mathbb{Z}$. If a is a square, then i is even. If a is a non-square, then i is odd. Note that

$$a^{\frac{q-1}{2}} = (\alpha^i)^{\frac{q-1}{2}} = (\alpha^{\frac{q-1}{2}})^i = (-1)^i,$$

by Proposition 2.8. Then in both cases $\eta(a) = a^{\frac{q-1}{2}}$.

□

Example 2.14. Let $q = 13$. We want to know if 2 is a square in $\mathbb{F}_{13}$. One way to do this is to calculate x^2 for every element of the field, like we did in Example 2.11, and see that

$$x^2 \not\equiv 2 \pmod{13},$$

for all $x \in \mathbb{F}_{13}$. Another and much simpler way is to use Proposition 2.13 and calculate

$$\eta(2) = 2^{\frac{q-1}{2}} = 2^6 = -1.$$

Recall that, in Example 2.7, we found that $\mathbb{F}_{13} = \langle 2 \rangle$. In Proposition 2.8, we proved that every primitive element is a non-square in the field.

◇

Proposition 2.15. Let q be odd and $\eta : \mathbb{F}_q{}^* \to \mu_2$ be defined as $\eta(a) = a^{\frac{q-1}{2}}$, where μ_2 denotes the set of square roots of unity in $\mathbb{F}_q$ $\{-1, 1\}$. Then $\eta(ab) = \eta(a)\eta(b)$.

Proof. By Proposition 2.13, we know that η is well defined. Let $a, b \in \mathbb{F}_q{}^*$, and note that

$$\eta(ab) = (ab)^{\frac{q-1}{2}} = a^{\frac{q-1}{2}} b^{\frac{q-1}{2}} = \eta(a)\eta(b).$$

□

Definition 2.16. Let n be a positive integer. The **Euler function**, denoted by $\phi(n)$, counts the number of positive integers not exceeding n that are relatively prime to n.

Example 2.17. Let $n = 8$. Then $\phi(8) = 4$ since $1, 3, 5, 7$ are the positive integers smaller than 8 that are relatively prime to 8.

$\diamond$

Proposition 2.18 ([7], Euler's Theorem)**.** *If* $\gcd(a, m) = 1$*, then* $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proposition 2.19 ([1], Theorem 7.1)**.** *Let* p *be prime and* ℓ *be a positive integer. Then*

$$\phi(p^\ell) = p^\ell - p^{\ell-1} = p^{\ell-1}(p-1).$$

Proposition 2.20 ([1], Proposition 7.2)**.** *Let* a, b *be positive integers. Euler's function* ϕ *is multiplicative; that is, if* $\gcd(a, b) = 1$*, then* $\phi(ab) = \phi(a)\phi(b)$.

Definition 2.21. Let p be prime and a be an integer, $a \neq 0$. We say that $\ell \in \mathbb{Z}$ is the **p-adic valuation** of a, denoted by $\nu_p(a)$, if $p^\ell \mid a$ and $p^{\ell+1} \nmid a$.

Proposition 2.22. Let p be prime and a, b be non-zero integers. Then $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

Proof. Let $\nu_p(a) = \ell$ and $\nu_p(b) = t$. Note that $p^\ell \mid a$ and $p^{\ell+1} \nmid a$ if and only if $p^\ell n = a$ and $p \nmid n$ for some $n \in \mathbb{Z}$. Similarly, there exists $m \in \mathbb{Z}$ such that $p^t m = b$ and $p \nmid m$. Then $ab = p^\ell n p^t m = p^{\ell+t} nm$ and $p \nmid nm$, that is $\nu_p(ab) = \ell + t$.

$\square$

The following proposition tells us when linear congruences have solutions and if so, how many incongruent solutions there exist. We use this proposition to find formulas for counting the fixed points.

Proposition 2.23 ([7], Proposition 3.3.1)**.** *Let* $d = \gcd(a, m)$*. The congruence* $ax \equiv b \pmod{m}$ *has a solution if and only if* $d \mid b$*. If* $d \mid b$*, then there are exactly*

d solutions. If x_0 is a solution, then the other solutions are given by $x_0 + \frac{m}{d}h$ where $h = 1, 2, \ldots, d-1$.

Note the following particular case of this proposition.

Corollary 2.24. The congruence $ax \equiv b \pmod{m}$ has a unique solution if and only if $\gcd(a, m) = 1$.

Now we present an example of how to use these propositions to solve a simple linear congruence and find all of its incongruent solutions.

Example 2.25. First we want to know if the linear congruence

$$3x \equiv 9 \pmod{12}$$

has solutions, and if so, what the incongruent solutions are. Note that $\gcd(3, 12) = 3$ and $3 \mid 9$, therefore there exist 3 incongruent solutions. To calculate all such solutions, we need to first find a particular solution. Note that

$$\begin{aligned} & 3x \equiv 9 \pmod{12} \\ \iff & 3x - 9 = 12k, \quad \text{for some } k \in \mathbb{Z} \\ \iff & x - 3 = 4k, \end{aligned}$$

that is, $x = 3$ is a particular solution. Therefore by Theorem 2.23 the incongruent solutions of $3x \equiv 9 \pmod{12}$ are

$$3,\ 3 + \left(\frac{12}{3}\right)1,\ 3 + \left(\frac{12}{3}\right)2,$$

that is, all the incongruent solutions are $3, 7, 11$.

We can verify that 7 and 11 are solutions by substituting then directly:

$$\begin{aligned} 3(7) &\equiv 21 \equiv 9 \pmod{12} \quad \text{and} \\ 3(11) &\equiv 33 \equiv 9 \pmod{12}. \end{aligned}$$

$\diamond$

Theorem 2.26 is a special case of the Chinese Remainder Theorem.

Theorem 2.26 ([9], Theorem 60)**.** *If* $a \equiv b \pmod{n_i}$ *for* $i = 1, 2, \ldots, v$, $v \geq 2$, *then* $a \equiv b \pmod{n}$ *where* n *is the least common multiple of* $n_1, n_2, \ldots, n_v$.

The following theorem is a special case of Theorem 87 in [9].

Theorem 2.27 ([9])**.** *Let* p *be a prime and* $e > 0$. *Then the number of solutions of* $x^2 \equiv 1 \pmod{p^e}$ *is*

$$\begin{cases} 1 & \text{if } p = 2,\ e = 1, \\ 2 & \text{if } p = 2,\ e = 2, \\ 4 & \text{if } p = 2,\ e > 2, \\ 2 & \text{if } p > 2. \end{cases}$$

Theorem 2.28 ([9], Theorem 71)**.** *Let* $m = p_1^{e_1} \cdots p_r^{e_r}$ *and* $f(x) \in \mathbb{Z}[x]$. *Then the number of solutions of* $f(x) \equiv 0 \pmod{m}$ *equals the product of the numbers of solutions of* $f(x) \equiv 0 \pmod{p_n^{e_n}}$ *for all* $n = 1, \ldots, r$.

We use Theorem 2.27 and Theorem 2.28 to count the number of solutions of

$$m^2 \equiv 1 \pmod{\frac{q-1}{2}}.$$

This will be of use to us in Chapter 4, where we provide explicit formulas for building m so that $x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$.

Corollary 2.29. Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, where e and each $e_i > 0$. The number of solutions of

$$x^2 \equiv 1 \pmod{\frac{q-1}{2}}$$

is

$$\begin{cases} 2^r & \text{if } e = 1, 2 \\ 2^{r+1} & \text{if } e = 3 \\ 2^{r+2} & \text{if } e \geq 4. \end{cases}$$

Proof. Note that $\frac{q-1}{2} = 2^{e-1}p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$. By Theorem 2.27, the number of solutions of $x^2 \equiv 1 \pmod{p_i^{e_i}}$ is 2 for all $i = 1, \dots, r$. Similarly, the number of solutions of $x^2 \equiv 1 \pmod{2^{e-1}}$ is

$$\begin{cases} 1 & \text{if } e = 2 \\ 2 & \text{if } e = 3 \\ 2^2 & \text{if } e \geq 4. \end{cases}$$

Note that if $e = 1$, then $\frac{q-1}{2} = p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$. Then using Theorem 2.28, we have that the number of solutions of $x^2 \equiv 1 \left(\mod \frac{q-1}{2}\right)$ is

$$\begin{cases} 2^r & \text{if } e = 1, 2 \\ 2^{r+1} & \text{if } e = 3 \\ 2^{r+2} & \text{if } e \geq 4. \end{cases}$$

□

Chapter 3

Permutations of the Form $x^m(x^{\frac{q-1}{2}} + a)$

As we stated before, our goal is to characterize involutions of $\mathbb{F}_q$ of the form $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ in terms of the number of fixed points and their fixed points. To do this we first need to study permutations of $\mathbb{F}_q$ of the same form. In this chapter we study permutations of the form $f(x)$ and their fixed points.

3.1 Permutations

For a function to be an involution of $\mathbb{F}_q$, it is necessary that it is a permutation. Hence, studying permutations of the form $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ gives us insight into involutions of the same form. In this section we present a characterization of permutations of the form $f(x)$.

Definition 3.1. A **permutation** of a finite set A is a bijective function from A to A. A **permutation polynomial** in $\mathbb{F}_q$ is a polynomial that produces a permutation of $\mathbb{F}_q$.

The following theorem characterizes a family of permutation polynomials that encompasses $f(x)$.

Theorem 3.2 ([11, 15, 18]). *Let m, s, r be positive integers, $sr = q - 1$ and $h(x) \in \mathbb{F}_q[x]$. Then $x^m h(x^s)$ is a permutation of $\mathbb{F}_q$ if and only if the following conditions hold:*

1. $\gcd(m, s) = 1$,
2. *$x^m h(x)^s$ permutes μ_r,*

where μ_r denotes the set of r^{th}-roots of unity in $\mathbb{F}_q$.

Let $r = 2$ and $h(x) = x + a$. Then the expression in the second condition of Theorem 3.2 becomes $x^m(x + a)^{\frac{q-1}{2}}$, but note that the second factor is the quadratic character of $\mathbb{F}_q$ evaluated at $x + a$. That is, $(x + a)^{\frac{q-1}{2}} = 1$ if $x + a$ is a non-zero square and $(x + a)^{\frac{q-1}{2}} = -1$ if it is a non-square. We make use of the properties of the quadratic character of $\mathbb{F}_q$ discussed in Section 2.2 to refine Theorem 3.2. Proposition 3.4 is a special case of Theorem 3.2.

Lemma 3.3. Let q be odd, m be a positive integer and $a \in {\mathbb{F}_q}^*$. Then $x^m(x+a)^{\frac{q-1}{2}}$ permutes μ_2 if and only if $\eta(a^2 - 1) = (-1)^{m+1}$.

Proof. Note that $\mu_2 = \{-1, 1\}$. Define $g(x) = x^m(x + a)^{\frac{q-1}{2}}$. Then

$$\begin{aligned}
& g(x) \text{ permutes } \mu_2 \\
\iff\ & g(1)g(-1) = -1 \\
\iff\ & (a+1)^{\frac{q-1}{2}}(-1)^m(a-1)^{\frac{q-1}{2}} = -1 \\
\iff\ & (-1)^m(a^2-1)^{\frac{q-1}{2}} = -1 \\
\iff\ & \eta(a^2 - 1) = (-1)^{m+1}.
\end{aligned}$$

□

Proposition 3.4. Let q be odd, m be a positive integer and $a \in {\mathbb{F}_q}^*$. Then $x^m(x^{\frac{q-1}{2}} + a)$ is a permutation of $\mathbb{F}_q$ if and only if the following conditions hold:

1. $\gcd\left(m, \frac{q-1}{2}\right) = 1$

2. $\eta(a^2-1) = (-1)^{m+1}$.

Proof. Using Theorem 3.2, fix $r = 2$ and $h(x) = x + a$. Then $s = \frac{q-1}{2}$ and, by Lemma 3.3,

$$x^m h(x)^s = x^m(x+1)^{\frac{q-1}{2}} \text{ permutes } \mu_2 \iff \eta(a^2-1) = (-1)^{m+1}.$$

The result now follows from Theorem 3.2.

□

We mainly use this characterization of permutations $f(x)$ of $\mathbb{F}_q$ throughout the thesis.

The next example illustrates the use of Proposition 3.4.

Example 3.5. Consider $f(x) = x^{11}(x^6+2) \in \mathbb{F}_{13}[x]$. We can verify if $f(x)$ is a permutation of $\mathbb{F}_{13}$ in two ways. One method is to evaluate $f(x)$ at each $x \in \mathbb{F}_{13}$ and get the permutation:

$$\begin{array}{lll} 0 \mapsto 0, & 5 \mapsto 8, & 10 \mapsto 12, \\ 1 \mapsto 3, & 6 \mapsto 11, & 11 \mapsto 6, \\ 2 \mapsto 7, & 7 \mapsto 2, & 12 \mapsto 10. \\ 3 \mapsto 1, & 8 \mapsto 5, & \\ 4 \mapsto 4, & 9 \mapsto 9, & \end{array}$$

We can also verify that $f(x)$ is a permutation of $\mathbb{F}_{13}$ by checking the conditions of Proposition 3.4. First, we have

$$\gcd\left(m, \frac{q-1}{2}\right) = \gcd(11, 6) = 1.$$

From Example 2.7, we have that $4^2 \equiv 3 \pmod{13}$. Therefore,

$$\eta(a^2-1) = \eta(2^2-1) = \eta(3) = 1 = (-1)^{11+1}.$$

◇

Note that the first condition of Proposition 3.4 does not depend on a. Consider the binomial $x^m(x^{\frac{q-1}{2}} - a)$. Then,

$$\eta((-a)^2 - 1) = \eta(a^2 - 1).$$

Therefore, if $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is a permutation of $\mathbb{F}_q$, then $x^m(x^{\frac{q-1}{2}} - a)$ is also a permutation of $\mathbb{F}_q$. The converse is also true. In other words, permutations of $f(x)$ come in pairs, and we have proved the following:

Proposition 3.6. Let q be odd, m be a positive integer and $a \in \mathbb{F}_q{}^*$. Then $x^m(x^{\frac{q-1}{2}} + a)$ is a permutation of $\mathbb{F}_q$ if and only if $x^m(x^{\frac{q-1}{2}} - a)$ is a permutation of $\mathbb{F}_q$.

Example 3.7. Consider $f(x) = x^4(x^5 + 3) \in \mathbb{F}_{11}[x]$. First we verify if $f(x)$ is a permutation by checking the conditions on Proposition 3.4:

$$\gcd\left(m, \frac{q-1}{2}\right) = \gcd(4, 5) = 1, \quad \text{and}$$
$$\eta(a^2 - 1) = \eta(3^2 - 1) = \eta(8) = 8^5 = -1 = (-1)^{4+1}.$$

Then by Proposition 3.6, $x^4(x^5 - 3) = x^4(x^5 + 8)$ is also a permutation of $\mathbb{F}_{11}$.

◇

Example 3.8. Let $q = 7$. To list all permutations of $\mathbb{F}_7$ of the form $f(x)$, we use Proposition 3.4. First we list all m's in $\mathbb{F}_7$ that are relatively prime to $\frac{q-1}{2} = 3$, these are $1, 2, 4, 5$. Now, for m even, we want to find a's such that $a^2 - 1$ is not a square; these are 2 and 5. Note that $5 \equiv -2 \pmod 7$. Similarly, for m odd, the only a's such that $a^2 - 1$ is a non-zero square are 3 and 4. Note that $4 \equiv -3 \pmod 7$. To summarize, we have the following table that lists all permutations $f(x)$ of $\mathbb{F}_7$.

m	a
1	2
1	-2
5	2
5	-2

m	a
2	3
2	-3
4	3
4	-3

Table 3.8.1: All values of m and a that produce permutations of $\mathbb{F}_7$ of the form $f(x) = x^m(x^3 + a)$.

From this table it is easy to see that all permutations come in pairs.

$\diamond$

3.2 Fixed Points

We had previously mentioned that the number of fixed points plays an important role in some applications of permutation polynomials. Now that we have characterized permutations of $\mathbb{F}_q$ of the form $x^m(x^{\frac{q-1}{2}} + a)$, we can start talking about their fixed points, when we have them and how many of them there are.

Definition 3.9. Let $f : A \to B$ be a function. Then $x \in A$ is a **fixed point** of f if $f(x) = x$.

Remark. We can rewrite $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ as a piecewise function

$$f(x) = \begin{cases} x^m(a+1), & \text{if } x \text{ is a square,} \\ x^m(a-1), & \text{if } x \text{ is a non-square.} \end{cases}$$

In [17] the authors represent involutions as piecewise functions using the roots of unity. For the binomial $f(x)$, we are only concerned with the square roots of unity, -1 and 1, as we saw in Section 3.1 when we characterized permutations $f(x)$ of $\mathbb{F}_q$.

It is easy to see that 0 is always a fixed point. The piecewise representation of $f(x)$ also makes it easier to see that to find and count the non-zero fixed points,

we need to study the solutions of two equations: $x^{1-m} = a \pm 1$. We get these equations by using the definition of a fixed point on the piecewise representation of $f(x)$ and solving for x. We present now a characterization of the fixed points of functions $f(x)$ which are not necessarily permutations.

Proposition 3.10. Let q be odd, m, k be a positive integers, $a \in \mathbb{F}_q{}^*$ and α be a primitive element of $\mathbb{F}_q$. Then α^k is a fixed point of $f(x) = x^m(x^{\frac{q-1}{2}} + a) \in \mathbb{F}_q[x]$ if and only if $\alpha^{k(1-m)} = a + (-1)^k$.

Proof. Note that

$$\begin{aligned} f(\alpha^k) &= \alpha^{km}((\alpha^k)^{\frac{q-1}{2}} + a) \\ &= \alpha^{km}((\alpha^{\frac{q-1}{2}})^k + a) \\ &= \alpha^{km}((-1)^k + a). \end{aligned}$$

Therefore α^k is a fixed point of $f(x)$ if and only if

$$f(\alpha^k) = \alpha^{km}((-1)^k + a) = \alpha^k \iff \alpha^{k(1-m)} = a + (-1)^k.$$

□

Corollary 3.11. Let q be odd, m, k_1, k_2 be a positive integers, $a \in \mathbb{F}_q{}^*$ and α be a primitive element of $\mathbb{F}_q$. Then the following hold:

1. α^{k_1} is a non-zero square fixed point of $f(x)$ if and only if $\alpha^{k_1(1-m)} = a + 1$ and k_1 is even.

2. α^{k_2} is a non-square fixed point of $f(x)$ if and only if $\alpha^{k_2(1-m)} = a - 1$ and k_2 is odd.

Proof. This proof follows directly from Proposition 3.10 by letting k be even or odd. If k is even then α^k is a non-zero square and a fixed point of $f(x)$ if and only if $\alpha^{k(1-m)} = a + 1$. The case where k is odd is similar.

□

Remark. The contrapositive of Corollary 3.11 gives us necessary and sufficient conditions for 0 to be the only fixed point of $f(x)$. Note that, by Statement 1, $f(x)$ does not have non-zero square fixed points if and only if $\alpha^{k_1(1-m)} \neq a+1$ for all k_1 even. This is equivalent to saying that either $\alpha^{k_1(1-m)} = a+1$ for some k_1 odd or $\alpha^{k_1(1-m)+r_1} = a+1$ for some k_1 even and $r_1 \in \mathbb{Z}$ such that $0 < r_1 < 1-m$. Similarly, $f(x)$ does not have non-square fixed points if and only if either $\alpha^{k_2(1-m)} = a-1$ for some k_2 even or $\alpha^{k_2(1-m)+r_2} = a-1$ for some k_2 odd and $r_2 \in \mathbb{Z}$ such that $0 < r_2 < 1-m$.

Example 3.12. Consider $f(x) = x^4(x^5+3) \in \mathbb{F}_{11}[x]$. Note that $\mathbb{F}_{11} = \langle 2 \rangle$; that is, 2 is a primitive element of $\mathbb{F}_{11}$.

First we check if $f(x)$ has square fixed points, note

$$a+1 = 4 = 2^2.$$

Now we verify if there exists k even such that $k(1-m) \equiv 2 \pmod{q-1}$. Note that

$$\begin{aligned} 0(-3) &\equiv 0 \pmod{10}, & \mathbf{6(-3) \equiv 2} &\pmod{10}, \\ 2(-3) &\equiv 4 \pmod{10}, & 8(-3) &\equiv 6 \pmod{10}. \\ 4(-3) &\equiv 8 \pmod{10}, \end{aligned}$$

Then $\alpha^k = 2^6 = 9$ is a square fixed point of $f(x)$.

We now do a similar process to see if $f(x)$ has non-square fixed points. First we note

$$a-1 = 2 = 2^1.$$

Now, we check if there exists k odd such that $k(1-m) \equiv 1 \pmod{q-1}$.

$$\begin{aligned} 1(-3) &\equiv 7 \pmod{10}, & 7(-3) &\equiv 9 \pmod{10}, \\ \mathbf{3(-3)} &\equiv \mathbf{1} \pmod{10}, & 9(-3) &\equiv 3 \pmod{10}. \\ 5(-3) &\equiv 5 \pmod{10}, \end{aligned}$$

Then $\alpha^k = 2^3 = 8$ is a non-square fixed point of $f(x)$. In short, the fixed points of $f(x)$ are $0, 8, 9$.

$\diamond$

We can now generate the fixed points of $f(x) = x^m(x^{\frac{q-1}{2}} + a)$. Now we want to know more about the fixed points of $f(x)$, specifically: When do we have them? How many are there? How can we calculate them more directly? In Example 3.12, we found the fixed points α^k by solving $k(1-m) \equiv u \pmod{q-1}$ for k, where $a + (-1)^k = \alpha^u$, for k even or odd, in a rather systematic way. Theorem 3.13 expands on Proposition 3.10 and specifies how many fixed points a permutation $f(x)$ of $\mathbb{F}_q$ has and provides formulas for fixed points that depend on q, m and a.

Theorem 3.13. Let q be odd, m be a positive integer, $a \in \mathbb{F}_q{}^*$, and α be a primitive element of $\mathbb{F}_q$. For $\ell, g, h \in \mathbb{Z}$ where $g \mid 1-m$ and $2g \mid q-1$, define $r = 2\left(\ell\left(\frac{1-m}{g}\right)^{-1} + \frac{q-1}{2g}h\right) \in \mathbb{Z}$, where $\left(\frac{1-m}{g}\right)^{-1}$ is reduced modulo $\frac{q-1}{2g}$. If $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is a permutation of $\mathbb{F}_q$, then, for $g = \gcd(m-1, \frac{q-1}{2})$, the following hold:

1. There exist non-zero square fixed points of $f(x)$ if and only if $a + 1 = \alpha^{2g\ell}$. In this case, the non-zero square fixed points are α^r for $h = 1, \ldots, g$.

2. There exist non-square fixed points of $f(x)$ if and only if $a - 1 = \alpha^{2g\ell+1-m}$. In this case, the non-square fixed points are α^{r+1} for $h = 1, \ldots, g$.

3. $f(x)$ has exactly $g+1$ fixed points if and only if it has either non-zero square fixed points or non-square fixed points, $2g + 1$ fixed points if and only if it

has both non-zero square and non-square fixed points, and only 1 fixed point if and only if $\alpha^{k(1-m)} \neq a + (-1)^k$ for all $k \in \mathbb{Z}$.

Proof. Let α^k be a fixed point of $f(x)$ and $a + 1 = \alpha^u$ for some $u \in \mathbb{Z}$. Suppose k is even. Then $k = 2i$, for some $i \in \mathbb{Z}$, and, by Statement 1 of Corollary 3.11,

$$\begin{aligned}
\alpha^{2i} \text{ is a non-zero square fixed point of } f(x) &\iff \alpha^{2i(1-m)} = a + 1 = \alpha^u, \quad u \in \mathbb{Z} \\
&\iff 2i(1-m) \equiv u \pmod{q-1} \\
&\iff \gcd(2(1-m), q-1) \mid u \\
&\iff 2g \mid u,
\end{aligned}$$

since $\gcd(2(1-m), q-1) = 2\gcd(m-1, \frac{q-1}{2}) = 2g$. That is, α^{2i} is a non-zero square fixed point of $f(x)$ if and only if $a+1 = \alpha^{2g\ell_1}$ in $\mathbb{F}_q$, for some $\ell_1 \in \mathbb{Z}$. Then,

$$2i(1-m) \equiv 2g\ell_1 \pmod{q-1} \iff i(1-m) \equiv g\ell_1 \pmod{\frac{q-1}{2}}.$$

By Proposition 2.23, the number of distinct solutions for i is $\gcd(m-1, \frac{q-1}{2}) = g$. Also, since $\gcd\left(\frac{1-m}{g}, \frac{q-1}{2g}\right) = 1$, then

$$i\left(\frac{1-m}{g}\right) \equiv \ell_1 \pmod{\frac{q-1}{2g}} \iff i \equiv \ell_1 \left(\frac{1-m}{g}\right)^{-1} \pmod{\frac{q-1}{2g}}.$$

Again by Proposition 2.23, the distinct solutions for i are $\ell_1 \left(\frac{1-m}{g}\right)^{-1} + \left(\frac{q-1}{2g}\right) h$ for $h = 1, 2, \ldots, g$. Therefore, α^r is a non-zero square fixed point of $f(x)$ if and only if

$$r = 2\left(\ell_1 \left(\frac{1-m}{g}\right)^{-1} + \left(\frac{q-1}{2g}\right) h\right).$$

Now, let $a - 1 = \alpha^v$ for some $v \in \mathbb{Z}$ and k be odd. Then $k = 2j + 1$, for some

$j \in \mathbb{Z}$, and, by Statement 2 of Corollary 3.11,

$$\begin{aligned}
\alpha^{2j+1} \text{ is a non-square fixed point of } f(x) &\iff \alpha^{(2j+1)(1-m)} = a - 1 = \alpha^v, \quad v \in \mathbb{Z} \\
&\iff (2j+1)(1-m) \equiv v \pmod{q-1} \\
&\iff 2j(1-m) + 1 - m \equiv v \pmod{q-1} \\
&\iff 2j(1-m) \equiv v + m - 1 \pmod{q-1} \\
&\iff \gcd(2(1-m), q-1) \mid v + m - 1 \\
&\iff 2g \mid v + m - 1,
\end{aligned}$$

since $\gcd(2(1-m), q-1) = 2g$. That is, α^{2j+1} is a non-square fixed point of $f(x)$ if and only if $a - 1 = \alpha^{2g\ell_2+1-m}$ for some $\ell_2 \in \mathbb{Z}$. Then,

$$2j(1-m) \equiv 2g\ell_2 \pmod{q-1} \iff j(1-m) \equiv g\ell_2 \pmod{\frac{q-1}{2}}.$$

By Proposition 2.23, the number of distinct solutions for j is $\gcd(m-1, \frac{q-1}{2}) = g$. Also, since $\gcd\left(\frac{1-m}{g}, \frac{q-1}{2g}\right) = 1$, then

$$j\left(\frac{1-m}{g}\right) \equiv \ell_2 \pmod{\frac{q-1}{2g}} \iff j \equiv \ell_2 \left(\frac{1-m}{g}\right)^{-1} \pmod{\frac{q-1}{2g}}.$$

Again by Proposition 2.23, the distinct solutions for j are $\ell_2 \left(\frac{1-m}{g}\right)^{-1} + \left(\frac{q-1}{2g}\right) h$ for $h = 1, 2, \ldots, g$. Therefore, α^{r+1} is a non-square fixed point of $f(x)$ if and only if

$$r = 2\left(\ell_2 \left(\frac{1-m}{g}\right)^{-1} + \left(\frac{q-1}{2g}\right) h\right).$$

Note that, besides 0, $f(x)$ can have either both square and non-square fixed points, only square fixed points or only non-square fixed points. By Proposition 2.23, $f(x)$ can have exactly g non-zero square fixed points and exactly g non-square fixed points. Then $f(x)$ has both square and non-square non-zero fixed points if and only if $f(x)$ has $2g + 1$ fixed points. Similarly, $f(x)$ only has square or non-square non-zero fixed points if and only if $f(x)$ has $g+1$ fixed points.

Lastly, $f(x)$ only has 0 as a fixed point if and only if $f(x)$ has no non-zero square or non-square fixed points. Therefore, the possible number of fixed points is either 1, $g+1$, or $2g+1$.

□

In the following example, we use Theorem 3.13 to verify if a permutation has non-zero fixed points.

Example 3.14. Let x^2+2x+2 be a primitive polynomial over $\mathbb{F}_3$ such that β is a root over $\mathbb{F}_9$. Consider $f(x) = x(x^4+\beta+1) \in \mathbb{F}_9[x]$. Note that $2g = 2\gcd(0,4) = 8$. Since

$$\gcd\left(m, \frac{q-1}{2}\right) = \gcd(1,4) = 1 \quad \text{and}$$
$$\eta(a^2-1) = \eta((\beta+1)^2-1) = \eta(1) = 1,$$

then $f(x)$ permutes $\mathbb{F}_9$ by Proposition 3.4. Now we determine if $f(x)$ has non-zero fixed points using Theorem 3.13. Note that $a+1 = \beta+2 = \beta^7$. By Statement 1 of Theorem 3.13, we want to determine if we can write $a+1 = \beta^{2g\ell} = \beta^{8\ell}$ for some $\ell \in \mathbb{Z}$. But $\beta^{8\ell} = \beta^0 = 1$ and $a+1 \neq 1$, therefore, $f(x)$ does not have non-zero square fixed points. We do a similar process to verify the existence of non-square fixed points using Statement 2 of Theorem 3.13. Note that $a-1 = \beta$ and $\beta \neq \beta^{2g\ell+1-m}$ since $2g\ell+1-m \equiv 8\ell+1-1 \equiv 0 \pmod 8$. Therefore, $f(x)$ does not have non-zero fixed points. That is, 0 is the only fixed point of $f(x)$.

◇

We now show an example where we apply Theorem 3.13 to calculate the fixed points of a polynomial over a non-prime field $\mathbb{F}_q$, that is $q = p^r$ where $r > 1$.

Example 3.15. Let x^2+4x+2 be a primitive polynomial over $\mathbb{F}_5$ such that β is a root over $\mathbb{F}_{25}$, and $f(x) = x^{11}(x^{12}+\beta+2) \in \mathbb{F}_{25}[x]$. Note that $g = \gcd(10,12) = 2$.

First we verify that $f(x)$ is a permutation of $\mathbb{F}_{25}$:

$$\gcd\left(m, \frac{q-1}{2}\right) = \gcd(11, 12) = 1,$$
$$\eta(a^2 - 1) = \eta((\beta + 2)^2 - 1) = \eta(1) = 1.$$

Then $f(x)$ permutes $\mathbb{F}_{25}$. We want to check if $f(x)$ has non-zero square or non-square fixed points and calculate them. Now, we can go about this in two ways. We can use Corollary 3.11 and find all k_1 even solutions of $\beta^{k_1(1-m)} = \beta^2$, if any, and all k_2 odd solutions of $\beta^{k_2(1-m)} = \beta^{22}$, if any, as we did in Example 3.15. The other option is to use the formula for r in Theorem 3.13 to calculate all fixed points of $f(x)$ directly. We follow this method. In this case, we first need to check if there exist any non-zero fixed points. By Statement 1 of Theorem 3.13, $f(x)$ has non-zero square fixed points if and only if $a+1$ can be written as $\beta^{2g\ell}$, where $g = \gcd(m-1, \frac{q-1}{2}) = 2$ and $\ell \in \mathbb{Z}$. But note that $a+1 = \beta+3 = \beta^2$ and $\beta^2 \neq \beta^{4\ell}$ since $2 \equiv 4\ell \pmod{24}$ does not have solutions by Proposition 2.23. Similarly, Statement 2 of Theorem 3.13 states that there exist non-square fixed points if and only if $a - 1 = \beta^{2g\ell+1-m}$ for some $\ell \in \mathbb{Z}$. Note that $a - 1 = \beta^{22} = \beta^{4\ell+1-11}$ where $\ell = 8$. Therefore $f(x)$ has non-square fixed points. Moreover, by Statement 3 of Theorem 3.13, $f(x)$ has exactly $g + 1 = 3$ fixed points.

Now we calculate the non-square fixed points. Note that $\frac{q-1}{2g} = \frac{24}{4} = 6$, then we have

$$\left(\frac{1-m}{g}\right)^{-1} \equiv \left(\frac{-10}{2}\right)^{-1} \equiv (-5)^{-1} \equiv 1^{-1} \equiv 1 \pmod{6}.$$

We can now calculate the values of $r + 1$. Note that

$$2\left(\ell\left(\frac{1-m}{g}\right)^{-1} + \frac{q-1}{2g}h\right) + 1 = 2(8 + 6h) + 1,$$

where $h = 1, 2$. Then the values of $r+1$ are $2(8+6)+1$, $2(8+12)+1$, i.e. $29, 41$.

Therefore the non-square fixed points are

$$\beta^{29} = \beta^{24}\beta^5 = 4\beta + 1,$$
$$\beta^{41} = \beta^{24}\beta^{17} = \beta + 4.$$

To summarize, the fixed points of $f(x)$ are $0,\ 4\beta + 1$, and $\beta + 4$.

$\diamond$

Note that in Example 3.15, we showed that $x^{11}(x^{12} + \alpha + 2) \in \mathbb{F}_{25}[x]$ has $g = 2$ non-zero fixed points, and in Example 3.12, we saw that $x^4(x^5 + 3) \in \mathbb{F}_{11}[x]$ has $2g = 2$ non-zero fixed points. These are examples of permutations, one of which has $g + 1$ fixed points and the other has $2g + 1$ fixed points.

Suppose x is a fixed point of $f(x)$. Then x is a square if and only if $f(x)$ is a square. This leads us to the next proposition.

Proposition 3.16. Let q be odd, m be a positive integer, $a \in \mathbb{F}_q^*$, and $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ be a permutation of $\mathbb{F}_q$ with at least one non-zero fixed point. Then $\eta(a + 1) = 1$.

Proof. Let α be a primitive element of $\mathbb{F}_q$ and $c \in {\mathbb{F}_q}^*$ be a fixed point of $f(x)$.

Suppose c is a square. Then, by Theorem 3.13,

$$\eta(a + 1) = \eta(\alpha^{2g\ell}) = 1, \quad \text{for some } l \in \mathbb{Z}.$$

Now, suppose that c is not a square. Then,

$$\eta(a - 1) = \eta(\alpha^{2g\ell+1-m}) = (\alpha^{2g\ell})^{\frac{q-1}{2}}(\alpha^{\frac{q-1}{2}})^{1-m} = (-1)^{1-m},$$

for some $\ell \in \mathbb{Z}$. But $f(x)$ is a permutation, therefore

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

$\square$

The converse of Proposition 3.16 is false. That means that we can have permutations with only one fixed point such that $a+1$ is a square.

Example 3.17. Consider $f(x) = x^5(x^6+11) \in \mathbb{F}_{13}[x]$. We first check that $f(x)$ is a permutation of $\mathbb{F}_q$ using Proposition 3.4. Since

$$\gcd\left(m, \frac{q-1}{2}\right) = \gcd(5,6) = 1 \quad \text{and}$$
$$\eta(a^2-1) = \eta(11^2-1) = \eta(3) = 1,$$

then $f(x)$ is a permutation of $\mathbb{F}_{13}$. Recall from Example 2.7 that 2 is a primitive element of $\mathbb{F}_{13}$. Hence,

$$a+1 = 12 = 2^6 \quad \text{and}$$
$$a-1 = 10 = 2^{10}.$$

Since $a+1$ is an even power of 2, then $\eta(a+1) = 1$. Note that $2g = 2\gcd(4,6) = (2)(2) = 4$. Now, using Theorem 3.13, we can determine if $f(x)$ has non-zero fixed points by checking if $a+1 = 2^{2g\ell} = 2^{4\ell}$ or $a-1 = 2^{2g\ell+1-m} = 2^{4\ell-4}$ for some $\ell \in \mathbb{Z}$. But, by Proposition 2.23, $4\ell \equiv 6 \pmod{12}$ has no solutions since $\gcd(4,12) = 4$ and $4 \nmid 6$. Similarly, by the same proposition, note that $4\ell - 4 \equiv 10 \pmod{12}$ has no solutions since $\gcd(4,12) = 4$ and $4 \nmid 10+4$. Therefore $f(x)$ does not have non-zero fixed points.

$\diamond$

3.2.1 Permutation Pairs

Proposition 3.6 states that $x^m(x^{\frac{q-1}{2}} + a)$ is a permutation of $\mathbb{F}_q$ if and only if $x^m(x^{\frac{q-1}{2}} - a)$ is a permutation of $\mathbb{F}_q$. That is, permutations $f(x)$ of $\mathbb{F}_q$ always come in pairs. We present now more results on fixed points for permutation pairs.

The following proposition tells us that when $q \equiv 1 \pmod{4}$ and m is odd, the additive inverse of any fixed point of $f(x)$ is also a fixed point of $f(x)$.

Proposition 3.18. Let $q \equiv 1 \pmod 4$, m be odd, $a \in {\mathbb{F}_q}^*$, $c \in {\mathbb{F}_q}^*$, and $f(x) = x^m(x^{\frac{q-1}{2}} + a) \in \mathbb{F}_q[x]$. Then c is a fixed point of $f(x)$ if and only if $-c$ is a fixed point of $f(x)$.

Proof. Let α be a primitive element in $\mathbb{F}_q$ and $k \in \mathbb{Z}$. Note that

$$\begin{aligned}\alpha^{(k+\frac{q-1}{2})(1-m)} &= \alpha^{k(1-m)}(\alpha^{\frac{q-1}{2}})^{1-m} \\ &= \alpha^{k(1-m)}(-1)^{1-m} \\ &= \alpha^{k(1-m)}.\end{aligned}$$

By Proposition 3.10, we have

$$\begin{aligned}-\alpha^k = \alpha^{k+\frac{q-1}{2}} \text{ is a fixed point of } f(x) &\iff \alpha^{(k+\frac{q-1}{2})(1-m)} = a + (-1)^{k+\frac{q-1}{2}} \\ &\iff \alpha^{k(1-m)} = a + (-1)^k(-1)^{\frac{q-1}{2}} \\ &\iff \alpha^{k(1-m)} = a + (-1)^k \\ &\iff \alpha^k \text{ is a fixed point of } f(x).\end{aligned}$$

□

Example 3.19. Let $f(x) = x^5(x^6 + 2) \in \mathbb{F}_{13}[x]$. From Example 2.7, we have that $\mathbb{F}_{13}^* = \langle 2 \rangle$, that is, 2 is a primitive element of $\mathbb{F}_{13}$. Now, note that

$$a + 1 = 3 = 2^4.$$

Therefore we want to find $\alpha^{k(1-m)}$ with k even such that $k(1-m) \equiv 4 \pmod{q-1}$. Now, note $2(-4) \equiv 4 \pmod{12}$. Then $2^2 = 4$ is a fixed point of $f(x)$, therefore $-2^2 = -4 = 9$ is also a fixed point of $f(x)$. We can check that these are all of the non-zero square fixed points of $f(x)$. We can do similar procedure to find the non-square fixed points. Note that

$$a - 1 = 1 = 2^0.$$

Since $3(-4) \equiv 0 \pmod{12}$, then $2^3 = 8$ is a fixed point of $f(x)$, therefore $-2^3 = -8 = 5$ is also a fixed point of $f(x)$. We can verify that these are all of the non-square fixed points of $f(x)$.

In summary, the fixed points of $f(x)$ are $0, 4, 5, 8, 9$.

$\diamond$

The following proposition complements Proposition 3.18 in the sense that $q \not\equiv 1 \pmod 4$ and m is even. Proposition 3.20 gives a relation between the fixed points of pairs of permutations, for this case.

Proposition 3.20. Let $q \equiv 3 \pmod 4$, m be even, $a \in {\mathbb{F}_q}^*$, and $c \in {\mathbb{F}_q}^*$. Then c is a fixed point of $f_0(x) = x^m(x^{\frac{q-1}{2}} + a)$ if and only if $-c$ is a fixed point of $f_1(x) = x^m(x^{\frac{q-1}{2}} - a)$.

Proof. Let α be a primitive element of $\mathbb{F}_q$ and $k \in \mathbb{Z}$. If $q \equiv 3 \pmod 4$, then $\frac{q-1}{2}$ is odd. Hence, by Proposition 3.10, we have that

$$\begin{aligned}
\alpha^k \text{ is a fixed point of } f_0(x) &\iff \alpha^{k(1-m)} = a + (-1)^k \\
&\iff -\alpha^{k(1-m)} = -(a + (-1)^k) \\
&\iff (\alpha^{\frac{q-1}{2}})^{1-m}\alpha^{k(1-m)} = -a + (-1)^k(-1)^{\frac{q-1}{2}} \\
&\iff (\alpha^{k+\frac{q-1}{2}})^{1-m} = -a + (-1)^{k+\frac{q-1}{2}} \\
&\iff -\alpha^k = \alpha^{k+\frac{q-1}{2}} \text{ is a fixed point of } f_1(x).
\end{aligned}$$

$\square$

Note that this implies that we are mapping square fixed points to non-square fixed points and vice-versa.

Example 3.21. Let $f_0(x) = x^4(x^5+3) \in \mathbb{F}_{11}[x]$. Then $f_1(x) = x^4(x^5-3) \in \mathbb{F}_{11}[x]$.

In Example 3.12, we saw that the fixed points of $f_0(x)$ are $0, 8, 9$. Now we use

Proposition 3.20 to calculate the non-zero fixed points of $f_1(x)$:

$$-8 = 3 \quad \text{and}$$
$$-9 = 2.$$

That is, the fixed points of $f_1(x)$ are $0, 2, 3$.

$\diamond$

▷ Summary

Given the wide range of applications permutations have and the importance of the number of fixed points for these applications, in this chapter we study the fixed points of permutations $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ of $\mathbb{F}_q$. First, we provide a general formula for the fixed points of $f(x)$ that is not necessarily a permutation. Then, for a permutation of $\mathbb{F}_q$ of the form $f(x)$, we give explicit formulas for calculating its fixed points. Unlike for monomial permutations of $\mathbb{F}_q$, where the number of non-zero fixed points is always $\gcd(m-1, q-1)$ [2], we find that the amount of non-zero fixed points of $f(x)$ can be 0, g or $2g$ where $g = \gcd\left(m-1, \frac{q-1}{2}\right)$.

Chapter 4

Involutions of the Form $x^m(x^{\frac{q-1}{2}} + a)$

In this chapter we present results on involutions of the form $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ of $\mathbb{F}_q$. In Section 4.1, an algorithm for generating all involutions of $\mathbb{F}_q$ of the form $f(x)$ is provided. We revisit the subject of fixed points in Section 4.2, this time in the context of involutions. In Section 4.3, we present constructions for m such that $f(x)$ is an involution and, in Section 4.4, we give a characterization of involutions $f(x)$ with more than one fixed points in terms of the number of fixed points.

4.1 Involutions

In this section we characterize involutions of $\mathbb{F}_q$ of the form $f(x) = x^m(x^{\frac{q-1}{2}} + a)$. Recall from Section 3.1 that these permutations always come in pairs, however, this is not always the case for involutions. In Section 4.1.1 we present conditions for some involutions to come in pairs.

Definition 4.1. A permutation $f(x)$ is an **involution** of $\mathbb{F}_q$ if it is its own inverse, that is $f(f(x)) = x$ for all $x \in \mathbb{F}_q$.

In [17], a characterization of involutions of $\mathbb{F}_q$ of the form $x^m h(x^s)$ was given. This family of binomials encompasses $f(x)$.

Theorem 4.2 ([17], Theorem 3)**.** *Let m, s, r be positive integers and $sr = q - 1$. Let $h'(x) = x^m h(x)^s$ for some polynomial $h(x) \in \mathbb{F}_q[x]$. The polynomial $f(x) = x^m h(x^s)$ is an involution of $\mathbb{F}_q$ if and only if the following conditions hold*

1. $m^2 \equiv 1 \pmod{s}$
2. $\phi(z) = z^{\frac{m^2-1}{s}}(h \circ h')(z)h(z)^m = 1 \ \forall \ z \in \mu_r,$

where μ_r denotes the set of r^{th} roots of unity in ${\mathbb{F}_q}^*$.

Note that for $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ with $a \in {\mathbb{F}_q}^*$ we can simplify Condition 2 in Theorem 4.2 by letting $h(x) = x + a$ and $r = 2$. This gives necessary and sufficient conditions for $f(x)$ to be an involution.

Proposition 4.3. Let q be odd, m be a positive integer, and $a \in {\mathbb{F}_q}^*$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ if and only if the following conditions hold

1. $m^2 \equiv 1 \ \left(\mathrm{mod}\ \frac{q-1}{2}\right)$
2. $(a+1)^m[(a+1)^{\frac{q-1}{2}} + a] = 1$
3. $(a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}} + a] = (-1)^{\frac{2(m^2-1)}{q-1}}$.

Proof. Let $h(x) = x + a$, $r = 2$, and $s = \frac{q-1}{2}$. Then, from Theorem 4.2, we have $h'(x) = x^m(x+a)^{\frac{q-1}{2}}$ and

$$\begin{aligned}\phi(z) &= z^{\frac{m^2-1}{s}}(h \circ h')(z)h(z)^m \\ &= z^{\frac{2(m^2-1)}{q-1}}[z^m(z+a)^{\frac{q-1}{2}} + a](z+a)^m.\end{aligned}$$

By Theorem 4.2, $f(x)$ is an involution of $\mathbb{F}_q$ if and only if $m^2 \equiv 1 \ \left(\mathrm{mod}\ \frac{q-1}{2}\right)$ and $\phi(z) = 1$ for all $z \in \mu_2$, where $\mu_2 = \{-1, 1\}$. Note that

$$\phi(1) = (a+1)^m[(a+1)^{\frac{q-1}{2}} + a],$$

and

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

Lastly, note that

$$\begin{aligned}\phi(-1) = 1 &\iff (-1)^{\frac{2(m^2-1)}{q-1}}(a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}} + a] = 1 \\ &\iff (a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}} + a] = (-1)^{\frac{2(m^2-1)}{q-1}}.\end{aligned}$$

Therefore, $f(x)$ is an involution of $\mathbb{F}_q$ if and only if Conditions 1, 2 and 3 hold.

□

As we state at the beginning of this thesis, the goal is to give explicit formulas for m such that $f(x)$ is an involution of $\mathbb{F}_q$ depending on the number of fixed points of $f(x)$. Our approach to this problem is to first design an algorithm that produces all involutions for a fixed q and then implement it for all q's in a specified range. One of the first things we asked was: If we are looking for m's that are greater than or equal to 1, then when should we stop looking for m's? Condition 1 from Proposition 4.3 states that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$, then should we only check m's up to $\frac{q-1}{2}$ or are there more m's that produce distinct involutions? Remember that we want to be able to construct all possible m's that produce involutions. The following lemma answers this question.

Lemma 4.4. Let q be odd, m be a positive integer, $a \in {\mathbb{F}_q}^*$, and $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ and $f'(x) = x^{m'}(x^{\frac{q-1}{2}} + a)$ be involutions of $\mathbb{F}_q$. Then $f(x) = f'(x)$ if and only if $m \equiv m' \pmod{q-1}$.

Proof. Since $f(x)$ and $f'(x)$ are permutations of $\mathbb{F}_q$, then by Proposition 3.4, $\eta(a^2-1) = (-1)^{m+1}$. This implies that $a \neq \pm 1$ by definition of quadratic character

of $\mathbb{F}_q$. Then,

$$\begin{aligned} f(x) = f'(x) &\iff x^m(x^{\frac{q-1}{2}} + a) = x^{m'}(x^{\frac{q-1}{2}} + a) \\ &\iff x^m = x^{m'} \\ &\iff m \equiv m' \pmod{q-1}. \end{aligned}$$

□

Lemma 4.4 states that if we want to find all m's that produce distinct involutions for a fixed q, then we need all m's that are solutions of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$ in the range $1 \leq m \leq q-1$. However, we can reduce this range further. Note that for every m that is a solution of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and such that $1 \leq m < \frac{q-1}{2}$, $m + \frac{q-1}{2}$ is also a solution of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and $\frac{q-1}{2} \leq m + \frac{q-1}{2} < q-1$; by Lemma 4.4, this is the range of m that covers all possible distinct involutions $f(x)$ of $\mathbb{F}_q$. This means that we can restrict the search for m to the range $1 \leq m < \frac{q-1}{2}$ and find a's that satisfy the conditions in Proposition 4.3 for m and $m + \frac{q-1}{2}$.

Another question is: Then how do we find a? A naive approach would be to check that for a fixed a, we have $f(f(x)) = x$ for all elements x of $\mathbb{F}_q$. The advantage that Proposition 4.3 gives us for designing Algorithm 1 is that for a fixed a, we only need to verify if two equations that only depend on q, m and a are satisfied, namely Conditions 2 and 3, instead of iterating through all $x \in \mathbb{F}_q$ and verifying $f(f(x)) = x$. Keep in mind that we may not find an appropriate a for either m or $m + \frac{q-1}{2}$; we may also find an a for m, but none for $m + \frac{q-1}{2}$ or vice-versa.

Algorithm 1 Generate all involutions of the form $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ for a fixed q.

Require: q is an odd power of a prime.

Input: q

Output: $\{(m, a) \mid f(x) \text{ is an involution of } \mathbb{F}_q\}$

```
for x = 1 to (q-1)/2 do
    if x^2 ≡ 1 (mod (q-1)/2) then
        for all m ∈ {x, x + (q-1)/2} and all a ∈ F_q* do
            if (a+1)^m[(a+1)^((q-1)/2) + a] = 1 and (a-1)^m[(-1)^m(a-1)^((q-1)/2) + a] =
            (-1)^(2(m^2-1)/(q-1)) then
                print (m, a)
            end if
        end for
    end if
end for
```

4.1.1 Involution Pairs

Before we begin to study m, let us recall from Chapter 3 that permutations $f(x)$ of $\mathbb{F}_q$ come in pairs. That is, $f_0(x) = x^m(x^{\frac{q-1}{2}} + a)$ is a permutation of $\mathbb{F}_q$ if and only if $f_1(x) = x^m(x^{\frac{q-1}{2}} - a)$ is a permutation of $\mathbb{F}_q$. We want to know if this is also true for involutions and if so, determine if there is any relation between the fixed points of $f_0(x)$ and $f_1(x)$.

Example 4.5. Table 4.5.1 lists all involutions $f(x) = x^m(x^{11} + a)$ of $\mathbb{F}_{23}$ generated by Algorithm 1. We also use Theorem 3.13 to calculate the fixed points for each involution. Recall that Statement 3 from Theorem 3.13 states that the number of non-zero fixed points is either g or $2g$.

m	g	a	Number of non-zero fixed points	Non-zero fixed points	Non-zero fixed points as powers of α	
1	11	18	0	none	none	1
10	1	8	2	3, 19	α^{16}, α^{8}	2
		-8	2	4, 20	α^{4}, α^{5}	3
		11	2	9, 17	α^{10}, α^{7}	4
		-11	2	6, 14	α^{18}, α^{21}	5
21	1	2	2	16, 22	α^{8}, α^{11}	6
		3	2	2, 5	α^{2}, α^{1}	7
		5	2	12, 21	α^{20}, α^{13}	8
		7	2	11, 13	α^{9}, α^{14}	9
		17	2	8, 19	α^{6}, α^{15}	10

Table 4.5.1: All involutions $x^m(x^{11} + a)$ of $\mathbb{F}_{23}$ and their respective fixed points, where $g = \gcd(m - 1, 11)$ and $\alpha = 5$ is a primitive element in $\mathbb{F}_{23}$.

The table suggests that involutions come in pairs only when m is even. Note that these pairs also have the same number of fixed points.

Recall from Algorithm 1 that for each $m < \frac{q-1}{2}$ that is a solution to $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$, $m + \frac{q-1}{2}$ is also a solution of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$. However, there may not be an $a \in {\mathbb{F}_q}^*$ for each solution. This is the case for $m = 1$, note that $1 + \frac{22}{2} = 12$ has no values of a such that $f(x)$ is an involution of $\mathbb{F}_{23}$.

$\diamond$

Proposition 4.6. Let q be odd, m be even and $a \in {\mathbb{F}_q}^*$. Then $f_0(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution if and only if $f_1(x) = x^m(x^{\frac{q-1}{2}} - a)$ is an involution. Moreover, they have the same number of fixed points.

Proof. Proposition 3.6 states that $f_0(x)$ is a permutation of $\mathbb{F}_q$ if and only if $f_1(x)$ is a permutation of $\mathbb{F}_q$. By Proposition 3.20, $f_0(x)$ and $f_1(x)$ have the same number of fixed points.

Suppose $f_0(x)$ and $f_1(x)$ are permutations of $\mathbb{F}_q$. It is sufficient to prove that Conditions 2 and 3 from Proposition 4.3 hold for both $f_0(x)$ and $f_1(x)$. Note that we do not need to check Condition 1 since it is the same for $f_0(x)$ and $f_1(x)$. Now, since $f_0(x)$ and $f_1(x)$ are permutations, then $\gcd\left(m, \frac{q-1}{2}\right) = 1$ by Proposition 3.4. But by hypothesis, m is even, this implies that $\frac{q-1}{2}$ and $\frac{2(m^2-1)}{q-1}$ are odd. Now, note that for $f_1(x)$ the equation on Condition 2 of Proposition 4.3 can be expressed as:

$$\begin{aligned}(-a+1)^m[(-a+1)^{\frac{q-1}{2}} - a] &= (-1)^m(a-1)^m[(-1)^{\frac{q-1}{2}}(a-1)^{\frac{q-1}{2}} - a] \\ &= (a-1)^m[(-1)(a-1)^{\frac{q-1}{2}} - a] \\ &= (-1)(a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}} + a].\end{aligned}$$

Therefore,

$$\begin{aligned}&(-a+1)^m[(-a+1)^{\frac{q-1}{2}} - a] = 1 \\ \iff\ &(a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}} + a] = -1.\end{aligned}$$

That is, Condition 2 holds for $f_1(x)$ if and only if Condition 3 holds for $f_0(x)$.

Similarly, we can rewrite the expression on Condition 3 of Proposition 4.3 for $f_1(x)$:

$$\begin{aligned}(-a-1)^m[(-1)^m(-a-1)^{\frac{q-1}{2}} - a] &= (-1)^m(a+1)^m[(-1)^{\frac{q-1}{2}}(a+1)^{\frac{q-1}{2}} - a] \\ &= (a+1)^m[(-1)(a+1)^{\frac{q-1}{2}} - a] \\ &= (-1)(a+1)^m[(a+1)^{\frac{q-1}{2}} + a].\end{aligned}$$

Therefore,

$$\begin{aligned}&(-a-1)^m[(-1)^m(-a-1)^{\frac{q-1}{2}} - a] = -1 \\ \iff\ &(a+1)^m[(a+1)^{\frac{q-1}{2}} + a] = 1.\end{aligned}$$

That is, Condition 3 holds for $f_1(x)$ if and only if Condition 2 holds for $f_0(x)$.

□

Proposition 4.6 tells us that indeed for a fixed odd q, even m and $a \in \mathbb{F}_q{}^*$, m and $-a$ also produce an involution of $\mathbb{F}_q$. Moreover, they have the same number of fixed points.

We mentioned in Example 4.5 that Table 4.5.1 suggests that involutions do not come in pairs when m is odd. In the following example we show that there are instances where there exist pairs of involutions $f_0(x)$ and $f_1(x)$ with m odd. We study these cases more closely after this example.

Example 4.7. We use Algorithm 1 to find all involutions of $f(x) = x^m(x^{14} + a)$ of $\mathbb{F}_{29}$, and Theorem 3.13 to calculate the fixed points for each involution. Recall that the number of non-zero fixed points is either g or $2g$ by Theorem 3.13.

m	g	a	**Number of non-zero fixed points**	**Non-zero fixed points**	**Non-zero fixed points as powers of α**	
13	2	5	0	none	none	1
		-5	4	5, 8, 21, 24	α^{22}, α^{3}, α^{17}, α^{8}	2
		6	2	6, 23	α^{6}, α^{20}	3
		-6	2	13, 16	α^{18}, α^{4}	4
		8	2	14, 15	α^{13}, α^{27}	5
		-8	2	3, 26	α^{5}, α^{19}	6
27	2	5	2	2, 27	α^{1}, α^{15}	7
		-5	2	5, 24	α^{22}, α^{8}	8
		6	4	6, 11, 18, 23	α^{6}, α^{25}, α^{11}, α^{20}	9
		-6	4	13, 14, 15, 16	α^{18}, α^{13}, α^{27}, α^{4}	10
		8	0	none	none	11
		-8	0	none	none	12

Table 4.7.1: All involutions $x^m(x^{14} + a)$ of $\mathbb{F}_{29}$ and their respective fixed points, where $g = \gcd(m - 1, 14)$ and $\alpha = 2$ is a primitive element of $\mathbb{F}_{29}$.

Note that $q_1 = 23 \equiv 3 \pmod 4$ and $q_2 = 29 \equiv 1 \pmod 4$. Tables 4.5.1 and

4.7.1 might suggest that if m is odd, involutions only come in pairs when $q \equiv 1 \pmod 4$.

$\diamond$

The following example shows involutions $f_0(x)$, where m is odd and $q \equiv 1 \pmod 4$, that do not have pairs $f_1(x)$ which are also involutions.

Example 4.8. Let $q = 49$, $\mathbb{F}_{49} = \mathbb{F}_7[x]/(x^2 + 6x + 3)$, and $m = 11$.

Since $m^2 \equiv 11^2 \equiv 1 \pmod{24}$, we can implement Algorithm 1 starting in line 4, to generate all involutions of the form $f(x)$ with $q = 49$ and $m = 11$. We calculate the fixed points using Theorem 3.13.

a	**Number of non-zero fixed points**	**Non-zero fixed points**	
5β	4	$\beta + 4,\ 4\beta + 3,\ 6\beta + 3,\ 3\beta + 4$	1
$2\beta + 5$	4	$3\beta,\ 6\beta + 5,\ 4\beta,\ \beta + 2$	2

Table 4.8.1: All involutions of $x^{11}(x^{24} + a)$ of $\mathbb{F}_{49}$ and their respective fixed points, where β is a root of $x^2 + 6x + 3$, a primitive polynomial over $\mathbb{F}_7$.

Note that $-a = -5\beta = 2\beta$ and $-a = -2\beta - 5 = 5\beta + 2$. That is, there are no pairs of involutions for $q = 49 \equiv 1 \pmod 4$ and $m = 11$ odd.

$\diamond$

Since for m odd and $q \equiv 1 \pmod 4$, there are cases for which involutions do not come in pairs, we want to determine when exactly these pairs occur.

Proposition 4.9. Let $q \equiv 1 \pmod 4$, m be odd, $a \in {\mathbb{F}_q}^*$ and $f_0(x) = x^m(x^{\frac{q-1}{2}} + a)$ be an involution of $\mathbb{F}_q$. Then $f_1(x) = x^m(x^{\frac{q-1}{2}} - a)$ is an involution of $\mathbb{F}_q$ if and only if $\frac{2(m^2-1)}{q-1}$ is even.

Proof. Since Condition 1 from Proposition 4.3 only depends on m, it also holds true for $f_1(x)$. It is sufficient to prove that Conditions 2 and 3 hold for $f_1(x)$ if and only if $\frac{2(m^2-1)}{q-1}$ is even. Now, note that, since $q \equiv 1 \pmod 4$, $\frac{q-1}{2}$ is even and

$$
\begin{aligned}
&(-a+1)^m[(-a+1)^{\frac{q-1}{2}} - a] \\
&= (-1)^m(a-1)^m[(-1)^{\frac{q-1}{2}}(a-1)^{\frac{q-1}{2}} - a] \\
&= (-1)^m(a-1)^m[(a-1)^{\frac{q-1}{2}} - a] \\
&= (a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}} + a] \\
&= (-1)^{\frac{2(m^2-1)}{q-1}}.
\end{aligned}
$$

Then Condition 2 to holds if and only if $\frac{2(m^2-1)}{q-1}$ is even. Now we verify Condition 3.

$$
\begin{aligned}
&(-a-1)^m[(-1)^m(-a-1)^{\frac{q-1}{2}} - a] \\
&= (-1)^m(a+1)^m[(-1)(-1)^{\frac{q-1}{2}}(a+1)^{\frac{q-1}{2}} - a] \\
&= (-1)(a+1)^m[(-1)(a+1)^{\frac{q-1}{2}} - a] \\
&= (a+1)^m[(a+1)^{\frac{q-1}{2}} + a] \\
&= 1.
\end{aligned}
$$

Hence Conditions 2 and 3 hold if and only if $\frac{2(m^2-1)}{q-1}$ is even. Then $f_1(x)$ is an involution of $\mathbb{F}_q$ if and only if $\frac{2(m^2-1)}{q-1}$ is even.

□

Example 4.10. Recall that in Example 4.7, we list all involutions of $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ for $q = 29$. Note that $q \equiv 1 \pmod 4$ and all of the involutions on Table 4.7.1 come in pairs for $m = 13$ and $m = 27$. Note

$$\frac{13^2-1}{14} = 12 \qquad \text{and} \qquad \frac{27^2-1}{14} = 52,$$

that is, $\frac{2(m^2-1)}{q-1}$ is even for all involutions of $\mathbb{F}_{29}$.

◇

4.2 Fixed Points

Our goal is to provide formulas for involutions with a prescribed number of fixed points. In this section, we study the fixed points of involutions $f(x)$ of $\mathbb{F}_q$ and characterize involutions that have more than one fixed point.

First, let us briefly discuss the case where $f(x)$ only has 0 as a fixed point. The contrapositive of Proposition 3.10, which tells us when $f(x) \in \mathbb{F}_q[x]$ has non-zero fixed points, gives necessary and sufficient conditions for $f(x)$ to have only 0 as a fixed point. We also saw in Example 3.17 that the converse of Proposition 3.16 is false, however note that the contrapositive states that if $a+1$ is a non-square then the permutation $f(x)$ only has 0 as a fixed point. Since for some applications of permutations it is preferred to have a low number of fixed points, in this case, we can choose $a+1$ to be a non-square and guarantee that the permutation or involution only has 0 as its fixed point. Another option for such applications is to choose an m such that $g = \gcd\left(m-1, \frac{q-1}{2}\right)$ is a small number. In case that we want to have exactly $g+1$ fixed points, we need a's such that $a+1 = \alpha^{k_1(1-m)}$ or $a-1 = \alpha^{k_2(1-m)}$, for some k_1 even or k_2 odd, but not both. Similarly, if we want to have $2g+1$ fixed points we have to select appropriate a's such that both $a+1 = \alpha^{k_1(1-m)}$ and $a-1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd.

Example 4.11. To generate involutions with only 0 as a fixed point for a fixed q using the contrapositive of Proposition 3.16, one can add the extra condition $(a+1)^{\frac{q-1}{2}} = -1$ after line 4 of Algorithm 1.

Let $\mathbb{F}_{25} = \mathbb{F}_5/(x^2+4x+2)$. Now, we use this modification of Algorithm 1 to generate the following table of involutions of $\mathbb{F}_{25}$ with only 0 as a fixed point.

m	a	
7	2	1
11	2	2
19	2	3
23	2	4

Table 4.11.1: Involutions $x^m(x^{12}+a)$ of $\mathbb{F}_{25}$ with only 0 as a fixed point, where β is a root of x^2+4x+2, a primitive polynomial over $\mathbb{F}_5$.

$\diamond$

It should be noted that Table 4.11.1 might not list all involutions of the form $f(x)$ of $\mathbb{F}_{25}$ such that their only fixed point is zero. This we know since Example 3.17 shows that the converse of Proposition 3.16 is false. If one wanted to construct all such involutions, one could instead use Statement 3 of Theorem 3.13 to modify Algorithm 1.

Example 4.12. To generate all involutions with only 0 as a fixed point for a fixed q using Statement 3 of Theorem 3.13, one can add the extra condition $a+(-1)^k \neq \alpha^{k(1-m)}$ for all $k \in \mathbb{Z}$ after line 4 of Algorithm 1.

Let $\mathbb{F}_{25} = \mathbb{F}_5/(x^2+4x+2)$. Now, we use this modification of Algorithm 1 to generate the following table of all involutions of $\mathbb{F}_{25}$ with only 0 as a fixed point.

m	a	$\eta(a)$	
7	2	1	1
	$3\beta+1$	-1	2
	$2\beta+4$	-1	3
11	2	1	4
19	2	1	5
23	2	1	6

Table 4.12.1: All involutions $x^m(x^{12}+a)$ of $\mathbb{F}_{25}$ with only 0 as a fixed point, where β is a root of x^2+4x+2, a primitive polynomial over $\mathbb{F}_5$.

Note that the only involutions that were not generated using the contrapositive of Proposition 3.16—listed in Table 4.11.1—are involutions on lines 2 and 3. Also note that these are the only values of a on Table 4.12.1 that are not squares in $\mathbb{F}_{25}$.

$\diamond$

Now we shift the focus to the non-zero fixed points of an involution $f(x)$ of $\mathbb{F}_q$. In Section 3.2, we proved that the number of fixed points of a permutation $f(x)$ of $\mathbb{F}_q$ is always 1, $g+1$, or $2g+1$, where $g = \gcd\left(m-1, \frac{q-1}{2}\right)$. This also holds true for involutions, however, it has an additional restriction that the number of non-zero fixed points must be even. In other words, permutations $f(x)$ of $\mathbb{F}_q$ with an odd number of non-zero fixed points cannot be involutions of $\mathbb{F}_q$.

Definition 4.13. Let f be a permutation of $\mathbb{F}_q$. Then f has a **cycle of length** $k \in \mathbb{Z}$ if there exists $i \in \mathbb{F}_q$ such that k is the smallest positive integer such that $f^k(i) = i$.

Proposition 4.14. Let q be odd, and f be a permutation of $\mathbb{F}_q$. Then $f(x)$ is an involution if and only if it decomposes into cycles of length two or one.

Proof. Note that for all $x \in \mathbb{F}_q$, $f(f(x)) = x$ if and only if $f^k(x) = x$ where $k \in \{1, 2\}$, since $f^1(x) = x$ implies $f^2(x) = f(f(x)) = x$.

$\square$

Proposition 4.15. Let q be odd, m be a positive integer, and $a \in \mathbb{F}_q^*$. If $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$, then the number of non-zero fixed points is even.

Proof. If $f(x)$ has no non-zero fixed points, then we are done. Suppose $f(x)$ has non-zero fixed points. Since $f(x)$ is an involution, it decomposes into cycles of length 2 and fixed points which are cycles of length 1, then the number of non-zero fixed points is equal to $q-1$ minus twice the number of cycles of length 2. Since $q-1$ is even, then the number of non-zero fixed points is also even.

$\square$

Example 4.16. Let $f(x) = x^{11}(x^6 + 2) \in \mathbb{F}_{13}[x]$. In Example 3.5 we presented the values of $f(x)$. Note that the cycle decomposition of $f(x)$ is

$$(1\ 3)(2\ 7)(5\ 8)(6\ 11)(10\ 12).$$

Therefore $f(x)$ decomposes into cycles of length 2 and is an involution by Proposition 4.14. Moreover, the fixed points of $f(x)$ are 0, 4 and 9. Note that $g = \gcd(m-1, \frac{q-1}{2}) = \gcd(-10, 6) = 2$, therefore, $f(x)$ has $g + 1 = 3$ fixed points.

$\diamond$

We now present a characterization of involutions $f(x)$ of $\mathbb{F}_q$ that have more than one fixed point. To do this, we need Lemmas 4.17 and 4.18.

Lemma 4.17. Let q be odd, m be a positive integer, α be a primitive element of $\mathbb{F}_q$, and $a \in {\mathbb{F}_q}^*$. If $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$, and $a + 1 = \alpha^{k(1-m)}$ where k is even, then $(a+1)^m[(a+1)^{\frac{q-1}{2}} + a] = 1$.

Proof. Since k is even, then $k = 2h$ for some $h \in \mathbb{Z}$. Then,

$$\begin{aligned}
(a+1)^m[(a+1)^{\frac{q-1}{2}} + a] &= (a+1)^m[(\alpha^{2h(1-m)})^{\frac{q-1}{2}} + a] \\
&= (a+1)^{m+1} \\
&= (\alpha^{2h(1-m)})^{m+1} \\
&= (\alpha^h)^{2(m^2-1)} \\
&= 1,
\end{aligned}$$

since $m^2 - 1 \equiv 0 \pmod{\frac{q-1}{2}}$ implies that $2(m^2-1) \equiv 0 \pmod{q-1}$.

$\square$

Lemma 4.18. Let q be odd, m be a positive integer, α be a primitive element of $\mathbb{F}_q$, and $a \in {\mathbb{F}_q}^*$. If $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$, and $a - 1 = \alpha^{k(1-m)}$ where k is odd, then $(a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}} + a] = (-1)^{\frac{2(m^2-1)}{q-1}}$. Moreover, $\eta(a-1) = (-1)^{m+1}$ and $(a-1)^{m+1} = (-1)^{\frac{2(m^2-1)}{q-1}}$.

Proof. Note that

$$m^2 \equiv 1 \pmod{\frac{q-1}{2}} \iff \frac{q-1}{2}h = 1 - m^2,\ h \in \mathbb{Z} \iff h = \frac{2(1-m^2)}{q-1}.$$

Then we have

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

Also, since $k = 2\ell + 1$ for some $\ell \in \mathbb{Z}$, then,

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

Lastly, note that

$$\begin{aligned}(a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}} + a] &= (a-1)^m[(-1)^m(-1)^{m+1} + a] \\ &= (a-1)^m[-1 + a] \\ &= (a-1)^{m+1} \\ &= (-1)^{\frac{2(m^2-1)}{q-1}}.\end{aligned}$$

□

Theorem 4.19. Let q be odd, m be a positive integer and α be a primitive element of $\mathbb{F}_q$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a),\ a \in \mathbb{F}_q{}^*$, is an involution of $\mathbb{F}_q$ with more than one fixed point if and only if the following conditions hold:

1. $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$,
2. $\eta(a^2-1) = (-1)^{m+1}$,
3. $(a^2-1)^{m+1} = (-1)^{\frac{2(m^2-1)}{q-1}}$,
4. $a + 1 = \alpha^{k_1(1-m)}$ or $a - 1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd.

Proof. ($\Rightarrow$) Since $f(x)$ is an involution, Conditions 1 and 2 hold by Proposition 3.4 and Proposition 4.3. Since $f(x)$ has more than one fixed point, then $\eta(a+1) = 1$

by Proposition 3.16. This implies that $\eta(a-1) = (-1)^{m+1}$. By Proposition 4.3, we have that

$$\begin{aligned} 1 &= (a+1)^m[(a+1)^{\frac{q-1}{2}} + a] \\ &= (a+1)^m[1+a] \\ &= (a+1)^{m+1}, \end{aligned}$$

and

$$\begin{aligned} (-1)^{\frac{2(m^2-1)}{q-1}} &= (a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}} + a] \\ &= (a-1)^m[(-1)^m(-1)^{m+1} + a] \\ &= (a-1)^m[-1+a] \\ &= (a-1)^{m+1}. \end{aligned}$$

Therefore $(a^2-1)^{m+1} = (-1)^{\frac{2(m^2-1)}{q-1}}$ and Condition 3 holds.

Lastly, by Corollary 3.11, Condition 4 holds since $f(x)$ has more than one fixed point.

($\Leftarrow$) It is sufficient to prove that Conditions 2 and 3 from Proposition 4.3 hold.

Suppose that $a+1 = \alpha^{k_1(1-m)}$ for k_1 even. Then by Lemma 4.17, we have

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

Now, note that $(-1)^{m+1} = \eta(a+1)\eta(a-1) = \eta(\alpha^{k_1(1-m)})\eta(a-1) = \eta(a-1)$ since $k_1 = 2\ell$ for some $\ell \in \mathbb{Z}$. Also, $1-m^2 \equiv 0 \pmod{\frac{q-1}{2}}$ if and only if $1-m^2 = \frac{q-1}{2}h$,

for some $h \in \mathbb{Z}$. Then,

$$\begin{aligned}(-1)^{\frac{2(1-m^2)}{q-1}} &= (a+1)^{m+1}(a-1)^{m+1} \\ &= (\alpha^{2\ell(1-m)})^{m+1}(a-1)^{m+1} \\ &= (\alpha^{2\ell})^{1-m^2}(a-1)^{m+1} \\ &= (\alpha^{2\ell})^{\frac{q-1}{2}h}(a-1)^{m+1}, \quad \text{where } h \in \mathbb{Z}, \\ &= (a-1)^{m+1}.\end{aligned}$$

Therefore,

$$\begin{aligned}&(a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}} + a] \\ &= (a-1)^m[(-1)^m(-1)^{m+1} + a] \\ &= (a-1)^m[-1+a] \\ &= (a-1)^{m+1} \\ &= (-1)^{\frac{2(m^2-1)}{q-1}}.\end{aligned}$$

Then $f(x)$ is an involution of $\mathbb{F}_q$. Since $a+1 = \alpha^{k_1(1-m)}$, k_1 even, then $f(x)$ has more than one fixed point by Theorem 3.13.

Suppose now that $a-1 = \alpha^{k_2(1-m)}$ for k_2 odd. Then, by Lemma 4.18, we have

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

Now, by Lemma 4.18, we have $(a-1)^{m+1} = (-1)^{\frac{2(m^2-1)}{q-1}}$ and $\eta(a-1) = (-1)^{m+1}$. By hypothesis, this implies that $(a+1)^{m+1} = 1$ and $\eta(a+1) = 1$. Then,

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

Therefore $f(x)$ is an involution of $\mathbb{F}_q$. Since $a-1 = \alpha^{k_2(1-m)}$ and k_2 is odd, $f(x)$ has more than one fixed point by Corollary 3.11.

□

In Theorem 4.19, Condition 4 guarantees that $f(x)$ has non-zero fixed points. A natural assumption would be that Conditions $1, 2$ and 3 are sufficient for $f(x)$ to be an involution, however, this statement is false.

Example 4.20. Consider $f(x) = x(x^3 + 3) \in \mathbb{F}_7[x]$. Note that

$$\begin{aligned} &m^2 \equiv 1 \pmod 3, \\ &\eta(a^2 - 1) = \eta(8) = \eta(1) = 1 = (-1)^{m+1} \quad \text{and} \\ &(a^2 - 1)^{m+1} = 8^2 = 1 = (-1)^{\frac{2(m^2-1)}{q-1}}. \end{aligned}$$

Then $f(x)$ satisfies Conditions $1, 2$ and 3 from Theorem 4.19. However,

$$\begin{aligned} &(a+1)^m[(a+1)^{\frac{q-1}{2}} + a] = 4^2 = 2 \quad \text{and} \\ &(a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}} + a] = 2^2 = 4. \end{aligned}$$

Therefore Conditions 2 and 3 from Proposition 4.3 do not hold and $f(x)$ is not an involution of $\mathbb{F}_7$.

$\diamond$

Now that we have a characterization of involutions $f(x)$ of $\mathbb{F}_q$ with more than one fixed point, we can modify Algorithm 1 to generate all such involutions.

Algorithm 2 Generate all involutions of the form $x^m(x^{\frac{q-1}{2}}+a)$ with more than one fixed point for a fixed q.

Require: q is an odd power of a prime and α is a primitive element of $\mathbb{F}_q$.

Input: q

Output: $\{(m,a) \mid f(x)$ is an involution of $\mathbb{F}_q$ with more than one fixed point$\}$

1: **for** $x = 1$ to $\frac{q-1}{2}$ **do**
2: **if** $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$ **then**
3: **for all** $m \in \{x, x+\frac{q-1}{2}\}$ **and all** $a \in \mathbb{F}_q{}^*$ **do**
4: **if** $\eta(a^2-1) = (-1)^{m+1}$ **and** $(a^2-1)^{m+1} = (-1)^{\frac{2(m^2-1)}{q-1}}$ **then**
5: **if** $a+1 = \alpha^{k_1(1-m)}$ **or** $a-1 = \alpha^{k_2(1-m)}$ for some k_1 even and k_2 odd **then**
6: **print** (m,a)
7: **end if**
8: **end if**
9: **end for**
10: **end if**
11: **end for**

Recall that Statement 3 of Theorem 3.13 tell us that the possible numbers of fixed points are 1, $g+1$ and $2g+1$ where $g = \gcd(m-1, \frac{q-1}{2})$. We use Theorem 4.19 to find more specific conditions for $f(x)$ to be an involution of $\mathbb{F}_q$ with exactly $g+1$ and $2g+1$ fixed points.

Proposition 4.21. Let q be odd, m be a positive integer, α be a primitive element of $\mathbb{F}_q$ and $g = \gcd\left(m-1, \frac{q-1}{2}\right)$. Then $f(x) = x^m(x^{\frac{q-1}{2}}+a)$, $a \in \mathbb{F}_q{}^*$, is an involution of $\mathbb{F}_q$ with exactly $2g+1$ fixed points if and only if the following conditions hold:

1. $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$,
2. $a+1 = \alpha^{k_1(1-m)}$ and $a-1 = \alpha^{k_2(1-m)}$ for some k_1 even and k_2 odd.

Proof. ($\Rightarrow$) By Theorem 4.19, Condition 1 holds, and $a+1 = \alpha^{k_1(1-m)}$ or $a-1 = \alpha^{k_2(1-m)}$ for some k_1 even and k_2 odd. Since $f(x)$ has exactly $2g+1$ fixed points,

then by Theorem 3.13, Condition 2 holds.

($\Leftarrow$) Conversely, note that, by Lemma 4.17

$$(a+1)^m[(a+1)^{\frac{q-1}{2}}+a]=1,$$

and by Lemma 4.18

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

Therefore, by Proposition 4.3, $f(x)$ is an involution. Lastly, Condition 2 implies that $f(x)$ has both square and non-square fixed points therefore it has $2g+1$ fixed points in total by Theorem 3.13.

□

Example 4.22. Let $f(x)=x^4(x^5+3)\in\mathbb{F}_{11}[x]$. Then $g=\gcd(-3,5)=1$. From Example 3.12, we verify that 2 is a primitive element of $\mathbb{F}_{11}$ and that $f(x)$ has $2g+1$ fixed points. To know if $f(x)$ is an involution with $2g+1$ fixed points, we can verify the conditions on Proposition 4.21. Since $m^2\equiv 4^2\equiv 1 \pmod 5$, Condition 1 holds. Now, note that $1-m=-3$ and

$$\begin{aligned} a+1&=4=2^2=2^{6(-3)}=2^{6(1-m)}, \quad \text{and}\\ a-1&=2=2^{3(-3)}=2^{3(1-m)}. \end{aligned}$$

Since 6 is even and 3 is odd, then Condition 2 holds. Then $f(x)$ is an involution with $2g+1$ fixed points.

◇

Also, note that involutions on lines $3,4,5,8,9$ from Table 4.5.1 have both square and non-square fixed points.

Proposition 4.23. Let q be odd, m be a positive integer, α be a primitive element of $\mathbb{F}_q$ and $g=\gcd\left(m-1,\frac{q-1}{2}\right)$. Then $f(x)=x^m(x^{\frac{q-1}{2}}+a)$, $a\in\mathbb{F}_q{}^*$, is an

involution of $\mathbb{F}_q$ with exactly $g+1$ square fixed points if and only if the following conditions hold:

1. $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$,
2. $\eta(a-1) = (-1)^{m+1}$,
3. $(a-1)^{m+1} = (-1)^{\frac{2(m^2-1)}{q-1}}$,
4. $a+1 = \alpha^{k_1(1-m)}$, where k_1 is even,
5. $a-1 \neq \alpha^{k_2(1-m)}$, for all k_2 odd.

Proof. ($\Rightarrow$) Since $f(x)$ is an involution, then Condition 1 holds. Since $f(x)$ only has square fixed points, then by Corollary 3.11, Conditions 4 and 5 hold. Also, since $f(x)$ has more than one fixed point, then by Proposition 3.16, $\eta(a+1) = 1$. Then, by Theorem 4.19,

$$(-1)^{m+1} = \eta(a+1)\eta(a-1) = \eta(a-1) = \eta(a-1),$$

and Condition 2 holds. Also, since $1 - m^2 = \frac{q-1}{2}\ell$ for some $\ell \in \mathbb{Z}$, then

$$\begin{aligned}(-1)^{\frac{2(m^2-1)}{q-1}} &= (a+1)^{m+1}(a-1)^{m+1} \\ &= (\alpha^{k_1(1-m)})^{m+1}(a-1)^{m+1} \\ &= (\alpha^{k_1})^{1-m^2}(a-1)^{m+1} \\ &= (\alpha^{k_1})^{\frac{q-1}{2}\ell}(a-1)^{m+1} \\ &= (a-1)^{m+1},\end{aligned}$$

and Condition 3 holds.

($\Leftarrow$) Conversely, by Lemma 4.17, Conditions 1 and 4 imply

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

Similarly, Conditions 2 and 3 imply

$$\begin{aligned}(a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}}+a] &= (a-1)^m[(-1)^m(a-1)^{\frac{q-1}{2}}+a] \\ &= (a-1)^{m+1} \\ &= (-1)^{\frac{2(m^2-1)}{q-1}}.\end{aligned}$$

Therefore, by Proposition 4.3, $f(x)$ is an involution. Conditions 4 and 5 imply that $f(x)$ has exactly $g+1$ square fixed points by Corollary 3.11.

□

Note that involutions on line $3, 4$ and 8 from Table 4.7.1 and involution on line 2 from Table 4.5.1 have exactly $g+1$ square fixed points.

Proposition 4.24. Let q be odd, m be a positive integer, α be a primitive element of $\mathbb{F}_q$ and $g = \gcd\left(m-1, \frac{q-1}{2}\right)$. Then $f(x) = x^m(x^{\frac{q-1}{2}}+a)$, $a \in {\mathbb{F}_q}^*$, is an involution of $\mathbb{F}_q$ with g non-square fixed points and no non-zero square fixed points if and only if the following conditions hold:

1. $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$,
2. $\eta(a+1) = 1$,
3. $(a+1)^{m+1} = 1$,
4. $a+1 \neq \alpha^{k_1(1-m)}$ for all k_1 even,
5. $a-1 = \alpha^{k_2(1-m)}$, where k_2 is odd.

Proof. ($\Rightarrow$) Since $f(x)$ is an involution with more than one fixed point, then Conditions 1 and 2 hold by Proposition 4.3 and Proposition 3.16 respectively. Now, also by Proposition 4.3,

$$1 = (a+1)^m[(a+1)^{\frac{q-1}{2}}+a] = (a+1)^m[1+a] = (a+1)^{m+1},$$

and Condition 3 holds. Lastly, since $f(x)$ has g non-square fixed points and no non-zero square fixed points, then Conditions 4 and 5 hold by Corollary 3.11.

($\Leftarrow$) Conversely, Conditions 2 and 3 imply

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

Similarly, note that, by Lemma 4.18, Conditions 1 and 4 imply

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

Therefore, by Proposition 4.3, $f(x)$ is an involution. By Corollary 3.11, Conditions 4 and 5 imply that $f(x)$ has g non-square fixed points and no non-zero square fixed points.

□

Note that involutions on lines $5, 6$ and 7 from Table 4.7.1 and involutions on lines $6, 7$ and 10 from Table 4.5.1 have exactly g non-square fixed points.

4.3 Explicit Formulas for m

The monomial x^m is an involution of $\mathbb{F}_q$ if and only if $m^2 \equiv 1 \pmod{q-1}$. In [2], explicit formulas to construct all such m's with a prescribed number of fixed points are given.

Theorem 4.25 ([2], Theorem 2.5)**.** *Let* $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $d = 2^f p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$, $f \leq e$, $\ell_s \in \{0, e_s\}$, *and* α *be a primitive element of* $\mathbb{F}_q$. *The monomial* x^m *is an involution of* $\mathbb{F}_q$ *with exactly* $d+1$ *fixed points if and only if* $m \equiv \left(\frac{q-1}{d}\right) k - 1$

(mod $q-1$) *where*

$$k = \begin{cases} 2\left(\dfrac{q-1}{d}\right)^{\phi(d)-1} & \text{if } f = e \geq 0, \\ \left(\dfrac{q-1}{2d}\right)^{\phi(d)-1} + \dfrac{d}{2} & \text{if } f = e-1 \geq 1, \\ \left(\dfrac{q-1}{2d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t,\ t \in \left\{0, \dfrac{d}{2}\right\} & \text{if } f = 1, e \geq 3, \end{cases}$$

is reduced modulo d and ϕ is the Euler function. Moreover, these are all the involutions of $\mathbb{F}_q$ given by monomials and the fixed points have the form $0, \alpha^j$, where $j = \frac{q-1}{d}l$, $l = 1, \ldots, d$.

Let us see first a simple example where Theorem 4.25 can be used to construct an involution with a prescribed number of fixed points.

Example 4.26. Let $q = 13$. Then $q - 1 = 12 = 2^2 \cdot 3$, and $e = 2$. We can construct an m such that x^m is an involution of $\mathbb{F}_{13}$ with d non-zero fixed points where $d \in \{2^1, 2^2, 2^1 \cdot 3, 2^2 \cdot 3\}$. For this example, we construct all monomial involutions of $\mathbb{F}_{13}$ with $d = 2$ non-zero fixed points. Now, since $f = e - 1 = 1$,

$$k = \left(\frac{q-1}{2d}\right)^{\phi(d)-1} + \frac{d}{2} = \left(\frac{12}{4}\right)^{\phi(2)-1} + 1 = 3^0 + 1 = 2 \equiv 0 \pmod 2.$$

We can now calculate m,

$$m \equiv \left(\frac{q-1}{d}\right) k - 1 \equiv \left(\frac{12}{2}\right) 0 - 1 \equiv -1 \equiv 11 \pmod{12}.$$

This gives us the involution x^{11} of $\mathbb{F}_{13}$ that has exactly 3 fixed points.

Note that 0 is always a fixed point. To calculate the two other fixed points of x^{11} we need to find a primitive element of $\mathbb{F}_{13}$. From Example 2.7, we know that 2 is a primitive element of $\mathbb{F}_{13}$. Theorem 4.25 says that the non-zero fixed points are α^j where $j = \left(\frac{q-1}{d}\right)\ell = 6\,\ell$ for $\ell = 1, 2$. Hence, the non-zero fixed points of the involution x^{11} of $\mathbb{F}_{13}$ are 0, $2^6 = 12$, and $2^{12} = 1$.

$\diamond$

Theorem 4.25 lets us do more than construct an involution with $d+1$ fixed points for a fixed q; it also tells us that there are at most four involutions with the same number of non-zero fixed points. In the next example, we use Theorem 4.25 to know how many involutions there are that have exactly 3 fixed points.

Example 4.27. Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ and $d = 2$, that is $f = \nu_2(d) = 1$. We use Theorem 4.25 to construct all involutions with $d = 2$.

Suppose $e = 1$, then

$$m = \left(\frac{q-1}{d}\right)\left[2\left(\frac{q-1}{d}\right)^{\phi(d)-1}\right] - 1 = 2\left(\frac{q-1}{2}\right)^{\phi(2)} - 1 = q-2.$$

Suppose now that $e = 2$, then

$$\begin{aligned} m &= \left(\frac{q-1}{d}\right)\left[\left(\frac{q-1}{2d}\right)^{\phi(d)-1} + \frac{d}{2}\right] - 1 \\ &= \left(\frac{q-1}{2}\right)\left[\left(\frac{q-1}{4}\right)^{\phi(2)-1} + 1\right] - 1 \\ &= \left(\frac{q-1}{2}\right)2 - 1 \\ &= q-2. \end{aligned}$$

Lastly, suppose $e \geq 3$, then

$$\begin{aligned} m &= \left(\frac{q-1}{d}\right)\left[\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t\right] - 1, \quad t \in \left\{0, \frac{d}{2}\right\} \\ &= \left(\frac{q-1}{2}\right)\left[\left(\frac{q-1}{4}\right)^{\phi(1)-1} + t\right] - 1, \quad t \in \{0,1\} \\ &= \left(\frac{q-1}{2}\right)[1+t] - 1, \end{aligned}$$

then $m = \frac{q-1}{2} - 1 = \frac{q-3}{2}$ or $m = \left(\frac{q-1}{2}\right)2 - 1 = q-2$. Therefore, we have

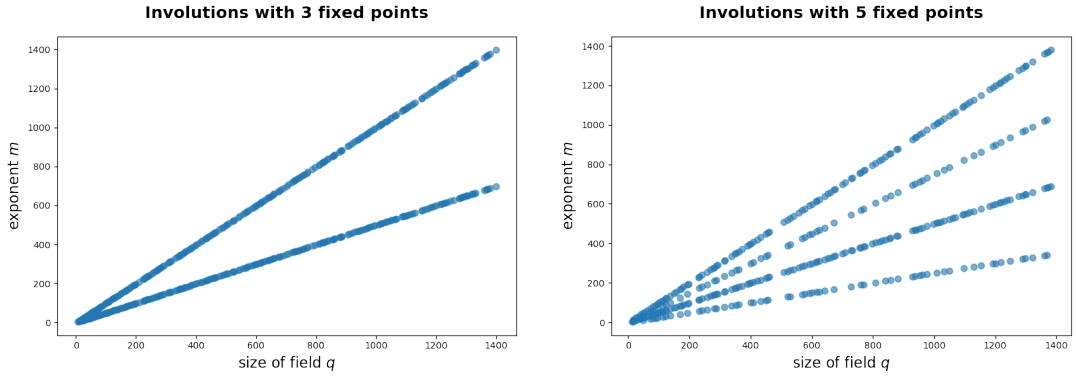
$$m = \begin{cases} q-2 & \text{if } e = 1,2 \\ \dfrac{q-3}{2},\ q-2 & \text{if } e \geq 3. \end{cases}$$

Theorem 4.25 tells us that there are at most two monomial involutions of $\mathbb{F}_q$ with $d+1=3$ fixed points.

$\diamond$

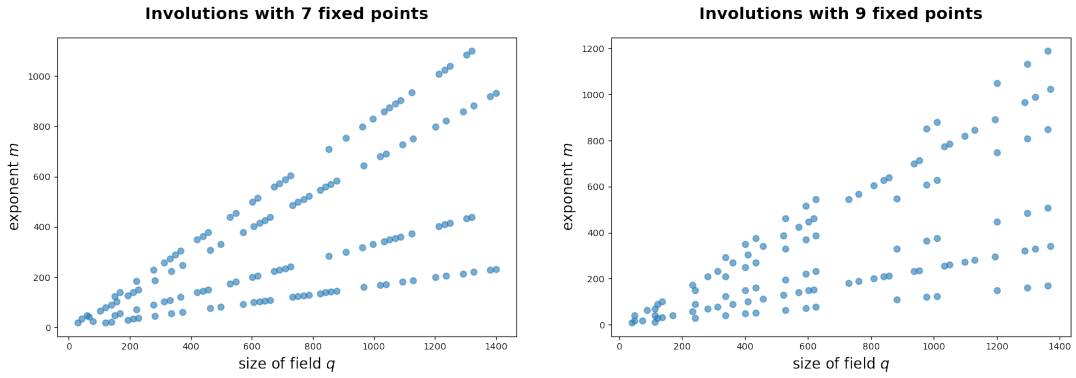
In this section we show a similar approach with the goal of constructing all possible m's for $f(x)=x^m(x^{\frac{q-1}{2}}+a)$ to be an involution with a prescribed number of fixed points. Note that for monomials, m is of the form $\left(\frac{q-1}{d}\right)k-1 \pmod{q-1}$. We want to know if there is a similar relationship between m and the number of non-zero fixed points for involutions $f(x)$ of $\mathbb{F}_q$. Also note that for monomials, 0 and 1 are always fixed. This implies that for monomial involutions, the number of non-zero fixed points d is always greater than or equal to 1. Yet this is not true for involutions $f(x)$ of $\mathbb{F}_q$. This is important since, for monomials, d is the number of non-zero fixed points. What this means for $f(x)$ is that m can only have a similar form to those of the monomial involutions if it has at least two non-zero fixed points—by Proposition 4.15, the number of non-zero fixed points of involutions $f(x)$ is always even. Since our approach was to expand the work done on monomial involutions in [2] to involutions $f(x)$ of $\mathbb{F}_q$, then we focused on finding formulas for m such that $f(x)$ is an involution with more than one fixed point.

We used Algorithm 2 to generate all involutions up to $q \leq 1399$ and partitioned them by the number of non-zero fixed points. Then we used the same approach as Pacheco-Tallaj in [10] and graphed m as a function of q for a fixed number of fixed points.



(a) (b)

Figure 4.27.1: Graphs(a) and (b) show m as a function of q where $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution with 3 and 5 fixed points, respectively, for some $a \in \mathbb{F}_q{}^*$.



(c) (d)

Figure 4.27.2: Graphs (c) and (d) show m as a function of q where $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution with 7 and 9 fixed points, respectively, for some $a \in \mathbb{F}_q{}^*$.

These graphs show that indeed, for each number of fixed points, there is a linear relationship between the exponent m and the size of the field q. In fact, they tell us more than that. Note that Graph (a) in Figure 4.27.1 has exactly two lines with seemingly no gaps. This implies that for a fixed q, there are at most two involutions with exactly 3 fixed points. Similarly, there are at most four involutions with 5 fixed points. From Graphs (a) and (b) one could conjecture that the maximum number of involutions for a fixed q is one less than the number of fixed points. But, in Figure 4.27.2, Graph (c) shows that there are at most

four involutions with 7 fixed points, not six. Graph (d) is similar in that it has 6 lines, but we are graphing involutions that have exactly 9 fixed points. One of the questions we will answer in Section 4.3 is what an upper bound on the number of m's that produce involutions for a fixed q is.

Another observation from Figures 4.27.1 and 4.27.2 is that there are gaps in some lines. Although Graph (a) seemingly has no gaps, Graphs (c) and (d) have many. Here it is easier to see what we mean by an upper bound on the number of involutions. Looking at Graph (c), for example, there is an odd power of a prime near 800 that has only two involutions with exactly 7 fixed points. These gaps may be due to the fact that involutions $f(x)$ and their fixed points depend on a. Hence, as we mentioned in Section 4.1, some m's might be solutions of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$, but there might not exist an a that satisfies the conditions necessary for $f(x)$ to be an involution. Later in this section we will see that these gaps also happen because the maximum number of involutions for a fixed q is related to its 2-valuation.

Going back to our initial observation from Figures 4.27.1 and 4.27.2, since m and q have a linear relationship, we would like to know what the slopes of the lines are on each graph. To study their form more closely, in the following example we make a table with the values of m for $q \leq 53$ where $f(x)$ is an involution with exactly 5 fixed points.

Example 4.28. We use Algorithm 2 and Theorem 3.13 to find involutions for $q \leq 53$ that have exactly 5 fixed points and we list all such involutions in the table below. Since we are interested in the relationship between q and m we do not list a.

q	$m = \left(\frac{q-1}{4}\right) k-1$
13	$5 = \left(\frac{12}{4}\right) 2-1$
17	$3 = \left(\frac{16}{4}\right) 1-1$
	$7 = \left(\frac{16}{4}\right) 2-1$
	$11 = \left(\frac{16}{4}\right) 3-1$
	$15 = \left(\frac{16}{4}\right) 4-1$
25	$11 = \left(\frac{24}{4}\right) 2-1$
	$23 = \left(\frac{24}{4}\right) 4-1$
29	$13 = \left(\frac{28}{4}\right) 2-1$
	$27 = \left(\frac{28}{4}\right) 4-1$
37	$17 = \left(\frac{36}{4}\right) 2-1$

q	$m = \left(\frac{q-1}{4}\right) k-1$
41	$19 = \left(\frac{40}{4}\right) 2-1$
	$29 = \left(\frac{40}{4}\right) 3-1$
	$39 = \left(\frac{40}{4}\right) 4-1$
49	$11 = \left(\frac{48}{4}\right) 1-1$
	$23 = \left(\frac{48}{4}\right) 2-1$
	$35 = \left(\frac{48}{4}\right) 3-1$
	$47 = \left(\frac{48}{4}\right) 4-1$
53	$25 = \left(\frac{52}{4}\right) 2-1$
	$51 = \left(\frac{52}{4}\right) 4-1$

Table 4.28.1: All values of $q \leq 53$ and m such that $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution with 5 fixed points for some $a \in \mathbb{F}_q{}^*$. Note that m is written as $\left(\frac{q-1}{4}\right) k - 1$, where $k \in \{1, 2, 3, 4\}$

From Graph (b) in Figure 4.27.1 it is clear that there are at most 4 possible m's for involutions with 5 fixed points for $q \leq 1399$. However, there are also cases where a fixed q does not generate four, three, two or even one m. Note that in Table 4.28.1: 13 has one m, 25 has two, 41 has three, and 49 has four. But there are also powers of primes that are not listed here and are in the range $3 \leq q \leq 53$, such as 19, that is, $\mathbb{F}_{19}$ does not have involutions with exactly 5 fixed points. These are the gaps that we see on the lines on Graph (b).

$\diamond$

From Table 4.28.1, note that there are four possibilities for k: $1, 2, 3$ and 4. We are interested in knowing if these k's correspond to the slopes of the lines on Graph (b) of Figure 4.27.1. The colors the following graph in Figure 4.28.1 represent the values of $k \in \{1, 2, 3, 4\}$.

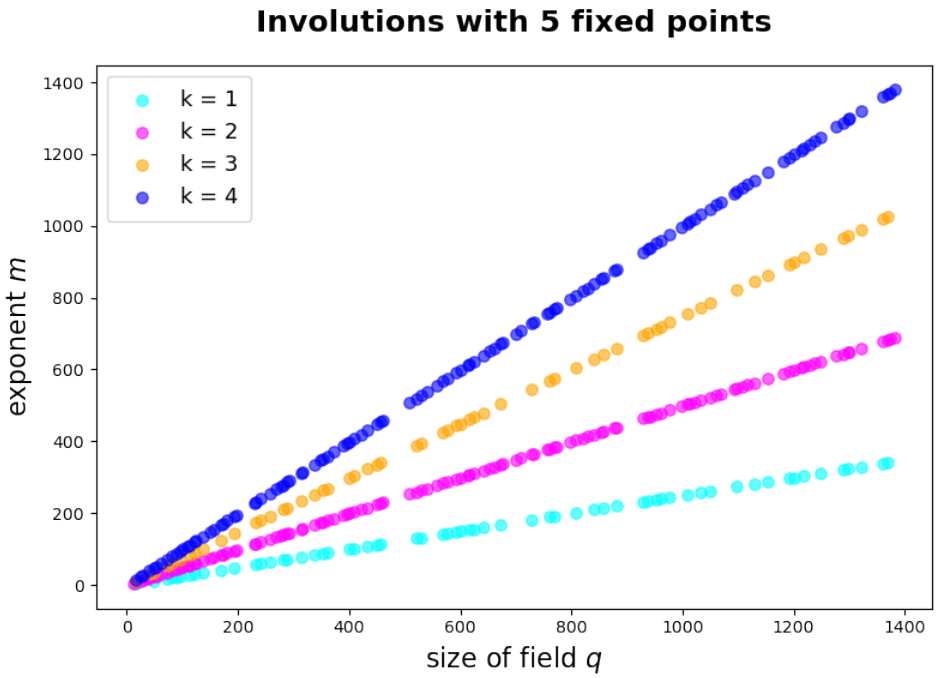
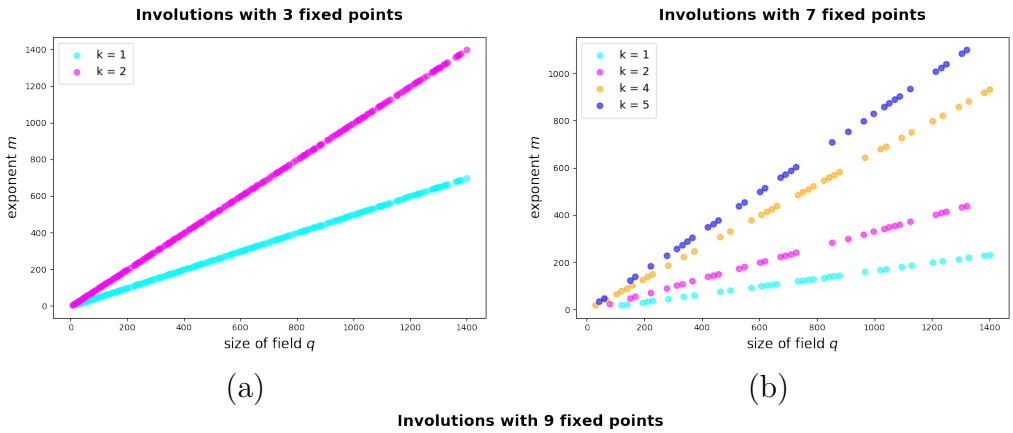
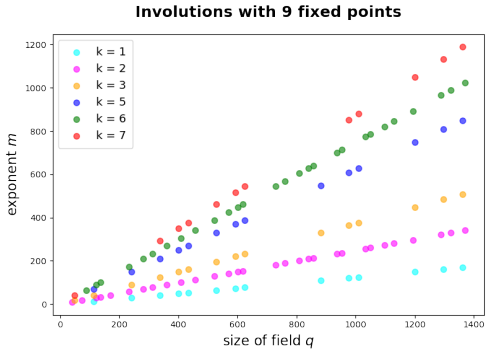


Figure 4.28.1: Graph of m as a function of q where $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with 5 fixed points for $q \leq 1399$ and some $a \in \mathbb{F}_q{}^*$. We color each involution by $k \in \{1, 2, 3, 4\}$ where $m \equiv \left(\frac{q-1}{4}\right) k - 1 \pmod{q-1}$.

Table 4.28.1 tells us that $m \equiv \left(\frac{q-1}{4}\right) k - 1 \pmod{q-1}$ where 4 is the number of non-zero fixed points and $k \in \mathbb{Z}$. Figure 4.28.1 suggests that writing m in this way is beneficial since each value of k corresponds to a different involution for a fixed q. Then by knowing the possible values of k, we can determine the maximum possible number of involutions for a fixed q. In the following figure we illustrate that the same is true for involutions with exactly 3, 7, and 9 fixed points.



(a) (b)



(c)

Figure 4.28.2: Graphs (a), (b), and (c) display m as a function of q, where $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with 3, 7, and 9 fixed points respectively, for $q \leq 1399$ and some $a \in \mathbb{F}_q{}^*$. We color each involution by k where $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$ and d is the number of non-zero fixed points.

Note that for involutions with 7 and 9 fixed points the values of k are not always consecutive as in the case of 5 fixed points.

After generating all involutions for $q \leq 1399$, we noted that, similar to monomials, $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$ where d is the number of non-zero fixed points and k corresponds to the slopes of the lines illustrated in Figures 4.28.1 and 4.28.2.

The goal for this section is to prove that $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$ is necessary and sufficient for $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. We start by proving that $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$ is sufficient for $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$, then we find explicit formulas for k. After this, we show that $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$ is also necessary for $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ by using a counting argument.

It is important to note that the results in this section are not tied to the number

of fixed points, this is done in Section 4.4. In this section, d is a divisor of $q-1$.

Lemma 4.29. If $d \mid (q-1)$, $m \equiv 1 \pmod{\frac{d}{2}}$ and $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$ for some $k \in \mathbb{Z}$, then $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$.

Proof. Note that $m+1 \equiv \left(\frac{q-1}{d}\right) k \pmod{\frac{q-1}{2}}$. Also, $m-1 \equiv 0 \pmod{\frac{d}{2}}$ if and only if $m-1 = \left(\frac{d}{2}\right) \ell$ for some $\ell \in \mathbb{Z}$. Therefore,

$$m^2 - 1 = (m+1)(m-1) \equiv \left(\frac{q-1}{d}\right) k \left(\frac{d}{2}\right) \ell \equiv \left(\frac{q-1}{2}\right) k\, \ell \equiv 0 \pmod{\frac{q-1}{2}}.$$

□

Lemma 4.30 provides the first formula for m and Lemma 4.31 provides us with the second formula for m.

Lemma 4.30. Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, and $d = 2^f p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$, $e \geq 1$, where $f \in \{1, e\}$ and $\ell_s \in \{0, e_s\}$. If $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$ where

$$k = 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\},$$

then $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and $\frac{d}{2} \mid (m-1)$.

Proof. By Lemma 4.29, it is sufficient to prove that $m \equiv 1 \pmod{\frac{d}{2}}$. Note that

$$\begin{aligned}\left(\frac{q-1}{d}\right) k - 1 &= \left(\frac{q-1}{d}\right)\left[2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t\right] - 1 \\ &= 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)} + t\left(\frac{q-1}{d}\right) - 1.\end{aligned}$$

Since $\gcd(\frac{d}{2}, \frac{q-1}{d}) = 1$, then by Euler's Theorem,

$$m \equiv 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)} + t\left(\frac{q-1}{d}\right) - 1 \equiv 2 - 1 \equiv 1 \pmod{\frac{d}{2}}.$$

□

Lemma 4.31. Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, and $d = 2^f p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$, where $e \geq 3$, $f \in \{2, e-1\}$ and $\ell_s \in \{0, e_s\}$. If $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$ where

$$k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t, \; t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\}$$

is reduced modulo d, then $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and $\frac{d}{2} \mid (m-1)$.

Proof. By Lemma 4.29, it is sufficient to show that $m \equiv 1 \pmod{\frac{d}{2}}$. Let $k_j = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + (j-1)\left(\frac{d}{4}\right)$ for $j = 1, 2, 3, 4$. Note that

$$\begin{aligned}\left(\frac{q-1}{d}\right) k_j - 1 &= \left(\frac{q-1}{d}\right)\left[\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + (j-1)\left(\frac{d}{4}\right)\right] - 1 \\ &= 2\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} + (j-1)\left(\frac{q-1}{4}\right) - 1.\end{aligned}$$

Also note that $\gcd\left(\frac{d}{4}, \frac{q-1}{2d}\right) = 1$, then by Euler's Theorem,

$$m \equiv 2 + (j-1)\left(\frac{q-1}{4}\right) - 1 \equiv 1 \pmod{\frac{d}{4}},$$

since $\frac{d}{4} \,\Big|\, \frac{q-1}{4}$. Lastly, since $\frac{d}{4} \,\Big|\, \frac{d}{2}$, then $m \equiv 1 \pmod{\frac{d}{2}}$.

□

Now that we have proved that the formulas for m and k are sufficient for m to be a solution of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$, we start a counting argument that helps us prove that the formulas are also necessary. More specifically, we use this counting to prove that these constructions are all the possibilities for m since they account for all the solutions of $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ that produce distinct involutions.

As we mentioned in Section 4.1, the m's that produce distinct involutions with more than one fixed point are solutions m of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$ that are in the range $1 \leq m < q-1$. We also talked about how, for every m in range $1 \leq m < \frac{q-1}{2}$ that is a solutions of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$, $m + \frac{q-1}{2}$ is also a solution of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and $\frac{q-1}{2} \leq m + \frac{q-1}{2} < q-1$. This implies that the number of distinct m's that produce involutions $f(x)$ of $\mathbb{F}_q$ with more than one fixed point

is twice the amount of the incongruent solutions of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$. Since Corollary 2.29 tells us the number of solutions of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$, then the number of m's that produce involutions with more than one fixed point is

$$\begin{cases} 2^{r+1} & \text{if } e = 1, 2, \\ 2^{r+2} & \text{if } e = 3, \\ 2^{r+3} & \text{if } e \geq 4, \end{cases}$$

We have proved the following proposition.

Proposition 4.32. Let q be odd and m be a positive integer. Then the number of m's that are solutions of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and are incongruent modulo $q-1$ is

$$\begin{cases} 2^{r+1} & \text{if } e = 1, 2, \\ 2^{r+2} & \text{if } e = 3, \\ 2^{r+3} & \text{if } e \geq 4. \end{cases}$$

Moreover, this is the maximum number of m's that produce distinct involutions of $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ of $\mathbb{F}_q$, where $a \in {\mathbb{F}_q}^*$.

We now count the number of distinct m's that we can construct using Lemmas 4.30 and 4.31. We claim that this number is the same as the number of possible m's that produce distinct involutions with more than one fixed point. Before we start counting, consider the following example.

Example 4.33. Let $q = 97$. Then $q - 1 = 2^5 \cdot 3$. Using Lemmas 4.30 and 4.31, we can construct the following m's.

$\underline{\boldsymbol{e=5}}$

		m				
f	d	$t=$	0	$\frac{d}{4}$	$\frac{d}{2}$	$\frac{3d}{4}$
1	2		95		47		1
	6		31		79		2
5	32		65		17		3
	96		1		49		4
2	4		23	47	71	95	5
	12		31	55	79	7	6
4	16		17	41	65	89	7
	48		1	25	49	73	8

Table 4.33.1: Values of m constructed using Lemmas 4.30 and 4.31.

Note that there are repetitions for some values of d. For example, when $d = 2$, using Lemma 4.30 with $t = 0$, and when $d = 4$ using Lemma 4.31 with $t = \frac{3d}{4}$, $m = 95$. Also note that for each m that is repeated, the values of d that generate them are multiples of each other.

$\diamond$

4.3.1 Formulas for Solutions m to $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$ of the Form $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$

Note that in Lemma 4.30, for a fixed $f = \nu_2(d)$, two formulas for m are given and, when you subtract them, the difference is the term $\left(\frac{q-1}{d}\right)\left(\frac{d}{2}\right) = \frac{q-1}{2}$. Since $m \not\equiv m + \frac{q-1}{2} \pmod{q-1}$, these m's produce distinct involutions by Lemma 4.4. Similarly, in Lemma 4.31, for a fixed q and f, the difference between the formulas for m are multiples of $\frac{q-1}{4}$ that are strictly less than $q-1$, therefore they are incongruent modulo $q-1$.

Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $d_i = 2^{f_i} p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$, where $\ell_s \in \{0, e_s\}$, and $m_{ij} \equiv$

$\left(\frac{q-1}{d_i}\right) k_j - 1 \pmod{q-1}$, where

$$k_j = \begin{cases} 2\left(\dfrac{q-1}{d_i}\right)^{\phi\left(\frac{d_i}{2}\right)-1} + (j-1)\left(\dfrac{d_i}{2}\right) & \text{for } i,j = 1,2, \\ \left(\dfrac{q-1}{2d_i}\right)^{\phi\left(\frac{d_i}{4}\right)-1} + (j-1)\left(\dfrac{d_i}{4}\right) & \text{for } i = 3,4 \text{ and } j = 1,2,3,4, \end{cases}$$

and $f_1 = 1$, $f_2 = e$, $f_3 = 2$, $f_4 = e-1$. We use the notation m_{ij} for the counting argument which we divide by cases for $e = \nu_2(q-1)$.

Note that we can simplify m_{ij}. For $i,j = 1,2$, we have

$$\begin{aligned} m_{ij} &\equiv \left(\frac{q-1}{d_i}\right)\left[2\left(\frac{q-1}{d_i}\right)^{\phi\left(\frac{d_i}{2}\right)-1} + (j-1)\left(\frac{d_i}{2}\right)\right] - 1 \pmod{q-1} \\ &\equiv 2\left(\frac{q-1}{d_i}\right)^{\phi\left(\frac{d_i}{2}\right)} + (j-1)\left(\frac{q-1}{2}\right) - 1 \pmod{q-1}. \end{aligned}$$

Similarly, for $i = 3,4$ and $j = 1,2,3,4$, we have

$$\begin{aligned} m_{ij} &\equiv \left(\frac{q-1}{d_i}\right)\left[\left(\frac{q-1}{2d_i}\right)^{\phi\left(\frac{d_i}{4}\right)-1} + (j-1)\left(\frac{d_i}{4}\right)\right] - 1 \pmod{q-1} \\ &\equiv 2\left(\frac{q-1}{2d_i}\right)^{\phi\left(\frac{d_i}{4}\right)} + (j-1)\left(\frac{q-1}{4}\right) - 1 \pmod{q-1}. \end{aligned}$$

⋆ Case $e = 1$

Note that, from Lemmas 4.30 and 4.31, the only option for $f = \nu_2(d)$ is in Lemma 4.30 with $f = 1 = e$. Then for a fixed d with $f = 1$, we can construct two distinct m's. To count how many d's we can choose with $f = 1$, note that d has a special form where for each odd prime p that divides d, $\nu_p(d) = \nu_p(q-1)$. Since $q-1$ has r distinct odd prime divisors, then there are 2^r possibilities for d, each of which give 2 distinct m's, then there are $2 \cdot 2^r = 2^{r+1}$ distinct m's when $e = 1$.

⋆ Case $e = 2$

Lemma 4.30 states that we have two ways to choose $\nu_2(d)$: $f = 1$ or $f = e = 2$. We will prove in Proposition 4.35 that $\nu_2(d_1) = f_1 = 1$ and $d_2 = 2d_1$, that is $\nu_2(d_2) = f_2 = 2$, give the same two values of m's modulo $q - 1$.

Lemma 4.34. Let $a \equiv b \pmod{n}$. If $\nu_2(a-b) = \nu_2(n) + s$, then $a \equiv b + 2^s n \pmod{2^{s+1}n}$.

Proof. For some $k \in \mathbb{Z}$, we have $nk = a - b$. Then $\nu_2(a-b) = \nu_2(nk) = \nu_2(n) + \nu_2(k)$, by Proposition 2.22. By hypothesis, $\nu_2(k) = s$, then $k = 2^s(2t+1)$, for some $t \in \mathbb{Z}$. Therefore,

$$a - b = n2^s(2t+1) = 2^{s+1}nt + 2^s n \iff a \equiv b + 2^s \pmod{2^{s+1}n}.$$

□

Let $d_1 = 2p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$ and $d_2 = 2^2p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$. Then

$$m_{11} = 2\left(\frac{q-1}{d_1}\right)^{\phi\left(\frac{d_1}{2}\right)} - 1 \quad \text{and} \quad m_{22} = 2\left(\frac{q-1}{d_2}\right)^{\phi\left(\frac{d_2}{2}\right)} + \frac{q-1}{2} - 1.$$

We claim that $m_{11} \equiv m_{22} \pmod{q-1}$. Note that this also implies that $m_{12} \equiv m_{21} \pmod{q-1}$, since $m_{11} + \frac{q-1}{2} \equiv m_{12} \pmod{q-1}$ and $m_{22} + \frac{q-1}{2} \equiv m_{21} \pmod{q-1}$.

Proposition 4.35. Let $q-1 = 2^2p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, $d_1 = 2p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$ and $d_2 = 2d_1$, where $\ell_s \in \{0, e_s\}$. Then $m_{11} \equiv m_{22} \pmod{q-1}$ where

$$m_{11} = 2\left(\frac{q-1}{d_1}\right)^{\phi\left(\frac{d_1}{2}\right)} - 1 \quad \text{and} \quad m_{22} = 2\left(\frac{q-1}{d_2}\right)^{\phi\left(\frac{d_2}{2}\right)} + \frac{q-1}{2} - 1.$$

Proof. Consider $m_{21} = 2\left(\frac{q-1}{d_2}\right)^{\phi\left(\frac{d_2}{2}\right)} - 1$. We claim that $m_{11} \equiv m_{21} \pmod{\frac{q-1}{4}}$.

Since $2\left(\frac{q-1}{d_2}\right) = \frac{q-1}{d_1}$, we can write $m_{11} = 2^{1+\phi\left(\frac{d_1}{2}\right)}\left(\frac{q-1}{d_2}\right)^{\phi\left(\frac{d_1}{2}\right)} - 1$. Then $m_{11} \equiv -1 \equiv m_{21} \pmod{\frac{q-1}{d_2}}$. Now, note that $d_1 = 2\frac{d_1}{2} = \frac{d_2}{2}$. Since $\gcd\left(2, \frac{d_1}{2}\right) =$

1, then $\phi(d_1) = \phi(2)\phi\left(\frac{d_1}{2}\right) = \phi\left(\frac{d_2}{2}\right)$ by Proposition 2.20. But $\phi(2) = 1$, therefore, $\phi\left(\frac{d_1}{2}\right) = \phi\left(\frac{d_2}{2}\right)$ and $m_{21} = 2\left(\frac{q-1}{d_2}\right)^{\phi\left(\frac{d_1}{2}\right)} - 1$. Since $\gcd\left(\frac{q-1}{d_1}, \frac{d_1}{2}\right) = 1$ and $\gcd\left(\frac{q-1}{d_2}, \frac{d_1}{2}\right) = 1$, then, by Euler's Theorem, $m_{11} \equiv 1 \equiv m_{21} \pmod{\frac{d_1}{2}}$. Now, by Theorem 2.26, m_{11} is congruent to m_{21} modulo the least common multiple of $\frac{q-1}{d_2}$ and $\frac{d_1}{2}$, that is $m_{11} \equiv m_{21} \pmod{\frac{q-1}{4}}$. Note that

$$\nu_2(m_{11} - m_{21}) = \nu_2\left(2\left[\left(\frac{q-1}{d_1}\right)^{\phi\left(\frac{d_1}{2}\right)} - \left(\frac{q-1}{d_2}\right)^{\phi\left(\frac{d_2}{2}\right)}\right]\right) = 1,$$

since $\frac{q-1}{d_1}$ is even and $\frac{q-1}{d_2}$ is odd. But $\nu_2\left(\frac{q-1}{4}\right) = 0$, therefore $1 = \nu_2(m_{11} - m_{21}) = \nu_2\left(\frac{q-1}{4}\right) + 1$ and, by Lemma 4.34, $m_{11} \equiv m_{21} + 2\left(\frac{q-1}{4}\right) \pmod{2^2\left(\frac{q-1}{2}\right)}$. That is, $m_{11} \equiv m_{22} \pmod{q-1}$.

□

Using Lemma 4.30 to construct m, although we have two options for the 2-valuation f of d, Proposition 4.35 tells us that we can only construct two distinct m's. Similar to the case $e = 1$, when $e = 2$, the number of possible d's that we can choose in this way are 2^r and since for each d we can construct 2 distinct m's, then there are a total of $2 \cdot 2^r = 2^{r+1}$ m's that are solutions to $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$.

⋆ Case $e = 3$

Using Lemma 4.30, again we have two ways to choose d: $f = 1$ or $f = e = 3$. Let $d_1 = 2p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$ and $d_2 = 2^3p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$. We claim that $m_{1j} \not\equiv m_{2j'}$ for $j \neq j'$. It is sufficient to prove that $m_{11} \not\equiv m_{2j} \pmod{q-1}$, $j \in \{1, 2\}$. For $j \in \{1, 2\}$, let

$$m_{11} = 2\left(\frac{q-1}{d_1}\right)^{\phi\left(\frac{d_1}{2}\right)} - 1 \quad \text{and} \quad m_{2j} = 2\left(\frac{q-1}{d_2}\right)^{\phi\left(\frac{d_2}{2}\right)} + (j-1)\left(\frac{q-1}{2}\right) - 1.$$

Note that

$$\nu_2(m_{11} - m_{2j}) = \nu_2\left(2\left[\left(\frac{q-1}{d_1}\right)^{\phi\left(\frac{d_1}{2}\right)} - \left(\frac{q-1}{d_2}\right)^{\phi\left(\frac{d_2}{2}\right)} - (j-1)\left(\frac{q-1}{4}\right)\right]\right) = 1,$$

since $\frac{q-1}{d_1}$ and $\frac{q-1}{4}$ are even and $\frac{q-1}{d_2}$ is odd. But $\nu_2(q-1)=3$, therefore $(q-1)\nmid (m_{11}-m_{2j})$, that is, $m_{11}\not\equiv m_{2j} \pmod{q-1}$, for $j=1,2$. Therefore when $e=3$, all m's constructed with pairs d_1, $d_2=2^2\,d_1$, $f_1=\nu_2(d_1)=1$ are distinct.

These are not the only m's we can construct with $e=3$, we can also use Lemma 4.31 and choose d with $f=e-1=2$. Let $d_3=2^2p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$. Note that

$$m_{31}=\left(\frac{q-1}{d_3}\right)\left[2\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)-1}\right]-1=2\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)}-1.$$

We claim that m's constructed with d_3 are the same as those constructed with d_1 and d_2. First we prove that $m_{31}\equiv m_{21} \pmod{q-1}$ or $m_{31}\equiv m_{22} \pmod{q-1}$.

Proposition 4.36. Let $q-1=2^3p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, $d_3=2^2p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$ and $d_2=2d_3$, where $\ell_s\in\{0,e_s\}$. Then $m_{31}\equiv m_{21} \pmod{q-1}$ or $m_{31}\equiv m_{21}+\frac{q-1}{2} \pmod{q-1}$ where

$$m_{31}=2\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)}-1 \quad \text{and} \quad m_{21}=2\left(\frac{q-1}{d_2}\right)^{\phi\left(\frac{d_2}{2}\right)}-1.$$

Proof. Since $\frac{q-1}{2d_3}=\frac{q-1}{d_2}$, then $m_{31}\equiv m_{21}\ \left(\mathrm{mod}\ \frac{q-1}{2d_3}\right)$. Note that $\frac{d_2}{2}=d_3=4\cdot\frac{d_3}{4}$. Since $\gcd\left(4,\frac{d_3}{4}\right)=1$, then by Proposition 2.20, $\phi\left(\frac{d_2}{2}\right)=\phi(4)\phi\left(\frac{d_3}{4}\right)$. Now, since $\phi(4)=2$ and $d_2=2d_3$, we can write $m_{21}=2\left(\frac{q-1}{2d_3}\right)^{2\phi\left(\frac{d_3}{4}\right)}-1$. Since $\gcd\left(\frac{q-1}{2d_3},\frac{d_3}{4}\right)=1$, this implies that $m_{31}\equiv -1\equiv m_{21}\left(\mathrm{mod}\ \frac{d_3}{4}\right)$. Then, by Theorem 2.26, $m_{31}\equiv m_{21}\left(\mathrm{mod}\ \frac{q-1}{8}\right)$ since $\mathrm{lcm}\left(\frac{q-1}{2d_3},\frac{d_3}{4}\right)=\frac{q-1}{8}$. Note that $\nu_2\left(\frac{q-1}{8}\right)=0$ and, in Lemma 4.34,

$$\begin{aligned}
s&=\nu_2(m_{31}-m_{21})\\
&=\nu_2\left(2\left[\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)}-\left(\frac{q-1}{2d_3}\right)^{2\phi\left(\frac{d_3}{4}\right)}\right]\right)\\
&=\nu_2\left(2\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)}\left[1-\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)}\right]\right)\\
&\geq 2,
\end{aligned}$$

since $\frac{q-1}{2d_3}$ is odd. Then by Lemma 4.34, $m_{31} \equiv m_{21} + 2^s \left(\frac{q-1}{8}\right) \pmod{2^{s+1}\left(\frac{q-1}{8}\right)}$, for $s \geq 2$. If $s = \nu_2(m_{31} - m_{21}) = 2$, then $m_{31} \equiv m_{21} + \frac{q-1}{2} \pmod{q-1}$. If $s > 2$, then $m_{31} \equiv m_{21} \pmod{q-1}$.

□

We have just proved that $m_{31} \equiv m_{21} \pmod{q-1}$ or $m_{31} \equiv m_{22} \pmod{q-1}$. This implies that $m_{33} \equiv m_{31} + \frac{q-1}{2} \equiv m_{22} \pmod{q-1}$ or $m_{33} \equiv m_{21} \pmod{q-1}$ respectively.

Note that $m_{31} + \frac{q-1}{4} \equiv m_{32} \pmod{q-1}$. Now we claim that $m_{32} \equiv m_{11} \pmod{q-1}$ or $m_{32} \equiv m_{12} \pmod{q-1}$.

Proposition 4.37. Let $q-1 = 2^3 p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $d_3 = 2^2 p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ and $d_1 = \frac{d_3}{2}$, where $\ell_s \in \{0, e_s\}$. Then $m_{32} \equiv m_{11} \pmod{q-1}$ or $m_{32} \equiv m_{11} + \frac{q-1}{2} \pmod{q-1}$ where

$$m_{32} = 2\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)} + \frac{q-1}{4} - 1 \quad \text{and} \quad m_{11} = 2\left(\frac{q-1}{d_1}\right)^{\phi\left(\frac{d_1}{2}\right)} - 1.$$

Proof. Since $2\left(\frac{q-1}{d_3}\right) = \frac{q-1}{d_1}$, we can write $m_{11} = 2^{2+\phi\left(\frac{d_1}{2}\right)}\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_1}{2}\right)} - 1$. Also, note that $\frac{q-1}{4} = \left(\frac{q-1}{2d_3}\right)\left(\frac{d_3}{2}\right)$, hence $m_{32} = 2\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)} + \left(\frac{q-1}{2d_3}\right)\left(\frac{d_3}{2}\right) - 1$. This implies that $m_{32} \equiv -1 \equiv m_{11} \left(\mod \frac{q-1}{2d_3}\right)$. Now, since $\frac{d_3}{4} = \frac{d_1}{2}$, $\phi\left(\frac{d_3}{4}\right) = \phi\left(\frac{d_1}{2}\right)$ and $m_{11} = 2\left(\frac{q-1}{d_1}\right)^{\phi\left(\frac{d_3}{4}\right)} - 1$. Also, $\frac{q-1}{4} = \left(\frac{q-1}{d_3}\right)\left(\frac{d_3}{4}\right)$, hence we can write $m_{32} = 2\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)} + \left(\frac{q-1}{d_3}\right)\left(\frac{d_3}{4}\right) - 1$. Since $\gcd\left(\frac{q-1}{d_1}, \frac{d_3}{4}\right) = 1$, this implies that $m_{32} \equiv 1 \equiv m_{11} \left(\mod \frac{d_3}{4}\right)$. Since $\operatorname{lcm}\left(\frac{q-1}{2d_3}, \frac{d_3}{4}\right) = \frac{q-1}{8}$, $m_{32} \equiv m_{11} \left(\mod \frac{q-1}{8}\right)$ by Theorem 2.26.

Lastly, note that $\nu_2\left(\frac{q-1}{8}\right) = 0$ and, in Lemma 4.34,

$$\begin{aligned} s &= \nu_2(m_{32} - m_{11}) \\ &= \nu_2\left(2\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)} - 2\left(\frac{q-1}{d_1}\right)^{\phi\left(\frac{d_1}{2}\right)} + \frac{q-1}{4}\right) \\ &= \nu_2\left(2\left[\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)} - \left(\frac{q-1}{d_1}\right)^{\phi\left(\frac{d_1}{2}\right)} + \frac{q-1}{8}\right]\right) \\ &\geq 2, \end{aligned}$$

since $\frac{q-1}{2d_3}$ and $\frac{q-1}{8}$ are odd and $\frac{q-1}{d_1}$ is even. Then, by Lemma 4.34, $m_{32} \equiv m_{11} + 2^s\left(\frac{q-1}{8}\right) \pmod{2^{s+1}\left(\frac{q-1}{8}\right)}$, for $s \geq 2$. If $s = \nu_2(m-m') = 2$, then $m_{32} \equiv m_{11} + \frac{q-1}{2} \pmod{q-1}$. If $s > 2$, then $m_{32} \equiv m_{11} \pmod{q-1}$.

□

We have proved that when $e = 3$, $m_{32} \equiv m_{11} \pmod{q-1}$ or $m_{32} \equiv m_{12} \pmod{q-1}$. Note that this implies that m_{34} is also congruent to either m_{12} or m_{11} modulo $q-1$, since $m_{34} \equiv m_{32} + \frac{q-1}{2} \pmod{q-1}$.

Now, to recap, when $e = 3$, for a fixed odd prime product of d, choosing $f = 1$ or $f = e = 3$ produces four distinct values for m: two with $f = 1$ and two with $f = 3$. However, choosing $f = e - 1 = 2$ produces the same four m's as those produced with $f = 1$ and $f = 3$.

Similar to the previous cases, there are 2^r ways of constructing the odd prime products for d, and, for each, there are four distinct values of m produced by the possible values of f. Therefore, there are a total of $2^2 \cdot 2^r = 2^{r+2}$ solutions m of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$.

⋆ Case $e \geq 4$

We have various ways to construct m. We can use Lemma 4.30 and construct d with $f = 1$ or $f = e$, and we can use Lemma 4.31 and construct d with $f = 2$ or $f = e - 1$.

Let $d_1 = 2p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$, $d_2 = 2^e p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$, $d_3 = 2^2 p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$ and $d_4 = 2^{e-1}p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$.

Similar to the previous cases, we focus on building m's for a fixed d_1, such that $2^{e-1}d_1 = 2^{e-2}d_3 = 2\,d_4 = d_2$ to count the incongruent m's modulo $q-1$, and then we count how many d's we can construct in this way.

First we prove that d_1 and d_2 produce distinct m's. It is sufficient to prove that $m_{11} \not\equiv m_{2j} \pmod{q-1}$ for $j = 1, 2$.

Note that

$$\begin{aligned}
\nu_2(m_{11} - m_{2j}) &= \nu_2\left(2\left(\frac{q-1}{d_1}\right)^{\phi\left(\frac{d_1}{2}\right)} - 2\left(\frac{q-1}{d_2}\right)^{\phi\left(\frac{d_2}{2}\right)} + (j-1)\left(\frac{q-1}{2}\right)\right) \\
&= \nu_2\left(2\left[\left(\frac{q-1}{d_1}\right)^{\phi\left(\frac{d_1}{2}\right)} - \left(\frac{q-1}{d_2}\right)^{\phi\left(\frac{d_2}{2}\right)} + (j-1)\left(\frac{q-1}{4}\right)\right]\right) \\
&= 1,
\end{aligned}$$

since $\frac{q-1}{d_1}$ and $\frac{q-1}{4}$ are even and $\frac{q-1}{d_2}$ is odd. But $\nu_2(q-1) = e > 1$, therefore $(q-1) \nmid (m_{11} - m_{2j})$ for $j = 1, 2$. We have proved that m's constructed with Lemma 4.30 are distinct when $e \geq 4$.

Now we claim that the m's constructed with Lemma 4.31 are also distinct when $e \geq 4$. Recall that $d_3 = 2^2 p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$ and $d_4 = 2^{e-1}p_1^{\ell_1}p_2^{\ell_2}\cdots p_r^{\ell_r}$. Note that for $j = 1, 2, 3, 4$

$$\begin{aligned}
\nu_2(m_{31} - m_{4j}) &= \nu_2\left(2\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)} - 2\left(\frac{q-1}{2d_4}\right)^{\phi\left(\frac{d_4}{4}\right)} - (j-1)\left(\frac{q-1}{4}\right)\right) \\
&= \nu_2\left(2\left[\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)} - \left(\frac{q-1}{2d_4}\right)^{\phi\left(\frac{d_4}{2}\right)} - (j-1)\left(\frac{q-1}{8}\right)\right]\right) \\
&= 1 < e,
\end{aligned}$$

since $\frac{q-1}{2d_3}$ and $\frac{q-1}{8}$ are even and $\frac{q-1}{2d_4}$ is odd. Therefore $m_{31} \not\equiv m_{4j} \pmod{q-1}$ for $j = 1, 2, 3, 4$.

We now need to check if there are repeated m's between those constructed

with Lemma 4.30 and those constructed with Lemma 4.31. Note that for a fixed d, Lemma 4.30 provides two values for m and Lemma 4.31 provides four values for m.

We start by constructing m using Lemma 4.30 with d_1 and using Lemma 4.31 with d_3. We claim that $m_{11} \equiv m_{3j} \pmod{q-1}$ for some $j = 1, 2, 3, 4$. Note that this implies that $m_{12} \equiv m_{3j} + \frac{q-1}{2} \equiv m_{3(j+2)} \pmod{q-1}$.

Proposition 4.38. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, e \geq 4$, $d_1 = 2p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ and $d_3 = 2d_1$, where $\ell_s \in \{0, e_s\}$. Then $m_{11} \equiv m_{3j} \pmod{q-1}$ for some $j = 1, 2, 3, 4$, where

$$m_{11} = 2\left(\frac{q-1}{d_1}\right)^{\phi\left(\frac{d_1}{2}\right)} - 1 \quad \text{and} \quad m_{3j} = 2\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)} + (j-1)\left(\frac{q-1}{4}\right) - 1.$$

Proof. Since $2^2 \left(\frac{q-1}{2d_3}\right) = \frac{q-1}{d_1}$, we can write $m_{11} = 2^{1+2\phi\left(\frac{d_1}{2}\right)} \left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_1}{2}\right)} - 1$. This implies that $m_{11} \equiv -1 \equiv m_{3j} \left(\mathrm{mod}\ \frac{q-1}{2d_3}\right)$ since $\frac{q-1}{2d_3} \mid \frac{q-1}{4}$. Now note $\frac{d_1}{2} = \frac{d_3}{4}$, hence $\phi\left(\frac{d_1}{2}\right) = \phi\left(\frac{d_3}{4}\right)$ and, since $\gcd\left(\frac{q-1}{d_1}, \frac{d_3}{4}\right) = 1$ and $\frac{d_3}{4} \mid \frac{q-1}{4}$, $m_{11} \equiv 1 \equiv m_{3j} \left(\mathrm{mod}\ \frac{d_3}{4}\right)$. Then by Theorem 2.26, $m_{11} \equiv m_{3j} \left(\mathrm{mod}\ \frac{q-1}{8}\right)$ since $\mathrm{lcm}\left(\frac{q-1}{2d_3}, \frac{d_3}{4}\right) = \frac{q-1}{8}$. But $\nu_2\left(\frac{q-1}{8}\right) = e - 3$ and, in Lemma 4.34,

$$\begin{aligned} e - 3 + s &= \nu_2(m_{11} - m_{3j}) \\ &= \nu_2\left(2^{1+2\phi\left(\frac{d_1}{2}\right)} \left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)} - 2\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)}\right) \\ &= \nu_2\left(2\left(\frac{q-1}{2d_3}\right)^{\phi\left(\frac{d_3}{4}\right)} \left[2^{2\phi\left(\frac{d_1}{2}\right)} - 1\right] - (j-1)\left(\frac{q-1}{2}\right)\right) \\ &\geq e - 2, \end{aligned}$$

since $\frac{q-1}{2d_3}$ is even. Then by Lemma 4.34, $m_{11} \equiv m_{3j} + 2^s \left(\frac{q-1}{8}\right) \left(\mathrm{mod}\ 2^{s+1}\left(\frac{q-1}{8}\right)\right)$ for $s \geq 1$. Now, if $s = 1$, $m_{11} \equiv m_{3j} + \frac{q-1}{4} \pmod{\frac{q-1}{2}}$ and if $s > 1$, $m_{11} \equiv m_{3j} \pmod{\frac{q-1}{2}}$. Similarly, if $m_{11} \equiv m_{3j} + \frac{q-1}{4} \pmod{\frac{q-1}{2}}$, then, in Lemma 4.34, $s \geq -1$ and either $m_{11} \equiv m_{3j} + \frac{q-1}{4} + \frac{q-1}{2} \equiv m_{3(j+3)} \pmod{q-1}$ or $m_{11} \equiv m_{3j} + \frac{q-1}{4} \equiv m_{3(j+1)} \pmod{q-1}$. Lastly, if $m_{11} \equiv m_{3j} \pmod{\frac{q-1}{2}}$, then either

$m_{11} \equiv m_{3j} + \frac{q-1}{2} \equiv m_{3(j+2)} \pmod{q-1}$ or $m_{11} \equiv m_{3j} \pmod{q-1}$. Both cases imply that $m_{11} \equiv m_{3j} \pmod{q-1}$ for some $j \in \{1,2,3,4\}$.

□

Now we construct m using Lemma 4.30 with d_2 and using Lemma 4.31 with d_4. Recall that $d_2 = 2^e p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ and $d_4 = 2^{e-1} p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$. We claim that $m_{21} \equiv m_{4j} \pmod{q-1}$ for some $j = 1,2,3,4$. Note that this implies that $m_{22} \equiv m_{4j} + \frac{q-1}{2} \equiv m_{4(j+2)} \pmod{q-1}$.

Proposition 4.39. Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, e \geq 4$, $d_2 = 2^e p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ and $d_4 = \frac{d_2}{2}$, where $\ell_s \in \{0, e_s\}$. Then $m_{21} \equiv m_{4j} \pmod{q-1}$ for some $j = 1,2,3,4$, where

$$m_{21} = 2\left(\frac{q-1}{d_2}\right)^{\phi\left(\frac{d_2}{2}\right)} - 1 \quad \text{and} \quad m_{4j} = 2\left(\frac{q-1}{2d_4}\right)^{\phi\left(\frac{d_4}{4}\right)} + (j-1)\left(\frac{q-1}{4}\right) - 1.$$

Proof. Note that $\frac{q-1}{d_2} = \frac{q-1}{2d_4}$, therefore $m_{21} \equiv -1 \equiv m_{4j} \left(\mathrm{mod}\ \frac{q-1}{2d_4}\right)$ since $\frac{q-1}{2d_1} \mid \frac{q-1}{4}$. Now note that $\frac{d_2}{2} = 2^{e-1}\left(\frac{d_2}{2^e}\right)$ and, since $\gcd\left(2^{e-1}, \frac{d_2}{2^e}\right) = 1$, then $\phi\left(\frac{d_2}{2}\right) = \phi(2^{e-1})\phi\left(\frac{d_2}{2^e}\right)$ by Proposition 2.20. Similarly, $\phi\left(\frac{d_4}{4}\right) = \phi(2^{e-3})\phi\left(\frac{d_4}{2^{e-1}}\right)$. By Proposition 2.19, $\phi(2^{e-1}) = 2^{e-2}$ and $\phi(2^{e-3}) = 2^{e-4}$. But $\frac{d_2}{2^e} = \frac{d_4}{2^{e-1}}$, therefore $2^2\phi\left(\frac{d_4}{4}\right) = \phi\left(\frac{d_2}{2}\right)$. Now we have $m_{21} = 2\left(\frac{q-1}{2d_4}\right)^{4\phi\left(\frac{d_4}{4}\right)} - 1$. This implies that $m_{21} \equiv 1 \equiv m_{4j} \left(\mathrm{mod}\ \frac{d_4}{4}\right)$ since $\frac{d_4}{4} \mid \frac{q-1}{4}$ and $\gcd\left(\frac{q-1}{2d_4}, \frac{d_4}{4}\right) = 1$. Theorem 2.26 implies that $m_{21} \equiv m_{4j} \left(\mathrm{mod}\ \frac{q-1}{8}\right)$ since $\mathrm{lcm}\left(\frac{q-1}{2d_4}, \frac{d_4}{4}\right) = \frac{q-1}{8}$.

Suppose $e \geq 4$, $\nu_2\left(\frac{q-2}{8}\right) \geq 1$ and, in Lemma 4.34,

$$\begin{aligned}
\nu_2\left(\frac{q-1}{8}\right) + s &= \nu_2(m_{21} - m_{4j}) \\
&= \nu_2\left(2\left(\frac{q-1}{2d_4}\right)^{4\phi\left(\frac{d_4}{4}\right)} - 2\left(\frac{q-1}{2d_4}\right)^{\phi\left(\frac{d_4}{4}\right)} - (j-1)\left(\frac{q-1}{4}\right)\right) \\
&= \nu_2\left(2\left(\frac{q-1}{2d_4}\right)^{\phi\left(\frac{d_4}{4}\right)}\left[\left(\frac{q-1}{2d_4}\right)^{3\phi\left(\frac{d_4}{4}\right)} - 1\right] - (j-1)\left(\frac{q-1}{4}\right)\right) \\
&\geq 2,
\end{aligned}$$

since $\frac{q-1}{2d_4}$ is odd and $\frac{q-1}{4}$ is even. Then $m_{21} \equiv m_{4j} + 2^s \left(\frac{q-1}{8}\right) \pmod{2^{s+1}\left(\frac{q-1}{8}\right)}$ for $s \geq 1$. If $s = 1$, then $m_{21} \equiv m_{4j} + \frac{q-1}{4} \pmod{\frac{q-1}{2}}$, and if $s > 1$, then $m_{21} \equiv m_{4j} + 2^{s-2}\left(\frac{q-1}{2}\right) \pmod{q-1}$. Note that $m_{4j} + 2^{s-2}\left(\frac{q-1}{2}\right)$ is of the form m_{4j}.

If $m_{21} \equiv m_{4j} + \frac{q-1}{4} \pmod{\frac{q-1}{2}}$, using Lemma 4.34 again, then $m_{21} \equiv m_{4j} + \frac{q-1}{4} + 2^s\left(\frac{q-1}{2}\right) \pmod{q-1}$ for $s \geq 0$. But $m_{4j} + \frac{q-1}{4} + 2^s\left(\frac{q-1}{2}\right)$ is again of the form m_{4j}.

□

To recap the case $e \geq 4$, we have that each d_1 and d_3 produce four distinct m's since the two values of m produced by d_1 are two of the four values produced by d_3, this is proved in Proposition 4.38. Similarly, each d_2 and d_4 produce four distinct m's since the two values of m produced by d_2 are two of the four values produced by d_4, this is proved in Proposition 4.39. These are the only repetitions for this case. Since there are 2^r ways to construct the odd prime products for d, and for each, there are 2^3 distinct values of m, then there are a total of $2^3 \cdot 2^r = 2^{r+3}$ distinct m's that are solutions of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$ when $e \geq 4$.

Therefore, the number of m's that can be constructed using Lemmas 4.30 and 4.31 is

$$\begin{cases} 2^{r+1} & \text{if } e = 1, 2, \\ 2^{r+2} & \text{if } e = 3, \\ 2^{r+3} & \text{if } e \geq 4. \end{cases}$$

By Proposition 4.32, we know that this is exactly the same number of possible m's that are solutions to $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and produce distinct involutions $f(x)$ of $\mathbb{F}_q$. Therefore, we have proved the following theorem.

Theorem 4.40. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, and $d = 2^f p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $1 \leq f \leq e$ and $\ell_s \in \{0, e_s\}$. Then $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ if and only if $m \equiv \left(\frac{q-1}{d}\right) k - 1$

(mod $q-1$) where

$$k = \begin{cases} 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\} & \text{if } f = 1 \text{ or } f = e, \\ \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\} & \text{if } f = 2 \text{ or } f = e-1, \text{ and } e \geq 3, \end{cases}$$

and ϕ is the Euler function.

By Proposition 4.3, we know that for all involutions of $\mathbb{F}_q$ of the form $f(x) = x^m(x^{\frac{q-1}{2}} + a)$, $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. Theorem 4.40 tells us that there are at most six distinct values of m that produce involutions.

Now we show some examples on how to use Theorem 4.40.

Example 4.41. Let $q = 25$. Then $q - 1 = 2^3 \cdot 3$. For $d = 6$, we construct m using Theorem 4.40. Since $f = 1$, then

$$\begin{aligned} k &= 2\left(\frac{24}{6}\right)^{\phi(3)-1} + t, \quad t \in \{0, 3\} \\ &= 2(4) + t \\ &= 8 + t. \end{aligned}$$

Therefore, $k = 8$ for $t = 0$ and $k = 11$ for $t = 3$. Now we substitute these values to construct m and we get

$$\begin{aligned} m_1 &\equiv \left(\frac{24}{6}\right)(8) - 1 \equiv 7 \pmod{24} \quad \text{and} \\ m_2 &\equiv \left(\frac{24}{6}\right)(11) - 1 \equiv 19 \pmod{24}. \end{aligned}$$

◇

Example 4.42. In Example 4.41, we chose $d = 6$, but this is not the only option for d. Now we list all possible m's for $q = 25$, note $q - 1 = 2^3 \cdot 3$.

$\underline{\boldsymbol{e=3}}$

		$\boldsymbol{m}$					
$\boldsymbol{f}$	$\boldsymbol{d}$	$\boldsymbol{t=}$	$\mathbf{0}$	$\frac{\boldsymbol{d}}{\mathbf{4}}$	$\frac{\boldsymbol{d}}{\mathbf{2}}$	$\frac{\mathbf{3}\boldsymbol{d}}{\mathbf{4}}$	
1	2		23		11		1
	6		7		19		2
3	8		17		5		3
	24		1		13		4
2	4		5	11	17	23	5
	12		1	7	13	19	6

Table 4.42.1: All possibilities for m constructed with Theorem 4.40 with $q = 25$.

Note that in lines 1, 3 and 5, we have repetitions. The m's generated with $d = 2$ and $d = 8$ are equal to the m's generated with $d = 4$. We proved this in Propositions 4.36 and 4.37. Lines 2, 4 and 6 are similar.

$\diamond$

We can use Theorem 4.40 to construct all m's for a fixed d.

Example 4.43. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, and $d = 2$. Then $f = 1$ and for $e \geq 1$, by Theorem 4.40, we have

$$k = 2\left(\frac{q-1}{2}\right)^{\phi(1)-1} + t, \quad t \in \{0, 1\}.$$

Therefore, $k = 2 + t$ for $t \in \{0, 1\}$. Now we substitute k to find m_1 and m_2.

$$m_1 \equiv \left(\frac{q-1}{2}\right) 2 - 1 \equiv -1 \pmod{q-1} \quad \text{and}$$

$$m_2 \equiv \left(\frac{q-1}{2}\right) 3 - 1 \equiv \frac{3q-5}{2} \pmod{q-1}.$$

Then for $e \geq 1$, $m_1 = q - 2$ and $m_2 = \frac{3q-5}{2}$.

$\diamond$

We can do a similar procedure as in Example 4.43 to produce all possible m's

for a fixed d:

1. Fix d.
2. If $f = 1$, use Lemma 4.30 to construct m's for $e = 1, 2$.
3. If $f > 1$, use Lemma 4.30 to construct m's for $e = f$.
4. If $f = 2$, use Lemma 4.31 to construct m's for $e \geq 3$.
5. If $f > 2$, use Lemma 4.31 to construct m's for $e = f + 1$.

Example 4.44. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ and $d = 4$. Then $f = 2$. Again we use Theorem 4.40 to construct all possible m's following the procedure described above. We get

$$k = \begin{cases} 2\left(\frac{q-1}{4}\right)^{\phi(2)-1} + t,\ t \in \{0, 2\} & \text{if } e = 2, \\ \left(\frac{q-1}{8}\right)^{\phi(1)-1} + t,\ t \in \{0, 1, 2, 3\} & \text{if } e \geq 3. \end{cases}$$

Substituting these values of k, we get the following m's:

$$m = \begin{cases} q - 2,\ \frac{q-3}{2} & \text{if } e = 2, \\ \frac{q-5}{4},\ \frac{q-3}{4},\ \frac{3q-7}{4},\ q - 2 & \text{if } e \geq 3. \end{cases}$$

◇

4.4 Main Results: Characterizations of Involutions in Terms of the Number of Fixed Points

The goal of this thesis is to give a characterization of involutions of $\mathbb{F}_q$ of the form $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ based on the size of the field q, and the number of fixed points.

In Figures 4.28.1 and 4.28.2, we illustrate how, for involutions $f(x)$ that have more than one fixed point, the exponent m can be written as $\left(\frac{q-1}{d}\right)k-1$ modulo $q-1$ where d represents the number of non-zero fixed points. In Section 4.3, we prove in Theorem 4.40 that for all such involutions, $m \equiv \left(\frac{q-1}{d}\right)k-1 \pmod{q-1}$ and provide formulas for k. However, an important observation from Theorem 4.40 is that d is only a divisor of $q-1$, it is not necessarily the number of non-zero fixed points of $f(x)$. In this section, we start by determining the value of d in terms of $g = \gcd(m-1, \frac{q-1}{2})$. Then we provide explicit formulas for obtaining involutions of $\mathbb{F}_q$ of the form $f(x)$ with a prescribed number of fixed points.

The following lemma brings us closer to tying this divisor d and the number of fixed points.

Lemma 4.45. If $d \mid (q-1)$, $\frac{d}{2} \mid (m-1)$ and $m \equiv \left(\frac{q-1}{d}\right)k-1 \pmod{q-1}$, for some $k \in \mathbb{Z}$, then $d = g$ or $d = 2g$, where $g = \gcd\left(m-1, \frac{q-1}{2}\right)$.

Proof. Since $\frac{d}{2} \mid (m-1)$ and $\frac{d}{2} \mid \frac{q-1}{2}$, then $\frac{d}{2} \mid g$. Therefore $g = \frac{d}{2}k_1$, for some $k_1 \in \mathbb{N}$, $\frac{q-1}{2} = \left(\frac{d}{2}\right)k_1 h$, for some $h \in \mathbb{Z}$, and

$$\left(\frac{d}{2}\right)k_1 \,\middle|\, m-1 \iff \left(\frac{d}{2}\right)k_1 \,\middle|\, \left(\left(\frac{dk_1h}{d}\right)k-2\right).$$

This implies that $k_1 \mid 2$, that is, $g = \frac{d}{2}$ or $g = \left(\frac{d}{2}\right)2 = d$.

□

Recall from Section 3.2 that the possible numbers of non-zero fixed points of $f(x)$ are 0, g, and $2g$. Since we are focusing on involutions $f(x)$ that have more than one fixed point, we first determine the conditions to have $d = g$ and $d = 2g$. Since Theorem 4.40 provides formulas for m depending on the value of $e = \nu_2(q-1)$ and $f = \nu_2(d)$, we will determine the value of d in terms of g for each case of Theorem 4.40, shown in Table 4.45.1. After this, we will see that there are various relations between d, q and the number of fixed points.

e	f
≥ 1	e
≥ 2	1
3	2
≥ 4	2
	$e-1$

Table 4.45.1: All distinct cases of Theorem 4.40 for constructing m's such that $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with more than one fixed point.

Proposition 4.46. Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 1$, and $d = 2^e p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$, where $\ell_s \in \{0, e_s\}$. If $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\},$$

then $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and $d = 2\gcd(m-1, \frac{q-1}{2})$.

Proof. By Lemma 4.30, $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$.

Let $g = \gcd(m-1, \frac{q-1}{2})$, and for $i \in \{1, 2\}$, let $m_i \equiv \left(\frac{q-1}{d}\right) k_i - 1 \pmod{q-1}$ where $k_i = 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + (i-1)\left(\frac{d}{2}\right)$. If $e = 1$, then $\nu_2\left(\frac{q-1}{2}\right) = 0$ and $\nu_2(g) = 0$. Suppose $e \geq 2$. Then, for some $h \in \mathbb{Z}$,

$$\begin{aligned} m_i - 1 &= \left(\frac{q-1}{d}\right)\left[2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + (i-1)\left(\frac{d}{2}\right)\right] - 2 + (q-1)h \\ &= 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)} + (i-1)\left(\frac{q-1}{2}\right) - 2 + (q-1)h \\ &= 2\left[\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)} + (i-1)\left(\frac{q-1}{4}\right) - 1 + \left(\frac{q-1}{2}\right)h\right]. \end{aligned}$$

Since $\gcd\left(\frac{q-1}{d}, \frac{d}{2}\right) = 1$, then $\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)} \equiv 1 \pmod{\frac{d}{2}}$. Then, for some $s \in \mathbb{Z}$, $\left(\frac{d}{2}\right) s = \left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)} - 1$. Therefore,

$$m_i - 1 = 2\left[\left(\frac{d}{2}\right)s + (i-1)\left(\frac{q-1}{4}\right) + \left(\frac{q-1}{2}\right)h\right].$$

Note that $\nu_2\left(\left(\frac{d}{2}\right)\, s\right) \geq e-1 \geq 1$ and $\nu_2\left(\left(\frac{q-1}{2}\right) h\right) \geq e-1 \geq 1$.

If $i=1$, then $\nu_2(m_1-1) \geq e$. Since $\nu_2\left(\frac{q-1}{2}\right) = e-1$, then $\nu_2(g) = e-1$.

Suppose now that $i=2$. Then we have two cases: $e=2$ and $e \geq 3$. If $e=2$, then $\nu_2\left(\frac{q-1}{2}\right) = 1$ and $\nu_2(m_2-1) = 1$ since $\nu_2\left(\frac{q-1}{4}\right) = 0$. This implies that $\nu_2(g) = 1$. If $e \geq 3$, then $\nu_2\left(\frac{q-1}{4}\right) = e-2$ and $\nu_2(m_2-1) \geq e-1$. Since $\nu_2\left(\frac{q-1}{2}\right) = e-1$, then $\nu_2(g) = e-1$.

For all cases, we have that $\nu_2(g) = e-1$. Lemma 4.45 implies that $d = 2g$.

□

Proposition 4.47. Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 2$, and $d = 2p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$, where $\ell_s \in \{0, e_s\}$. If $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\},$$

then $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and $d = \gcd(m-1, \frac{q-1}{2})$.

Proof. By Lemma 4.30, $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$.

Let $g = \gcd(m-1, \frac{q-1}{2})$ and, for $i \in \{1,2\}$, $m_i \equiv \left(\frac{q-1}{d}\right) k_i - 1 \pmod{q-1}$ where $k_i = 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + (i-1)\left(\frac{d}{2}\right)$. Then, for some $h \in \mathbb{Z}$,

$$\begin{aligned}
m_i - 1 &= \left(\frac{q-1}{d}\right) k_i - 2 + (q-1)h \\
&= \left(\frac{q-1}{d}\right)\left[2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + (i-1)\left(\frac{d}{2}\right)\right] - 2 + (q-1)h \\
&= 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)} + (i-1)\left(\frac{q-1}{2}\right) - 2 + (q-1)h \\
&= 2\left[\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)} + (i-1)\left(\frac{q-1}{4}\right) - 1 + \left(\frac{q-1}{2}\right) h\right].
\end{aligned}$$

Note that since $e \geq 2$ and $f = 1$, then $\nu_2\left(\frac{q-1}{d}\right) = e-1 \geq 1$ and $\nu_2\left(\left(\frac{q-1}{2}\right) h\right) \geq e-1 \geq 1$.

If $i=1$, then $\nu_2(m_1-1) = 1$ and $\nu_2(g) = 1$. Suppose now that $i=2$. If $e=2$, then $\nu_2\left(\frac{q-1}{4}\right) = 0$ and $\nu_2(m_2-1) \geq 2$. But $\nu_2\left(\frac{q-1}{2}\right) = 1$, therefore $\nu_2(g) = 1$. If

$e \geq 3$, then $\nu_2\left(\frac{q-1}{4}\right) = e-2 \geq 1$ and $\nu_2(m_2-1) = 1$. This implies that $\nu_2(g) = 1$.

For all cases, $\nu_2(g) = 1$. Then, by Lemma 4.45, $d = g$.

□

Proposition 4.48. Let $q-1 = 2^3 p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, and $d = 2^2 p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$. If $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\},$$

then $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and

$$d = \begin{cases} \gcd\left(m-1, \dfrac{q-1}{2}\right) & \text{if } t \in \left\{0, \dfrac{d}{2}\right\} \\ 2\gcd\left(m-1, \dfrac{q-1}{2}\right) & \text{if } t \in \left\{\dfrac{d}{4}, \dfrac{3d}{4}\right\}. \end{cases}$$

Proof. By Lemma 4.31, $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$.

Let $g = \gcd(m-1, \frac{q-1}{2})$ and, for $i \in \{1,2,3,4\}$, $m_i \equiv \left(\frac{q-1}{d}\right) k_i - 1 \pmod{q-1}$ where $k_i = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + (i-1)\left(\frac{d}{4}\right)$. Then, for some $h \in \mathbb{Z}$,

$$\begin{aligned} m_i - 1 &= \left(\frac{q-1}{d}\right) k_i - 2 + (q-1)h \\ &= \left(\frac{q-1}{d}\right)\left[\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + (i-1)\left(\frac{d}{4}\right)\right] - 2 + (q-1)h \\ &= 2\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} + (i-1)\left(\frac{q-1}{4}\right) - 2 + (q-1)h \\ &= 2\left[\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} + (i-1)\left(\frac{q-1}{8}\right) - 1 + \left(\frac{q-1}{2}\right)h\right]. \end{aligned}$$

Note that $\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} - 1$ is even and $\nu_2\left(\left(\frac{q-1}{2}\right)h\right) \geq 2$.

If $i = 1$, then $\nu_2(m_1 - 1) \geq 2$. If $i = 3$, then $\nu_2(m_3 - 1) \geq 2$ since $\nu_2\left(\frac{q-1}{4}\right) = 1$. But $\nu_2\left(\frac{q-1}{2}\right) = 2$, therefore for both cases $i \in \{1,3\}$, $\nu_2(g) = 2$. This implies that $d = g$ by Lemma 4.45.

Suppose now that $i \in \{2,4\}$. Then $\nu_2\left((i-1)\left(\frac{q-1}{8}\right)\right) = 0$ and $\nu_2(g) = \nu_2(m_i -$

1) = 1. Then by Lemma 4.45, $d = 2g$.

□

When $e = 3$ and $f = 2$, we see in Proposition 4.48 that the value of d also depends on the value of t. This means that, although Theorem 4.40 with these values of e and f provide four formulas for m, the value of d is not the same for all four m's. That is, we can not determine whether $d = g$ or $d = 2g$ only from the values of e and f. We will see later that this is not the only case where this happens.

Proposition 4.49. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 4$, and $d = 2^2 p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$. If $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\},$$

then $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and $d = 2\gcd(m-1, \frac{q-1}{2})$.

Proof. By Lemma 4.31, $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$.

Let $g = \gcd(m-1, \frac{q-1}{2})$ and, for $i \in \{1, 2, 3, 4\}$, $m_i \equiv \left(\frac{q-1}{d}\right) k_i - 1 \pmod{q-1}$ where $k_i = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + (i-1)\left(\frac{d}{4}\right)$. Then, for some $h \in \mathbb{Z}$,

$$\begin{aligned}
m_i - 1 &= \left(\frac{q-1}{d}\right) k_i - 2 + (q-1)h \\
&= \left(\frac{q-1}{d}\right)\left[\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + (i-1)\left(\frac{d}{4}\right)\right] - 2 + (q-1)h \\
&= 2\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} + (i-1)\left(\frac{q-1}{4}\right) - 2 + (q-1)h \\
&= 2\left[\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} + (i-1)\left(\frac{q-1}{8}\right) - 1 + \left(\frac{q-1}{2}\right)h\right].
\end{aligned}$$

Note that $\nu_2\left(\frac{q-1}{2d}\right) = e - 3 \geq 1$ and $\nu_2\left(\left(\frac{q-1}{2}\right)h\right) \geq e - 1 \geq 3$.

If $i = 1$, then $\nu_2(m_1 - 1) = 1$. If $i \neq 1$, then $\nu_2\left((i-1)\left(\frac{q-1}{8}\right)\right) \geq e - 3 \geq 1$. Therefore $\nu_2(m_i - 1) = 1$. For both cases, we have that $\nu_2(g) = 1$. Lemma 4.45

implies that $d = 2g$.

□

To determine whether $d = g$ or $d = 2g$ when $e \geq 4$ and $f = e - 1$, we need to consider again the value of t and also of $\Omega = \nu_2(\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} - 1)$. The following lemma gives us bounds for the 2-valuation of $m - 1$ and Ω.

Lemma 4.50. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 4$, and $d = 2^{e-1} p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$. If $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where $k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t$, $t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\}$, then $\nu_2(m-1) \geq e-2$. Moreover, if $q-1 = 2d$, then $\nu_2(m-1) = e - 2$, and, if $q - 1 \neq 2d$, then $\Omega \geq e - 3$ where $\Omega = \nu_2(\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} - 1)$.

Proof. Let $i = 1, 2, 3, 4$. Then, for some $h \in \mathbb{Z}$,

$$\begin{aligned} m - 1 &= \left(\frac{q-1}{d}\right)\left[\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + (i-1)\left(\frac{d}{4}\right)\right] - 2 + (q-1)h \\ &= 2\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} + (i-1)\left(\frac{q-1}{4}\right) - 2 + (q-1)h \\ &= 2\left[\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} + (i-1)\left(\frac{q-1}{8}\right) - 1 + \left(\frac{q-1}{2}\right)h\right]. \end{aligned}$$

Suppose that $q-1 = 2d$. Then $\frac{q-1}{2d} = 1$ and $m-1 = 2\left[(i-1)\left(\frac{q-1}{8}\right) + \left(\frac{q-1}{2}\right)h\right]$. Since $\nu_2\left(\frac{q-1}{8}\right) = e-3$ and $\nu_2\left(\frac{q-1}{2}\right) = e-1$, then $\nu_2(m-1) = 1 + e - 3 = e - 2$.

Suppose now that $q-1 \neq 2d$. Since $\gcd(\frac{q-1}{2d}, \frac{d}{4}) = 1$, then, by Euler's Theorem, $\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} \equiv 1 \pmod{\frac{d}{4}}$. That is, $\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} - 1 = \left(\frac{d}{4}\right)s$ for some $s \in \mathbb{Z}$. Therefore,

$$\begin{aligned} m - 1 &= 2\left[\left(\frac{d}{4}\right)s + (i-1)\left(\frac{q-1}{8}\right) + \left(\frac{q-1}{2}\right)h\right] \\ &= 2\left(\frac{d}{4}\right)\left[s + (i-1)\left(\frac{q-1}{2d}\right) + 2\left(\frac{q-1}{d}\right)h\right]. \end{aligned}$$

This implies that $\nu_2(m-1) \geq e-2$, by Proposition 2.22.

Lastly, since $\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} - 1 = \left(\frac{d}{4}\right) s$, then, by Proposition 2.22, if $q - 1 \neq 2d$,

$$\Omega = \nu_2\left(\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} - 1\right) = \nu_2\left(\frac{d}{4}\right) + \nu_2(s) \geq e - 3.$$

□

From the bound of Ω, given by Lemma 4.50, we know that we cover all of the possibilities for d in Proposition 4.51.

Proposition 4.51. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 4$, $d = 2^{e-1} p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, and $\Omega = \nu_2\Big(\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} - 1\Big)$. If $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where $k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t$ and

1. $t \in \left\{0, \frac{d}{2}\right\}$, then

$$d = \begin{cases} g & \text{if } \Omega > e - 3 \text{ or } d = \dfrac{q-1}{2}, \\ 2g & \text{if } \Omega = e - 3, \end{cases}$$

2. $t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$, then

$$d = \begin{cases} g & \text{if } \Omega = e - 3, \\ 2g & \text{if } \Omega > e - 3 \text{ or } d = \dfrac{q-1}{2}, \end{cases}$$

for $g = \gcd(m - 1, \frac{q-1}{2})$. Moreover, $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$.

Proof. By Lemma 4.31, $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. Let $i = 1, 2, 3, 4$ and $k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + (i-1)\left(\frac{d}{4}\right)$. By Lemma 4.50, $\nu_2(m-1) \geq e-2$. Note that by Euler's Theorem, we can write $\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} - 1 = \left(\frac{d}{4}\right) s$, for some $s \in \mathbb{Z}$. This implies that we can write

$$m - 1 = 2\left(\frac{d}{4}\right)\left[s + (i-1)\left(\frac{q-1}{2d}\right) + 2\left(\frac{q-1}{d}\right) h\right],$$

for some $h \in \mathbb{Z}$, as we did in the proof of Lemma 4.50.

Let $t \in \left\{0, \frac{d}{2}\right\}$. Then $i \in \{1, 3\}$ and $(i-1)\left(\frac{q-1}{2d}\right)$ is even.

If $\Omega = e - 3$, then s is odd and $\nu_2(m-1) = e - 2$. Therefore, $\nu_2(g) = e - 2$ and, by Lemma 4.45, $d = 2g$. If $\Omega > e - 3$, then s is even and $\nu_2(m-1) > e - 2$. Similarly, if $d = \frac{q-1}{2}$, then $s = 0$ and $\nu_2(m-1) > e - 2$. Therefore, if $\Omega > e - 3$ or $d = \frac{q-1}{2}$, then $\nu_2(m-1) > e - 2$ and, since $\nu_2\left(\frac{q-1}{2}\right) = e - 1$, $\nu_2(g) = e - 1$ and $d = g$ by Lemma 4.45.

Let $t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$. Then $i \in \{2, 4\}$ and $(i-1)\left(\frac{q-1}{2d}\right)$ is odd.

If $\Omega = e - 3$, then s is odd and $\nu_2(m-1) > e - 2$. Since $\nu_2\left(\frac{q-1}{2}\right) = e - 1$, then $\nu_2(g) = e - 1 = \nu_2(d)$ and, by Lemma 4.45, $d = g$. If $\Omega > e - 3$, then s is even and $\nu_2(m-1) = e - 2$. Similarly, if $d = \frac{q-1}{2}$, then $s = 0$ and $\nu_2(m-1) = e - 2$. Therefore, if $\Omega > e - 3$ or $d = \frac{q-1}{2}$, then $\nu_2(g) = e - 2 = \nu_2(d) - 1$ and, by Lemma 4.45, $d = 2g$.

□

We have related d with $g = \gcd(m-1, \frac{q-1}{2})$. However, this is not sufficient to say that d is the number of non-zero fixed points. Recall that if $f(x)$ is an involution with more than one fixed point, then the number of non-zero fixed points is g or $2g$. Statement 3 of Theorem 3.13 states that $f(x)$ has g non-zero fixed points when it only has square non-zero fixed points or only non-square fixed points, and $f(x)$ has $2g$ non-zero fixed points when it has both square and non-square fixed points.

Suppose $e \geq 1$ and $f = e$. Proposition 4.46 tells us that $d = 2g$. If $f(x)$ is an involution of $\mathbb{F}_q$ with either square or non-square non-zero fixed points, then $f(x)$ has $g + 1 = \frac{d}{2} + 1$ fixed points. Similarly, if $f(x)$ has both square and non-square non-zero fixed points, then it has exactly $2g + 1 = d + 1$ fixed points.

Suppose now that $e \geq 2$ and $f = 1$. Then $d = g$ by Proposition 4.47. If $f(x)$ has either non-zero square or non-square fixed points, then $f(x)$ has $g + 1 = d + 1$ fixed points. If $f(x)$ has both square and non-square fixed points, then $f(x)$ has $2g + 1 = 2d + 1$ fixed points.

We can do a similar procedure for the other cases of e and f. That is, for each

case where we proved $d = g$ or $d = 2g$, we get two possibilities for the number of fixed points. We summarize these cases in Table 4.51.1. Note that, since we cover all of the possible cases of Theorem 4.40, we also cover all of the involutions of $\mathbb{F}_q$ of the form $f(x)$.

e	f	d Reference	$f(x)$ has square and non-square fixed points	Number of non-zero fixed points	Proposition
≥ 1	e	$2g$ Proposition 4.46	yes	d	4.53
			no	$d/2$	4.52
≥ 2	1	g Proposition 4.47	yes	$2d$	4.55
			no	d	4.54
3	2	$2g$ Proposition 4.48 $\left(t \in \left\{0, \frac{d}{2}\right\}\right)$	yes	d	4.57
			no	$d/2$	4.56
		g Proposition 4.48 $\left(t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}\right)$	yes	$2d$	4.58
			no	d	4.57
≥ 4	2	$2g$ Proposition 4.49	yes	d	4.60
			no	$d/2$	4.59
	$e-1$	g Proposition 4.51	yes	$2d$	4.63
			no	d	4.62
		$2g$ Proposition 4.51	yes	d	4.62
			no	$d/2$	4.61

Table 4.51.1: Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 1$, $d = 2^f p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$. Rows represent the cases for the number of fixed points of involutions of $\mathbb{F}_q$ of the form $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ in terms of d. Column d shows the value of d in terms of $g = \gcd(m-1, \frac{q-1}{2})$ and references the propositions where we determine these values for d. The last column provides the propositions where we prove each case.

▷ Case $e \geq 1$, $f = e$

As we previously mentioned, for this case, we have two types of involutions: involutions with $g + 1 = \frac{d}{2} + 1$ fixed points and involutions with $2g + 1 = d + 1$ fixed points. These are proved in Propositions 4.52 and 4.53 respectively.

Proposition 4.52. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 1$, $d = 2^e p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, and α be a primitive element of $\mathbb{F}_q$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $\dfrac{d}{2} + 1$ fixed points if and only if the following conditions hold:

1. $m \equiv \left(\dfrac{q-1}{d}\right) k - 1 \pmod{q-1}$, where $k = 2\left(\dfrac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t$, $t \in \left\{0, \dfrac{d}{2}\right\}$
2. $\eta(a^2 - 1) = (-1)^{m+1}$
3. $(a^2 - 1)^{m+1} = (-1)^{\frac{2(m^2-1)}{q-1}}$
4. Either $a + 1 = \alpha^{k_1(1-m)}$ or $a - 1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd.

Proof. Let $g = \gcd(m - 1, \frac{q-1}{2})$ and $f = \nu_2(d) = e$.

($\Rightarrow$) Theorem 4.19 implies Conditions 2 and 3 and $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. By Theorem 4.40, Condition 1 holds since $e \geq 1$ and $f = e$. Therefore, $d = 2g$ by Proposition 4.46. That is, $f(x)$ has $g + 1$ fixed points. By Statement 3 of Theorem 3.13, $f(x)$ has either non-zero square fixed points or non-square fixed points. Then, by Statements 1 and 2 of Theorem 3.13, Condition 4 holds.

($\Leftarrow$) By Proposition 4.46, Condition 1 implies that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and that $d = 2g$. Therefore, by Theorem 4.19, $f(x)$ is an involution with more than one fixed point. Condition 4 implies, by Statements 1 and 2 of Theorem 3.13, $f(x)$ has either non-zero square fixed points or non-square fixed points. Then, by Statement 3 of Theorem 3.13, $f(x)$ has $g + 1 = \frac{d}{2} + 1$ fixed points.

□

Proposition 4.53. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 1$, $d = 2^e p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, and α be a primitive element of $\mathbb{F}_q$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is

an involution of $\mathbb{F}_q$ with exactly $d+1$ fixed points if and only if the following conditions hold:

1. $m \equiv \left(\frac{q-1}{d}\right) k-1 \pmod{q-1}$, where $k = 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t, t \in \left\{0, \frac{d}{2}\right\}$
2. $a+1 = \alpha^{k_1(1-m)}$ and $a-1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd.

Proof. Let $g = \gcd(m-1, \frac{q-1}{2})$ and $f = \nu_2(d) = e$.

($\Rightarrow$) Since $f(x)$ is an involution with more than one fixed point, $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ by Theorem 4.19. But $e \geq 1$ and $f = e$, therefore Theorem 4.40 implies Condition 1 and Proposition 4.46 implies $d = 2g$. Then $f(x)$ has $2g+1$ fixed points and by Proposition 4.21, Condition 2 holds.

($\Leftarrow$) By Proposition 4.46, Condition 1 implies that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and $d = 2g$. Then by Proposition 4.21, $f(x)$ is an involution with $2g+1$ fixed points, that is $d+1$ fixed points.

□

▷ Case $e \geq 2$, $f = 1$

As we saw earlier, this case has two possibilities for the number of fixed points of involutions $f(x)$: $g+1 = d+1$ and $2g+1 = 2d+1$.

Proposition 4.54. Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 2$, $d = 2p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, and α be a primitive element of $\mathbb{F}_q$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $d+1$ fixed points if and only if the following conditions hold:

1. $m \equiv \left(\frac{q-1}{d}\right) k-1 \pmod{q-1}$, where $k = 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t, t \in \left\{0, \frac{d}{2}\right\}$
2. $\eta(a^2-1) = (-1)^{m+1}$
3. $(a^2-1)^{m+1} = (-1)^{\frac{2(m^2-1)}{q-1}}$
4. Either $a+1 = \alpha^{k_1(1-m)}$ or $a-1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd.

Proof. Let $g = \gcd(m-1, \frac{q-1}{2})$ and $f = \nu_2(d) = 1$.

($\Rightarrow$) Since $f(x)$ is an involution with more than one fixed point, then $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and Conditions 2 and 3 hold by Theorem 4.19. By Theorem 4.40, Condition 1 holds and, by Proposition 4.47, $d = g$. By hypothesis, $f(x)$ has $g+1$ fixed points. Then, by Statement 3 of Theorem 3.13, $f(x)$ has either non-zero square fixed points or non-square fixed points. Therefore, by Statements 1 and 2 of Theorem 3.13, Condition 4 holds.

($\Leftarrow$) By Proposition 4.47, Condition 1 implies $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and $d = g$. Therefore, $f(x)$ is an involution with more than one fixed point by Theorem 4.19. Condition 4 implies, by Statements 1 and 2 of Theorem 3.13, that $f(x)$ has either non-zero square fixed points or non-square fixed points. Then $f(x)$ has $g+1 = d+1$ fixed points, by Statement 3 of Theorem 3.13.

□

Proposition 4.55. Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 2$, $d = 2p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, and α be a primitive element of $\mathbb{F}_q$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $2d+1$ fixed points if and only if the following conditions hold:

1. $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where $k = 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t, t \in \left\{0, \frac{d}{2}\right\}$
2. $a + 1 = \alpha^{k_1(1-m)}$ and $a - 1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd.

Proof. Let $g = \gcd(m-1, \frac{q-1}{2})$ and $f = \nu_2(d) = 1$.

($\Rightarrow$) Since $f(x)$ is an involution with more than one fixed point, then by Theorem 4.19, $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. But since $e \geq 2$ and $f = 1$, then Condition 1 holds by Theorem 4.40. Now, by Proposition 4.47, $d = g$. Then $f(x)$ has $2g+1$ fixed points and, by Proposition 4.21, Condition 2 holds.

($\Leftarrow$) By Proposition 4.47, Condition 1 implies that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and that $d = g$. Then by Proposition 4.21, $f(x)$ is an involution with $2g+1$ fixed points, that is $2d+1$ fixed points.

□

▷ Case $e = 3,\ f = 2$

Recall from Proposition 4.48 that when $e = 3$ and $f = 2$, the value of d is different for different values of t. In Table 4.51.1 we saw that this give us three cases for the number of involutions: $\frac{d}{2}+1$, $d+1$, and $2d+1$. First we prove the case where $f(x)$ has $g+1 = \frac{d}{2}+1$ fixed points. Note that this is the case where $f(x)$ either has square or non-square non-zero fixed points. This case only happens when $t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$.

Proposition 4.56. Let $q-1 = 2^3 p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $d = 2^2 p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, and α be a primitive element of $\mathbb{F}_q$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $\dfrac{d}{2}+1$ fixed points if and only if the following conditions hold:

1. $m \equiv \left(\dfrac{q-1}{d}\right) k-1 \pmod{q-1}$, where $k = \left(\dfrac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t$, $t \in \left\{\dfrac{d}{4}, \dfrac{3d}{4}\right\}$
2. $\eta(a^2-1) = (-1)^{m+1}$
3. $(a^2-1)^{m+1} = (-1)^{\frac{2(m^2-1)}{q-1}}$
4. Either $a+1 = \alpha^{k_1(1-m)}$ or $a-1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd.

Proof. Let $g = \gcd(m-1, \frac{q-1}{2})$ and $f = \nu_2(d) = 2$.

($\Rightarrow$) By Theorem 4.19, Conditions 2 and 3 hold and $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. Then, since $e = 3$ and $f = 2$, by Theorem 4.40, $k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t$ and $t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\}$. Now, Proposition 4.48 states that if $t \in \left\{0, \frac{d}{2}\right\}$ then $d = g$ and if $t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$ then $d = 2g$. But if $d = g$, then $f(x)$ would have $\frac{g}{2}+1$ fixed points which is a contradiction to Statement 3 of Theorem 3.13. Therefore, $d = 2g$, $t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$ and Condition 1 holds. Since $f(x)$ has $\frac{d}{2}+1$ fixed points, then it has $g+1$ fixed points. Then, by Statement 3 of Theorem 3.13, $f(x)$ has either non-zero square fixed points or non-square fixed points. Lastly, by Statements 1 and 2 of Theorem 3.13, Condition 4 holds.

($\Leftarrow$) By Proposition 4.48, Condition 1 implies that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and that $d = 2g$. Therefore, by Theorem 4.19, $f(x)$ is an involution with more than one

fixed point. Condition 4 implies that $f(x)$ has either non-zero square fixed points or non-square fixed points by Statements 1 and 2 of Theorem 3.13. Therefore, by Statement 3 of Theorem 3.13, $f(x)$ has $g+1 = \frac{d}{2}+1$ fixed points.

□

The next possibility for the number of fixed points is $d+1$. However, from Table 4.51.1, we have two cases where the number of fixed points is $d+1$. The first is when $f(x)$ has $2g+1$ fixed points and $t \in \left\{0, \frac{d}{2}\right\}$, and the second is when $f(x)$ has $g+1$ fixed points and $t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$.

Proposition 4.57. Let $q-1 = 2^3 p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $d = 2^2 p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, and α be a primitive element of $\mathbb{F}_q$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $d+1$ fixed points if and only if exactly one of the following holds:

1. (a) $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$$

   (b) $a+1 = \alpha^{k_1(1-m)}$ and $a-1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd,

2. (a) $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\}$$

   (b) $\eta(a^2-1) = (-1)^{m+1}$

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

   (d) Either $a+1 = \alpha^{k_1(1-m)}$ or $a-1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd.

Proof. Let $g = \gcd(m-1, \frac{q-1}{2})$ and $f = \nu_2(d) = 2$.

($\Rightarrow$) Since $f(x)$ has more than one fixed point, then by Theorem 4.19, $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. Since $e = 3$ and $f = 2$, then Theorem 4.40 implies that $m \equiv \left(\frac{q-1}{d}\right)\left[\left(\frac{q-1}{2}\right)^{\phi\left(\frac{d}{4}\right)-1} + t\right] - 1$, where $t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\}$.

Suppose $t \in \left\{0, \frac{d}{2}\right\}$. Then Condition 2(a) and, by Theorem 4.19, Conditions 2(b) and 2(c) hold. Now, by Proposition 4.48, we have $d = g$ and $f(x)$ has exactly $g+1$ fixed points. Since $f(x)$ has $g+1$ fixed points, then $f(x)$ has either non-zero square fixed points or non-square fixed points by Statement 3 of Theorem 3.13. Therefore, by Statements 1 and 2 of Theorem 3.13, Condition 2(d) holds.

Suppose now that $t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$. Then Condition 1(a) holds. By Proposition 4.48, $d = 2g$, that is, $f(x)$ is an involution with $2g+1$ fixed points. Then by Proposition 4.21, Condition 1(b) holds.

($\Leftarrow$) Suppose that Condition 1 holds. Since $e = 3$ and $f = 2$, then by Theorem 4.40, Condition 1(a) implies that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. This, together with Condition 1(b) and Proposition 4.21 imply that $f(x)$ is an involution with exactly $2g+1$ fixed points. But by Proposition 4.48, Condition 1(a) implies that $d = 2g$. Then $f(x)$ has exactly $d+1$ fixed points.

Suppose now that Condition 2 holds. Condition 2(a) implies that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ by Theorem 4.40. Then by Theorem 4.19, $f(x)$ is an involution with more than one fixed point. Condition 2(d) implies, by Statements 1 and 2 of Theorem 3.13, that $f(x)$ has either non-zero square fixed points or non-square fixed points. Then, by Statement 3 of Theorem 3.13, $f(x)$ has $g+1$ fixed points. But by Proposition 4.48, Condition 2(a) implies that $d = g$. Then $f(x)$ has exactly $d+1$ fixed points.

□

The last possibility for the number of fixed points is $2d+1$. This happens when $f(x)$ has both square and non-square fixed points, that is $2g+1 = 2d+1$.

Proposition 4.58. Let $q-1 = 2^3 p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $d = 2^2 p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, and α be a primitive element of $\mathbb{F}_q$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $2d+1$ fixed points if and only if the following conditions

hold:

1. $m \equiv \left(\frac{q-1}{d}\right)k - 1 \pmod{q-1}$, where $k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t$, $t \in \left\{0, \frac{d}{2}\right\}$
2. $a + 1 = \alpha^{k_1(1-m)}$ and $a - 1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd.

Proof. ($\Rightarrow$) Let $g = \gcd(m-1, \frac{q-1}{2})$ and $f = \nu_2(d) = 2$.

By Theorem 4.19, $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. Since $e = 3$ and $f = 2$, then by Theorem 4.40, $k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t$ where $t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\}$. Now, Proposition 4.48 implies that if $t \in \left\{0, \frac{d}{2}\right\}$ then $d = g$ and if $t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$ then $d = 2g$. But if $d = 2g$, then $f(x)$ would have $4g + 1$ fixed points which is a contradiction to Statement 3 of Theorem 3.13. Therefore $t \in \left\{0, \frac{d}{2}\right\}$ and $d = g$. This implies that Condition 1 holds. Since $f(x)$ has $2g + 1$ fixed points, then by Proposition 4.21, Condition 2 holds.

($\Leftarrow$) By Proposition 4.48, Condition 1 implies that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and that $d = g$. Then by Proposition 4.21, $f(x)$ is an involution with $2g + 1$ fixed points, that is $2d + 1$ fixed points.

□

▷ Case $e \geq 4$, $f = 2$

This case is similar to the case $e \geq 1$ and $f = e$ since the value of d only depends on e and f and $d = 2g$ for both cases. Therefore, here we present involutions when $e \geq 4$ and $f = 2$ with $\frac{d}{2} + 1$ and $d + 1$ fixed points.

Proposition 4.59. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 4$, $d = 2^2 p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, and α be a primitive element of $\mathbb{F}_q$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $\dfrac{d}{2} + 1$ fixed points if and only if the following conditions hold:

1. $m \equiv \left(\frac{q-1}{d}\right)k - 1 \pmod{q-1}$ where

$$k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t, \; t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\}$$

2. $\eta(a^2-1) = (-1)^{m+1}$

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

4. Either $a+1 = \alpha^{k_1(1-m)}$ or $a-1 = \alpha^{k_2(1-m)}$ for some k_1 even and k_2 odd.

Proof. Let $g = \gcd(m-1, \frac{q-1}{2})$ and $f = \nu_2(d) = 2$.

($\Rightarrow$) By Theorem 4.19, Conditions 2 and 3 hold and $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. Since $e \geq 4$ and $f = 2$, then, by Theorem 4.40, Condition 1 holds. By Proposition 4.49, $d = 2g$. Since $f(x)$ has $\frac{d}{2}+1 = g+1$ fixed points, then, by Statement 3 of Theorem 3.13, $f(x)$ has either non-zero square fixed points or non-square fixed points. By Statements 1 and 2 of Theorem 3.13, Condition 4 holds.

($\Leftarrow$) By Proposition 4.49, Condition 1 implies that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and that $d = 2g$. Then by Theorem 4.19, $f(x)$ is an involution with more than one fixed point. Condition 4 implies that $f(x)$ has either non-zero square fixed points or non-square fixed points, by Statements 1 and 2 of Theorem 3.13. Therefore, $f(x)$ has $g+1 = \frac{d}{2}+1$ fixed points by Statement 3 of Theorem 3.13.

□

Proposition 4.60. Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 4$, $d = 2^2 p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, and α be a primitive element of $\mathbb{F}_q$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $d+1$ fixed points if and only if the following conditions hold:

1. $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\}$$

2. $a+1 = \alpha^{k_1(1-m)}$ and $a-1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd.

Proof. Let $g = \gcd(m-1, \frac{q-1}{2})$ and $f = \nu_2(d) = 2$.

($\Rightarrow$) Since $f(x)$ is an involution with more than one fixed point, then $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ by Theorem 4.19. Since $e \geq 4$ and $f = 2$, then by Theorem 4.40,

Condition 1 holds and, by Proposition 4.49, $d = 2g$. That is, $f(x)$ has $2g+1$ fixed points and, by Proposition 4.21, Condition 2 holds.

($\Leftarrow$) By Proposition 4.49, Condition 1 implies that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and $d = 2g$. Then by Proposition 4.21, $f(x)$ is an involution with $2g+1$ fixed points, that is $d+1$ fixed points.

□

▷ Case $e \geq 4$, $f = e - 1$

This case is similar to the case $e = 3$ and $f = 2$ in the sense that we have three possibilities for the number of fixed points: $\frac{d}{2} + 1$, $d + 1$, or $2d + 1$. However, the conditions for determining d depend on the value of t as well as the value of $\Omega = \nu_2\Big(\big(\frac{q-1}{2d}\big)^{\phi\left(\frac{d}{4}\right)} - 1\Big)$.

Proposition 4.61. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 4$, $d = 2^{e-1} p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, α be a primitive element of $\mathbb{F}_q$, and, if $q - 1 \neq 2d$, $\Omega = \nu_2\Big(\big(\frac{q-1}{2d}\big)^{\phi\left(\frac{d}{4}\right)} - 1\Big)$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $\frac{d}{2} + 1$ fixed points if and only if the following conditions hold:

1. $m \equiv \left(\dfrac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = \begin{cases} \left(\dfrac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \dfrac{d}{2}\right\} & \text{if } \Omega = e - 3, \\ \left(\dfrac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{\dfrac{d}{4}, \dfrac{3d}{4}\right\} & \text{if } \Omega > e - 3 \text{ or } d = \dfrac{q-1}{2}, \end{cases}$$

2. $\eta(a^2 - 1) = (-1)^{m+1}$

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

4. Either $a + 1 = \alpha^{k_1(1-m)}$ or $a - 1 = \alpha^{k_2(1-m)}$ for some k_1 even and k_2 odd.

Proof. ($\Rightarrow$) Since $f(x)$ is an involution, then, by Theorem 4.19, Conditions 2 and 3 hold and $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. By Theorem 4.40, $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$

where $k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t$ for $t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\}$. By Lemma 4.45, we know that $d \in \{g, 2g\}$. This implies that $d = 2g$, since if $d = g$, then $f(x)$ would have $\frac{g}{2} + 1$ fixed points which is a contradiction to Theorem 3.13. Then $f(x)$ has exactly $\frac{d}{2} + 1 = g + 1$ fixed points. Hence, $f(x)$ has either non-zero square fixed points or non-square fixed points, that is Condition 4 holds, by Theorem 3.13.

Note that $\Omega \geq e - 3$ or $q - 1 = 2d$ by Lemma 4.50. Suppose $t \in \left\{0, \frac{d}{2}\right\}$ and $\Omega > e - 3$. Then by Statement 1 of Proposition 4.51, $d = g$, which is a contradiction, therefore $\Omega = e - 3$. Similarly, suppose $t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$. Note that by Statement 2 of Proposition 4.51, $\Omega = e - 3$ implies that $d = g$ which is a contradiction. Therefore $\Omega > e - 3$ or $d = \frac{q-1}{2}$, and Condition 1 holds.

($\Leftarrow$) By Proposition 4.51, Condition 1 implies that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and $d = 2g$. Then by Theorem 4.19, $f(x)$ is an involution with more than one fixed point. Lastly, Condition 4 implies, by Theorem 3.13, that $f(x)$ has exactly $g + 1$ fixed points. But $d = 2g$, therefore, $f(x)$ has $\frac{d}{2} + 1$ fixed points.

□

In Table 4.51.1, when $e \geq 4$ and $f = e - 1$, we see that again we have two cases where $f(x)$ has $d + 1$ fixed points; one for each possibility of non-zero fixed points: g and $2g$.

Proposition 4.62. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 4$, $d = 2^{e-1} p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, α be a primitive element of $\mathbb{F}_q$, and, if $q - 1 \neq 2d$, $\Omega = \nu_2\Big(\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} - 1\Big)$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $d + 1$ fixed points if and only if the following conditions hold:

1. (a) $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = \begin{cases} \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\} & \text{if } \Omega > e - 3 \text{ or } d = \frac{q-1}{2}, \\ \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\} & \text{if } \Omega = e - 3, \end{cases}$$

   (b) $\eta(a^2 - 1) = (-1)^{m+1}$

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

(d) Either $a+1 = \alpha^{k_1(1-m)}$ or $a-1 = \alpha^{k_2(1-m)}$ for some k_1 even and k_2 odd,

2. (a) $m \equiv \left(\frac{q-1}{d}\right)k - 1 \pmod{q-1}$, where

$$k = \begin{cases} \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\} & \text{if } \Omega = e-3, \\ \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\} & \text{if } \Omega > e-3 \text{ or } d = \frac{q-1}{2}, \end{cases}$$

(b) $a+1 = \alpha^{k_1(1-m)}$ and $a-1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd.

Proof. ($\Rightarrow$) Since $f(x)$ is an involution, then, by Corollary 4.3, $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. Since $e \geq 4$ and $f = e-1$, then, by Theorem 4.40, we have $m \equiv \left(\frac{q-1}{d}\right)k - 1 \pmod{q-1}$, where $k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t$, $t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\}$. Note that, by Lemma 4.50, $\Omega \geq e-3$ or $q-1 = 2d$. Therefore, Conditions 1(a) and 2(a) hold.

Suppose $t \in \left\{0, \frac{d}{2}\right\}$. If $\Omega = e-3$, then by Statement 1 of Proposition 4.51, $d = 2g$. Therefore, $f(x)$ has $2g+1$ fixed points. By Proposition 4.21, Condition 2(b) holds. Similarly, if $\Omega > e-3$ or $d = \frac{q-1}{2}$, then by Statement 1 of Proposition 4.51, $d = g$. That is, $f(x)$ has $g+1$ fixed points. Then by Theorem 4.19, Conditions 1(b) and 1(c) hold. Since $f(x)$ has $g+1$ fixed points, then, by Theorem 3.13, $f(x)$ has either non-zero square fixed points or non-square fixed points and, therefore, Condition 1(d) holds.

Suppose $t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$. If $\Omega = e-3$, then $d = g$ by Statement 2 of Proposition 4.51. That is, $f(x)$ has $g+1$ fixed points. Then, by Statement 3 of Theorem 3.13, $f(x)$ has either non-zero square fixed points or non-square fixed points. Hence, by Statements 1 and 2 of Theorem 3.13, Condition 1(d) holds. By Theorem 4.19, Conditions 1(b) and 1(c) hold. If $\Omega > e-3$ or $d = \frac{q-1}{2}$, then by Statement 2 of Proposition 4.51, $d = 2g$. This implies that $f(x)$ has $2g+1$ fixed points and, by Proposition 4.21, Condition 1(b) holds.

($\Leftarrow$) Conditions 1(a) and 2(a) imply that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ by Theorem 4.40.

Suppose $t \in \left\{0, \frac{d}{2}\right\}$. If $\Omega = e-3$, Statement 1 of Proposition 4.51 implies that $d = 2g$. Condition 2 implies that $f(x)$ is an involution with $2g+1 = d+1$ fixed points by Proposition 4.21. If $\Omega > e-3$ or $d = \frac{q-1}{2}$, then $d = g$ by Statement 1 of Proposition 4.51. Then Condition 1 implies that $f(x)$ is an involution with more than one fixed point, by Theorem 4.19. By Theorem 3.13, $f(x)$ has $g+1 = d+1$ fixed points.

Suppose $t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$. If $\Omega = e-3$, then $d = g$, by Statement 2 of Proposition 4.51. As in the previous case, Condition 1 implies that $f(x)$ is an involution with $g+1 = d+1$ fixed points by Theorems 4.19 and 3.13. If $\Omega > e-3$ or $d = \frac{q-1}{2}$, then $d = 2g$, by Statement 2 of Proposition 4.51. Condition 2 implies that $f(x)$ is an involution with $2g+1 = d+1$ fixed points by Proposition 4.21.

□

Proposition 4.63. Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 4$, $d = 2^{e-1} p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, α be a primitive element of $\mathbb{F}_q$, and, if $q-1 \neq 2d$, $\Omega = \nu_2\Big(\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} - 1\Big)$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $2d+1$ fixed points if and only if the following conditions hold:

1. $m \equiv \left(\dfrac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = \begin{cases} \left(\dfrac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \dfrac{d}{2}\right\} & \text{if } \Omega > e-3 \text{ or } d = \dfrac{q-1}{2}, \\ \left(\dfrac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{\dfrac{d}{4}, \dfrac{3d}{4}\right\} & \text{if } \Omega = e-3, \end{cases}$$

2. $a+1 = \alpha^{k_1(1-m)}$ and $a-1 = \alpha^{k_2(1-m)}$, for some k_1 even and k_2 odd.

Proof. ($\Rightarrow$) Since $f(x)$ is an involution, then $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ by Corollary 4.3. But $e \geq 4$ and $f = e-1$, therefore, $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where $k = \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t$ for $t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\}$ by Theorem 4.40. By Lemma 4.45, we know $d \in \{g, 2g\}$. Then $d = g$, since if $d = 2g$, then $f(x)$ would have $4g+1$ fixed points

which is a contradiction to Theorem 3.13. This implies that $f(x)$ has $2g+1$ fixed points and, by Proposition 4.21, Condition 2 holds.

Note that $\Omega \geq e-3$ or $q-1=2d$ by Lemma 4.50. Suppose $t \in \left\{0, \frac{d}{2}\right\}$ and $\Omega = e-3$. Then by Statement 1 of Proposition 4.51, $d=2g$, which is a contradiction, therefore $\Omega > e-3$ or $d=\frac{q-1}{2}$. Similarly, suppose that $t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}$. Note that by Statement 2 of Proposition 4.51, $\Omega > e-3$ implies that $d=2g$ which is a contradiction. Therefore, $\Omega = e-3$. This implies that Condition 1 holds.

($\Leftarrow$) By Proposition 4.51, Condition 1 implies that $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$ and $d=g$. Then, by Proposition 4.21, $f(x)$ is an involution with $2g+1=2d+1$ fixed points.

□

Note that the cases for e and f in Table 4.45.1 are independent. Also note that, in the propositions where $f(x)$ has $\frac{d}{2}+1$ fixed points, Conditions 2, 3 and 4 are the same. This means that we can join all of the cases for involutions with $\frac{d}{2}+1$ fixed points. We can also do this for involutions with $d+1$ and $2d+1$ fixed points. We summarize Propositions 4.52 through 4.63 in the following theorems.

The propositions summarized in Theorem 4.64 are: Propositions 4.52, 4.56, 4.59 and 4.61. Note that all involutions generated with Theorem 4.64 have exactly $g+1$ fixed points.

Theorem 4.64. Let $q-1=2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 1$, $d=2^f p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, α be a primitive element of $\mathbb{F}_q$, and, if $q-1 \neq 2d$, $\Omega = \nu_2\Big(\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)}-1\Big)$. Then $f(x)=x^m(x^{\frac{q-1}{2}}+a)$ is an involution of $\mathbb{F}_q$ with exactly $\frac{d}{2}+1$ fixed points if and only if the following conditions hold:

1. $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = \begin{cases} 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\}, & \text{if } f = e, \\ \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}, & \text{if } f = 2 \text{ and } e = 3, \text{ or} \\ & f = e-1, \Omega > e-3 \\ & \text{or } d = \frac{q-1}{2}, \text{ and } e \geq 4, \\ \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\}, & \text{if } f = 2 \text{ and } e \geq 4, \\ \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\}, & \text{if } f = e-1, \Omega = e-3 \\ & \text{and } e \geq 4, \end{cases}$$

2. $\eta(a^2 - 1) = (-1)^{m+1}$,

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

4. Either $a + 1 = \alpha^{k_1(1-m)}$ or $a - 1 = \alpha^{k_2(1-m)}$ for some k_1 even and k_2 odd.

Note that Proposition 4.54 generates involutions with $d + 1$ fixed points that have either square or non-square non-zero fixed points; Propositions 4.53 and 4.60 generate involutions with both square and non-square fixed points; and Propositions 4.57 and 4.62 generate both involutions with $g + 1$ and $2g + 1$ fixed points. These are the cases summarized in Theorem 4.66.

Theorem 4.65. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 1$, $d = 2^f p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, α be a primitive element of $\mathbb{F}_q$, and, if $q - 1 \neq 2d$, $\Omega = \nu_2\Big(\left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)} - 1\Big)$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $d + 1$ fixed points if and only if exactly one of the following conditions hold:

1. (a) $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = \begin{cases} 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\}, & \text{if } f = e, \\ \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}, & \text{if } f = 2 \text{ and } e = 3, \text{ or} \\ & f = e-1, \Omega > e-3 \\ & \text{or } d = \frac{q-1}{2}, \text{ and } e \geq 4, \\ \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \frac{d}{4}, \frac{d}{2}, \frac{3d}{4}\right\}, & \text{if } f = 2 \text{ and } e \geq 4, \\ \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\}, & \text{if } f = e-1, \Omega = e-3 \\ & \text{and } e \geq 4, \end{cases}$$

   (b) $a + 1 = \alpha^{k_1(1-m)}$ and $a - 1 = \alpha^{k_2(1-m)}$ for some k_1 even and k_2 odd.

2. (a) $m \equiv \left(\frac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = \begin{cases} 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\}, & \text{if } f = 1 \text{ and } e \geq 2, \\ \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \frac{d}{2}\right\}, & \text{if } f = 2 \text{ and } e = 3, \text{ or} \\ & f = e-1, \Omega > e-3 \\ & \text{or } d = \frac{q-1}{2}, \text{ and } e \geq 4, \\ \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\}, & \text{if } f = e-1, \Omega = e-3 \\ & \text{and } e \geq 4, \end{cases}$$

   (b) $\eta(a^2 - 1) = (-1)^{m+1}$

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

   (d) Either $a + 1 = \alpha^{k_1(1-m)}$ or $a - 1 = \alpha^{k_2(1-m)}$ for some k_1 even and k_2 odd.

Similar to the previous cases, although we know that involutions with $2d + 1$ fixed points are involutions with $2g + 1$ fixed points, we do not need to know

the value of g to generate these involutions. Theorem 4.66 includes the Propositions 4.55, 4.58 and 4.63.

Theorem 4.66. Let $q-1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 2$, $d = 2^f p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$ where $\ell_s \in \{0, e_s\}$, α be a primitive element of $\mathbb{F}_q$, and, if $q-1 \neq 2d$, $\Omega = \nu_2\Big(\big(\frac{q-1}{2d}\big)^{\phi\left(\frac{d}{4}\right)} - 1\Big)$. Then $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ is an involution of $\mathbb{F}_q$ with exactly $2d+1$ fixed points if and only if the following conditions hold:

1. $m \equiv \left(\dfrac{q-1}{d}\right) k - 1 \pmod{q-1}$, where

$$k = \begin{cases} 2\left(\dfrac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t,\ t \in \left\{0, \dfrac{d}{2}\right\}, & \text{if } f = 1, \\ \left(\dfrac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{0, \dfrac{d}{2}\right\}, & \text{if } f = 2 \text{ and } e = 3, \text{ or} \\ & f = e-1, \Omega > e-3 \text{ or } d = \dfrac{q-1}{2}, \\ & \text{and } e \geq 4, \\ \left(\dfrac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t,\ t \in \left\{\dfrac{d}{4}, \dfrac{3d}{4}\right\}, & \text{if } f = e-1, \Omega = e-3 \text{ and } e \geq 4, \end{cases}$$

2. $a+1 = \alpha^{k_1(1-m)}$ and $a-1 = \alpha^{k_2(1-m)}$ for some k_1 even and k_2 odd.

Before we close this chapter, we show an example of how to use Theorems 4.64, 4.65 and 4.66 to find involutions of $\mathbb{F}_{49}$ of the form $f(x) = x^m(x^{20} + a)$, $a \in \mathbb{F}_{41}^*$, with a prescribed number of fixed points.

Example 4.67. Let $q = 41$. Then $q-1 = 2^3 \cdot 5$, that is, $e = 3$.

From Theorem 4.65, the only values of d that produce involutions with $d+1$ fixed points are $d = 2, 4$ for Condition 2 and $d = 4, 8$ for Condition 1. But before we construct involutions with Theorem 4.65, first we use Theorem 4.64 to construct involutions with $\frac{d}{2}+1$ fixed points. The only values of d for which there exists at least one a are $d = 4$ and $d = 8$.

If $d = 4$, then $f = 2$ and, since $e = 3$, by Theorem 4.64,

$$\begin{aligned} k &= \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t, \quad t \in \left\{\frac{d}{4}, \frac{3d}{4}\right\} \\ &= \left(\frac{40}{8}\right)^{\phi(1)-1} + t, \quad t \in \{1, 3\} \\ &= 1 + t. \end{aligned}$$

Hence, $k = 2$ or $k = 4$. Therefore, since $m \equiv \left(\frac{40}{4}\right) k - 1 \pmod{40}$, then $m = 19$ or $m = 39$.

For $m = 19$, the a's that satisfy Conditions 2,3 and 4 from Theorem 4.64 are $a = 17$ and $a = 24$. Similarly, for $m = 39$, the a's that satisfy Conditions 2,3 and 4 are also $a = 17$ and $a = 24$. Then involutions produced with Theorem 4.64 that have exactly $\frac{4}{2} + 1 = 3$ fixed points are the following:

m	a	**Number of fixed points**
19	17	3
	24	3
39	17	3
	24	3

Table 4.67.1: Involutions of $\mathbb{F}_{41}$ of the form $f(x) = x^m(x^{20} + a)$, $a \in \mathbb{F}_{41}^*$, produced with Theorem 4.64 and $d = 4$.

Now, if $d = 8$, then $f = 3$ and, by Theorem 4.64,

$$\begin{aligned} k &= 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t, \quad t \in \left\{0, \frac{d}{2}\right\} \\ &= 2\left(\frac{40}{8}\right)^{\phi(4)-1} + t, \quad t \in \{0, 4\} \\ &= 2(5) + t. \end{aligned}$$

Hence, $k = 10$ or $k = 14$. Since $m \equiv \left(\frac{40}{8}\right) k - 1 \equiv 5k - 1 \pmod{40}$, then $m = 9$

or $m = 29$.

For $m = 9$, there are no a's that satisfy Conditions 2,3 and 4 from Theorem 4.64. For $m = 29$, the a's that satisfy Conditions 2,3 and 4 are $a = 17$ and $a = 24$. Then involutions produced with Theorem 4.64 that have exactly $\frac{8}{2}+1 = 5$ fixed points are the following:

m	a	**Number of fixed points**
29	17	5
	24	5

Table 4.67.2: Involutions of $\mathbb{F}_{41}$ of the form $f(x) = x^m(x^{20}+a)$, $a \in \mathbb{F}_{41}^*$, produced with Theorem 4.64 and $d = 8$.

Note that the involutions produced with Theorem 4.64 have exactly $g + 1$ fixed points where $g = \gcd(m - 1, \frac{q-1}{2})$. This is clear from Condition 4 since it guarantees, by Statement 1 and 2 of Theorem 3.13, that $f(x)$ has either non-zero square or non-square fixed points. By Statement 3 of Theorem 3.13, we know this implies that $f(x)$ has $g+1$ fixed points. Similarly, Condition 2 from Theorem 4.65 also generates involutions with $g + 1$ fixed points.

We used Theorem 4.64 with $d = 4$ and $d = 8$ to construct involutions with 3 and 5 fixed points respectively. If we use Condition 2 from Theorem 4.65 with $d = 2$ and $d = 4$, then we generate involutions with 3 and 5 fixed points respectively. The involutions generated in this way are the following:

m	a	Number of fixed points
19	17	3
	24	3
39	17	3
	24	3
29	17	5
	24	5

Table 4.67.3: Involutions of $\mathbb{F}_{41}$ of the form $f(x) = x^m(x^{20} + a)$, $a \in \mathbb{F}_{41}^*$, produced with Theorem 4.65 and $d = 2, 4$.

We now use Theorem 4.66 to construct involutions with $2d + 1$ fixed points. The only values of d for which there exists at least one a are $d = 2$ and $d = 4$.

If $d = 2$, then $f = 1$ and, by Theorem 4.66,

$$\begin{aligned} k &= 2\left(\frac{q-1}{d}\right)^{\phi\left(\frac{d}{2}\right)-1} + t, \quad t \in \left\{0, \frac{d}{2}\right\} \\ &= 2\left(\frac{40}{2}\right)^{\phi(1)-1} + t, \quad t \in \{0, 1\} \\ &= 2 + t. \end{aligned}$$

Hence, $k = 2$ or $k = 3$. Therefore, since $m \equiv \left(\frac{40}{2}\right) k - 1 \pmod{40}$, then $m = 39$ or $m = 19$.

For $m = 39$, the a's that satisfy Condition 2 from Theorem 4.66 are $3, 9$ and 22. Similarly, for $m = 19$, the a's that satisfy Condition 2 are also $3, 9$ and 22. Then involutions produced with Theorem 4.66 that have exactly $2(2)+1 = 5$ fixed points are the following:

m	a	Number of fixed points
19	3	5
	2	5
	22	5
39	3	5
	9	5
	22	5

Table 4.67.4: Involutions of $\mathbb{F}_{41}$ of the form $f(x) = x^m(x^{20} + a)$, $a \in \mathbb{F}_{41}^*$, produced with Theorem 4.66 and $d = 2$.

If $d = 4$, then $f = 2$ and, by Theorem 4.66,

$$\begin{aligned} k &= \left(\frac{q-1}{2d}\right)^{\phi\left(\frac{d}{4}\right)-1} + t, \quad t \in \left\{0, \frac{d}{2}\right\} \\ &= \left(\frac{40}{8}\right)^{\phi(1)-1} + t, \quad t \in \{0, 2\} \\ &= 1 + t. \end{aligned}$$

Hence, $k = 1$ or $k = 3$. Therefore, since $m \equiv \left(\frac{40}{4}\right) k - 1 \pmod{40}$, then $m = 9$ or $m = 29$.

For $m = 9$, the only a that satisfies Condition 2 from Theorem 4.66 is $a = 17$. For $m = 29$, there are no a's that satisfy Condition 2. Then involutions produced with Theorem 4.66 that have exactly $2(4) + 1 = 8$ fixed points are the following:

m	a	Number of fixed points
9	17	9

Table 4.67.5: Involutions of $\mathbb{F}_{41}$ of the form $f(x) = x^m(x^{20} + a)$, $a \in \mathbb{F}_{41}^*$, produced with Theorem 4.66 and $d = 4$.

Note that the involutions produced with Theorem 4.66 have exactly $2g+1$ fixed

points where $g = \gcd(m-1, \frac{q-1}{2})$. This is because, by Theorem 3.13, Condition 2 of Theorem 4.66 guarantees that $f(x)$ has both non-zero square and non-square fixed points, that is, $f(x)$ has $2g+1$ fixed points. Similarly, Condition 1 from Theorem 4.65 also generates involutions with $2g+1$ fixed points.

We use Theorem 4.66 with $d = 2$ and $d = 4$. If we use Condition 1 from Theorem 4.65 with $d = 4$ and $d = 8$, the involutions generated are the following:

m	a	**Number of fixed points**
19	3	5
	9	5
	22	5
39	3	5
	9	5
	22	5
9	17	9

Table 4.67.6: Involutions of $\mathbb{F}_{41}$ of the form $f(x) = x^m(x^{20}+a)$, $a \in \mathbb{F}_{41}^*$, produced with Theorem 4.65 and $d = 4, 8$.

Note that the involutions generated with Theorem 4.64, shown in Tables 4.67.1 and 4.67.2, are exactly the same as those generated by Condition 2 of Theorem 4.65, shown in Table 4.67.3. Also note that the involutions generated with Theorem 4.66 are the same as those generated by Condition 1 of Theorem 4.65—we can corroborate this by revising Tables 4.67.4, 4.67.5, and 4.67.6.

To verify if we generated all of the involutions of $\mathbb{F}_{41}$ of the form $f(x) = x^m(x^{20}+a), a \in \mathbb{F}_{41}^*$, we implement Algorithm 2 and compare both results.

d	m	a	Number of fixed points
2	19	17	3
		24	3
	39	17	3
		24	3
4	19	3	5
		9	5
		22	5
	29	17	5
		24	5
	39	3	5
		9	5
		22	5
8	9	17	9

(a)

m	a	Number of fixed points
9	17	9
19	24	3
	3	5
	22	5
	9	5
	17	3
29	24	5
	17	5
39	24	3
	3	5
	22	5
	9	5
	17	3

(b)

Table 4.67.7: Table (a) lists involutions of $\mathbb{F}_{41}$ of the form $f(x) = x^m(x^{20} + a)$, $a \in \mathbb{F}_{41}^*$, produced with Theorem 4.65 for $d = 2, 4, 8$. Table (b) lists all involutions of $\mathbb{F}_{41}$ of the form $f(x)$ with more than one fixed point generated by Algorithm 2. On Table (b), the number of fixed points was calculated using Theorem 3.13.

Simple rearrangement of Table 4.67.7 (a) will show that these are all the involutions of $\mathbb{F}_{41}$ of the form $f(x)$ with more than one fixed point.

$\diamond$

Example 4.67 suggests that Theorem 4.65 produces all of the involutions of $\mathbb{F}_q$ of the form $f(x)$ that have more than one fixed point. Computationally, this is true up to $q \leq 1499$.

Conjecture 4.68. Let $q - 1 = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $e \geq 1$, m be a positive integer and $a \in \mathbb{F}_q{}^*$. All of the involutions of $\mathbb{F}_q$ of the form $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ that have more than one fixed point are given by Theorem 4.65.

The following example gives us an idea of how involutions constructed using Theorems 4.64 and 4.66 with certain values of d can also be constructed using Theorem 4.65.

Example 4.69. Let $q-1 = 2^2 p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Note that $e = 2$. For this example, we use the m_{ij} notation from Section 4.3.1.

Consider using Theorem 4.66 with $f_1 = 1$. This produces m_{11} and m_{12}; we can find a's in ${\mathbb{F}_q}^*$ that satisfy Condition 2 of Theorem 4.66 to construct involutions with $2d_1 + 1$ fixed points. Now, consider using Theorem 4.65 with $f_2 = e = 2$ and $d_2 = 2d_1$. This produces m_{21} and m_{22} which, by Proposition 4.35, are equivalent to m_{11} and m_{12} modulo $q-1$, respectively. If we find a's that satisfy Condition 1(b) of Theorem 4.65, we construct involutions with $d_2 + 1 = 2d_1 + 1$ fixed points. But Condition 1(b) of Theorem 4.65 is the same as Condition 2 from Theorem 4.66, hence, we construct the same involutions with both theorems. This is an example of how we can write d's that we can use with Theorem 4.66 as other d's that we can use with Theorem 4.65 to construct the same involutions.

Now let us see a similar example using Theorem 4.64. Consider using Theorem 4.64 with $f_2 = e = 2$. This produces m_{21} and m_{22}. If there exists $a \in {\mathbb{F}_q}^*$ that satisfies Conditions 2, 3 and 4 from Theorem 4.64, we construct involutions with $\frac{d_2}{2} + 1$ fixed points. Similar to the previous case, using Theorem 4.65 with $f_1 = 1$ and $d_1 = \frac{d_2}{2}$, produces m_{11} and m_{12}. If there exists $a \in {\mathbb{F}_q}^*$ that satisfies Conditions 2(b), 2(c) and 2(d) from Theorem 4.65, we construct involutions with $d_1 + 1 = \frac{d_2}{2} + 1$ fixed points. By Proposition 4.35, $m_{11} \equiv m_{22} \pmod{q-1}$ and $m_{12} \equiv m_{21} \pmod{q-1}$. Since Conditions 2(b), 2(c) and 2(d) from Theorem 4.65 are the same as Conditions 2, 3 and 4 from Theorem 4.64, these values of d produce the same involutions with both theorems.

$\diamond$

▷ Summary

At the beginning of Chapter 4, we gave a characterization of involutions of $\mathbb{F}_q$ of the form $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ with more than one fixed point. In Section 4.2, we provided formulas for m that were solutions to $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$, a condition that is necessary for involutions of $\mathbb{F}_q$ of the form $f(x)$. In Section 4.3, we showed that all of the solutions to $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$ are generated by the formulas we provided for m; we did this by counting the distinct m's generated with the formulas and showing that they are the same as the amount of solutions of $x^2 \equiv 1 \pmod{\frac{q-1}{2}}$. Note that Theorem 4.40 gives a refinement of Zheng et al.'s Theorem (Theorem 4.2) with $s = \frac{q-1}{2}$ since we provide explicit formulas that are equivalent to the first condition of Zheng et al.'s Theorem for polynomial involutions of the form $x^m h(x^{\frac{q-1}{2}})$; these formulas are given in terms of a variable d. At the beginning of Section 4.4, we related the variable d with $g = \gcd(m-1, \frac{q-1}{2})$ and with the number of fixed points of involutions of the form $f(x)$. We closed this chapter by providing a characterization of involutions of $\mathbb{F}_q$ of the form $f(x)$ that allows us to construct all such involutions with a prescribed number of fixed points.

Chapter 5

Conclusions

In this work, we characterize involutions of $\mathbb{F}_q$ of the form $f(x) = x^m(x^{\frac{q-1}{2}} + a)$ with a prescribed number of fixed points, presenting formulas for m related to the number of fixed points, which is the main contribution of this thesis. By doing this, we expand the work on monomial involutions of $\mathbb{F}_q$ done by Castro et al. to the binomial $f(x)$. We also count the number of m's that produce distinct involutions of $f(x)$ and provide explicit formulas for these m's that are equivalent to the solutions of $m^2 \equiv 1 \pmod{\frac{q-1}{2}}$. This gives, as a consequence, a refinement of Zheng et al.'s Theorem for polynomial involutions of $\mathbb{F}_q$ of the form $x^m h(x^{\frac{q-1}{2}})$. In Chapter 3, we give a characterization of the fixed points of $f(x)$ that tells us when and how many fixed points $f(x)$ has, as well as formulas for calculating them.

The next step to continue the work on involutions of $\mathbb{F}_q$ of the form $f(x)$ would be to prove if Conjecture 4.68 holds, that is, if all of the involutions of $\mathbb{F}_q$ of the form $f(x)$ with more than one fixed point are generated by Theorem 4.65. After this, a possible next step would be to characterize involutions that only have 0 as a fixed point. Another possible future work would be to find explicit formulas for a that also depend on the number of fixed points. To find such formulas for a, it would also be beneficial to be able to count all of the involutions $f(x)$ of $\mathbb{F}_q$.

Bibliography

[1] Burton, D. M. (1989). *Elementary Number Theory* (2 ed.)., Chapter 7, pp. 156. Wm. C. Brown Publishers.

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

[3] Charpin, P., S. Mesnager, and S. Sarkar (2015). On involutions of finite fields. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 186–190.

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

[5] Cáceres, A. and O. Colón-Reyes (1997, Sept). Some criteria for permutation binomials. Preprint. University of Puerto Rico at Humacao.

[6] Gong, Z., S. Nikova, and Y. W. Law (2012). Klein: A new family of lightweight block ciphers. In A. Juels and C. Paar (Eds.), *RFID. Security and Privacy*, pp. 1–18. Springer Berlin Heidelberg.

[7] Ireland, K. and M. Rosen (1990). *A Classical Introduction to Modern Number Theory* (2 ed.), Volume 84 of *Graduate Texts in Mathematics*, Chapter 3, pp. 31–36. Springer-Verlag New York.

[8] Kong, J. H., L.-M. Ang, and K. P. Seng (2015). A comprehensive survey

of modern symmetric cryptographic solutions for resource constrained environments. *Journal of Network and Computer Applications 49*, 15–50.

[9] Landau, E., P. T. Bateman, and E. E. Kohlbecker (1958). *Elementary number theory*, Volume 125, Chapter 4 and 6, pp. 37–52 and 62–64. Chelsea Publishing Company Incorporated.

[10] Pacheco-Tallaj, N. (2015, December). Monomial permutations that generate involutions with more than three fixed points. Technical report, University of Puerto Rico, Río Piedras.

[11] Park, Y. H. and J. B. Lee (2001). Permutation polynomials and group permutation polynomials. *Bulletin of the Australian Mathematical Society 63*(1), 67–74.

[12] Rubio, I. M. and C. J. Corrada-Bravo (2003). Cyclic decomposition of permutations of finite fields obtained using monomials. In *International Conference on Finite Fields and Applications*, pp. 254–261. Springer.

[13] Sakzad, A., D. Panario, M.-R. Sadeghi, and N. Eshghi (2010). Self-inverse interleavers based on permutation functions for turbo codes. In *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 22–28.

[14] Takeshita, O. (2006). On maximum contention-free interleavers and permutation polynomials over integer rings. *IEEE Transactions on Information Theory 52*(3), 1249–1253.

[15] Wang, Q. (2007). Cyclotomic mapping permutation polynomials over finite field. In *Sequences, Subsequences, and Consequences*, Volume 4893 of *Lecture Notes in Computer Science*, pp. 119–128. Springer, Berlin, Heidelberg.

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

[17] Zheng, D., M. Yuan, N. Li, L. Hu, and X. Zeng (2019). Constructions of involutions over finite fields. *IEEE Transactions on Information Theory 65*(12), 7876–7883.

[18] Zieve, M. E. (2009). On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{\frac{q-1}{2}})$. In *Proceedings of the American Mathematical Society*, Volume 137, pp. 2209–2216.