Some Results Concerning Permutation Polynomials over Finite Fields

Stephen Lappano
University of South Florida, slappano@mail.usf.edu

Follow this and additional works at: http://scholarcommons.usf.edu/etd
Part of the Mathematics Commons

Scholar Commons Citation

This Thesis is brought to you for free and open access by the Graduate School at Scholar Commons. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Scholar Commons. For more information, please contact scholarcommons@usf.edu.
Some Results Concerning Permutation Polynomials over Finite Fields

by

Stephen Lappano

A dissertation submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy
Department of Mathematics and Statistics
College of Arts and Sciences
University of South Florida

Major Professor: Xiang-dong Hou, Ph.D.
Brian Curtin, Ph.D.
Mohamed Elhamdadi, Ph.D.
Dmytro Savchuk, Ph.D.

Date of Approval:
June 28, 2016

Keywords: Finite field, Permutation polynomial, Dickson polynomial, Hermite Criterion, Trinomial, Binomial, Monomial Graph

Copyright © 2016, Stephen Lappano
Acknowledgments

I would first like to thank my advisor, Dr. Xiang-dong Hou, for his guidance, support, and patience. Without his input this work would have not been a success. I hope to one day see as deeply as he does.

I would also like to thank my committee members Dr. Brian Curtin, Dr. Mohamed Elhamdadi, and Dr. Dymtro Savchuk for taking the time to read this dissertation and providing their input as well as Dr. Ke Qin Feng for chairing the defense. I am grateful to Dr. Leslaw Skrzypek and Dr. Stephen Suen for giving me the opportunity to develop as an educator as well as the front office staff for their support in various ways.

I would like to thank my family and friends for their support and encouragement in times of need. A special thank you goes out to tennis professional Eric Dobsha, without him and his students I would never have stayed sane during this process.

Last, but certainly not least, I would like to thank God Almighty, through whom all things are possible.
# Table of Contents

List of Tables iv

Abstract v

1 Introduction 1
   1.1 Dickson polynomials and their offspring 4
   1.2 Permutation binomials and trinomials of $\mathbb{F}_{q^2}$ taking a special form 7
   1.3 Permutation polynomials and cryptography 9

2 The Polynomial $g_{n,q}$ 12
   2.1 Background 12
   2.2 Desirable Triples of the form $(q^a - q^b - 1, e; q)$ 16
   2.3 Desirable Triples of the form $(q^a - q^b - 1, 2; q)$ 20
   2.4 Connection between $g_{n,q}$ and PPs of the form $f = x(a + x^{2(q-1)})$ 30

3 Permutation Polynomials of the form $f = x^d(a + bx^{q-1} + x^{r(q-1)})$ 36
   3.1 Background 36
   3.2 PPs of the form $f = x(a + x^{r(q-1)})$ 39
      Computations 41
      Proof of Theorem 3.2.3 46
   3.3 PPs of the form $f = x^3(a + x^{2(q-1)})$ 48
3.4 PPs of the form $f = x^3(a + bx^{a-1} + x^{2(q-1)})$

3.5 Technical Lemmas

4 Permutation Polynomials of the form $x^{1+2^k} + L(x)$

4.1 Background

4.2 $L(x) = (x + x^{2^k})^{2^{k+1}}$ or $L(x) = (x + x^{2^k})^{2^{k+1}}$

5 On Monomial Graphs of Girth Eight

5.1 Background

Prior Status of Conjecture A

Prior Status of Conjecture B

5.2 Power Sums of $A_k$ and $B_k$

5.3 Facts concerning $A_k$ and $B_k$

5.4 A Theorem on $A_k$

5.5 A Theorem on $B_k$

5.6 A Theorem on monomial graphs of girth eight

6 Conclusion

7 References

8 Appendices

8.1 Appendix A - Copyrights and Permissions
List of Tables

2.1 Desirable triples \((q^a - q^b - 1, 2; q)\), \(q \leq 97\), \(0 < b < a < 2p\), \(b\) odd, \(b \neq p\),

\((a, b) \neq (2, 1)\)
Abstract

Let $p$ be a prime, $q$ a power of $p$ and $\mathbb{F}_q$ the finite field with $q$ elements. Any function $\phi : \mathbb{F}_q \to \mathbb{F}_q$ can be uniquely represented by a polynomial, $f_{\phi}$ of degree $< q$. If the map $x \mapsto f_{\phi}(x)$ induces a permutation on the underlying field we say $f_{\phi}$ is a permutation polynomial. Permutation polynomials have applications in many diverse fields of mathematics. In this dissertation we are generally concerned with the following question: Given a polynomial $f$, when does the map $x \mapsto f(x)$ induce a permutation on $\mathbb{F}_q$?

In the second chapter we are concerned the permutation behavior of the polynomial $g_{n,q}$, a $q$-ary version of the reversed Dickson polynomial, when the integer $n$ is of the form $n = q^a - q^b - 1$. This leads to the third chapter where we consider binomials and trinomials taking special forms. In this case we are able to give explicit conditions that guarantee the given binomial or trinomial is a permutation polynomial.

In the fourth chapter we are concerned with permutation polynomials of $\mathbb{F}_q$, where $q$ is even, that can be represented as the sum of a power function and a linearized polynomial. These types of permutation polynomials have applications in cryptography. Lastly, chapter five is concerned with a conjecture on monomial graphs that can be formulated in terms of polynomials over finite fields.
Let $p$ be a prime and $q$ a power of $p$ (i.e. $q = p^e, z \in \mathbb{N}$). We use $\mathbb{F}_q$ to denote the (unique) finite field consisting of $q$ elements and $\overline{\mathbb{F}}_q$ to denote its algebraic closure. Finite fields are *polynomially complete* in the sense that any function $\phi : \mathbb{F}_q \rightarrow \mathbb{F}_q$ can be represented by a polynomial. Further, if we require the degree of this polynomial to be less than $q$, the polynomial representation of $\phi$ is unique. Given a function $\phi : \mathbb{F}_q \rightarrow \mathbb{F}_q$, the unique polynomial of degree less than $q$ representing $\phi$, $f_\phi$, is given by

$$f_\phi(x) = \sum_{a \in \mathbb{F}_q} \phi(a) \left(1 - (x - a)^{q-1}\right).$$

(1.0.1)

The fact that $\mathbb{F}_q$ is polynomially complete was first noted by Hermite [35] when $q$ is prime and by Dickson [16] for general $q$. In fact Redei and Szele [79] showed that the only non zero commutative rings that are polynomially complete are the finite fields; Heisler [33] obtained the same result without the assumption of commutativity.

A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (PP) if the associated polynomial function $c \mapsto f(c)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$. Because of the finiteness of $\mathbb{F}_q$, the definition of a permutation polynomial can be expressed in the following way.

**Lemma 1.0.1** ([64]) A polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if one of the following conditions hold:

(i) the function $f : c \mapsto f(c)$ is onto;

(ii) the function $f : c \mapsto f(c)$ is one-to-one;
(iii) $f(x) = a$ has a solution for each $a \in \mathbb{F}_q$;

(iv) $f(x) = a$ has a unique solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$;

(v) The polynomial $\frac{f(x) - f(y)}{x - y} \in \mathbb{F}_q[x, y]$ has no roots $(x, y) \in \mathbb{F}_q^2$ with $x \neq y$.

The general study of permutation polynomials of the prime fields originates with Hermite [35] while Dickson was the first to study permutation polynomials over arbitrary finite fields [16]. The study of permutation polynomials is a major subject in the theory and applications of finite fields. In fact, many problems involving finite fields can be reduced to permutation properties of polynomials. For an early history of the subject see [18].

The study of permutation polynomials over finite fields is essentially about relations between the algebraic and combinatorial structures of finite fields. Nontrivial permutation polynomials are often the result the sometimes mysterious interplay between the two structures. Permutation polynomials have applications in finite geometries, coding theory, computer science, cryptography, and various other fields.

A main question concerning permutation polynomials is how to recognize them. To this end we have the following theorem, which was first established by Hermite for the prime fields and Dickson for arbitrary finite fields.

**Theorem 1.0.2 (Theorem 7.4 [64]) (Hermite’s Criterion).** Let $\mathbb{F}_q$ be of characteristic $p$. Then $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions hold:

(i) $f$ has exactly one root in $\mathbb{F}_q$;

(ii) for each integer $s$ with $1 \leq s \leq q - 2$ and $s \not\equiv 0 \pmod{p}$, the reduction of $f(x)^s \pmod{(x^q - x)}$ has degree $\leq q - 2$.

The first condition of the above theorem is clearly equivalent to:

$$\sum_{x \in \mathbb{F}_q} f(x)^{q-1} = q - 1.$$
While the second is equivalent to:

$$\sum_{x \in \mathbb{F}_q} f(x)^s = 0 \quad 1 \leq s \leq q - 2.$$ 

Thus a reformulation of Hermite’s Criterion is given by the following theorem.

**Theorem 1.0.3** Let $f \in \mathbb{F}_q[x]$. Then $f$ is a permutation polynomial of $\mathbb{F}_q$ if and only if

$$\sum_{x \in \mathbb{F}_q} f(x)^s = \begin{cases} 
0 & \text{if } 1 \leq s \leq q - 2 \\
-1 & \text{if } s = q - 1.
\end{cases}$$

Another useful result for determining (or constructing) permutation polynomials is the following, which is commonly referred to as the Akbary-Ghioca-Wang (AGW) criterion.

**Theorem 1.0.4 ([1])** Let $A$, $S$ and $\bar{S}$ be finite sets such that $|S| = |\bar{S}|$, and let $f : A \to B$, $\bar{f} : S \to \bar{S}$, $\lambda : A \to S$ and $\bar{\lambda} : A \to \bar{S}$ be mappings such that $\lambda$ and $\bar{\lambda}$ are onto and $\bar{\lambda} \circ f = \bar{f} \circ \lambda$. Then, the following statements are equivalent.

(i) $f$ is a permutation of $A$.

(ii) $\bar{f}$ is a bijection and $f$ is one-to-one on $\lambda^{-1}(s)$ for all $s \in S$.

Permutation polynomials with no additional requirements are not hard to construct, pick your favorite permutation of $\mathbb{F}_q$ and construct a polynomial representing this permutation using (1.0.1). In general the study of permutation polynomials is concerned with polynomials that have an especially simple algebraic appearance, for instance polynomials containing only a few terms, or polynomials that possess other extraordinary qualities. These extraordinary qualities are usually demanded by the applications of the permutation polynomial in question. For example, in cryptographic applications we may require a high degree of non-linearity in the permutation polynomial; for geometric applications we may require both the maps $x \mapsto f(x)$ and $x \mapsto \frac{f(x)}{x}$ to be permutations on $\mathbb{F}_q$.
While the criteria listed in Lemma 1.0.1, Theorem 1.0.2 and Theorem 1.0.3 are often useful in proving a given function is indeed a permutation polynomial, the simple ideas should not be equated with methods. A vast majority of the research on permutation polynomials is concerned with developing methods to apply the above criteria in certain situations. The remainder of this introduction is devoted to providing background and results related to the topics discussed in the following chapters of this dissertation. Throughout this dissertation, letters in typewriter font, \(x, y, z\) are reserved for indeterminants, while letters in standard font \(x, y, z\) are reserved for elements of a given finite field. We write \(\mathbb{N}_{\mathbb{F}_{q^e}}\) and \(T_{\mathbb{F}_{q^e}/\mathbb{F}_{q^j}}\) for the norm and trace maps from \(\mathbb{F}_{q^e}\) to \(\mathbb{F}_{q^j}\).

1.1 Dickson polynomials and their offspring

Let \(n \in \mathbb{N}\). It is known that the polynomials \(x_1x_2\) and \(x_1 + x_2\) generate the ring of symmetric polynomials in \(\mathbb{Z}[x_1, x_2]\) so there is a unique polynomial \(D_n(x_1, x_2) \in \mathbb{Z}[x_1, x_2]\) such that

\[
x_1^n + x_2^n = D_n(x_1 + x_2, x_1x_2).
\]

The explicit form of \(D_n(x_1, x_2)\) is given by Warings formula \[64\], we have

\[
D_n(x_1, x_2) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-x_2)^j x_1^{n-2j}.
\]  

(1.1.2)

For a fixed \(a \in \mathbb{F}_q\), \(D_n(x, a)\) is the Dickson polynomial of degree \(n\) and parameter \(a\) over \(\mathbb{F}_q\). Working over the complex numbers, the Dickson polynomials are closely related to the Chebyshev polynomials of the first kind \(T_n(x) = \cos (n \arccos (x))\); in fact \(D_n(2xa, a^2) = 2a^n T_n(x)\). Notice by (1.1.2) we have

\[
D_n(x, ab^2) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-a)^j b^k b^{-(k-2j)} x^{k-2j} = b^k D_n(b^{-1}x, a).
\]
Thus if $q$ is even then every Dickson polynomial $D_n(x, a), a \in \mathbb{F}_q^*$ over $\mathbb{F}_q$ can be expressed in terms of $D_n(x, 1)$; if $q$ is odd then every Dickson polynomial $D_n(x, a), a \in \mathbb{F}_q^*$ can be expressed in terms of $D_n(x, 1)$ and $D_n(x, c)$ for a fixed non square $c \in \mathbb{F}_q^*$. Also notice $D_n(x, 0) = x^n$.

The permutation behavior of the Dickson polynomials, $D_n(x, a)$, over $\mathbb{F}_q$ is completely known. If $a = 0$, then $D_n(x, a) = x^n$ so $D_n(x, a)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $gcd(n, q - 1) = 1$. If $a \in \mathbb{F}_q^*$, then we have the following theorem:

**Theorem 1.1.1 (Theorem 7.16 [64])** The Dickson polynomial $D_n(x, a), a \in \mathbb{F}_q^*$, is a permutation polynomial of $\mathbb{F}_q$ if and only if $gcd(n, q^2 - 1) = 1$.

Dickson polynomials are connected to a famous conjecture of Schur[81] to the effect that any $f \in \mathbb{Z}[x]$ that is a permutation polynomial of $\mathbb{F}_p$ for infinitely many primes $p$ must be a composition of binomials of the form $ax^n + b$ and Dickson polynomials. After several partial results by different authors, Schur’s conjecture was proved completely by Fried [27].

The reversed Dickson polynomial is obtained from the Dickson polynomial by reversing the roles of the variable and the parameter. There is a connection between the reversed Dickson polynomial and *almost perfect nonlinear* (APN) functions (see Definition 1.3.1).

**Theorem 1.1.2 (Hou, Mullen, Sellers, Yucas [49])** Let $p$ be a prime and $n$ be a positive integer. Further assume that $n$ is odd when $p > 2$. Then, we have the following relations:

$$x^n \text{ is APN on } \mathbb{F}_{p^e} \Rightarrow D_n(1, x) \text{ is a PP of } \mathbb{F}_{p^e} \Rightarrow x^n \text{ is APN on } \mathbb{F}_{p^e}.$$ 

For the reversed Dickson polynomial we have

$$D_n(0, x) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ 2(-x)^k & \text{if } n = 2k, \end{cases}$$
so $D_n(0, x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $n = 2k$ and $gcd(k, q-1) = 1$. When $a \in \mathbb{F}_q^*$, we have

$$D_n(a, x) = a^n D_n(1, \frac{x}{a^2}),$$

so we only need to consider $D_n(1, x)$. Unlike the Dickson polynomial, the permutation behavior of the reversed Dickson polynomial is not completely known. We have the following conjecture for the prime fields.

**Conjecture 1.1.3 (Hou, Mullen, Sellers, Yucas [49])** Let $p > 3$ be a prime, and let $1 \leq n \leq p^2 - 1$. Then, $D_n(1, x)$ is a PP on $\mathbb{F}_p$ if and only if

$$n = \begin{cases} 
2, 2p, 3, 3p, p + 1, p + 2, 2p + 1 & \text{if } p \equiv 1 \pmod{12}, \\
2, 2p, 3, 3p, p + 1 & \text{if } p \equiv 5 \pmod{12}, \\
2, 2p, 3, 3p, p + 2, 2p + 1 & \text{if } p \equiv 7 \pmod{12}, \\
2, 2p, 3, 3p & \text{if } p \equiv 11 \pmod{12}.
\end{cases}$$

See [49] for more information regarding reversed Dickson polynomials.

In characteristic 2, the functional equation for $D_n(1, x)$ can be expressed as

$$D_n(1, x^2 - x) = x^n + (1 - x)^n = \sum_{a \in \mathbb{F}_2} (x + a)^n.$$

X. Hou [39] introduced the polynomial $g_{n,q} \in \mathbb{F}_p[x]$ (where $p$ is the characteristic of $\mathbb{F}_q$) as a $q$-ary generalization of the reversed Dickson polynomial in characteristic 2. The polynomial $g_{n,q}$ satisfies the functional equation

$$g_{n,q}(x^q - x) = \sum_{a \in \mathbb{F}_q} (x + a)^n.$$

This family of polynomials is a rich source of permutation polynomials; completely determining the permutation behavior of $g_{n,q}$ is an open and challenging problem. Results concerning the permutation behavior of the polynomial $g_{n,q}$ is precisely the topic of the second chapter.
1.2 Permutation binomials and trinomials of $\mathbb{F}_{q^2}$ taking a special form

An early systematic study of permutation polynomials of the form $x^d h(x^{(q-1)/t})$, where $t \mid q-1$, $1 \leq d \leq (q-1)/t$ and $h \in \mathbb{F}_q[x]$, can be found in [83]. A criterion, equivalent to Theorem 1.2.1, for a polynomial of this form to be a permutation polynomial of $\mathbb{F}_q$ was given in [83]. In fact, this criterion has been rediscovered independently by several different authors ([73], [84], [88]). Let $\mu_t$ denote the set of $t$-th roots of unity in $\mathbb{F}_q$. We have the following theorem

**Theorem 1.2.1 ([73],[84],[88])** Let $d$ and $t$ be positive integers with $t \mid q-1$. Let $f = x^d h(x^{(q-1)/t})$, where $h \in \mathbb{F}_q[x]$. Then, $f$ is a PP of $\mathbb{F}_q$ if and only if

(i) $\gcd(d, \frac{q-1}{t}) = 1$

(ii) $x^d h(x^{\frac{q-1}{t}})$ permutes $\mu_t$.

The above theorem is actually a special case of Theorem 1.0.4, with $A = \mathbb{F}_q$, $S = \mathbb{F}$ = $\mu_t$, $\lambda = \lambda = x^{(q-1)/t}$ and $f = x^d h(x)^{(q-1)/t}$. The key step in applying Theorem 1.2.1 is verifying that $x^d h(x)^{\frac{q-1}{t}}$ permute the set of $t$-th roots of unity. Unfortunately this is not an easy question in general.

The simplest types of polynomials are those involving few terms. While the permutation behavior of a monomial mapping of $\mathbb{F}_q$ is completely understood, $x \mapsto x^n$ is a permutation of of $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$, the situation for polynomials involving more than one term is quite complicated. It is worth mentioning that the simplicity as a polynomial is not equivalent to simplicity as a permutation on $\mathbb{F}_q$. For example, using (1.0.1), we can see the polynomial $f_a$ ($a \neq 0$), that induces the transposition $(0a)$, is given by

$$f_a(x) = -a^2 \left[ ((x-a)^{q-2} + a^{-1})^{q-2} - a \right]^{q-2}.$$

Even for permutation binomials the situation is complex. Several authors have considered permutation binomials, but it seems a complete determination of permutation binomials over finite fields is out of reach for the time being. The following
nonexistence result of Niederreiter and Robinson is one of the earliest dealing with a general binomial.

**Theorem 1.2.2 ([71])** Let \( f = ax^n + x^m \in \mathbb{F}_q[x] \), where \( a \neq 0 \) and \( m > 2 \) is not a power of the characteristic of \( \mathbb{F}_q \). If \( q \geq (m^2 - 4m + 6)^2 \), then \( f \) is not a permutation polynomials of \( \mathbb{F}_q \).

For more background and similar results see the survey [46].

Given a binomial \( f = ax^n + x^m \in \mathbb{F}_q[x] \), we can transform \( f \) into the form

\[
    f = x^n(a + x^{\frac{q-1}{t}})
\]

where \( t | q - 1 \); (see [46]). Thus for a generic binomial one can use Theorem 1.2.1; the difficulty lies in verifying condition (ii). Some of the results in chapter 3 are concerned with a binomial of the form \( x(a + x^{r(q-1)}) \in \mathbb{F}_{q^2}[x] \). In this case, condition (ii) of Theorem 1.2.1 is precisely verifying that the map \( x \mapsto x(a + x^r)^{q-1} \) is a permutation on \( \mu_{q+1} \). In this special case, a method of M. Zieve can be used to construct bijective maps (via degree one rational functions) from \( \mu_{q+1} \rightarrow \mathbb{F}_q \cup \{\infty\} \). While this idea is not used directly in chapter 3, these "nice" maps (via degree one rational functions) can be used to prove nonexistence results for permutation binomials of the form \( x(a + x^{r(q-1)}) \) when \( q \) is big enough in relation to \( r \). We refer the interested reader to [89] for more details.

The trinomial case does not appear to be as well studied as the binomial case. While there do not seem to be criteria which guarantee a general trinomial is a permutation polynomial, there are still existence and nonexistence results considering trinomials. While studying hyperovals of projective planes, Cherowitzo ([15]) discovered a class of permutation trinomials in characteristic 2 with additional extraordinary properties.

**Theorem 1.2.3 ([15])** \( f = x^{2^m} + x^{2^m+2} + x^{3 \cdot 2^m+4} \) is an \( o \)-polynomial of \( \mathbb{F}_{2^{2m-1}} \), that is, \( f \) is a permutation polynomial of \( \mathbb{F}_{2^{2m-1}} \) with \( f(0) = 0 \) and \( f(1) = 1 \) and \( (f(x + \gamma) + f(\gamma))/x \) is a permutation polynomial of \( \mathbb{F}_{2^{2m-1}} \) for all \( \gamma \in \mathbb{F}_{2^{2m-1}} \).
Ball and Zieve discovered a class of permutation trinomials in characteristic 3 given by the following theorem.

**Theorem 1.2.4 ([2])** Let $q = 3^{2h+1}$, $\alpha = 3^{h+1}$, and $a \in \mathbb{F}_q$. Then $x^{2\alpha+3} + (ax)^{\alpha} - a^2x$ is a permutation polynomial of $\mathbb{F}_q$.

A special permutation trinomial was a key ingredient in Dobbertin’s proof the claim that $x^{2^m+3}$ is maximally nonlinear on $\mathbb{F}_{2^{2m+1}}$ (the Welch conjecture).

**Theorem 1.2.5 ([21])** $f = x^{2^{m+1}+1} + x^3 + x$ is a permutation polynomial of $\mathbb{F}_{2^{2m+1}}$.

The results contained in chapter 3 of this dissertation are concerned with binomials and trinomials of the form $x^d(a + bx^{q-1} + x^{r(q-1)})$ that are permutation polynomials of $\mathbb{F}_{q^2}$. Without additional restrictions placed on the coefficients we are able to produce suprisingly explicit results.

### 1.3 Permutation polynomials and cryptography

The fundamental objective of cryptography is to allow two people, commonly referred to as Alice and Bob, to send information over an insecure channel. Ideally this communication is such that an unknown adversary eavesdropping on the channel cannot understand what is being said. This information that Alice wishes to send is called the plaintext. Alice encrypts (using a key known to herself and Bob) this plaintext and sends the resulting ciphertext over the insecure channel. Bob, who knows the key, is able to decrypt the message and recover the plain text, while an adversary with no knowledge of the key is left in the dark.

Often times we may assume the information we wish to communicate is simply an element in $\mathbb{F}_{2^n}$. Thus the encryption of the plaintext and decryption of the ciphertext are (invertible) maps of $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Permutation polynomials can be used to construct cryptographic systems, we refer the interested reader to Levine and Brawley [61].
In an ideal world, the adversary without knowledge of the key would have no hope of recovering the plaintext. In practice much research is devoted to developing methods to “break” certain cryptographic systems. For more information regarding cryptographic systems and well known attacks we refer the reader to [82] and the references there.

In order to prevent against well known attacks, these maps used for encryption and decryption should have certain desirable properties. The differential properties of \( f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \) consist of the number of solutions to the following equation

\[
f(x + a) + f(x) = b \quad a \in \mathbb{F}_{2^n}^*, \ b \in \mathbb{F}_{2^n}.
\]

(1.3.3)

**Definition 1.3.1** A function \( f : \mathbb{F}_q \to \mathbb{F}_q \) is called almost perfect nonlinear (APN) if for each \( a \in \mathbb{F}_q^* \) and \( b \in \mathbb{F}_q \), equation (1.3.3) has at most two solutions in \( \mathbb{F}_q \).

APN functions are significant in cryptography as such a function has the highest resistance to differential cryptanalysis ([74], [3]). The nonlinearity of \( f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \) is measured through the extended Walsh transformed defined as

\[
W_f(\lambda, \gamma) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}_{2^n/2}(\gamma f(x)+\lambda x)} \quad \lambda \in \mathbb{F}_{2^n}, \ \gamma \in \mathbb{F}_{2^n}^*.
\]

(1.3.4)

**Definition 1.3.2** The linearity of a map \( f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \) is given by

\[
L(f) = \max\{|W_f(\lambda, \gamma)| : \lambda \in \mathbb{F}_{2^n}, \ \gamma \in \mathbb{F}_{2^n}^*\}.
\]

It is desirable to find mappings \( f \) with the minimum possible value for \( L(f) \). These mappings that achieve the minimum possible value for \( L(f) \) are called almost bent (AB) or maximally nonlinear. Such functions have the best resistance against linear cryptanalysis ([67]).

When \( n \) is odd, the are several classes of APN functions that may be permutations on \( \mathbb{F}_{2^n} \); when \( n \) is even the situation is not so transparent. In fact, it was a long standing conjecture that no APN permutation can exist when \( n \) is even. The
conjecture was confirmed true for \( n = 4 \) and for a class of permutation polynomials \( p(x) = \sum_{i=0}^{2^n-1} a_i x^i \in \mathbb{F}_{2^n/2}[x] \) ([38]). The only known APN permutation on \( \mathbb{F}_{2^n}, n \) even, was discovered by Browning, Dillon, McQuistan and Wolfe in 2009 ([9]).

**Definition 1.3.3** A polynomial of the form

\[
L(x) = \sum_{i=0}^{m} a_i x^{q^i} \in \mathbb{F}_q[x]
\]

is called a linearized polynomial over \( \mathbb{F}_q \). Note the map \( x \mapsto L(x) \) is a linear function on \( \mathbb{F}_q \).

In attempt to construct an APN permutation on \( \mathbb{F}_{2^n} \) one can start with a non-permuting power function, \( x^d \) and attempt to find a linearized polynomial \( L(x) \) so the sum \( x^d + L(x) \) is a permutation polynomial. It is quite obvious if the power function \( x^d \) is APN on \( \mathbb{F}_{2^n} \), then so is the sum \( x^d + L(x) \). In general it is a challenging problem to take a non-permuting function and determine if there is a matching linearized polynomial so the sum becomes a permutation polynomial. A special case of this question is considered in chapter 4. We present the proof of a conjecture of Xin Gong ([30]), see Theorem 4.2.1.
2.1 Background

Let $p$ be a prime and $q$ a power of $p$.

In $\mathbb{F}_q[x]$ we have $x^q - x = \prod_{a \in \mathbb{F}_q} (x + a)$. Let $t$ be another indeterminate and substitute $t + x$ for $x$. Then we have

$$t^q - t + x^q - x = (t + x)^q - (t + x) = \prod_{a \in \mathbb{F}_q} (t + x + a) = \sum_{k=0}^q \sigma_k((x + a)_{a \in \mathbb{F}_q})t^{q-k}, \quad (2.1.1)$$

where $\sigma_k$ is the $k$th elementary symmetric polynomial in $q$ variables. A comparison of the coefficients of $t$ on both sides of (2.1.1) tells that

$$\sigma_k((x + a)_{a \in \mathbb{F}_q}) = \begin{cases} 
1 & \text{if } k = 0, \\
-1 & \text{if } k = q - 1, \\
x^q - x & \text{if } k = q, \\
0 & \text{otherwise}. 
\end{cases}, \quad (2.1.2)$$

Let $n \geq 0$ be an integer. By Waring’s formula [64, Theorem 1.76] and (2.1.2), we have

$$\sum_{a \in \mathbb{F}_q} (x + a)^n = \sum_{\alpha(q-1)+\beta q = n} (-1)^\alpha (\alpha + \beta - 1)! n \frac{(x^q - x)^\beta}{\alpha! \beta!}$$

$$= \sum_{\frac{n}{q} \leq l \leq \frac{n}{q} - 1} \frac{(l - 1)! n}{(lq - n)! (n - l(q - 1))!} (x^q - x)^{n-l(q-1)} \quad (l = \alpha + \beta)$$

*Portions of this chapter are taken from [25] which is published in the Journal of Finite Fields and their Applications, and [26] which is published in the Journal of Discrete Mathematics.*
\[ = \sum_{\frac{n}{q} \leq l \leq \frac{n}{q-1}} \frac{n}{l} \left( n - l(q - 1) \right) (x^q - x)^{n-l(q-1)}. \]

Set
\[ g_{n,q}(x) = \sum_{\frac{n}{q} \leq l \leq \frac{n}{q-1}} \frac{n}{l} \left( n - l(q - 1) \right) x^{n-l(q-1)} \in \mathbb{Z}[x]. \]

(Note that the coefficients of \( g_{n,q}(x) \) are integers since the coefficients in Waring's formula are integers.) Then in \( \mathbb{F}_q[x] \) we have
\[ \sum_{a \in \mathbb{F}_q} (x + a)^n = g_{n,q}(x^q - x). \quad (2.1.3) \]

In fact, we may take the above functional equation as the definition of the polynomial \( g_{n,q} \). Notice when \( q = 2 \), \( g_{n,2} \) is the \( n \)-th reversed Dickson polynomial over \( \mathbb{F}_2 \). This is because in characteristic 2 we have
\[ g_{n,2}(x^2 - x) = x^n + (x + 1)^n = x^n + (1 - x)^n = D_n(1, x(1 - x)) = D_n(1, x^2 - x). \]

With this observation in hand, Hou introduced the polynomial \( g_{n,q} \) in [39] as the \( q \)-ary version of the reversed Dickson polynomial in characteristic 2. A main objective of his study was the following question: When does the map \( x \mapsto g_{n,q}(x) \) permute the finite field \( \mathbb{F}_q \)? With this in mind, we have the following definition:

**Definition 2.1.1 (Desirable triple).** If \( g_{n,q} \) is a permutation polynomial of \( \mathbb{F}_{qe} \), we say that the triple \((n, e; q)\) is desirable.

With the help of a computer it is not difficult to generate all desirable triples for a fixed (small) \( q \) and fixed \( e \). The difficulty of the problems lies in classifying these explicit triples. We consider a desirable triple classified if it belongs to a known infinite family. For the remainder of this section, we gather known results about the polynomial \( g_{n,q} \) to be used in the upcoming sections.

Like its predecessors, the Dickson and Reversed Dickson polynomials, the polynomial \( g_{n,q} \) satisfies a recurrence relation.
Proposition 2.1.2 ([40]). The polynomial $g_{n,q}$ satisfies the recurrence relation

\[
\begin{cases}
g_{0,q} = \cdots = g_{q-2,q} = 0, \\
g_{q-1,q} = -1, \\
g_{n,q} = xg_{n,q} + g_{n-q+1,q}, \quad n \geq q.
\end{cases}
\]  

(2.1.4)

Using this recurrence, it is possible to extend the definition of $g_{n,q}$ to $n < 0$, we have

\[
g_{n,q} = \frac{1}{x}(g_{n+q,q} - g_{n+1,q}).
\]

(2.1.5)

For $n < 0$, $g_{n,q} \in \mathbb{F}_p[x, x^{-1}]$, the ring of Laurent polynomials in $x$ over $\mathbb{F}_p$. Thus the functional equation in (2.1.1) holds for all $n \in \mathbb{Z}$.

Fact 2.1.3 Let $e$ be a positive integer and $p$ be the characteristic of $\mathbb{F}_q$. Every $x \in \mathbb{F}_{q^e}$ can be written as $y^q - y$ with $y \in \mathbb{F}_{q^{pe}}$.

To see this is the case, define

\[
V = \{y \in \mathbb{F}_q | y^q - y \in \mathbb{F}_{q^e}\}.
\]

The map $y \mapsto y^q - y$ is clearly a $\mathbb{F}_q$-linear $q$-to-one onto map from $V$ to $\mathbb{F}_{q^e}$ with kernel $\mathbb{F}_q$. We want to show $V \subset \mathbb{F}_{q^e}$. We can choose $\alpha \in \mathbb{F}_{q^e}$ such that $\text{Tr}_{q^e/q}(\alpha) = 1$. Then we have $\text{Tr}_{q^e/q^e}(\alpha) = \text{Tr}_{q^e/q}(\text{Tr}_{q^e/q^e}(\alpha)) = \text{Tr}_{q^e/q}(p \cdot \alpha) = 0$, so there is some $\beta \in \mathbb{F}_{q^e}$ with $\beta^q - \beta = \alpha$. It follows that

\[
V = \bigcup_{u \in \mathbb{F}_q} (u \beta + \mathbb{F}_{q^e}).
\]

Proposition 2.1.4

(i) $g_{pm,q} = g_{n,q}$.

(ii) If $n_1, n_2 > 0$ are integers such that $n_1 \equiv n_2 \pmod{q^{pe} - 1}$, then $g_{n_1,q} \equiv g_{n_2,q} \pmod{x^{q^e} - x}$.

Proof.
(i) We have
\[ g_{pn,q}(x^q - x) = \sum_{a \in \mathbb{F}_q} (x + a)^{pn} = \left( \sum_{a \in \mathbb{F}_q} (x + a)^n \right)^p = [g_{n,q}(x^q - x)]^p. \]

(ii) For all \( x \in \mathbb{F}_{q^e} \), we have
\[ g_{n_1,q}(x^q - x) = \sum_{a \in \mathbb{F}_q} (x + a)^{n_1} = \sum_{a \in \mathbb{F}_q} (x + a)^{n_2} = g_{n_2,q}(x^q - x). \]
In particular, \( g_{n_1,q}(x) = g_{n_2,q}(x) \) for all \( x \in \mathbb{F}_{q^e} \), i.e., \( g_{n_1,q} \equiv g_{n_2,q} \pmod{x^{q^e} - x}. \)

\[ \square \]

Given two integers \( m, n > 0 \), we say \( m \) and \( n \) belong to the same \( p \)-cyclotomic coset \((\mod q^e - 1)\) whenever \( m \equiv p^i \cdot n \pmod{q^e - 1} \) for some integer \( i > 0 \). If two integers \( m, n > 0 \) belong to the same \( p \)-cyclotomic coset modulo \( q^e - 1 \), the two triples \((m, e; q)\) and \((n, e; q)\) are called equivalent, and we write \((m, e; q) \sim (n, e; q)\) or \( m \sim_{(e,q)} n \). Proposition 2.1.4 verifies that desirability of triples is preserved under the \( \sim \) equivalence.

**Lemma 2.1.5** ([40]). Let \( l \) and \( i > 0 \) be integers. Then
\[ g_{l+q^i,q} = g_{l+1,q} + S_i \cdot g_{l,q}, \quad (2.1.6) \]
where \( S_i = x + x^q + \cdots + x^{q^{i-1}} \).

From (2.1.6), we have
\[ (S_a - S_b)g_{n,q} = g_{n+q^e,q} - g_{n+q^e,q}, \quad (2.1.7) \]
where \( a, b > 0 \) are integers. Also note that
\[ S_a - S_b \equiv S_{a-b} \pmod{x^{q^e} - x} \quad \text{if} \; b \equiv 0 \; \text{or} \; a \pmod{e}. \]

If \( a < 0 \), we define \( S_a = S_{p+e+a} \).
Given integers $d > 1$ and $a = a_0 d^0 + \cdots + a_t d^t$, $0 \leq a_i \leq d - 1$, the base $d$ weight of $a$ is $w_d(a) = a_0 + \cdots + a_t$. Let $n \geq 0$ be any integer and $w_q(n)$ denote the base $q$ weight of $n$. If the base $q$ weight of $n$ is small, the form of $g_{n,q}$ is determined by the following lemma.

**Lemma 2.1.6 ([40])**. Let $n = \alpha_0 q^0 + \cdots + \alpha_t q^t$, $0 \leq \alpha_i \leq q - 1$ and $w_q(n)$ be the base $q$ weight of $n$,

$$g_{n,q} = \begin{cases} 
0 & \text{if } w_q(n) < q - 1, \\
-1 & \text{if } w_q(n) = q - 1, \\
\alpha_0 x^{q^0} + (\alpha_0 + \alpha_1) x^{q^1} + \cdots + (\alpha_0 + \cdots + \alpha_t) x^{q^t} + \delta & \text{if } w_q(n) = q,
\end{cases}$$

(2.1.8)

where

$$\delta = \begin{cases} 
1 & \text{if } q = 2, \\
0 & \text{if } q > 2.
\end{cases}$$

### 2.2 Desirable Triples of the form $(q^a - q^b - 1, e; q)$

A massive computer search suggests that $n$ of the form $n = q^a - q^b - 1$ is special, that is, the family of polynomials $g_{q^a-q^b-1,q}$ contains many permutation polynomials.

Assume $n > 0$ and $n \equiv q^a - q^b - 1 \pmod{q^{pe}-1}$ for some integers $a, b \geq 0$. If $a = 0$ or $a = b$, then $n \sim_{(e,q)} q^{pe}-2$, where $(q^{pe-2}, e; q)$ is desirable if and only if $q > 2$ [40, Proposition 3.2 (i)]. If $b = 0$ and $a > 0$, we have $n \equiv q^a - 2 \pmod{q^{pe}-1}$.

By Proposition 2.1.4 and Lemma 2.1.6,

$$g_{q^a-2,q} = \frac{1}{x} (g_{q^a+q-2,q} - g_{q^a-1,q})$$

$$= \frac{1}{x} \left[ -1 - \frac{1}{x} (g_{q^a+q-1,q} - g_{q^a,q}) \right]$$

$$= \frac{1}{x} \left( -1 + \frac{S_a}{x} \right)$$

16
For which $a$, $e$ and $q$ is $g_{q^a-2,q}$ a PP of $\mathbb{F}_q$? The complete answer is not known. We have the following conjecture.

**Conjecture 2.2.1** Let $e \geq 2$ and $2 \leq a < pe$. Then $(q^a - 2, e; q)$ is desirable if and only if

(i) $a = 3$ and $q = 2$, or

(ii) $a = 2$ and $\gcd(q - 2, q^e - 1) = 1$.

**Note.** When $q$ is even, 

$$g_{q^a-2,q} = \left(\frac{x^{\frac{1}{q}q^1} + x^{\frac{1}{q}q^2} + \cdots + x^{\frac{1}{q}q^{a-1}}}{x}\right)^2,$$

and the claim of the conjecture follows from Payne’s Theorem which says that the linearized polynomials $f(x) \in \mathbb{F}_{2^n}[x]$ such that $f(x)$ and $f(x)/x$ are permutations of $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^n}^*$ respectively, are exactly of the form $f(x) = ax^{2k}$ with $a \in \mathbb{F}_{2^n}^*$ and $\gcd(k, n) = 1$ [36, §8.5], [37, 76, 77].

For a general $q$, the “if” part is obvious. So for the conjecture, one only has to prove that if $q$ is odd, $e \geq 2$, and $a > 2$, then $(q^a - 2, e; q)$ is not desirable.

Now assume $n > 0$ and $n \equiv q^a - q^b - 1 \pmod{q^{pe} - 1}$, where $0 < a, b < pe$ and $a \neq b$. If $a < b$, we have

$$n \sim_{(e,q)} q^{pe-b} n \equiv q^{pe-b}(q^a - q^b - 1) \equiv q^{pe+a-b} - q^{pe-b} - 1 \pmod{q^{pe} - 1},$$

where $0 < pe - b < pe + a - b < pe$. Therefore we may assume $0 < b < a < pe$. 

17
By (2.1.6), we have

\[ S_b \cdot g_{q^a - q^b - 1, q} = g_{q^a - 1, q} - g_{q^b, q} \]
\[ = g_{q^a - 1, q} - (g_{q^{a-b} - 1, q})^{q^b} \]
\[ = -\frac{S_a}{x} + \left(\frac{S_{a-b}}{x}\right)^{q^b} \]
\[ = -\frac{S_a - S_{a-b}^{q^b}}{x} + \left(\frac{1}{x^{q^b}} - \frac{1}{x}\right)S_{a-b}^{q^b} \]
\[ = -\frac{S_b}{x} - \frac{S_b}{x^{q^b+1}} S_{a-b}^{q^b} \].

So

\[ g_{q^a - q^b - 1, q} = \frac{1}{x} - \frac{(S_{b}^{q-1} - 1)S_{a-b}^{q^b}}{x^{q^b+1}}. \] (2.2.10)

(Note that (2.2.10) also holds for \( b = 0 \); see (2.2.9).) Assume \( e \geq 2 \). Write

\[ a - b = a_0 + a_1 e, \quad b = b_0 + b_1 e, \]

where \( a_0, a_1, b_0, b_1 \in \mathbb{Z} \) and \( 0 \leq a_0, b_0 < e \). Then from (2.2.10) we have

\[ g_{q^a - q^b - 1, q} \equiv -x^{q^e - 2} - x^{q^e - q^{b_0} - 2}(a_1 S_e + S_{a_0}^{b_0})((b_1 S_e + S_{b_0})^{q-1} - 1) \pmod{x^{q^e} - x}. \] (2.2.11)

**Corollary 2.2.2** We have

\[ g_{q^2 - q - 1, q} = -x^{q^2 - 2}. \]

In particular, \((q^2 - q - 1, e; q)\) is desirable if and only if \( q > 2 \) and \( \gcd(q-2, q^e-1) = 1 \).

**Proof.** It follows from (2.2.10).

---

The following theorem is a generalization of [40, Proposition 3.2 (i)].

**Theorem 2.2.3** Assume \( e \geq 2 \). Let \( 0 < b < a < pe \). Then

\[ g_{q^a - q^b - 1, q} \equiv -x^{q^e - 2} \pmod{x^{q^e} - x} \] (2.2.12)
if and only if $a \equiv b \equiv 0 \pmod{e}$. In particular, if $0 < b < a < pe$, and $a \equiv b \equiv 0 \pmod{e}$, then $(q^a - q^b - 1, e; q)$ is a desirable triple.

Proof. $(\Leftarrow)$ In the notation of (2.2.11), we have $a_0 = b_0 = 0$ and $0 < b_1 < p$. So

$$
\begin{align*}
g_{q^a - q^b - 1, q} & \equiv -x^{q^a - 2} - x^{q^a - 3}a_1S_e((b_1S_e)^{q - 1} - 1) \pmod{x^{q^e} - x} \\
& = -x^{q^a - 2} - x^{q^a - 3}a_1S_e(S_q^{q-1} - 1) \\
& = -x^{q^a - 2} - x^{q^a - 3}a_1(S_q^q - S_e) \\
& \equiv -x^{q^a - 2} \pmod{x^{q^e} - x}.
\end{align*}
$$

(2.2.13)

$(\Rightarrow)$ Assume (2.2.12) holds. Then by (2.2.10),

$$(x^{q^b} - x)S_{a-b}^{q^b} = (S_b^q - S_b)S_{a-b}^{q^b} \equiv 0 \pmod{x^{q^e} - x}.$$

For $f \in \mathbb{F}_q[x]$, denote $\{ x \in \mathbb{F}_q : f(x) = 0 \}$ by $V(f)$, where $\mathbb{F}_q$ is the algebraic closure of $\mathbb{F}_q$. Then $V(x^{q^e} - x) \subset V(x^{q^b} - x) \cup V(S_{a-b})$, i.e., $\mathbb{F}_{q^e} \subset \mathbb{F}_{q^b} \cup V(S_{a-b})$. Since $V(S_{a-b})$ is a vector space over $\mathbb{F}_q$, we must have $\mathbb{F}_{q^e} \subset \mathbb{F}_{q^b}$ or $\mathbb{F}_{q^e} \subset V(S_{a-b})$. However, since $0 < a < pe$,

$$S_{a-b} = S_{a_1e+a_0} \equiv a_1S_e + a_0 \neq 0 \pmod{x^{q^e} - x}.$$

So we must have $\mathbb{F}_{q^e} \subset \mathbb{F}_{q^b}$. Hence $b \equiv 0 \pmod{e}$. Now by (2.2.11) and the calculation in (2.2.13), we have

$$S_{a_0}(S_q^{q-1} - 1) \equiv 0 \pmod{x^{q^e} - x}.$$

(2.2.14)

If $a_0 > 0$, then

$$\deg S_{a_0}(S_q^{q-1} - 1) = (q - 1)q^{e-1} + q^{a_0-1} = q^e - q^{e-1} + q^{a_0-1} < q^e,$$

which is a contradiction to (2.2.14). So we must have $a_0 = 0$, i.e., $a \equiv 0 \pmod{e}$.

Remark. If $(q^a - q^b - 1, 2; q)$ is desirable, where $0 < b < a < 2p$ and $b \equiv 0 \pmod{2}$, then we must have $a \equiv 0 \pmod{2}$. Otherwise, with $e = 2$, $a_0 = 1$, $b_0 = 0$ in (2.2.11),
we have

\[ g_{q^a - q^b - 1, q} \equiv -x^{q^2 - 2} - x^{q^2 - 3}(a_1 S_2 + x)((b_1 S_2)^{q-1} - 1) \pmod{x^{q^2} - x}. \]

Then \( g_{q^a - q^b - 1, q}(x) = 0 \) for every \( x \in \mathbb{F}_{q^2} \) with \( \text{Tr}_{q^2/q}(x) = 0 \), which is a contradiction.

The results of our computer search suggest that when \( e \geq 3 \), the only desirable triples \( (q^a - q^b - 1, e; q), \ 0 < b < a < pe \), are those given by Corollary 2.2.2 and Theorem 5.5.2. This leads us to conjecture the following:

**Conjecture 2.2.4** Let \( e \geq 3 \) and \( n = q^a - q^b - 1, \ 0 < b < a < pe \). Then \((n, e; q)\) is desirable if and only if

(i) \( a = 2, \ b = 1, \) and \( \gcd(q - 2, q^e - 1) = 1 \), or

(ii) \( a \equiv b \equiv 0 \pmod{e} \).

### 2.3 Desirable Triples of the form \((q^a - q^b - 1, 2; q)\)

In light of Conjecture 2.2.4, we see the permutation behavior of \( g_{q^a - q^b - 1, q} \) is fairly predictable when \( e > 2 \). This situation becomes more chaotic when \( e = 2 \). A computer search suggests that desirable triples of the form \((q^a - q^b - 1, 2; q)\), \( 0 < b < a < 2p \), are quite common (see table 2.1). For the remainder of this chapter, we consider desirable triples of the form \((q^a - q^b - 1, 2; q)\), \( 0 < b < a < 2p \).

Experimental evidence suggests that desirable triples of the form \((q^a - q^b - 1, 2; q)\) are abundant. These triples appear so often, we remove them from Table 2.1, for convenience of reading and in the hope it will allow other patterns to surface. The following two theorems deal with the case \( b = p \).

**Theorem 2.3.1** Let \( p \) be an odd prime and \( q \) a power of \( p \).

(i) \( \mathbb{F}_{q^2} \setminus \mathbb{F}_q \) consists of the roots of \((x - x^q)^{q-1} + 1\). 
(ii) Let $0 < i \leq \frac{1}{2}(p - 1)$ and $n = q^{p+2i} - q^p - 1$. Then

$$g_{n,q}(x) = \begin{cases} 
(2i - 1)x^{q-2} & \text{if } x \in \mathbb{F}_q, \\
\frac{2i - 1}{x} + \frac{2i}{x^q} & \text{if } x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q.
\end{cases}$$

(iii) For the $n$ in (ii), $(n, 2; q)$ is desirable if and only if $4i \not\equiv 1 \pmod{p}$.

Proof. (i) We have

$$(x^q - x)[(x - x^q)^{q-1} + 1] = -(x - x^q)^q + x^q - x = x^{q^2} - x.$$ Hence the claim.

(ii) Let $e = 2$, $a = p + 2i$, $b = p$. In the notation of (5.5.45), $a_0 = 0$, $a_1 = i$, $b_0 = 1$, $b_1 = \frac{p-1}{2}$. Thus

$$g_{n,q} \equiv -x^{q^2-2} - ix^{q^2-q-2}S_2\left[\left(-\frac{1}{2}S_2 + x\right)^{q-1} - 1\right] \pmod{x^{q^2} - x}$$

$$= -x^{q^2-2} - ix^{q^2-q-2}(x + x^q)[(x - x^q)^{q-1} - 1].$$

When $x \in \mathbb{F}_q$, $x - x^q = 0$, so

$$g_{n,q}(x) = -x^{q^2-2} + ix^{q^2-q-2}(x + x^q) = (2i - 1)x^{q-2}.$$ When $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, by (i), $(x - x^q)^{q-1} = -1$. Thus

$$g_{n,q}(x) = -x^{-1} + 2ix^{q^2-q-2}(x + x^q)$$

$$= -x^{-1} + 2ix^{q^2-q-1} + 2ix^{q^2-2}$$

$$= (2i - 1)x^{-1} + 2ix^{-q}.$$ (iii) Since $0 < 2i - 1 < p$, $(2i - 1)x^{q-2}$ permutes $\mathbb{F}_q$. We claim that $(2i - 1)x^{-1} + 2ix^{-q}$ maps $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ to itself. In fact, for $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$,

$$\left[\frac{2i - 1}{x} + \frac{2i}{x^q} - \left(\frac{2i - 1}{x} + \frac{2i}{x^q}\right)^q\right]^{q-1} = \left(-\frac{1}{x} + \frac{1}{x^q}\right)^{q-1} = \left(\frac{x - x^q}{x^{q+1}}\right)^{q-1} = -1.$$
since \((x - x^q)^{q-1} = -1\).

Therefore, \(g_{n,q}\) is a PP of \(\mathbb{F}_{q^2}\) if and only if \((2i - 1)x^{-1} + 2ix^{-q}\) is 1-1 on \(\mathbb{F}_{q^2} \setminus \mathbb{F}_q\), i.e., if and only if \((2i - 1)x + 2ix^q\) is 1-1 on \(\mathbb{F}_{q^2} \setminus \mathbb{F}_q\). So, it remains to show that \((2i - 1)x + 2ix^q\) is 1-1 on \(\mathbb{F}_{q^2} \setminus \mathbb{F}_q\) if and only if \(4i \not\equiv 1 \pmod{p}\).

\((\Leftarrow)\) Assume \(4i \not\equiv 1 \pmod{p}\). We claim that \((2i - 1)x + 2ix^q\) is a PP of \(\mathbb{F}_{q^2}\). Otherwise, there exists \(0 \neq x \in \mathbb{F}_{q^2}\) such that \((2i - 1)x + 2ix^q = 0\). Then \(x^{q-1} = -\frac{2i-1}{2i}\). Hence

\[
1 = (x^{q-1})^{q+1} = \left(-\frac{2i-1}{2i}\right)^{q+1} = \left(\frac{2i-1}{2i}\right)^2.
\]

So \((2i - 1)^2 \equiv (2i)^2 \pmod{p}\), i.e., \(4i - 1 \equiv 0 \pmod{p}\), which is a contradiction.

\((\Rightarrow)\) Assume \(4i \equiv 1 \pmod{p}\). Then \((2i - 1)x + 2ix^q = 2i(x^q - x)\), which is clearly not 1-1 on \(\mathbb{F}_{q^2} \setminus \mathbb{F}_q\).

\[\blacksquare\]

**Theorem 2.3.2** Let \(p\) be an odd prime and \(q\) a power of \(p\).

(i) Let \(0 < i \leq \frac{1}{2}(p - 1)\) and \(n = q^{p+2i-1} - q^p - 1\). Then

\[
g_{n,q}(x) = \begin{cases} 
2(i - 1)x^{q-2} & \text{if } x \in \mathbb{F}_q, \\
\frac{2i - 1}{x} + \frac{2i - 2}{x^q} & \text{if } x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q.
\end{cases}
\]

(ii) For the \(n\) in (i), \((n, 2; q)\) is desirable if and only if \(i > 1\) and \(4i \not\equiv 3 \pmod{p}\).

**Proof.** (i) Let \(e = 2\), \(a = p + 2i - 1\), \(b = p\). In the notation of (2.2.11), \(a_0 = 1\), \(a_1 = i - 1\), \(b_0 = 1\), \(b_1 = \frac{p-1}{2}\). Thus

\[
g_{n,q} \equiv -x^{q^2-2} - x^{q^2-q-2}((i - 1)S_2 + x^q)[\left(-\frac{1}{2}S_2 + x\right)^{q-1} - 1] \pmod{x^{q^2} - x}
\]

\[= -x^{q^2-2} - x^{q^2-q-2}(i(x + x^q) - x)(x - x^q)^{q-1} - 1].
\]

When \(x \in \mathbb{F}_q\), \(x - x^q = 0\), so

\[
g_{n,q}(x) = -x^{q^2-2} + x^{q^2-q-1}(2i - 1) = 2(i - 1)x^{q-2}.
\]
When $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, by (i), $(x - x^q)^{q-1} = -1$. Thus

$$g_{n,q}(x) = -x^{-1} + 2x^{q^2 - q - 2}((i - 1)x + ixq^2)$$

$$= -x^{-1} + 2(i - 1)x^{q^2 - q - 1} + 2ixq^{2 - 2}$$

$$= (2i - 1)x^{-1} + (2i - 2)x^{-q}.$$

(ii) Since $0 < 2i - 2 < p$, $2(i - 1)x^{q - 2}$ permutes $\mathbb{F}_q$. We claim that $(2i - 1)x^{-1} + (2i - 2)x^{-q}$ maps $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ to itself. In fact, for $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$,

$$\left[ \frac{2i - 1}{x} + \frac{2i - 2}{x^q} - \left( \frac{2i - 1}{x} + \frac{2i - 2}{x^q} \right)^q \right] q^{-1} = \left( \frac{1}{x} - \frac{1}{x^q} \right)^q = \left( \frac{x - x^q}{x^{q+1}} \right) q^{-1} = -1$$

since $(x - x^q)^{q-1} = -1$.

Therefore, $g_{n,q}$ is a PP of $\mathbb{F}_{q^2}$ if and only if $(2i - 1)x^{-1} + (2i - 2)x^{-q}$ is 1-1 on $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, i.e., if and only if $(2i - 1)x + (2i - 2)x^q$ is 1-1 on $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. So, it remains to show that $(2i - 1)x + (2i - 2)x^q$ is 1-1 on $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ if and only if $4i \not\equiv 3 \pmod{p}$.

$(\Leftarrow)$ Assume $4i \not\equiv 3 \pmod{p}$. We claim that $(2i - 1)x + (2i - 2)x^q$ is a PP of $\mathbb{F}_{q^2}$. Otherwise, there exists $0 \neq x \in \mathbb{F}_{q^2}$ such that $(2i - 1)x + (2i - 2)x^q = 0$. Then $x^{q-1} = -\frac{2i - 1}{2i - 2}$. Hence

$$1 = (x^{q-1})^{q+1} = \left( \frac{2i - 1}{2i - 2} \right)^{q+1} = \left( \frac{2i - 1}{2i - 2} \right)^2.$$

So $(2i - 1)^2 \equiv (2i - 2)^2 \pmod{p}$, i.e., $4i - 3 \equiv 0 \pmod{p}$, which is a contradiction.

$(\Rightarrow)$ Assume $4i \equiv 3 \pmod{p}$. Then $(2i - 1)x + (2i - 2)x^q = (2i - 2)(x^q - x)$, which is clearly not 1-1 on $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

\[\blacksquare\]

**Theorem 2.3.3** Let $q = 2^s$, $n = q^3 - q - 1$.

(i) For $x \in \mathbb{F}_{q^2}$,

$$g_{n,q}(x) = \begin{cases} 
0 & \text{if } x = 0, \\
 x^{q-2} + \text{Tr}_{q^2/q}(x^{-1}) & \text{if } x \neq 0. 
\end{cases}$$
(ii) $g_{n,q}$ is a PP of $\mathbb{F}_{q^2}$ if and only if $s$ is even.

Proof. (i) It is obvious that $g(0) = 0$. Let $0 \neq x \in \mathbb{F}_{q^2}$. By (2.2.11) (with $a_0 = 0$, $a_1 = 1$, $b_0 = 1$, $b_1 = 0$),

$$
g_{n,q}(x) = x^{-1} + x^{-q-1}S_2(x)(x^{q-1} + 1)$$
$$= x^{-1} + x^{-q-1}(x + x^q)(x^{q-1} + 1)$$
$$= x^{-1} + x^{q-2} + x^{-q}$$
$$= x^{q-2} + \text{Tr}_{q^2/q}(x^{-1}).$$

(ii) 1° We show that for every $c \in \mathbb{F}_{q^2}^*$, the equation

$$x^{q-2} + x^{-1} + x^{-q} = c$$

(2.3.15)

has at most one solution $x \in \mathbb{F}_{q^2}^*$.

Assume that $x \in \mathbb{F}_{q^2}^*$ is a solution of (2.3.15). Then

$$cx^{-q} = x^{-2} + x^{-q-1} + x^{-2q} = N_{q^2/q}(x^{-1}) + \text{Tr}_{q^2/q}(x^{-2}) \in \mathbb{F}_q.$$ 

Let $t = c^{-q}x = (cx^{-q})^{-q} \in \mathbb{F}_{q^2}^*$. Then $x = tc^q$. Making this substitution in (2.3.15), we have

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

So

$$t = c^{-2} + c^{-2q} + c^{-q-1}.$$ 

Hence $x$ is unique.

2° Assume $s$ is even. We show that

$$x^{q-2} + \text{Tr}_{q^2/q}(x^{-1}) = 0$$

(2.3.16)

has no solution in $\mathbb{F}_{q^2}^*$. Assume to the contrary that $x \in \mathbb{F}_{q^2}^*$ is a solution of (2.3.16).
Then \( x^{q-2} \in \mathbb{F}_q \). Since \( s \) is even, we have \( \gcd(q - 2, q^2 - 1) = 1 \). So \( x \in \mathbb{F}_q \). Then \( \text{Tr}_{q^2/q}(x^{-1}) = 0 \), and \( x^{q-2} = 0 \), which is a contradiction.

3\textsuperscript{o} Assume \( s \) is odd. We show that (2.3.16) has a solution in \( \mathbb{F}^*_q \). Let \( x \in \mathbb{F}^*_q \). Then \( x^2 + x + 1 = 0 \) and \( x^3 = 1 \). So

\[
\begin{align*}
    x^{q-2} + \text{Tr}_{q^2/q}(x^{-1}) &= x^{q-2} + x^{-1} + x^{-q} \\
    &= 1 + x^2 + x \\n    &= 0.
\end{align*}
\]

The following theorem is particularly interesting as the polynomial \( g_{n,q} \) acts on \( \mathbb{F}_{q^2} \) as a binomial. This observation pays dividends in the following chapters.

**Theorem 2.3.4**  
(i) Assume \( q > 2 \). We have

\[
g_{q^{2i}-q-1,q} \equiv (i - 1)x^{2i-2} - ix^{q-2} - (i - 1)S_2 + x^q \equiv (i - 1)x^{2i-2} - ix^{q-2} + x \\n(\mod x^{q^2} - x).
\]

(ii) Assume that \( q \) is odd. Then \( x^{q^2-q-1} + x^{q-2} \) is a PP of \( \mathbb{F}_{q^2} \) if and only if \( q \equiv 1 \pmod{4} \).

(iii) Assume that \( q \) is odd. Then \( (q^{p+1} - q - 1, 2; q) \) is desirable if and only if \( q \equiv 1 \pmod{4} \).

**Proof.** In the notation of (2.2.11), we have \( e = 2, a = 2i, b = 1, a_0 = 1, a_1 = i - 1, b_0 = 1, b_1 = 0 \). Thus

\[
g_{q^{2i}-q-1,q} \equiv -x^{q^2-2} - x^{q^2-q^2} - (i - 1)S_2 + x^q \equiv (i - 1)x^{2i-2} - ix^{q-2} \\n- (i - 1)x + ix^q \equiv (i - 1)x^{2i-2} - ix^{q-2} - (i - 1)S_2 + x^q \\n\equiv (i - 1)x^{2i-2} - ix^{q-2} \quad (\mod x^{q^2} - x).
\]
(ii) \( \Leftrightarrow \) Let \( f = x^{q^2 - q} + x^{q - 2} \). Then

\[
f(x) = \begin{cases} 
0 & \text{if } x = 0, \\
x^{-q} + x^{q - 2} & \text{if } x \in \mathbb{F}_q^*.
\end{cases}
\]

1° We show that for every \( c \in \mathbb{F}_q^* \), the equation

\[
x^{-q} + x^{q - 2} = c
\]

has at most one solution \( x \in \mathbb{F}_q^* \).

Assume \( x \in \mathbb{F}_q^* \) is a solution of \( (2.3.17) \). Then

\[
(cx)^{-q} = x^{-2q} + x^{-2} = \text{Tr}_{q^2/q}(x^{-2}) \in \mathbb{F}_q.
\]

Let \( t = c^{-q}x = (cx^{-q})^{-q} \in \mathbb{F}_q^* \). Then \( x = tc^q \). So \( (2.3.17) \) becomes

\[
\frac{1}{t}(c^{-1} + c^{q(q-2)}) = c.
\]

Thus \( t = c^{-2} + c^{-2q} \). Hence \( x \) is unique.

2° We show that \( x^{-q} + x^{q - 2} = 0 \) has no solution \( x \in \mathbb{F}_q^* \).

Assume that \( x \in \mathbb{F}_q^* \) is a solution. Then \( x^{2q-2} = -1 \). Since \( \frac{1}{2}(q + 1) \) is odd, we have \( -1 = (x^{2q-2})^{\frac{1}{2}(q+1)} = x^{q^2-1} = 1 \), which is a contradiction.

\( \Rightarrow \) Assume to the contrary that \( q \equiv -1 \) (mod \( 4 \)). We show that \( x^{-q} + x^{q - 2} = 0 \) has a solution \( x \in \mathbb{F}_q^* \). Since \( 4(q-1) \mid q^2-1 \), there exists \( x \in \mathbb{F}_q^* \) with \( o(x) = 4(q-1) \). Then \( x^{2(q-1)} = -1 \), i.e., \( x^{-q} + x^{q - 2} = 0 \).

(iii) It follows from (i) and (ii).

\[\blacksquare\]

**Theorem 2.3.5** Let \( p \) be an odd prime and \( q \) a power of \( p \). Let \( 0 \leq i \leq p - 2 \) and
\[ n = q^{p+i+1} - q^{2i+1} - 1. \]

If

\[
\left( \frac{2i+1}{q} \right) = \begin{cases} 
1 & \text{if } i \text{ is odd}, \\
(-1)^{\frac{q-1}{2}} & \text{if } i \text{ is even},
\end{cases}
\]  \hspace{1cm} (2.3.18)

where \( \left( \frac{a}{b} \right) \) is the Jacobi symbol, then \( (q^{p+i+1} - q^{2i+1} - 1, 2; q) \) is desirable.

**Proof.** Throughout the proof, “\( \equiv \)” means “\( \equiv (\mod q^2 - x) \)”.

Let \( e = 2, a = p + i + 1, b = 2i + 1. \)

**Case 1:** \( i \) is odd.

In the notation of (2.2.11), \( a_0 = 0, a_1 = \frac{p-i}{2}, b_0 = 1, b_1 = i. \)

Write \( g = g_{q^{p+i+1} - q^{2i+1} - 1, q}, \)

\[
g \equiv -x^{q^2-2} - x^{q^2-q-2}(\frac{p-i}{2}S_2)((iS_2 + S_1)^{q-1} - 1) \pmod{x^q - x} \\
= -x^{q^2-2} + \frac{i}{2}x^{q^2-q-2}(x + x^q)(((i+1)x + ix^q)^{q-1} - 1].
\]

Clearly, \( g(0) = 0. \) When \( x \in \mathbb{F}_{q^2}, \)

\[
g(x) = -x^{-1} + \frac{i}{2}x^{-q-1}(x + x^q)((i+1)x + ix^q)^q - ((i+1)x + ix^q)
\]

\[
= -x^{-1} + \frac{i}{2}(x^{-q} + x^{-1}) \frac{x^q - x}{(i+1)x + ix^q}
\]

\[
= -x^{-1} + \frac{i}{2}(x^{-q} + x^{-1}) \frac{x^{-1} - x^{-q}}{(i+1)x - q + ix^{-1}}
\]

\[
= y + \frac{i}{2}(y^q + y)^{(y^q - y)/(i+1)y^q + iy}
\]

\[
= \frac{iy^{2q} + 2(i+1)y^{q+1} + iy^2}{2(i+1)y^q + 2iy}. \hspace{1cm} (y = -x^{-1})
\]

Let \( w = 2(i+1)y^q + 2iy. \) Then \( y = \frac{1}{2(2i+1)}((i+1)w^q - iw). \)

Note: \( 2(i+1)x^q + 2ix \) is a PP of \( \mathbb{F}_{q^2}, \) and \( \frac{1}{2(2i+1)}((i+1)x^q - x) \) is the inverse PP.
So
\[
g(x) = \frac{1}{(4i + 2)^2} \frac{iu^{2q} + 2(i + 1)u^{q+1} + iw^2}{w},
\]
where \(u = (i + 1)w^q - iw\).

The proof will be complete if we can show that for \(c \in \mathbb{F}_{q^2}\),
\[
\frac{iu^{2q} + 2(i + 1)u^{q+1} + iw^2}{w} = c,
\]
i.e.,
\[
 \frac{i((i + 1)w^q - iw)^{2q} + 2(i + 1)((i + 1)w^q - iw)^{q+1} + i((i + 1)w^q - iw)^2}{w} = c
\]
has at most one solution \(w \in \mathbb{F}_{q^2}^\ast\) if \(c \neq 0\) and has no solution \(w \in \mathbb{F}_{q^2}^\ast\) if \(c = 0\).

First assume \(c \neq 0\). Let \(t = wc\). By (2.3.20), \(t \in \mathbb{F}_q\). Then (2.3.20) becomes
\[
\frac{it^{2}\nu^{2q} + 2t^{2}(i + 1)v^{q+1} + it^{2}v^{2}}{tc^{-1}} = c,
\]
where \(v = (i + 1)c^{-q} - ic^{-1}\). So
\[
t = \frac{1}{iv^{2q} + 2(i + 1)v^{q+1} + iv^{2}},
\]
which is unique. Hence \(w\) is unique.

Now assume \(c = 0\).

Assume to the contrary that (2.3.20) has a solution \(w \in \mathbb{F}_{q^2}^\ast\). Then
\[
\frac{i((i + 1)w^q - iw)^{2q-2} + 2(i + 1)((i + 1)w^q - iw)^{q-1} + i}{w} = 0.
\]
Let \(z = ((i + 1)w^q - iw)^{q-1} \in \mathbb{F}_{q^2}^\ast\). Then
\[
iz^2 + 2(i + 1)z + i = 0.
\]
Since \(i\) is odd \(2i+1\) is a square in \(\mathbb{F}_q\). So (2.3.21) implies that \(z \in \mathbb{F}_q\). Then we have 
\[ z^2 = z^{q+1} = ((i+1)w^q - iw)^{q-1} = 1. \]
So \(z = \pm 1\), which contradicts (2.3.21).

**Case 2:** \(i\) is even.

In the notation of (5.5.45), \(a_0 = 1, a_1 = \frac{p-i-1}{2}, b_0 = 1, b_1 = i\).

\[
g \equiv -x^{q^2-2} - x^{q^2-q-2}(S_2 + S_1^q)((iS_2 + x)^{q-1} - 1) \\
= -x^{q^2-2} + \frac{1}{2}x^{q^2-q-2}((i+1)x + (i-1)x^q)[((i+1)x + ix^q)^{q-1} - 1].
\]

Clearly, \(g(0) = 0\). When \(x \in \mathbb{F}_q^*\),

\[
g(x) = -x^{-1} + \frac{1}{2}x^{-q-1}((i+1)x + (i-1)x^q) \frac{(i+1)x + ix^q - ((i+1)x + ix^q)}{(i+1)x + ix^q}.
\]

Note that \((i+1)x + ix^q \neq 0\).

\[
g(x) = -x^{-1} + \frac{1}{2}((i+1)x^{-q} + (i-1)x^{-1}) \frac{x^{-q} - x}{(i+1)x + ix^q} \\
= -x^{-1} + \frac{1}{2}((i+1)x^{-q} + (i-1)x^{-1}) \frac{x^{-1} - x^{-q}}{(i+1)x^{-q} + ix^{-1}} \\
= y + \frac{1}{2}((i+1)y^q + (i-1)y) \frac{y^q - y}{(i+1)y^q + iy} \\
= \frac{(i+1)y^{2q} + 2iy^{q+1} + (i+1)y^2}{2(i+1)y^q + 2iy}.
\]

Let \(w = 2(i+1)y^q + 2iy\). Then 
\[
y = \frac{1}{2(2i+1)}((i+1)w^q - iw).
\]

Note: \(2(i+1)x^q + 2ix\) is a PP of \(\mathbb{F}_q^2\), and 
\[
\frac{1}{2(2i+1)}((i+1)x^q - ix)\]
is the inverse PP.

So
\[
g(x) = \frac{1}{(4i + 2)^2} \frac{(i+1)u^{2q} + 2iu^{q+1} + (i+1)u^2}{w},
\]
where \(u = (i+1)w^q - iw\).

The proof will be complete if we can show that for \(c \in \mathbb{F}_q^2\),

\[
\frac{(i+1)u^{2q} + 2iu^{q+1} + (i+1)u^2}{w} = c,
\]
(2.3.22)
\[
\frac{(i + 1)((i + 1)w^q - iw)^{q+1} + (i + 1)((i + 1)w^q - iw)^q + (i + 1)i(i + 1)w^2}{w} = c
\]

has at most one solution \(w \in \mathbb{F}_{q^2}^*\) if \(c \neq 0\) and has no solution \(w \in \mathbb{F}_{q^2}^*\) if \(c = 0\).

Assume \(c \neq 0\). Let \(t' = wc\). By (2.3.23), \(t' \in \mathbb{F}_q\). Then (2.3.23) becomes

\[
\frac{(i + 1)t^2v^{q+2} + 2it^2v^{q+1} + (i + 1)t^2v^2}{t'c^{-1}} = c,
\]

where \(v = (i + 1)c^{-q} - ic^{-1}\). So

\[
t' = \frac{1}{(i + 1)v^{2q} + 2iv^{q+1} + (i + 1)v^2},
\]

which is unique. Hence \(w\) is unique.

Now assume \(c = 0\). Assume to the contrary that (2.3.23) has a solution \(w \in \mathbb{F}_{q^2}^*\). Then

\[
(i + 1)((i + 1)w^q - iw)^{q-2} + 2i((i + 1)w^q - iw)^{q-1} + (i + 1) = 0.
\]

Let \(z = ((i + 1)w^q - iw)^{q-1} \in \mathbb{F}_{q^2}^*\). Then

\[
(i + 1)z^2 + 2iz + (i + 1) = 0. \tag{2.3.24}
\]

Since \(i\) is even \(\left(\frac{2i + 1}{q}\right) = (-1)^{q+1}\), i.e. \(- (2i + 1)\) is a square in \(\mathbb{F}_q\). So (2.3.24) implies that \(z \in \mathbb{F}_q\). Then we have \(z^2 = z^{q+1} = ((i + 1)w^q - iw)^{q^2-1} = 1\). So \(z = \pm 1\), which contradicts (2.3.24).

\[\blacksquare\]

### 2.4 Connection between \(g_{n,q}\) and PPs of the form \(f = x(a + x^{2(q-1)})\)

Assume that \(e \geq 2, n > 0, \) and \(n \equiv q^a - q^b - 1 \pmod{q^{pe} - 1}\), where \(0 \leq a, b \leq pe\).

Examining the evidence in the previous two sections we see there is little activity
when \( e \geq 3 \) (see Conjecture 2.2.4), however when \( e = 2 \), the situation appears to be quite chaotic. In fact, a computer search reveals many desirable triples of the form \((q^a - q^b - 1, 2; q)\) which are not covered by results in the previous sections, see Table 2.1. Based on some of these desirable triples and Theorem 2.3.4 we conjectured the following, which was later proved by Hou ([41]).

**Conjecture 2.4.1** Let \( f = x^{q-2} + tx^{q^2-1} \), \( t \in \mathbb{F}_q^* \). Then \( f \) is a PP of \( \mathbb{F}_{q^2} \) if and only if one of the following occurs:

(i) \( t = 1 \), \( q \equiv 1 \pmod{4} \);

(ii) \( t = -3 \), \( q \equiv \pm 1 \pmod{12} \);

(iii) \( t = 3 \), \( q \equiv -1 \pmod{6} \).

Suppose a polynomial of the form \( f = x^{q-2} + tx^{q^2-1} \) is a permutation polynomial of \( \mathbb{F}_{q^2} \). Noting that the map \( x \mapsto x^{q^2-1} \) is a permutation of \( \mathbb{F}_{q^2} \) and substituting \( x^{q^2-1} \) for \( x \) in Conjecture 2.4.1, we see Conjecture 2.4.1 is equivalent to the following theorem of Hou.

**Theorem 2.4.2 ([41])** Let \( f = tx + x^{2q-1} \), \( t \in \mathbb{F}_q^* \). Then \( f \) is a PP of \( \mathbb{F}_{q^2} \) if and only if one of the following occurs:

(i) \( t = 1 \), \( q \equiv 1 \pmod{4} \);

(ii) \( t = -3 \), \( q \equiv \pm 1 \pmod{12} \);

(iii) \( t = 3 \), \( q \equiv -1 \pmod{6} \).

It turns out that when \( n \) is of the form \( n = q^a - q^b - 1 \), the polynomial function \( g_{n,q}(x) \) on \( \mathbb{F}_{q^2} \) can be transfered into the form \( Ax + Bx^q + Cx^{2q-1} \) through an invertible change of variables. Using this connection, a theorem of Hou ([42]) can be used to determine all desirable triples of the form \((q^a - q^b - 1, 2; q)\). This leads to a study of permutation polynomials over \( \mathbb{F}_{q^2} \) of the form \( x^d(a + bx^{q-1} + x^{(q-1)}) \) (for explicit values of \( d \) and \( r \)) which is precisely the topic of the next chapter.
Table 2.1: Desirable triples \((q^a - q^b - 1, 2; q), q \leq 97, 0 < b < a < 2p, b \text{ odd}, b \neq p, (a, b) \neq (2, 1)\)

<table>
<thead>
<tr>
<th>(q)</th>
<th>(a)</th>
<th>(b)</th>
<th>(a)</th>
<th>(b)</th>
<th>(a)</th>
<th>(b)</th>
<th>(a)</th>
<th>(b)</th>
<th>(a)</th>
<th>(b)</th>
<th>(a)</th>
<th>(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(q = 2)</td>
<td>10</td>
<td>5</td>
<td>24</td>
<td>13</td>
<td>40</td>
<td>7</td>
<td>38</td>
<td>13</td>
<td>50</td>
<td>25</td>
<td>60</td>
<td>37</td>
</tr>
<tr>
<td>(q = 2^2)</td>
<td>26</td>
<td>1</td>
<td>42</td>
<td>37</td>
<td>40</td>
<td>31</td>
<td>54</td>
<td>33</td>
<td>63</td>
<td>43</td>
<td>73</td>
<td>59</td>
</tr>
<tr>
<td>(q = 2^3)</td>
<td>6</td>
<td>1</td>
<td>27</td>
<td>19</td>
<td>43</td>
<td>39</td>
<td>41</td>
<td>3</td>
<td>57</td>
<td>7</td>
<td>64</td>
<td>11</td>
</tr>
<tr>
<td>(q = 2^4)</td>
<td>8</td>
<td>1</td>
<td>28</td>
<td>21</td>
<td>45</td>
<td>13</td>
<td>41</td>
<td>19</td>
<td>58</td>
<td>41</td>
<td>64</td>
<td>45</td>
</tr>
<tr>
<td>(q = 2^5)</td>
<td>9</td>
<td>3</td>
<td>33</td>
<td>5</td>
<td>41</td>
<td>3</td>
<td>59</td>
<td>5</td>
<td>65</td>
<td>49</td>
<td>76</td>
<td>51</td>
</tr>
<tr>
<td>(q = 2^6)</td>
<td>10</td>
<td>5</td>
<td>15</td>
<td>11</td>
<td>42</td>
<td>21</td>
<td>62</td>
<td>49</td>
<td>67</td>
<td>51</td>
<td>77</td>
<td>67</td>
</tr>
<tr>
<td>(q = 3)</td>
<td>12</td>
<td>5</td>
<td>21</td>
<td>3</td>
<td>46</td>
<td>29</td>
<td>62</td>
<td>55</td>
<td>69</td>
<td>3</td>
<td>78</td>
<td>9</td>
</tr>
<tr>
<td>(q = 3^2)</td>
<td>12</td>
<td>9</td>
<td>17</td>
<td>9</td>
<td>26</td>
<td>21</td>
<td>49</td>
<td>35</td>
<td>63</td>
<td>39</td>
<td>70</td>
<td>57</td>
</tr>
<tr>
<td>(q = 3^3)</td>
<td>13</td>
<td>11</td>
<td>23</td>
<td>7</td>
<td>30</td>
<td>1</td>
<td>49</td>
<td>37</td>
<td>64</td>
<td>39</td>
<td>70</td>
<td>65</td>
</tr>
<tr>
<td>(q = 3^4)</td>
<td>16</td>
<td>10</td>
<td>30</td>
<td>23</td>
<td>33</td>
<td>7</td>
<td>51</td>
<td>39</td>
<td>69</td>
<td>63</td>
<td>77</td>
<td>33</td>
</tr>
<tr>
<td>(q = 3^5)</td>
<td>18</td>
<td>13</td>
<td>33</td>
<td>17</td>
<td>36</td>
<td>3</td>
<td>57</td>
<td>51</td>
<td>73</td>
<td>71</td>
<td>80</td>
<td>83</td>
</tr>
<tr>
<td>(q = 3^6)</td>
<td>19</td>
<td>15</td>
<td>34</td>
<td>29</td>
<td>36</td>
<td>13</td>
<td>58</td>
<td>53</td>
<td>80</td>
<td>77</td>
<td>85</td>
<td>83</td>
</tr>
<tr>
<td>(q = 4)</td>
<td>20</td>
<td>5</td>
<td>35</td>
<td>9</td>
<td>41</td>
<td>23</td>
<td>59</td>
<td>13</td>
<td>72</td>
<td>47</td>
<td>80</td>
<td>73</td>
</tr>
<tr>
<td>(q = 4^2)</td>
<td>20</td>
<td>17</td>
<td>36</td>
<td>5</td>
<td>42</td>
<td>25</td>
<td>60</td>
<td>5</td>
<td>72</td>
<td>41</td>
<td>82</td>
<td>77</td>
</tr>
<tr>
<td>(q = 4^3)</td>
<td>22</td>
<td>5</td>
<td>37</td>
<td>23</td>
<td>46</td>
<td>29</td>
<td>62</td>
<td>23</td>
<td>78</td>
<td>73</td>
<td>85</td>
<td>59</td>
</tr>
<tr>
<td>(q = 5)</td>
<td>25</td>
<td>11</td>
<td>31</td>
<td>19</td>
<td>49</td>
<td>43</td>
<td>64</td>
<td>5</td>
<td>77</td>
<td>53</td>
<td>85</td>
<td>59</td>
</tr>
<tr>
<td>(q = 5^2)</td>
<td>26</td>
<td>13</td>
<td>32</td>
<td>5</td>
<td>50</td>
<td>9</td>
<td>65</td>
<td>7</td>
<td>72</td>
<td>47</td>
<td>80</td>
<td>73</td>
</tr>
<tr>
<td>(q = 5^3)</td>
<td>28</td>
<td>15</td>
<td>34</td>
<td>21</td>
<td>42</td>
<td>21</td>
<td>50</td>
<td>37</td>
<td>67</td>
<td>53</td>
<td>72</td>
<td>61</td>
</tr>
<tr>
<td>(q = 7)</td>
<td>29</td>
<td>15</td>
<td>34</td>
<td>21</td>
<td>42</td>
<td>21</td>
<td>50</td>
<td>37</td>
<td>67</td>
<td>53</td>
<td>72</td>
<td>61</td>
</tr>
</tbody>
</table>

32
Table 2.1 (Continued)

<p>| | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>68</td>
<td>41</td>
<td>58</td>
<td>5</td>
<td>98</td>
<td>19</td>
<td>77</td>
<td>35</td>
<td>115</td>
</tr>
<tr>
<td>68</td>
<td>57</td>
<td>58</td>
<td>9</td>
<td>98</td>
<td>9</td>
<td>78</td>
<td>37</td>
<td>116</td>
</tr>
<tr>
<td>70</td>
<td>7</td>
<td>59</td>
<td>11</td>
<td>99</td>
<td>91</td>
<td>83</td>
<td>7</td>
<td>116</td>
</tr>
<tr>
<td>70</td>
<td>45</td>
<td>59</td>
<td>29</td>
<td>100</td>
<td>67</td>
<td>85</td>
<td>39</td>
<td>q = 61</td>
</tr>
<tr>
<td>73</td>
<td>39</td>
<td>59</td>
<td>37</td>
<td>100</td>
<td>93</td>
<td>85</td>
<td>51</td>
<td>q = 61</td>
</tr>
<tr>
<td>73</td>
<td>51</td>
<td>60</td>
<td>13</td>
<td>101</td>
<td>95</td>
<td>87</td>
<td>35</td>
<td>38</td>
</tr>
<tr>
<td>75</td>
<td>55</td>
<td>61</td>
<td>15</td>
<td>102</td>
<td>97</td>
<td>90</td>
<td>61</td>
<td>52</td>
</tr>
<tr>
<td>76</td>
<td>33</td>
<td>62</td>
<td>17</td>
<td>103</td>
<td>37</td>
<td>90</td>
<td>81</td>
<td>59</td>
</tr>
<tr>
<td>76</td>
<td>57</td>
<td>63</td>
<td>57</td>
<td>103</td>
<td>55</td>
<td>91</td>
<td>63</td>
<td>60</td>
</tr>
<tr>
<td>77</td>
<td>59</td>
<td>66</td>
<td>25</td>
<td>103</td>
<td>99</td>
<td>92</td>
<td>65</td>
<td>62</td>
</tr>
<tr>
<td>77</td>
<td>65</td>
<td>67</td>
<td>43</td>
<td>105</td>
<td>11</td>
<td>94</td>
<td>69</td>
<td>62</td>
</tr>
<tr>
<td>77</td>
<td>67</td>
<td>68</td>
<td>29</td>
<td>q = 59</td>
<td>94</td>
<td>71</td>
<td>63</td>
<td>3</td>
</tr>
<tr>
<td>79</td>
<td>63</td>
<td>71</td>
<td>11</td>
<td>q = 59</td>
<td>95</td>
<td>71</td>
<td>64</td>
<td>5</td>
</tr>
<tr>
<td>82</td>
<td>33</td>
<td>72</td>
<td>37</td>
<td>16</td>
<td>13</td>
<td>96</td>
<td>63</td>
<td>64</td>
</tr>
<tr>
<td>82</td>
<td>69</td>
<td>72</td>
<td>49</td>
<td>20</td>
<td>3</td>
<td>96</td>
<td>73</td>
<td>66</td>
</tr>
<tr>
<td>83</td>
<td>71</td>
<td>73</td>
<td>5</td>
<td>23</td>
<td>17</td>
<td>97</td>
<td>75</td>
<td>66</td>
</tr>
<tr>
<td>84</td>
<td>59</td>
<td>75</td>
<td>21</td>
<td>24</td>
<td>15</td>
<td>98</td>
<td>77</td>
<td>67</td>
</tr>
<tr>
<td>84</td>
<td>73</td>
<td>75</td>
<td>43</td>
<td>30</td>
<td>1</td>
<td>99</td>
<td>79</td>
<td>68</td>
</tr>
<tr>
<td>85</td>
<td>75</td>
<td>77</td>
<td>47</td>
<td>31</td>
<td>9</td>
<td>101</td>
<td>9</td>
<td>69</td>
</tr>
<tr>
<td>86</td>
<td>13</td>
<td>78</td>
<td>13</td>
<td>39</td>
<td>27</td>
<td>103</td>
<td>87</td>
<td>71</td>
</tr>
<tr>
<td>86</td>
<td>77</td>
<td>78</td>
<td>49</td>
<td>50</td>
<td>13</td>
<td>104</td>
<td>89</td>
<td>74</td>
</tr>
<tr>
<td>87</td>
<td>79</td>
<td>80</td>
<td>1</td>
<td>56</td>
<td>21</td>
<td>104</td>
<td>101</td>
<td>74</td>
</tr>
<tr>
<td>89</td>
<td>83</td>
<td>81</td>
<td>35</td>
<td>58</td>
<td>1</td>
<td>105</td>
<td>7</td>
<td>75</td>
</tr>
<tr>
<td>90</td>
<td>85</td>
<td>82</td>
<td>57</td>
<td>61</td>
<td>3</td>
<td>106</td>
<td>51</td>
<td>79</td>
</tr>
<tr>
<td>91</td>
<td>27</td>
<td>82</td>
<td>79</td>
<td>61</td>
<td>27</td>
<td>106</td>
<td>93</td>
<td>81</td>
</tr>
<tr>
<td>q = 53</td>
<td>83</td>
<td>59</td>
<td>61</td>
<td>33</td>
<td>107</td>
<td>95</td>
<td>82</td>
<td>41</td>
</tr>
<tr>
<td>85</td>
<td>63</td>
<td>63</td>
<td>7</td>
<td>108</td>
<td>83</td>
<td>84</td>
<td>45</td>
<td>120</td>
</tr>
<tr>
<td>27</td>
<td>23</td>
<td>88</td>
<td>13</td>
<td>66</td>
<td>13</td>
<td>108</td>
<td>97</td>
<td>84</td>
</tr>
<tr>
<td>32</td>
<td>3</td>
<td>88</td>
<td>69</td>
<td>66</td>
<td>19</td>
<td>109</td>
<td>31</td>
<td>85</td>
</tr>
<tr>
<td>50</td>
<td>21</td>
<td>91</td>
<td>29</td>
<td>67</td>
<td>15</td>
<td>110</td>
<td>25</td>
<td>86</td>
</tr>
<tr>
<td>51</td>
<td>43</td>
<td>92</td>
<td>23</td>
<td>69</td>
<td>19</td>
<td>110</td>
<td>101</td>
<td>86</td>
</tr>
<tr>
<td>54</td>
<td>1</td>
<td>92</td>
<td>77</td>
<td>73</td>
<td>27</td>
<td>113</td>
<td>107</td>
<td>87</td>
</tr>
<tr>
<td>57</td>
<td>7</td>
<td>94</td>
<td>81</td>
<td>76</td>
<td>33</td>
<td>114</td>
<td>109</td>
<td>89</td>
</tr>
</tbody>
</table>
Table 2.1 (Continued)

<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>a</th>
<th>b</th>
<th>a</th>
<th>b</th>
<th>a</th>
<th>b</th>
<th>a</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>140</td>
<td>5</td>
<td>111</td>
<td>79</td>
<td>75</td>
<td>3</td>
<td>106</td>
<td>65</td>
<td>108</td>
<td>7</td>
</tr>
<tr>
<td>131</td>
<td>7</td>
<td>104</td>
<td>81</td>
<td>105</td>
<td>3</td>
<td>107</td>
<td>67</td>
<td>68</td>
<td>9</td>
</tr>
<tr>
<td>103</td>
<td>11</td>
<td>113</td>
<td>83</td>
<td>119</td>
<td>3</td>
<td>108</td>
<td>69</td>
<td>52</td>
<td>11</td>
</tr>
<tr>
<td>78</td>
<td>13</td>
<td>114</td>
<td>85</td>
<td>69</td>
<td>5</td>
<td>109</td>
<td>71</td>
<td>85</td>
<td>11</td>
</tr>
<tr>
<td>95</td>
<td>13</td>
<td>114</td>
<td>85</td>
<td>78</td>
<td>5</td>
<td>92</td>
<td>75</td>
<td>125</td>
<td>11</td>
</tr>
<tr>
<td>47</td>
<td>15</td>
<td>115</td>
<td>87</td>
<td>98</td>
<td>7</td>
<td>111</td>
<td>75</td>
<td>129</td>
<td>11</td>
</tr>
<tr>
<td>79</td>
<td>15</td>
<td>120</td>
<td>87</td>
<td>78</td>
<td>9</td>
<td>112</td>
<td>77</td>
<td>43</td>
<td>13</td>
</tr>
<tr>
<td>80</td>
<td>17</td>
<td>117</td>
<td>91</td>
<td>128</td>
<td>15</td>
<td>113</td>
<td>79</td>
<td>135</td>
<td>13</td>
</tr>
<tr>
<td>81</td>
<td>19</td>
<td>118</td>
<td>93</td>
<td>137</td>
<td>15</td>
<td>114</td>
<td>81</td>
<td>121</td>
<td>15</td>
</tr>
<tr>
<td>121</td>
<td>19</td>
<td>119</td>
<td>95</td>
<td>108</td>
<td>17</td>
<td>116</td>
<td>85</td>
<td>88</td>
<td>17</td>
</tr>
<tr>
<td>82</td>
<td>21</td>
<td>120</td>
<td>97</td>
<td>123</td>
<td>17</td>
<td>94</td>
<td>87</td>
<td>89</td>
<td>19</td>
</tr>
<tr>
<td>101</td>
<td>21</td>
<td>131</td>
<td>97</td>
<td>83</td>
<td>19</td>
<td>118</td>
<td>89</td>
<td>55</td>
<td>23</td>
</tr>
<tr>
<td>41</td>
<td>23</td>
<td>107</td>
<td>103</td>
<td>85</td>
<td>23</td>
<td>119</td>
<td>91</td>
<td>59</td>
<td>23</td>
</tr>
<tr>
<td>30</td>
<td>27</td>
<td>119</td>
<td>103</td>
<td>86</td>
<td>25</td>
<td>112</td>
<td>97</td>
<td>91</td>
<td>23</td>
</tr>
<tr>
<td>85</td>
<td>27</td>
<td>123</td>
<td>103</td>
<td>87</td>
<td>27</td>
<td>122</td>
<td>97</td>
<td>121</td>
<td>27</td>
</tr>
<tr>
<td>88</td>
<td>33</td>
<td>124</td>
<td>105</td>
<td>103</td>
<td>29</td>
<td>137</td>
<td>99</td>
<td>70</td>
<td>29</td>
</tr>
<tr>
<td>99</td>
<td>35</td>
<td>113</td>
<td>107</td>
<td>104</td>
<td>29</td>
<td>114</td>
<td>103</td>
<td>94</td>
<td>29</td>
</tr>
<tr>
<td>98</td>
<td>37</td>
<td>119</td>
<td>107</td>
<td>67</td>
<td>31</td>
<td>126</td>
<td>105</td>
<td>95</td>
<td>31</td>
</tr>
<tr>
<td>97</td>
<td>39</td>
<td>125</td>
<td>107</td>
<td>91</td>
<td>35</td>
<td>135</td>
<td>107</td>
<td>96</td>
<td>33</td>
</tr>
<tr>
<td>67</td>
<td>41</td>
<td>114</td>
<td>111</td>
<td>46</td>
<td>37</td>
<td>128</td>
<td>109</td>
<td>98</td>
<td>37</td>
</tr>
<tr>
<td>92</td>
<td>41</td>
<td>127</td>
<td>111</td>
<td>92</td>
<td>37</td>
<td>129</td>
<td>111</td>
<td>100</td>
<td>41</td>
</tr>
<tr>
<td>93</td>
<td>43</td>
<td>128</td>
<td>113</td>
<td>99</td>
<td>39</td>
<td>126</td>
<td>113</td>
<td>137</td>
<td>41</td>
</tr>
<tr>
<td>78</td>
<td>47</td>
<td>130</td>
<td>117</td>
<td>81</td>
<td>41</td>
<td>133</td>
<td>119</td>
<td>83</td>
<td>45</td>
</tr>
<tr>
<td>88</td>
<td>47</td>
<td>131</td>
<td>119</td>
<td>94</td>
<td>41</td>
<td>134</td>
<td>121</td>
<td>110</td>
<td>45</td>
</tr>
<tr>
<td>62</td>
<td>51</td>
<td>137</td>
<td>131</td>
<td>127</td>
<td>41</td>
<td>135</td>
<td>123</td>
<td>143</td>
<td>45</td>
</tr>
<tr>
<td>75</td>
<td>51</td>
<td>138</td>
<td>133</td>
<td>118</td>
<td>43</td>
<td>139</td>
<td>125</td>
<td>95</td>
<td>49</td>
</tr>
<tr>
<td>106</td>
<td>51</td>
<td>139</td>
<td>135</td>
<td>59</td>
<td>49</td>
<td>137</td>
<td>127</td>
<td>137</td>
<td>49</td>
</tr>
<tr>
<td>98</td>
<td>53</td>
<td>140</td>
<td>137</td>
<td>98</td>
<td>49</td>
<td>142</td>
<td>137</td>
<td>105</td>
<td>51</td>
</tr>
<tr>
<td>102</td>
<td>61</td>
<td>69</td>
<td>51</td>
<td>145</td>
<td>143</td>
<td>106</td>
<td>53</td>
<td>148</td>
<td>137</td>
</tr>
<tr>
<td>104</td>
<td>65</td>
<td>101</td>
<td>55</td>
<td>107</td>
<td>55</td>
<td>151</td>
<td>137</td>
<td>80</td>
<td>21</td>
</tr>
<tr>
<td>106</td>
<td>69</td>
<td>102</td>
<td>57</td>
<td>129</td>
<td>55</td>
<td>151</td>
<td>143</td>
<td>95</td>
<td>23</td>
</tr>
<tr>
<td>118</td>
<td>69</td>
<td>13</td>
<td>1</td>
<td>113</td>
<td>57</td>
<td>108</td>
<td>57</td>
<td>152</td>
<td>145</td>
</tr>
<tr>
<td>130</td>
<td>69</td>
<td>72</td>
<td>1</td>
<td>119</td>
<td>57</td>
<td>156</td>
<td>5</td>
<td>110</td>
<td>61</td>
</tr>
<tr>
<td>128</td>
<td>73</td>
<td>74</td>
<td>1</td>
<td>104</td>
<td>61</td>
<td>27</td>
<td>7</td>
<td>113</td>
<td>67</td>
</tr>
<tr>
<td>109</td>
<td>75</td>
<td>135</td>
<td>1</td>
<td>97</td>
<td>63</td>
<td>54</td>
<td>7</td>
<td>77</td>
<td>69</td>
</tr>
</tbody>
</table>

$q = 34$

$q = 83$
<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>112</td>
<td>35</td>
<td>142</td>
<td>117</td>
<td>71</td>
<td>17</td>
<td>152</td>
</tr>
<tr>
<td>95</td>
<td>37</td>
<td>128</td>
<td>119</td>
<td>98</td>
<td>17</td>
<td>132</td>
</tr>
<tr>
<td>127</td>
<td>37</td>
<td>143</td>
<td>119</td>
<td>133</td>
<td>17</td>
<td>151</td>
</tr>
<tr>
<td>109</td>
<td>39</td>
<td>132</td>
<td>121</td>
<td>155</td>
<td>19</td>
<td>155</td>
</tr>
<tr>
<td>150</td>
<td>39</td>
<td>145</td>
<td>123</td>
<td>77</td>
<td>21</td>
<td>133</td>
</tr>
<tr>
<td>106</td>
<td>45</td>
<td>146</td>
<td>125</td>
<td>100</td>
<td>21</td>
<td>135</td>
</tr>
<tr>
<td>158</td>
<td>49</td>
<td>147</td>
<td>127</td>
<td>133</td>
<td>21</td>
<td>136</td>
</tr>
<tr>
<td>109</td>
<td>51</td>
<td>163</td>
<td>127</td>
<td>102</td>
<td>25</td>
<td>138</td>
</tr>
<tr>
<td>75</td>
<td>53</td>
<td>148</td>
<td>129</td>
<td>77</td>
<td>27</td>
<td>139</td>
</tr>
<tr>
<td>110</td>
<td>53</td>
<td>149</td>
<td>131</td>
<td>35</td>
<td>29</td>
<td>121</td>
</tr>
<tr>
<td>133</td>
<td>55</td>
<td>156</td>
<td>131</td>
<td>163</td>
<td>33</td>
<td>124</td>
</tr>
<tr>
<td>112</td>
<td>57</td>
<td>150</td>
<td>133</td>
<td>109</td>
<td>39</td>
<td>142</td>
</tr>
<tr>
<td>113</td>
<td>59</td>
<td>152</td>
<td>137</td>
<td>46</td>
<td>41</td>
<td>142</td>
</tr>
<tr>
<td>152</td>
<td>59</td>
<td>154</td>
<td>141</td>
<td>141</td>
<td>43</td>
<td>143</td>
</tr>
<tr>
<td>115</td>
<td>63</td>
<td>156</td>
<td>145</td>
<td>112</td>
<td>45</td>
<td>144</td>
</tr>
<tr>
<td>115</td>
<td>69</td>
<td>157</td>
<td>147</td>
<td>113</td>
<td>47</td>
<td>145</td>
</tr>
<tr>
<td>155</td>
<td>69</td>
<td>158</td>
<td>149</td>
<td>165</td>
<td>47</td>
<td>173</td>
</tr>
<tr>
<td>148</td>
<td>71</td>
<td>159</td>
<td>151</td>
<td>173</td>
<td>47</td>
<td>150</td>
</tr>
<tr>
<td>81</td>
<td>73</td>
<td>162</td>
<td>157</td>
<td>114</td>
<td>49</td>
<td>151</td>
</tr>
<tr>
<td>120</td>
<td>73</td>
<td></td>
<td></td>
<td>100</td>
<td>51</td>
<td>156</td>
</tr>
<tr>
<td>121</td>
<td>75</td>
<td>q = 89</td>
<td>92</td>
<td>53</td>
<td>159</td>
<td>123</td>
</tr>
<tr>
<td>95</td>
<td>77</td>
<td>41</td>
<td>1</td>
<td>116</td>
<td>53</td>
<td>149</td>
</tr>
<tr>
<td>126</td>
<td>85</td>
<td>90</td>
<td>1</td>
<td>117</td>
<td>55</td>
<td>152</td>
</tr>
<tr>
<td>127</td>
<td>87</td>
<td>134</td>
<td>1</td>
<td>139</td>
<td>55</td>
<td>132</td>
</tr>
<tr>
<td>154</td>
<td>87</td>
<td>139</td>
<td>1</td>
<td>170</td>
<td>55</td>
<td>154</td>
</tr>
<tr>
<td>110</td>
<td>89</td>
<td>92</td>
<td>5</td>
<td>118</td>
<td>57</td>
<td>155</td>
</tr>
<tr>
<td>128</td>
<td>89</td>
<td>94</td>
<td>5</td>
<td>102</td>
<td>61</td>
<td>156</td>
</tr>
<tr>
<td>131</td>
<td>95</td>
<td>176</td>
<td>5</td>
<td>123</td>
<td>67</td>
<td>154</td>
</tr>
<tr>
<td>149</td>
<td>95</td>
<td>151</td>
<td>7</td>
<td>150</td>
<td>67</td>
<td>159</td>
</tr>
<tr>
<td>132</td>
<td>97</td>
<td>166</td>
<td>7</td>
<td>124</td>
<td>69</td>
<td>169</td>
</tr>
<tr>
<td>133</td>
<td>99</td>
<td>94</td>
<td>9</td>
<td>125</td>
<td>71</td>
<td>168</td>
</tr>
<tr>
<td>134</td>
<td>101</td>
<td>95</td>
<td>11</td>
<td>161</td>
<td>71</td>
<td>166</td>
</tr>
<tr>
<td>115</td>
<td>105</td>
<td>44</td>
<td>13</td>
<td>126</td>
<td>73</td>
<td>168</td>
</tr>
<tr>
<td>136</td>
<td>105</td>
<td>127</td>
<td>13</td>
<td>129</td>
<td>79</td>
<td>170</td>
</tr>
<tr>
<td>139</td>
<td>111</td>
<td>49</td>
<td>15</td>
<td>130</td>
<td>81</td>
<td>173</td>
</tr>
</tbody>
</table>
3 Permutation Polynomials of the form \( f = x^d(a + bx^{q-1} + x^{(q-1)}) \) *

3.1 Background

The results of the previous chapter show the permutation behavior of \( g_{q^\alpha - q^\beta - 1,q} \) on \( \mathbb{F}_{q^2} \) appears to be quite chaotic. The following lemma shows that \( g_{q^\alpha - q^\beta - 1,q} \) is a permutation polynomial of \( \mathbb{F}_{q^2} \) if and only if a certain trinomial is a permutation polynomial on \( \mathbb{F}_{q^2} \).

**Lemma 3.1.1 ([42])** Assume \( q > 2 \). Let \( n = q^\alpha - q^\beta - 1 \), where \( 0 < \beta < \alpha < 2p, \beta \) is odd and \( \beta \neq p \). Write \( \alpha - \beta = a_0 + 2a_1, 0 \leq a_0 \leq 1 \), and \( \beta = 1 + 2b_1 \). Then

\[
g_{n,q}(x) = A\phi(x) + B\phi(x)^q + C\phi(x)^{2q-1} \quad \text{for all} \quad x \in \mathbb{F}_{q^2},
\]

where \( \Phi \) is a permutation of \( \mathbb{F}_{q^2} \) and

\[
\begin{align*}
A &= \frac{1}{\beta}(a_0b_1 + b_1 + a_1), \\
B &= a_0 - \frac{b_1 + 1}{\beta} \\
C &= -\frac{1}{\beta}(a_0b_1 + a_0 + a_1)
\end{align*}
\]

Now to determine when the triple \((q^\alpha - q^\beta - 1, 2; q)\) is desirable, we only have to determine conditions on the coefficients of \( f = ax + bx^q + x^{2q-1} \in \mathbb{F}_q[x] \) that force \( f \) to be a permutation polynomial of \( \mathbb{F}_{q^2} \). To this end we have the following theorems of Hou:

*Portions of this chapter are taken from [53] which is published in the Journal of Finite Fields and their Applications*
Theorem 3.1.2 ([42]) Let $f = ax + bx^q + x^{2q-1} \in \mathbb{F}_q[x]$, where $q$ is odd. Then $f$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if one of the following is satisfied.

(i) $a(a - 1)$ is a square in $\mathbb{F}_q^*$, and $b^2 = a^2 + 3a$.

(ii) $a = 1$, and $b^2 - 4a$ is a square in $\mathbb{F}_q^*$.

(iii) $a = 3, b = 0, q \equiv -1 \pmod{6}$.

(iv) $a = b = 0, q \equiv 1, 3 \pmod{6}$.

Theorem 3.1.3 ([42]) Let $f = ax + bx^q + x^{2q-1} \in \mathbb{F}_q[x]$, where $q$ is even. Then $f$ is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if one of the following is satisfied.

(i) $q > 2, a \neq 1, \text{Tr}_{q/2} \left( \frac{1}{a+1} \right) = 0, b^2 = a^2 + a$.

(ii) $q > 2, a = 1, b \neq 0, \text{Tr}_{q/2} \left( \frac{1}{b} \right) = 0$.

The proofs of the previous theorems are especially interesting in the sense that complicated computations that appear to head nowhere produce surprisingly nice results. We will see in a later section that this pleasant surprise appears again relating to permutation polynomials of the form $ax^3 + bx^{q+2} + x^{2q+1}$.

Using Lemma 3.1.1, Theorem 3.1.2 and Theorem 3.1.3 completely determine desirable triples of the form $(q^\alpha - q^\beta - 1, 2; q)$. This is summarized in the following two theorems.

Theorem 3.1.4 ([42]) Let $q$ be even and $n = q^\alpha - q^\beta - 1$, where $0 \leq \beta < \alpha < 2 \cdot 2$. Then $(n, 2; q)$ is desirable if and only if one of the following occurs.

(i) $q \equiv 1 \pmod{3}, (\beta, \alpha) = (0, 2), (1, 2), (1, 3)$.

(ii) $q = 2, (\beta, \alpha) = (0, 3)$

Theorem 3.1.5 ([42]) Let $q$ be odd and $n = q^\alpha - q^\beta - 1$, where $0 \leq \beta < \alpha < 2p$. Then $(n, 2; q)$ is desirable if and only if one of the following occurs.
(i) \( q \equiv 1 \pmod{3}, (\beta, \alpha) = (0, 2) \).

(ii) \( \beta > 0, \beta \equiv \alpha \equiv 0 \pmod{2} \).

(iii) \( (\beta, \alpha) = (p, p + i), 0 < i < p, 2i \not\equiv (-1)^i \pmod{p} \)

(iv) \( \beta \neq p, \beta = 1 + 2b_1, \alpha - \beta = a_0 + 2a_1, a_0, a_1, b_1 \in \mathbb{N}, 0 \leq a_0 \leq 1, \) and one of the following is satisfied.

(a) \( (a_1 + b_1)(2a_1 + b_1) + a_0(a_1 - 2a_1b_1 - b^2) \) is a square in \( \mathbb{F}_q^* \) and

\[
1 + 2b_1 + 2a_1^2 + a_1b_1 + a_0(-1 - 2b_1 + b_1^2 + a_1(3 + 2b_1)) \equiv 0 \pmod{p}
\]

(b)

\[
\begin{cases}
a_0 + 2a_2 + b_1 \equiv 0 \pmod{p}, \\
(1 + b_1)^2 - 4a_1^2 - a_0(5 + 10b_1 + 4b_1^2 + 8a_1(1 + b_1)) \equiv 0 \pmod{p}
\end{cases}
\]

(c)

\[
\begin{cases}
a_0 = 1, b_1 = 0, \\
4a_1 + 3 \equiv 0 \pmod{p}, \\
q \equiv -1 \pmod{6}
\end{cases}
\]

(d)

\[
\begin{cases}
a_0 = 1, a_1 = 0, b_1 = 0, \\
q \equiv 1, 3 \pmod{6}
\end{cases}
\]

A method similar to that employed by Hou to prove the previous theorems can be applied to study polynomials of the form \( f = x^d(a + bx^{q-1} + x^{r(q-1)}) \). For the remainder of this chapter we focus on the following two questions:

1. When does a binomial of the form \( f = x^d(a + bx^{q-1}) \) permute the field \( \mathbb{F}_{q^2} \)?

2. When does a trinomial of the form \( f = x^3(a + bx^{q-1} + x^{2(q-1)}) \) permute the field \( \mathbb{F}_{q^2} \)?
In both cases we are able to give explicit conditions on the coefficients that guarantee \( f \) is a permutation polynomial of \( \mathbb{F}_{q^2} \).

We should also note that permutation polynomials of the form \( f = x^d(a + bx^{q-1} + x^{r(q-1)}) \), have been studied by other authors as well ([88], [89]). Our approach is quite different, as we do not place any additional assumptions on the coefficients of the polynomial in question.

### 3.2 PPs of the form \( f = x(a + x^{r(q-1)}) \)

Consider a binomial of the form \( f = ax + x^{2q-1} \in \mathbb{F}_q[x] \), where \( a \neq 0 \). The necessary and sufficient conditions for \( f \) to be a permutation polynomial of \( \mathbb{F}_{q^2} \) are given in Theorem 2.4.2. The result can actually be extended to allow \( a \in \mathbb{F}_{q^2} \) (see [43]). With this consideration in mind we have a binomial of the above form with \( a \in \mathbb{F}_{q^2} \) is a permutation polynomial of \( \mathbb{F}_{q^2} \) if and only if one of the following occurs:

- \( a^{q+1} = 1, (-a)^{(q+1)/\gcd(2,q+1)} \neq 1; \)
- \( a^{q+1} \neq 1, q \) is odd, \((-a)^{(q+1)/2} = 3. \)

In fact, if \( a^{q+1} = 1 \) then the binomial, \( x(a + x^{r(q-1)}) \), is a permutation polynomial of \( \mathbb{F}_{q^2} \) if and only if \((-a)^{(q+1)/\gcd(r,q+1)} \neq 1 \) and \( \gcd(r-1,q+1) = 1 \) [90]. It is natural to ask if the second case above generalizes to arbitrary values of \( r \). The answer to this question is negative, as we will see from the following theorems.

**Remark 3.2.1** It is interesting to note that the proof of the sufficiency of Theorem 2.4.2 cases (ii) and (iii) led to the discovery of a curious hypergeometric identity. Surprisingly, this same identity resurfaces in the next section.

For the remainder of this section, our objective is to prove the following theorems:

**Theorem 3.2.2 ([47])** Let \( f = ax + x^{3q-2} \in \mathbb{F}_{q^2}[x] \), where \( a \in \mathbb{F}_{q^2}^* \). Then, \( f \) is a PP of \( \mathbb{F}_{q^2} \) if and only if one of the following occurs:
(i) \( q = 2^{2k+1} \) and \( a^{\frac{q+1}{3}} \) is a primitive 3rd root of unity.

(ii) \( q = 5 \) and \( a^2 \) is a root of \((x + 1)(x + 2)(x - 2)(x^2 - x + 1)\).

(iii) \( q = 2^3 \) and \( a^3 \) is a root of \( x^3 + x + 1 \).

(iv) \( q = 11 \) and \( a^4 \) is a root of \((x - 5)(x + 2)(x^2 - x + 1)\).

(v) \( q = 17 \) and \( a^6 = 4, 5 \).

(vi) \( q = 23 \) and \( a^8 = -1 \).

(vii) \( q = 29 \) and \( a^{10} = -3 \).

**Theorem 3.2.3** Let \( f = ax + x^{5q-4} \in \mathbb{F}_{q^2}[x] \), where \( a \in \mathbb{F}_{q^2}^* \). Then, \( f \) is a PP of \( \mathbb{F}_{q^2} \) if and only if one of the following occurs:

(i) \( q = 2^{4k+2} \) and \( a^{\frac{q+1}{5}} \) is a primitive 5th root of unity.

(ii) \( q = 3^2 \) and \( a^2 \) is a root of \((x + 1)(x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2)(x^4 + x^2 + x + 1)(x^2 + 3x + x^2 + 1)(x^4 + 2x^3 + x^2 + 2x + 1)\).

(iii) \( q = 19 \) and \( a^4 \) is a root of \((x + 1)(x + 2)(x + 3)(x + 4)(x + 5)(x + 9)(x + 10)(x + 13)(x + 17)(x^2 + 3x + 16)(x^2 + 4x + 1)(x^2 + 18x + 6)\).

(iv) \( q = 29 \) and \( a^6 \in \{15, 18, 22, 23\} \).

(v) \( q = 7^2 \) and \( a^{10} \) is a root of \( x^2 + 4x + 1 \).

(vi) \( q = 59 \) and \( a^{12} \) is a root of \((x + 4)(x + 55)(x^2 + 36)\).

(vii) \( q = 2^6 \) and \( a^{13} \) is a root of \((x^2 + x + 1)(x^2 + x + 1)\).

**Theorem 3.2.4** Let \( f(x) = ax + x^{7q-6} \in \mathbb{F}_{q^2}[x] \), where \( a \in \mathbb{F}_{q^2}^* \). Then \( f \) is a PP of \( \mathbb{F}_{q^2} \) if and only if one of the following occurs:

(i) \( q = 13 \) and \( a^2 \) is a root of \((1 + x)(2 + x)(3 + x)(4 + x)(5 + x)(6 + x)(7 + x)(8 + x)(9 + x)(10 + x)(11 + x)(12 + x + x^2)(9 + 2x + x^2)(10 + 3x + x^2)(9 + 4x + x^2)(12 + 4x + x^2)(10 + 5x + x^2)(3 + 6x + x^2)(1 + 7x + x^2)(4 + 7x + x^2)(1 + 8x + x^2)(12 + 9x + x^2)(1 + 10x + x^2)(3 + 12x + x^2)(4 + 12x + x^2)(12 + 12x + x^2)\)
(ii) $q = 3^3$ and $a^4$ is a root of $(2 + x + x^2 + x^3)(1 + 2x + x^2 + x^3)(1 + x + 2x^2 + x^3)(2 + 2x + 2x^2 + x^3)(1 + 2x + x^2 + 2x^3 + x^4 + 2x^5 + x^6)$

(iii) $q = 41$ and $a^6$ is a root of $(9 + x)(10 + x)(26 + x)(30 + x)(32 + x)(34 + x)(35 + x)(37 + x)(39 + 2x + x^2)(1 + 14x + x^2)(20 + 40x + x^2)$

The above three theorems can all be proved via the same method. We will only prove Theorem 3.2.3, i.e. we completely determine all PPs of $\mathbb{F}_{q^2}$ of the form $ax + x^{5q-4} \in \mathbb{F}_{q^2}[x]$.

**Computations**

Let $f = ax + x^{5q-4} \in \mathbb{F}_{q^2}[x]$, where $a \neq 0$, and let $0 \leq \alpha, \beta \leq q-1$ with $(\alpha, \beta) \neq (0,0)$. First suppose $q < 5$.

- When $q = 2$, we have $f(a^{-1}) = 0 = f(0)$, so $f$ cannot be a PP.
- When $q = 3$, we have $f(-a) = 0 = f(0)$, so $f$ cannot be a PP.
- When $q = 4$, we have $f = ax + x^{16} \equiv (a + 1)x \pmod{x^{15} - 1}$. In this case, $f$ is clearly a PP if and only if $a \neq 1$.

Now suppose $q \geq 5$. We compute

$$\sum_{x \in \mathbb{F}_{q^2}} f(x)^{\alpha + \beta q} = \sum_{x \in \mathbb{F}_{q^2}} (ax + x^{5q-4})^\alpha (a^q.x^q + x^{5q-4})^\beta$$

$$= \sum_{x \in \mathbb{F}_{q^2}} \sum_{i,j} \binom{\alpha}{i} (ax)^{\alpha - i} x^{(5q-4)i} \binom{\beta}{j} (a^q.x^q)^{(\beta - j)} x^{(5q-4)j}$$

$$= a^{\alpha + \beta q} \sum_{i,j} \binom{\alpha}{i} \binom{\beta}{j} a^{-i-jq} \sum_{x \in \mathbb{F}_{q^2}} x^{\alpha + \beta q + 5(q-1)(i-j)} \quad (3.2.1)$$

It is clear the inner sum is 0 unless $\alpha + \beta q \equiv 0 \pmod{q-1}$, that is, $\alpha + \beta = q - 1$.

With $0 \leq \alpha \leq q - 1$ and $\beta = q - 1 - \alpha$ the right side of (5.2.4) becomes

$$-a^{(\alpha + 1)(1-q)} \sum_{\alpha - 1 + 5(i-j) \equiv 0 \pmod{q+1}} \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{-i-jq} \quad (3.2.2)$$

41
Since $0 \leq i \leq \alpha$ and $0 \leq j \leq q - 1 - \alpha$ it follows

$$4\alpha + 4 - 5q \leq -\alpha - 1 + 5(i - j) \leq 4\alpha - 1 \quad (3.2.3)$$

Define $\Gamma(q, \alpha) := \{ n \in (q + 1)\mathbb{Z} : 4\alpha + 4 - 5q \leq n \leq 4\alpha - 1 \}$. Now we have

$$\sum_{x \in \mathbb{F}_{q^2}} f(x)^{\alpha + \beta q} = -a^{(\alpha+1)(1-q)} \Lambda(q, \alpha, a) \quad (3.2.4)$$

where

$$\Lambda(q, \alpha, a) = \sum_{-\alpha-1+5(i-j)\in\Gamma(q,\alpha)} \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{-i-jq} \quad (3.2.5)$$

Now Hermite’s criterion implies $f$ is a PP of $\mathbb{F}_{q^2}$ if and only if $0$ is the only root of $f$ in $\mathbb{F}_{q^2}$ and

$$\Lambda(q, \alpha, a) = 0 \text{ for each } 0 \leq \alpha \leq q - 1. \quad (3.2.6)$$

**Remark 3.2.5** Notice if $q + 1 \equiv 0 \pmod{5}$, then $0$ is the only root of $f$ if and only if $a^{\frac{q+1}{5}} \neq 1$.

**Lemma 3.2.6** If $f$ is a PP of $\mathbb{F}_{q^2}$, then $q + 1 \equiv 0 \pmod{5}$

*Proof.* Assume $f$ is a PP and $q \geq 5$. First suppose $5 \leq q < 8$. Note that

$$\Gamma(q, 0) = \{-3(q + 1), -2(q + 1), -(q + 1)\}.$$

By (3.2.6) we have

$$0 = \Lambda(5, 0, a) = \binom{5 - 1}{1} a^{-5} = -a^{-5}$$

and

$$0 = \Lambda(7, 0, a) = \binom{7 - 1}{1} a^{-21} = -a^{-21}.$$

In either case we have a contradiction. Now suppose $q \geq 8$. In this case notice

$$\Gamma(q, 0) = \{-4(q + 1), -3(q + 1), -2(q + 1), -(q + 1)\}.$$
So again by (3.2.6) we have

\[ 0 = \Lambda(q, 0, a) = \sum_{k=1}^{4} \left( \frac{q - 1}{k(q+1) - 1} \right)^* a^{-\left(\frac{k(q+1)-1}{5}\right)q} \]

where

\[ \binom{n}{m}^* = \begin{cases} \binom{n}{m} & \text{if } m \in \mathbb{Z} \text{ and } m \geq 0 \\ 0 & \text{otherwise} \end{cases} \]

Now if \( q + 1 \not\equiv 0 \pmod{5} \) then exactly one of \( \left( \frac{q-1}{k(q+1)-1} \right)^* \) is nonzero which contradicts (3.2.6). Thus if \( f \) is a PP of \( \mathbb{F}_{q^2} \) we must have \( q + 1 \equiv 0 \pmod{5} \).

\[ \blacksquare \]

**Remark 3.2.7** Assume \( q + 1 \equiv 0 \pmod{5} \) and \( \alpha > 0 \). The previous lemma together with (3.2.5) imply the sum \( \Lambda(q, \alpha, a) \) is empty unless \( \alpha + 1 \equiv 0 \pmod{5} \).

**Remark 3.2.8** We note that the proof of Lemma 3.2.6 goes through with 5 replaced by an odd prime \( r \). Thus if \( f = ax + x^{r(q-1)+1} \in \mathbb{F}_{q^2}[x] \), where \( a \neq 0 \) is a PP of \( \mathbb{F}_{q^2} \), then \( q + 1 \equiv 0 \pmod{r} \).

**Lemma 3.2.9** Assume \( q+1 \equiv 0 \pmod{5} \), \( \alpha > 0 \), \( \alpha + 1 \equiv 0 \pmod{5} \) and \( q \geq 4\alpha+8 \). Set \( v = a^{-\frac{q+1}{q}} \), then

\[ \Lambda(q, \alpha, a) = (-a)^{-\frac{q+1}{q}} \frac{\alpha}{q} \sum_{i=0}^{\alpha} (-1)^i \left( \frac{\alpha}{i} \right) \sum_{l=0}^{4} \left( i + \frac{4\alpha-1+l}{5} \right) v^{5i+l} \]

**Proof.** Since \( q \geq 4\alpha + 8 \) we have

\[ \Gamma(q, \alpha) = \{-4(q+1), -3(q+1), -2(q+1), -(q+1), 0\} \]

Using (3.2.5) we see

\[ \Lambda(q, \alpha, a) = \sum_{-\alpha-1+5(i-j) \in \Gamma(q, \alpha)} \left( \frac{\alpha}{i} \right) \left( \frac{q - 1 - \alpha}{j} \right) a^{-i-jq} \]
\[
\sum_{i=0}^{\alpha} \left( \binom{\alpha}{i} \right) \sum_{l=0}^{4} \left( \frac{1}{5} \left( l(q+1) - \alpha - 1 \right) + i \right) a^{-i - \frac{1}{5} \left( l(q+1) - \alpha - 1 \right) + i} q
\]

\[
= (-1)^{\alpha + 1} q a^{\frac{\alpha + 1}{5}} q \sum_{i=0}^{\alpha} \left( \binom{\alpha}{i} \right) \sum_{l=0}^{4} \left( \frac{1}{5} \left( l(q+1) - \alpha - 1 \right) + i + \frac{\alpha - 1 + l}{\alpha} \right) a^{-\frac{2\alpha + 1}{5} q(l+5)}
\]

\[
= (-a)^{\frac{\alpha + 1}{5} q} \sum_{i=0}^{\alpha} (-1)^i \left( \frac{\alpha}{i} \right) \sum_{l=0}^{4} \left( i + \frac{4\alpha - 1 + l}{\alpha} \right) q^5 i + l.
\]

Between the second and third line we use \((-m)_n = (-1)^n \binom{n+m-1}{m-1}\).

**Lemma 3.2.10** Assume \(q + 1 \equiv 0 \pmod{5}\), \(\alpha + 1 \equiv 0 \pmod{5}\), and \(\alpha > 0\). Then \(\Gamma(q, \alpha)\) contains exactly five consecutive multiples of \(q + 1\) unless \(\alpha = \frac{q-1}{2} \in \mathbb{Z}\), \(\alpha = \frac{q-3}{4} \in \mathbb{Z}\), or \(\alpha = \frac{3q-1}{4} \in \mathbb{Z}\).

**Proof.** Since \(\Gamma(q, \alpha)\) is contained in the interval \([4\alpha + 4 - 5q, 4\alpha - 1]\), which has length \(5(q - 1)\), we must have \(4 \leq |\Gamma(q, \alpha)| \leq 5\).

Suppose \(4 = |\Gamma(q, \alpha)|\). Choose \(k\) so \((k - 3)(q + 1), (k - 2)(q + 1), (k - 1)(q + 1), k(q + 1) = \Gamma(q, \alpha)\). Note \(q \geq 9\) and \(\alpha > 0\) force \(k \in \{0, 1, 2, 3\}\). We have the following inequalities

\[
\begin{cases}
4\alpha - 1 \leq k(q + 1) + q \\
(k - 3)(q + 1) - q \leq 4\alpha + 4 - 5q.
\end{cases} \tag{3.2.7}
\]

Since \(4\alpha - 1, 4\alpha + 4 - 5q \equiv 0 \pmod{5}\) it follows

\[
\begin{cases}
4\alpha - 1 \leq k(q + 1) + q - 4 \\
(k - 3)(q + 1) - q + 4 \leq 4\alpha + 4 - 5q.
\end{cases} \tag{3.2.8}
\]

Since \(a \leq q - 1\) and \(0 \leq k \leq 3\), taking the sum of the inequalities in (3.2.8) reveals \(k \in \{0, 1, 2\}\). If \(k = 0\) then \(\alpha = \frac{q-3}{4}\), if \(k = 1\) then \(\alpha = \frac{q-1}{2}\), and if \(k = 2\) then \(\alpha = \frac{3q-1}{4}\).
Lemma 3.2.11 Assume \( q + 1 \equiv 0 \pmod{5} \) and \( y := a^{q+1} \neq 1 \) is a 5th root of unity. If \( \alpha + 1 \not\equiv 0 \pmod{5} \), then \( \Lambda(q, \alpha, a) = 0 \). If \( \alpha + 1 \equiv 0 \pmod{5} \), then for \( 1 \leq \alpha \leq q - 1 \) we have

\[
\Lambda(q, \alpha, a) = \begin{cases} 
-a^{-\frac{1}{5}(\alpha+1)}(1 + y + y^2 + y^3) & \text{if } \alpha = \frac{q-1}{4}, \; \alpha \in \mathbb{Z} \\
-a^{-\frac{1}{5}(\alpha+1)}(y^{-1} + 1 + y + y^2) & \text{if } \alpha = \frac{q-1}{2}, \; \alpha \in \mathbb{Z} \\
-a^{-\frac{1}{5}(\alpha+1)}(y^{-2} + y^{-1} + 1 + y) & \text{if } \alpha = \frac{3q-1}{4}, \; \alpha \in \mathbb{Z} \\
0 & \text{otherwise.}
\end{cases}
\]

Proof. If \( \alpha + 1 \not\equiv 0 \pmod{5} \), then Remark 3.2.7 gives the desired result. Assume \( \alpha + 1 \equiv 0 \pmod{5} \). First suppose \( \alpha \notin \{\frac{q-3}{4}, \frac{q-1}{2}, \frac{3q-1}{4}\} \). Lemma 3.2.10 implies we can find a set, \( K \), of five consecutive integers such that \( K(q+1) = \Gamma(q, \alpha) \).

We have

\[
\Lambda(q, \alpha, a) = \sum_{-\alpha-1+5(i-j)\in\Gamma(q, \alpha)} \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{-i-jq}
= \sum_{k\in K} \sum_{-\alpha-1+5(i-j)=k(q+1)} \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{-i+j}
= \sum_{k\in K} a^{-\frac{1}{5}[\alpha+1+k(q+1)]} \sum_{i-j=\frac{1}{5}[\alpha+1+k(q+1)]} \binom{\alpha}{\alpha-i} \binom{q-1-\alpha}{j}
= a^{-\frac{1}{5}(\alpha+1)} \sum_{k\in K} y^{-k} \sum_{\alpha-i=\frac{1}{5}[4\alpha-1-k(q+1)]} \binom{q-1}{\alpha-i}
= a^{-\frac{1}{5}(\alpha+1)} \sum_{k\in K} y^{-k} \left(\frac{q-1}{\frac{1}{5}[4\alpha-1-k(q+1)]}\right)
= -a^{-\frac{1}{5}(\alpha+1)} \sum_{k\in K} y^{-k} = 0.
\]

Now suppose \( \alpha = \frac{q-1}{2} \). By the above computation and the previous lemma we have \( K = \{-2, -1, 0, 1\} \), thus

\[
\Lambda(q, \alpha, a) = -a^{-\frac{1}{5}(\alpha+1)}(y^{-1} + 1 + y + y^2). \quad (3.2.10)
\]
Similarly if $\alpha = \frac{q - 3}{4}$, we have

$$\Lambda(q, \alpha, a) = -a^{-\frac{1}{5}(\alpha+1)}(1 + y + y^2 + y^3).$$

(3.2.11)

Lastly, if $\alpha = \frac{3q - 1}{4}$, we have

$$\Lambda(q, \alpha, a) = -a^{-\frac{1}{5}(\alpha+1)}(y^{-2} + y^{-1} + 1 + y).$$

(3.2.12)

Proof of Theorem 3.2.3

Proof. $(\Leftarrow)$ Cases (ii)-(vii) are easily verified by a computer. Assume (i), that is $q = 2^{4k+2}$ and $a^{\frac{q+1}{5}} \neq 1$ is a fifth root of unity. Lemma 3.2.11 gives $\Lambda(q, \alpha, a) = 0$ for each $0 \leq \alpha \leq q - 1$. Also, by Remark 3.2.5, 0 is the only root of $f$, so $f$ is a PP of $\mathbb{F}_{q^2}$ by (3.2.5).

$(\Rightarrow)$ Assume $f$ is a PP. By Lemma 3.2.6 we have $q + 1 \equiv 0 \pmod{5}$. Let $y := a^{\frac{q+1}{5}}$. If $y \neq 1$ is a fifth root of unity then Lemma 3.2.11 implies $q$ must be even. Thus $q = 2^{4k+2}$ and we have case (i).

Now suppose $1 + y + y^2 + y^3 + y^4 \neq 0$. The sum in the RHS of Lemma 3.2.9 is a polynomial in $v (= y^{-q})$ and can be easily computed for small values of $\alpha$ with the help of a computer algebra system. For a few values of $\alpha$ we find

$$\Lambda(q, \alpha, a) = (-a)^{\frac{4+1}{5}q}v(1+v+v^2+v^3+v^4)$$

$$\begin{cases} 5^{-4}g_4(v) & \text{if } \alpha = 4, q \geq 24 \\ 5^{-10}g_9(v) & \text{if } \alpha = 9, q \geq 44 \\ 5^{-16}g_{14}(v) & \text{if } \alpha = 14, q \geq 64 \\ 5^{-28}g_{24}(v) & \text{if } \alpha = 24, q \geq 104. \\ \end{cases}$$

(3.2.13)
Write $R(p_1, p_2)$ for the resultant of polynomials $p_1, p_2$, it follows

$$GCD(R(g_4, g_9), R(g_4, g_{14})) = 2^{15}3^35^{197}. \quad (3.2.14)$$

Thus if $q \geq 64$ we must have $p (= char\mathbb{F}_{q^2}) \in \{2, 3\}$. Since $q + 1 \equiv 0 \pmod{5}$ there are only a few prime powers $q < 64$ with $p (= char\mathbb{F}_{q^2}) \neq 2, 3$.

- When $q = 19$, a computer search results in case (iii)
- When $q = 29$, a computer search results in case (iv)
- When $q = 49$, a computer search results in case (v)
- When $q = 59$, a computer search results in case (vi)

When $p = 2$ we have $GCD(g_4, g_{24}) = x$ thus $q < 104$. Since $q + 1 \equiv 0 \pmod{5}$ and $q > 4$ we only need to consider $q = 64$. A computer search results in case (vii).

When $p = 3$ we have $GCD(g_4, g_9) = 1$ thus $q < 44$. Again since $q + 1 \equiv 0 \pmod{5}$ we only need to consider $q = 9$. A computer search results in case (ii).

Both Theorem 3.2.2 and Theorem 3.2.4 are proved using a similar method. It seems that such a method can be applied to binomials of the form $f = ax + x^{r(q-1)+1}$ where $r$ is an odd prime. This naturally leads to the following, which was a conjecture but is now a theorem of Hou.

**Theorem 3.2.12 ([44])** Let $r > 2$ be a fixed prime. If both $(q + 1) \equiv 0 \pmod{r}$ and $a^{\frac{q+1}{r}}$ is not an $r$-th root of unity; we conjecture there are only finitely many values $(q, a)$ where $a \in \mathbb{F}_{q^2}^*$, for which $f = ax + x^{r(q-1)+1} \in \mathbb{F}_{q^2}[x]$ is a permutation polynomial of $\mathbb{F}_{q^2}$.

We note that based on computer search evidence, it appears the requirement that $r > 2$ be a prime in the above theorem can be relaxed to simply $r > 2$. 

47
3.3 PPs of the form \( f = x^3(a + x^{(q-1)}) \)

As shown in the previous section, it seems that when \( q \) is large enough in relation to \( r \) and \( a^{q+1} \neq 1 \), the binomial \( f = x(a + x^{r(q-1)}) \) is not a permutation polynomial of \( \mathbb{F}_{q^2} \). In particular, there is no extension of Theorem 2.4.2 cases (ii) and (iii) to values of \( r > 2 \). However, it turns out that we can prove a similar theorem for \( d = 3 \). The purpose of the present section is to prove the following theorem.

**Theorem 3.3.1** Let \( f = x^3(a + x^{(q-1)}) \) \( \in \mathbb{F}_q[x] \), with \( a \neq 0 \). Then \( f \) is a PP of \( \mathbb{F}_{q^2} \) if and only if one of the following occurs:

1. \( a = 1 \) and \( q \equiv 1 \) (mod 4)
2. \( a = \frac{1}{3} \) and \( q \equiv -1 \) (mod 6)
3. \( a = -\frac{1}{3} \) and \( q \equiv -1 \) (mod 12).

**Preliminaries**

In order to prove the Theorem 3.3.1 we need a few preliminary results. Let \( \mathbb{Z}_p \) denote the ring of \( p \)-adic integers and \( \mathbb{Q}_p \) it's field of fractions. For an integer \( a \geq 0 \) and \( z \in \mathbb{Q}_p \), we define \( (z)_a^\ast = \frac{(z-a+1)_a}{(1)_a} \). If \( z \in \mathbb{Q} \), we also define

\[
(z)_a^\ast = \begin{cases} 
(\frac{z}{a}) & \text{if } z \in \mathbb{Z} \\
0 & \text{otherwise.}
\end{cases}
\]

**Lemma 3.3.2** ([42]) Let \( q \) be a power of a prime \( p \) and \( a \) and integer with \( 0 \leq a \leq q - 1 \). Let \( z_1, z_2 \in \mathbb{Z}_p \) such that \( z_1 \equiv z_2 \pmod q \). Then \( (\frac{z_1}{a}) \equiv (\frac{z_2}{a}) \pmod p \).

**Lemma 3.3.3** Let \( 0 \leq s < q^2 - 1 \). Write \( s = \alpha + \beta q \) where \( 0 \leq \alpha, \beta \leq q - 1 \). Assume
$(3, q - 1) = 1$, (note that this must be the case if $f$ is a PP). Then we have

$$\sum_{x \in \mathbb{F}_{q^2}} f(x)^* = \begin{cases} 
0 & \text{if } \alpha + \beta \neq q - 1 \\
(-1)^{q - \frac{\alpha + 1}{2}} a^{-\frac{\alpha - 1}{2} - q} \left[ (-1)^{\frac{\alpha + 1}{2}} a^{\frac{\alpha - 1}{2}} \sum_i \left( \frac{\alpha + 1}{2} - i \right)^* (-1)^i a^{2i+1} \right] + \sum_i \left( \frac{\alpha + 1}{2} - i \right)^* (-1)^i a^{2i} & \text{if } \alpha + \beta = q - 1.
\end{cases}$$

Proof.

$$\sum_{x \in \mathbb{F}_{q^2}} f(x)^{\alpha+\beta} = \sum_{x \in \mathbb{F}_{q^2}} x^{3(\alpha+\beta)} (a + x^{2(q-1)})^\alpha (a + x^{2(1-q)})^\beta$$

$$= \sum_{x \in \mathbb{F}_{q^2}} x^{3(\alpha+\beta)} \sum_i \begin{pmatrix} \alpha \\ i \end{pmatrix} a^{\alpha-i} x^{2(q-1)} \sum_j \begin{pmatrix} \beta \\ j \end{pmatrix} a^{\beta-j} x^{2j(1-q)}$$

$$= a^{\alpha+\beta} \sum_{i,j} \begin{pmatrix} \alpha \\ i \end{pmatrix} \begin{pmatrix} \beta \\ j \end{pmatrix} a^{-(i+j)} \sum_{x \in \mathbb{F}_{q^2}} x^{3(\alpha+\beta) + 2(q-1)(i-j)}.$$  

Since $(3, q - 1) = 1$, the inner sum is 0 unless $\alpha + \beta q \equiv 0 \pmod{q - 1}$. This forces $\alpha + \beta = q - 1$. With $\beta = q - 1 - \alpha$ the above becomes:

$$= - \sum_{2(i-j)-3(\alpha+1)\equiv 0 \pmod{q+1}} \begin{pmatrix} \alpha \\ i \end{pmatrix} \begin{pmatrix} q - 1 - \alpha \\ j \end{pmatrix} a^{-(i+j)}.$$  

Since $0 \leq i \leq \alpha$ and $0 \leq j \leq q - 1 - \alpha$ we must have

$$-\alpha - 1 - 2q \leq 2(i - j) - 3(\alpha + 1) \leq -\alpha - 3,$$

or equivalently

$$\alpha + 1 - q \leq i - j \leq \alpha.$$  

Thus if $2(i-j)-3(\alpha+1) \equiv 0 \pmod{q+1}$ then $2(i-j)-3(\alpha+1) \in \{-2(q+1), -(q+1)\}$. Now the sum $-\sum_{x \in \mathbb{F}_{q^2}} g_3(x)^{\alpha+\beta q}$ becomes

$$= \sum_{-3(\alpha+1)+2(i-j)=-2(q+1),-2(q+1)} \begin{pmatrix} \alpha \\ i \end{pmatrix} \begin{pmatrix} q - 1 - \alpha \\ j \end{pmatrix} a^{-(i+j)} \quad (3.3.15)$$
Theorem 3.3.4 Let \( n > 0 \) be a positive integer. Then

\[
\sum_{k \leq 2n+1} \binom{2n+1}{k} \left[ \prod_{j=1}^{2n+1} (2n+1-2k-2j) \right] (-1)^k \left( \frac{1}{3} \right)^{2k+1} + \\
\sum_{k \leq 2n+1} \binom{2n+1}{k} \left[ \prod_{j=0}^{2n} (2n-2k-2j) \right] (-1)^k \left( \frac{1}{3} \right)^{2k} = 0
\]
Proof. Define

\[ F_1(n, k) = \binom{2n+1}{k} \left[ \prod_{j=1}^{2n+1} (2n+1-2k-2j) \right] (-1)^k \left( \frac{1}{3} \right)^{2k+1} \]
\[ F_2(n, k) = \binom{2n+1}{k} \left[ \prod_{j=0}^{2n} (2n-2k-2j) \right] (-1)^k \left( \frac{1}{3} \right)^{2k} \]

\[ S_1(n) = \sum_k F_1(n, k) \]
\[ S_2(n) = \sum_k F_2(n, k). \]

Now with the help of Zeilberger’s algorithm we find:

\[ 27F_1(n+2, k) + 8 \left( 36n^2 + 126n + 113 \right) F_1(n+1, k) + 192(n+1)^2(2n+3)^2 F_1(n, k) = G_1(n, k + 1) - G_1(n, k) \]

where \( G_1(n, k) = F_1(n, k)R_1(n, k) \), and

\[ R_1(n, k) = \left( \frac{1}{\prod_{j=2}^{5}(2n-k+j)} \right) \cdot (9k(2n-2k+1)(32n+1)(2n+3) \]
\[ (12n^2 + 48n + 49)k^2 - 4(n+1)(2n+3)(96n^3 + 468n^2 + 720n + 343)k \]
\[ + 4(n+1)(2n+3)(24n^4 + 156n^3 + 358n^2 + 337n + 105))) \]

Using the same algorithm we see:

\[ 27F_2(n+2, k) + 8 \left( 36n^2 + 126n + 113 \right) F_2(n+1, k) + 192(n+1)^2(2n+3)^2 F_2(n, k) = G_2(n, k + 1) - G_2(n, k) \]

where \( G_2(n, k) = F_2(n, k)R_2(n, k) \), and

\[ R_2(n, k) = \left( \frac{1}{\prod_{j=2}^{5}(2n-k+j)} \right) \cdot (9k(n-k+1)(64(n+1)(2n+3) \]
Thus we can conclude both $S_1(n)$ and $S_2(n)$ satisfy the same second order recurrence:

\[
27S_1(n + 2) + 8 \left(36n^2 + 126n + 113\right) S_1(n + 1) + 192(n + 1)^2(2n + 3)^2 S_1(n) = 0
\]

\[
27S_2(n + 2) + 8 \left(36n^2 + 126n + 113\right) S_2(n + 1) + 192(n + 1)^2(2n + 3)^2 S_2(n) = 0.
\]

It is simple to verify that

\[
S_1(0) = -\frac{2}{9} = -S_2(0)
\]

\[
S_1(1) = \frac{368}{243} = -S_2(1).
\]

Therefore $S_1(n) = -S_2(n)$ for all positive integers $n$, so the proof of the Theorem is complete.

As per Remark 3.2.1, making the substitution $k \mapsto 2n + 1 - k$ and $j \mapsto 2n + 1 - j$ shows the above theorem is simply a reformulation of [Theorem 1.2 [42]].

**Proof of Theorem 3.3.1**

Proof. ($\Rightarrow$) First we show $q$ must be odd. Suppose $q$ is even and let $\alpha = 1, \beta = q - 2$ in Lemma 3.3.3. Notice only the second sum appears since $\frac{\alpha + q}{2} \notin \mathbb{Z}$. Then we have

\[
\sum_{x \in \mathbb{F}_{q^2}^*} f(x)^{1+(q-2)q} = \sum_{i=0}^{1} \binom{1}{i} \binom{q-1}{1} (-1)^i a^{2i} = a^2 \neq 0.
\]
Since \( f(0) = 0 \), it follows \( f \) is a PP only when \( q \) is odd.

Now assume \( q \) is odd. Again take \( \alpha = 1, \beta = q - 2 \), and note \( g_3(0) = 0 \). From (3.3.15) we see:

\[
- \sum_{x \in \mathbb{F}_{q^2}} f(x)^{1+(q-2)q} = \sum_{2(i-j)=-(q+1)+6} \left( \frac{1}{i} \right) \left( \frac{q-2}{j} \right) a^{-(i+j)} + \quad (3.3.17)
\]

\[
\sum_{2(i-j)=-2(q+1)+6} \left( \frac{1}{i} \right) \left( \frac{q-2}{j} \right) a^{-(i+j)}
\]

\[
= \left( \frac{q-2}{q-5} \right) a^{-\frac{q-3}{2}} + \left( \frac{q-2}{q-3} \right) a^{-\frac{q-1}{2}} + \left( \frac{q-2}{q-2} \right) a^{-(q-2)}
\]

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

\[
= \frac{1}{2} \left[ (-1)^{\frac{q+1}{2}} a^{-\frac{q-1}{2}} [3a^2 - 1] + 2a \right]
\]

Set \( \epsilon = (-1)^{\frac{q+1}{2}} a^{-\frac{q-1}{2}} (= \pm 1 \in \mathbb{F}_q) \)

\[
= \frac{1}{2} \left[ \epsilon [3a^2 - 1] + 2a \right]
\]

The above takes value 0 only when

\[
3a^2 + 2\epsilon a - 1 = (3a - \epsilon)(a + \epsilon) = 0 \quad (3.3.18)
\]

i.e. we must have

\[
a = \frac{\epsilon}{3} \text{ or } -\epsilon \implies a \in \{ \pm 1, \pm \frac{1}{3} \}.
\]

First suppose \( a = -\epsilon (= \pm 1) \), then

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

- If \( q \equiv 1 \pmod{4} \) then \( a^{\frac{q+1}{2}} = 1 \), so we must have \( a = 1 \). This is case (1)

- If \( q \equiv 3 \pmod{4} \) then \( a^{\frac{q+1}{2}} = -1 \) which is impossible (since \( a = \pm 1 \) and \( \frac{q+1}{2} \) is even).

53
Now suppose \( a = \frac{\xi}{3} (= \pm \frac{1}{3}) \), and \( \epsilon = 1 \). It follows that \( \epsilon^{\frac{q+1}{2}} = (-1)^{\frac{q+1}{2}} \eta(\frac{1}{3}) \).

If \( \epsilon = -1 \), then \( \eta(\frac{1}{3}) = 1 \implies q \equiv \pm 1 \pmod{12} \implies q \equiv -1 \pmod{12} \), since we require \((3, q-1) = 1\). This is case (3).

If \( \epsilon = 1 \) then there are two possibilities:

- \((-1)^{\frac{q+1}{2}} = 1 = \eta(\frac{1}{3})\)
  
  In this case we have \( q \equiv -1 \pmod{4} \) and \( q \equiv \pm 1 \pmod{12} \implies q \equiv -1 \pmod{12} \).

- \((-1)^{\frac{q+1}{2}} = -1 = \eta(\frac{1}{3})\)
  
  In this case we have \( q \equiv 1 \pmod{4} \) and \( q \equiv \pm 5 \pmod{12} \implies q \equiv -1 \pmod{6} \).

• Both of these possibilities give case (2).

(\( \equiv \)) First consider case (1). Then \( q \equiv 1 \pmod{4} \) and \( a = 1 \). From Lemma 3.3.3, we may assume \( \alpha + \beta = q - 1 \) and \( \alpha \) is odd. By (3.3.16) we have:

\[
- \sum_{x \in \mathbb{F}_q^2} f(x)^{\alpha + \beta q} = \left( \sum_{i+j = \frac{q-\alpha}{2}} + \sum_{i+j = q - \frac{\alpha+1}{2}} \right) \left( q - 1 - \alpha \right) (\alpha \choose i) (\frac{q-1}{j}) a^{-(\alpha-i+j)} \\
= \left( q - 1 \right) \left( \frac{q-1}{\frac{q-\alpha}{2}} \right) + \left( q - 1 \right) \left( q - \frac{\alpha+1}{2} \right) \\
= (-1)^{\frac{q-\alpha}{2}} - 1 + (-1)^{\frac{q-\alpha+1}{2}} \\
= - \left[ (-1)^{\frac{1-\alpha}{2}} + (-1)^{\frac{\alpha+1}{2}} \right] \\
= 0.
\]

Now consider cases (2) and (3). By Lemma 2.2 it suffices to show that for each odd integer \( 0 \leq \alpha \leq q - 1 \) we have

\[
(-1)^{\frac{q+1}{2}} a^{\frac{q+1}{2}} \sum_{i} \left( \frac{\alpha}{i} \right) \left( \frac{\alpha+q-1-i}{\alpha} \right) (-1)^i a^{2i+1} + \sum_{i} \left( \frac{\alpha}{i} \right) \left( q + \frac{\alpha-1}{2} - i \right) (-1)^i a^{2i} = 0.
\]

In case (2) we have \((-1)^{\frac{q+1}{2}} (a)^{\frac{q+1}{2}} = (-1)^{\frac{q+1}{2}} (\frac{1}{3})^{\frac{q+1}{2}} = 1\). While in case (3) we have \((-1)^{\frac{q+1}{2}} (a)^{\frac{q-1}{2}} = (-1)^{\frac{q+1}{2}} (-\frac{1}{3})^{\frac{q-1}{2}} = -1\). Thus in either case, the first sum takes the
same value as
\[ \sum_i \left( \frac{\alpha + q}{2} - 1 - i \right) (-1)^i \left( \frac{1}{3} \right)^{2i+1}. \]

Now we only have to show that
\[ \sum_i \left( \frac{\alpha + q}{2} - 1 - i \right) (-1)^i \left( \frac{1}{3} \right)^{2i+1} + \sum_i \left( \frac{q + \alpha - 1}{2} - i \right) (-1)^i \left( \frac{1}{3} \right)^{2i} = 0 \]
in \( \mathbb{F}_p \). Write \( \alpha = 2n + 1 \), using Lemma 5.3.5 the LHS of the above becomes
\[
\frac{1}{\alpha!2^n} \left[ \sum_i \left( \begin{array}{c} 2n + 1 \\ i \end{array} \right) \left( \prod_{j=1}^{2n+1} (2n + 1 - 2i - 2j) \right) (-1)^i \left( \frac{1}{3} \right)^{2i+1} + \sum_i \left( \begin{array}{c} 2n + 1 \\ i \end{array} \right) \left( \prod_{j=0}^{2n} (2n - 2i - 2j) \right) (-1)^i \left( \frac{1}{3} \right)^{2i} \right].
\]

Thus Theorem 3.3.4 gives the above sum is zero, so the proof of Theorem 3.3.1 is complete.

At this point, it is natural to wonder if these results can be generalized to binomials of the form \( f = x^d (a + x^{2(q-1)}) \) where \( d > 3 \). Unfortunately continuing with the current method fails. Notice when \( d > 3 \), the sum in (3.3.17) contains more than three terms, so we are not able to derive necessary conditions from (3.3.17) alone.

### 3.4 PPs of the form \( f = x^3(a + bx^{q-1} + x^{2(q-1)}) \)

In this section we wish to completely determine PPs of \( \mathbb{F}_{q^2} \) of the form \( f = x^3(a + bx^{q-1} + x^{2(q-1)}) \) \( \in \mathbb{F}_q[x] \), with \( b \neq 0 \). Notice if \( b = 0 \), then \( f \) is of the form \( f = x^3(a + x^{2(q-1)}) \) \( \in \mathbb{F}_q[x] \) and the permutation behavior of \( f \) is completely determined by Theorem 3.3.1. To this end we have the following theorem

**Theorem 3.4.1** Let \( p \) be an odd prime and \( q \) a power of \( p \). Define \( f = x^3(a + bx^{q-1} + x^{2(q-1)}) \) \( \in \mathbb{F}_q[x] \). Then \( f \) is a PP of \( \mathbb{F}_{q^2} \) if and only if \( (3, q - 1) = 1 \) and one of the following occurs:
(1) $a = b = 0$ and $(2q + 1, q^2 - 1) = 1$

(2) $a = 1$ and $b^2 - 4$ is a square in $\mathbb{F}_q^\times$.

(3) $b = 0$ and one of the following occurs:
   
   (i) $a = 1$ and $q \equiv 1$ (mod 4)
   
   (ii) $a = \frac{1}{3}$ and $q \equiv -1$ (mod 6)
   
   (iii) $a = -\frac{1}{3}$ and $q \equiv -1$ (mod 12).

(4) $a = 0$ and $b \neq \pm 1$

(5) $a(a - 1)b \neq 0$, $b^2 = 3a + 1$, and $1 - a$ is a square in $\mathbb{F}_q^\times$.

**Preliminaries**

Before we are ready to prove the above theorem, we need a few preliminary results.

**Proposition 3.4.2** Suppose $f \in \mathbb{F}_q[x]$ is an irreducible cubic. Then the discriminant of $f$, $D(f)$, must be a square in $\mathbb{F}_q$.

**Proof.** We may assume $f$ is monic. Write $f = (x - r_1)(x - r_2)(x - r_3)$. It is clear that $\mathbb{F}_{q^3}$ is a splitting field for $f$. It follows that the Galois group of $f$ is $Aut(\mathbb{F}_{q^3}/\mathbb{F}_q) = A_3$. Since $Aut(\mathbb{F}_{q^3}/\mathbb{F}_q)$ contains only even permutations, $D(f)$ must be a square in $\mathbb{F}_q$. ■

Let $f$ be defined as above and let $s \in \mathbb{Z}$ with $1 \leq s \leq q^2 - 2$. Write $s = \alpha + \beta q$, with $0 \leq \alpha, \beta \leq q - 1$. We compute the power sum

$$
\sum_{x \in \mathbb{F}_q^2} f(x)^s = \sum_{x \in \mathbb{F}_q^2} x^{3(\alpha+\beta q)}(a + bx^{q-1} + x^{2(q-1)})^\alpha(a + bx^{1-q} + x^{2(1-q)})^\beta
$$

$$
= \sum_{x} x^{3(\alpha+\beta q)} \sum_{i,j} \binom{\alpha}{i} \binom{\beta}{j} a^{\alpha - i}b^{i-k}x^{(q-1)(i-k+2k)} a^{\beta - j}b^{j-l}x^{(1-q)(j-l+2l)}
$$

56
\[
= \sum_{i,j} \binom{\alpha}{i} \binom{\beta}{j} \binom{i}{k} \binom{j}{l} a^{\alpha+\beta-i-j} b^{i-k+j-l} \sum_x x^{3(\alpha+\beta q) + (q-1)(i+k-j-l)}
\]

It is clear that the above sum is 0 unless \(\alpha + \beta q \equiv 0 \pmod{q-1}\), or equivalently \(\beta = q-1 - \alpha\). Using this fact we see \(3(\alpha + \beta q) \equiv -3(\alpha + 1)(q-1) \pmod{q^2-1}\), so the above sum becomes

\[
= \sum_{i,j} \binom{\alpha}{i} \binom{\beta}{j} \binom{i}{k} \binom{j}{l} a^{\alpha+\beta-i-j} b^{i-k+j-l} \sum_x x^{(q-1)(-3(\alpha+1)+i+k-j-l)}
\]

\[
= - \sum_{-3(\alpha+1)+i+k-j-l \equiv 0 \pmod{q+1}} \binom{\alpha}{i} \binom{\beta}{j} \binom{i}{k} \binom{j}{l} a^{\alpha+\beta-i-j} b^{i-k+j-l}
\]

\[
= -S_q(\alpha, a, b).
\]

By Hermite's Criterion, \(f\) is a PP of \(\mathbb{F}_{q^2}\) if and only if

- 0 is the only root of \(f\) and
- \(S_q(\alpha, a, b) = 0\) for each \(0 \leq \alpha \leq q-1\).

**Proof of Theorem 3.4.1 under the assumption** \(a(a-1)b = 0\)

Recall that \(q\) is a power of an odd prime \(p\), and \((3, q-1) = 1\).

**Case (1):** We have \(f = x^{2q+1}\) which is clearly a PP of \(\mathbb{F}_{q^2}\) if and only if \((2q+1, q^2-1) = 1\).

**Case (2):** We claim \(f = x^3(1+bx^{q-1}+x^{2q-1})\) is a PP of \(\mathbb{F}_{q^2}\) if and only if \(b^2 - 4\) is a square in \(\mathbb{F}_q^*\). Note that \(b^2 - 4\) is a square in \(\mathbb{F}_q^*\) if and only if the polynomial \(g = x^2 + bx + 1 \in \mathbb{F}_q[x]\) has two distinct roots in \(\mathbb{F}_q\).

**Proof.** (Of the claim) \((\Leftarrow)\) Let \(x \in \mathbb{F}_{q^2}\) and set \(y = f(x)\).

1° Suppose \(y \neq 0\). Clearly \(x \neq 0\). Let \(t = \frac{y}{x} = x^2 + bx^{q+1} + x^{2q} \in \mathbb{F}_q\). Then \(x = \frac{y}{t}\), so

\[
y = \left(\frac{y}{t}\right)^3 + b \left(\frac{y}{t}\right)^{q+2} + \left(\frac{y}{t}\right)^{2q+1} = \frac{1}{t^3} (y^3 + by^{q+2} + y^{2q+1}).
\]
Thus $t^3$ is unique and $(3, q - 1) = 1$, so $t$ is unique.

2º Now suppose $y = 0$. We want to show $x = 0$ as well. Suppose $x \neq 0$. Then we have

$$1 + bx^{q-1} + x^{2(q-1)} = 0,$$

so $x^{q-1}$ is a root of $g = x^2 + bx + 1 \in \mathbb{F}_q[x]$, thus we can conclude $x^{q-1} \in \mathbb{F}_q$. This gives

$$1 = (x^{q-1})^{q-1} = x^{(q-1)^2} = x^{q^2 - 2q + 1} = (x^{1-q})^2.$$

It follows that $x^{q-1} = \pm 1$, so $b = \pm 2$, thus $g = (x \pm 1)^2$ which is a contradiction. In either case $x$ is uniquely determined by $y = f(x)$, so the sufficiency in this case is complete.

$(\Rightarrow)$ Suppose for contradiction that $g = x^2 + bx + 1 \in \mathbb{F}_q[x]$ does not have two distinct roots in $\mathbb{F}_q$.

1º Assume $g$ is irreducible over $\mathbb{F}_q$. Let $\epsilon \in \mathbb{F}_q^2$ be a root of $g$. Then $\epsilon^{q+1} = 1$, so there is some $x_1 \in \mathbb{F}_q^2$ with $x_1^{q-1} = \epsilon$. It follows that

$$f(x_1) = x_1^3(1 + bx_1^{q-1} + x_1^{2(q-1)}) = x_1^3f(\epsilon) = 0 = f(0)$$

which contradicts the fact that $f$ is a PP of $\mathbb{F}_q^2$.

2º Assume $g$ is reducible. Then we must have $g = (x + \epsilon)^2$ with $\epsilon = \pm 1$. In either case we have $\epsilon^{q+1} = 1$ so again there is some $x_1 \in \mathbb{F}_q^2$ with $x_1^{q-1} = \epsilon$, which again gives $f(x_1) = 0 = f(0)$ a contradiction.

**Case (3):** This is precisely Theorem 3.3.1

**Case IV:** In this case we have $f = x^3(bx^{q-1} + x^{2(q-1)})$.

First assume $b = \pm 1$. It is clear $f(0) = 0$. We claim that there is some $x_1 \in \mathbb{F}_q^*$ with $f(x_1) = 0$. Since $(-b)^{q+1} = b^2 = 1$, there is some $x_1 \in \mathbb{F}_q^*$ with $x_1^{q-1} = -b$. Thus

$$f(x_1) = x_1^3(bx_1^{q-1} + x_1^{2(q-1)}) = x_1^3(-b^2 + b^2) = 0 = f(0),$$

58
so $f$ cannot be a PP if $b = \pm 1$. 

Now assume $b \neq \pm 1$. We use Hermite’s Criterion to show $f$ is a PP. Suppose for contradiction that $f$ has a root $x_1$ in $\mathbb{F}_{q^2}^*$. Then we have 

$$x_1^3(bx^{q-1} + x^{2(q-1)}) = 0 \implies -b = x^{q-1} \implies (-b)^{q+1} = 1 \implies b^2 = 1,$$

which is clearly a contradiction. Thus if $b \neq \pm 1$, then 0 is the only root of $f$. Now we compute the power sum as before to see:

$$\sum_{x \in \mathbb{F}_{q^2}} f(x)^{\alpha + \beta q} = \sum_{x \in \mathbb{F}_{q^2}^*} (x^3(bx^{q-1} + x^{2(q-1)})^{\alpha + \beta q}
\left(\begin{array}{c}
\alpha \\
\beta
\end{array}\right)
\left(\begin{array}{c}
q-1-
\alpha
\beta
\\
\beta
\end{array}\right)

b^{-(i+j)}.

(3.4.19)$$

Letting $i$ run over the interval $[0, \alpha]$ and $j$ over the interval $[0, q-1-\alpha]$ we see

$$-2q-1 \leq -\alpha + i - j - q - 2 \leq -q-2.$$ 

Since $-2(q + 1) < -2q - 1$ and $-(q + 1) > -q - 2$, the sum in (3.4.19) is empty, i.e. it has value 0. Thus by Hermite’s Criterion, $f$ is a PP. We conclude $f = x^3(bx^{q-1} + x^{2(q-1)})$ is a PP of $\mathbb{F}_q^2$ if and only if $b \neq \pm 1$, so the proof of this case is complete.

**Sufficiency of Theorem 3.4.1 under the assumption $a(a-1)b \neq 0$.**

We use the notation $\text{Tr}(z)$ for $\text{Tr}_{q^2/q}(z)$, and $N(z)$ for $\mathbb{N}_{q^2/q}(z)$.

**Proposition 3.4.3** Assume $a(a-1)b \neq 0$. Suppose $b^2 = 3a + 1$ and $1 - a$ is a square in $\mathbb{F}_q$. Then we must have $f(\mathbb{F}_{q^2} \setminus \mathbb{F}_q) \subseteq \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

**Proof.** Suppose $x \neq x^q$ and $f(x) = f(x)^q$. We have

$$ax^3 + bx^{q+2} + x^{2q+1} = ax^{3q} + bx^{2q+1} + x^{q+2}.$$
It follows that
\[ a(x - x^q)(x^2 + x^{2q}) + (a + b - 1)(x - x^q)x^{q+1} = 0. \] (3.4.20)

Since \( x - x^q \neq 0 \), (3.4.20) becomes
\[ ax^{2q-2} + (a + b - 1)x^{q-1} + a = 0. \] (3.4.21)

With \( b^2 = 3a + 1 \), we observe that \( (a + b - 1) - 4a^2 = (b - 1)^2(1 - a) \) which is a square in \( \mathbb{F}_q \). Thus \( g = ax^2 + (a + b - 1)x + a \) is reducible over \( \mathbb{F}_q \), so \( x^{q-1} \in \mathbb{F}_q \). Now we have
\[ 1 = (x^{q-1})^{q-1} = x^{(q-1)^2} = x^{q^2-2q+1} = x^{2-2a} = (x^{1-q})^2. \]

Since \( x \not\in \mathbb{F}_q \), we must have \( x^{1-q} = -1 = x^{q-1} \). With \( x^{q-1} = -1 \), (3.4.21) becomes \( a + 1 - b = 0 \). But we also have
\[ (a + 1 - b)(a + 1 + b) = (a + 1)^2 - b^2 = (a + 1)^2 - (3a + 1) = a(a - 1) \neq 0, \]
which is clearly a contradiction. Thus \( g(\mathbb{F}_q^2 \setminus \mathbb{F}_q) \subseteq \mathbb{F}_q^2 \setminus \mathbb{F}_q \).

\[ \square \]

**Corollary 3.4.4** Write \( y = g(x) \). If \( y \in \mathbb{F}_q \), then \( x^3 = \frac{y}{a+b+1} \) and since \( (3, q - 1) = 1 \), we can conclude \( x \) is uniquely determined by \( y \).

**Proposition 3.4.5** Assume \( a(a-1)b \neq 0 \). Suppose \( b^2 = 3a + 1 \) and \( 1 - a \) is a square in \( \mathbb{F}_q \). Let \( x \in \mathbb{F}_q^2 \setminus \mathbb{F}_q \), and set \( y = f(x) \). Then \( \text{Tr}(x) \), and \( N(x) \) are uniquely determined by \( y \).

**Proof.** By definition \( g(x) = ax^3 + bx^{q+2} + x^{2q+1} \). Therefore we have
\[
\text{Tr}(g(x)) = (ax^3 + bx^{q+2} + x^{2q+1}) + (ax^3 + bx^{q+2} + x^{2q+1})^q \\
= a\text{Tr}(x^3) + (b + 1)\text{Tr}(x^{q+2}) \] (3.4.22)
\[
N(g(x)) = (ax^3 + bx^{q+2} + x^{2q+1})(ax^3 + bx^{q+2} + x^{2q+1})^q
\]
\[ = (a^2 + b^2 + 1)N(x)^3 + (ab + b)\text{Tr}(x^{q+2q}) + a\text{Tr}(x^{q+5}) \quad (3.4.23) \]

Combining (3.4.22) and (3.4.23) gives the following system:

\[
\begin{align*}
\text{Tr}(y) &= a\text{Tr}(x^3) + (b + 1)\text{Tr}(x^{q+2}) \\
N(y) &= (a^2 + b^2 + 1)N(x)^3 + (ab + b)\text{Tr}(x^{q+2q}) + a\text{Tr}(x^{q+5})
\end{align*} \quad (3.4.24)
\]

It is not difficult to verify the following formulas hold for \( z \in \mathbb{F}_{q^2} \):

\[
\begin{align*}
\text{Tr}(z^3) &= \text{Tr}(z)^3 - 2N(z) \quad (3.4.25) \\
\text{Tr}(z^{q+2}) &= N(z)\text{Tr}(z) \quad (3.4.26) \\
\text{Tr}(z^{q+2q}) &= \text{Tr}(z)^2N(z)^2 - 2N(z)^3 \quad (3.4.27) \\
\text{Tr}(z^{q+5}) &= \text{Tr}(z)^4Nz - 4\text{Tr}(z)^2N(z)^2 + 2N(z)^3 \quad (3.4.28)
\end{align*}
\]

Write \( \text{Tr}(x) = t, N(x) = n, \text{Tr}(y) = r, \) and \( N(y) = s \). Making the substitutions (3.4.25) - (3.4.28), system (3.4.24) becomes:

\[
\begin{align*}
\begin{cases}
atk^3 - n(3a - b - 1)t = r \\
ant^4 + (ab + b - 4a)n^2t^2 + n^3(a - b + 1)^2 = s
\end{cases} \quad (3.4.29)
\end{align*}
\]

We want to show the system (3.4.29) has at most one solution \((t, n) \in \mathbb{F}_q \times \mathbb{F}_q\).

**Remark 3.4.6** Since \( x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \), the polynomial \( f_x = x^2 - tx + n \in \mathbb{F}_q[x] \), is irreducible over \( \mathbb{F}_q \). Thus \( t^2 - 4n \) is a non square in \( \mathbb{F}_q \), which also implies \( \frac{t^2}{n} \left( \frac{t^2}{n} - 4 \right) \) is a non square as well.

1° Assume \( r = 0 \). We claim \( t = 0 \) as well. If \( t \neq 0 \), then we have

\[
\frac{t^2}{n} = \frac{3a - b - 1}{a}.
\]
Using the relation $b^2 = 3a + 1$, it follows that

$$\frac{t^2}{n} \left( \frac{t^2}{n} - 4 \right) = \frac{3a - b - 1}{a} \cdot \frac{-a - b - 1}{a} = (b + 1)^2(1 - a) \quad (3.4.30)$$

which is a square in $\mathbb{F}_q$. Therefore $x$ must be in $\mathbb{F}_q$ which is a contradiction.

2° Assume $r \neq 0$. It is clear $t \neq 0$ as well. Set $u = \frac{t^2}{n}$, and $\gamma = \frac{r^2}{n}$, then system (3.4.29) becomes:

$$\begin{cases} t(au + b + 1 - 3a) = \frac{r}{n} \\ t^2(au + ab + b - 4a + \frac{(a-b+1)^2}{u}) = \frac{1}{\gamma} \cdot \frac{r^2}{n^2}. \end{cases} \quad (3.4.31)$$

Therefore we have

$$t^2 \left( \frac{au + b + 1 - 3a}{\gamma} \right)^2 = t^2 \left( \frac{(au + ab + b - 4a)u + (a - b + 1)^2}{u} \right),$$

or equivalently

$$a^2u^3 - (6a^2 - 2ab - 2a + a\gamma)u^2 + [(3a - b - 1)^2 + \gamma(4a - b - ab)] u - (a - b + 1)^2\gamma = 0. \quad (3.4.32)$$

Let $p(u) \in \mathbb{F}_q[u]$ denote the LHS of (3.4.32). The problem is now reduced to showing $p(u)$ has at most one root in $\mathbb{F}_q$. With the help of a computer algebra machine we find the discriminant of $p$ is given by

$$D(p) = \gamma(\gamma - 4)a^2(a - 1)^2h(\gamma) \quad (3.4.33)$$

where

$$h(\gamma) = -27a^4 + 18a^2b^2 - 18a^2b\gamma + 36a^2b + 18a^2 + 4ab^3\gamma - 8ab^3 - 24ab^2 + 12ab\gamma$$

$$-24ab - 4a\gamma^2 + 16a\gamma - 8a + b^4 - 2b^3\gamma + 4b^3 + b^2\gamma^2 - 4b^2\gamma + 6b^2 - 2b\gamma + 4b + 1.$$
Using the relation \( b^2 = 3a + 1 \) gives

\[
h(\gamma) = (1 - a)(\gamma + b^2 - 3b - 2)^2. \tag{3.4.34}
\]

Using (3.4.34), (3.4.33) becomes

\[
D(p) = \gamma(\gamma - 4)a^2(a - 1)^2(1 - a)(\gamma + (b + 1)^2(b - 2))^2. \tag{3.4.35}
\]

Here we note that \( y \notin \mathbb{F}_q \) so \( \gamma(\gamma - 4) \) is not a square in \( \mathbb{F}_q \). Now if \( \gamma \neq -(b + 1)^2(b - 2) \), then \( D(p) \) is not a square in \( \mathbb{F}_q \) so (3.4.32) has at most one solution in \( \mathbb{F}_q \) and we are done. All that remains is to show that (3.4.32) has at most one solution in \( \mathbb{F}_q \) when \( \gamma = -(b + 1)^2(b - 2) \).

Assume \( \gamma = -(b + 1)^2(b - 2) \). Now we have

\[
\gamma(\gamma - 4) = (b + 1)^2(b - 2) [(b + 1)^2(b - 2) + 4] = 27a^2(a - 1). \tag{3.4.36}
\]

Since \( \gamma(\gamma - 4) \) is a nonsquare we must have \( (3, q) = 1 \). Using this fact with the relation \( b^2 = 3a + 1 \), (3.4.32) becomes

\[
p(u) = a^2u^3 + 3a^2(b - 2)u^2 + 3a^2(b - 2)^2u + a^2(b - 2)^3
\]

\[
= a^2(u + (b - 2))^3 \tag{3.4.37}
\]

Clearly \( p(u) \) has a unique root in \( \mathbb{F}_q \) so the proof is complete.

**Corollary 3.4.7** Assume \( f(x) = y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \). Then \( x \) is uniquely determined by \( y \).

**Proof.** Suppose \( x_1 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \) with \( f(x_1) = y = f(x) \). Since \( \text{Tr}(x) \) and \( \text{N}(x) \) are uniquely determined by \( y \), we must have \( \text{Tr}(x_1) = \text{Tr}(x) \) and \( \text{N}(x_1) = \text{N}(x) \). It follows that \( x_1 = x \) or \( x_1 = x^q \). Since \( f(x^q) = y^q \neq y \), it must be the case that \( x_1 = x \).

---

63
Neccesity of Theorem 3.4.1 under the assumption $a(a - 1)b \neq 0$.

$$\sum_{x \in \mathbb{F}_{q^2}} f(x)^s$$

$$= \sum_{x \in \mathbb{F}_{q^2}} x^{3(\alpha + \beta q)} (a + bx^{q-1} + x^{2(q-1)})^\alpha (a + bx^{1-q} + x^{2(1-q)})^\beta$$

$$= \sum_{x} x^{3(\alpha + \beta q)} \sum_{i,j} \left(\begin{array}{c}
\alpha \\
i
\end{array}\right) \left(\begin{array}{c}
i \\
k
\end{array}\right) a^{-i-j} x^{(q-1)(i-k+2k)} \left(\begin{array}{c}
\beta \\
j
\end{array}\right) \left(\begin{array}{c}
j \\
l
\end{array}\right) a^{\alpha + \beta - j - b - k - j - l} \sum_{x} x^{3(\alpha + \beta q) + (q-1)(i+k-j-l)}$$

It is clear that the above sum is 0 unless $\alpha + \beta q \equiv 0 \pmod{q-1}$, or equivalently $\beta = q - 1 - \alpha$. Using this fact we see $3(\alpha + \beta q) \equiv -3(\alpha + 1)(q-1) \pmod{q^2 - 1}$, so the above sum becomes

$$= \sum_{i,j} \left(\begin{array}{c}
\alpha \\
i
\end{array}\right) \left(\begin{array}{c}
i \\
k
\end{array}\right) \left(\begin{array}{c}
q-1-\alpha \\
j
\end{array}\right) \left(\begin{array}{c}
j \\
l
\end{array}\right) a^{-i-j} b^{i-k-j-1} \sum_{x} x^{(q-1)(-3(\alpha+1) + i + k - j - l)}$$

$$= -\sum_{-3(\alpha+1) + i + k - j - l \equiv 0 \pmod{q+1}} \left(\begin{array}{c}
\alpha \\
i
\end{array}\right) \left(\begin{array}{c}
i \\
k
\end{array}\right) \left(\begin{array}{c}
q-1-\alpha \\
j
\end{array}\right) \left(\begin{array}{c}
j \\
l
\end{array}\right) a^{-i-j} b^{i-k-j-l} \tag{3.4.38}$$

$$= -S_q(\alpha, a, b). \tag{3.4.39}$$

Now suppose $g$ is a PP of $\mathbb{F}_{q^2}$. By Hermite’s Criterion, we must have

$$S_q(\alpha, a, b) = 0$$

for each $0 \leq \alpha \leq q - 1$.

Set $\alpha = 0$. Since $0 \leq k \leq i \leq \alpha$, and $0 \leq l \leq j \leq q - 1 - \alpha$,

$$-3(\alpha + 1) + i + k - j - l \equiv 0 \pmod{q+1} \implies j + l = q - 2 \text{ and } 0 \leq l \leq \frac{q-2}{2}.$$ 

Therefore the sum in (5.5.45) becomes

$$0 = \sum_{-3-j-l \equiv 0 \pmod{q+1}} \left(\begin{array}{c}
q-1 \\
j
\end{array}\right) \left(\begin{array}{c}
j \\
l
\end{array}\right) a^{-j} b^{j-l}$$
\[ \sum_{0 \leq l \leq \frac{q-2}{2}} \left( \frac{q-1}{q-2-l} \right) \left( \frac{q-2-l}{l} \right) a^{-(q-2-l)}b^{q-2-2l} \]

\[ = \frac{a}{b} \sum_{0 \leq l \leq \frac{q-2}{2}} \left( \frac{q-2-l}{l} \right) (-1)^{q-2-l}a^l b^{-2l} \]

\( (z = -\frac{a}{b^2}) \)

\[ = -\frac{a}{b} \sum_{0 \leq l \leq \frac{q-2}{2}} \left( \frac{q-2-l}{l} \right) z^l \]

\( (l \mapsto (l-2)) \)

\[ = -\frac{a}{b} \sum_{2 \leq l \leq \frac{q-2}{2}+2} \left( \frac{-l}{l-2} \right) z^{l-2} \]

\[ = -\frac{a}{b} (z^{-2}) \sum_{0 \leq l \leq q-1} \left( \frac{-l}{l-2} \right) z^l. \]

Thus by lemma 3.5.1, the polynomial \( x^2 + x - z \) has two distinct roots in \( \mathbb{F}_q \). In particular we have \( 1 + 4z \) is a square in \( \mathbb{F}_q \) which gives \( b^2 - 4a \) is a square in \( \mathbb{F}_q \).

Now take \( \alpha = 1 \). In this case the sum in (5.5.45) becomes

\[ 0 = \sum_{-6+i+k-j-l \equiv 0 \pmod{q+1}} \binom{1}{i} \binom{i}{k} \binom{q-2}{j} \binom{j}{l} a^{-(i+j)}b^{i+j-k-l} \]

\[ = \sum_{-6-j-l=-2(q+1), -(q+1)} \binom{q-2}{j} \binom{j}{l} a^{-j} b^{-l} + \]

\[ \sum_{-5-j-l=-q+1} \binom{q-2}{j} \binom{j}{l} a^{1-j} b^{1+j-l} + \sum_{-4-j-l=-q+1} \binom{q-2}{j} \binom{j}{l} a^{-1-j} b^{-l} \]

\[ = \binom{q-2}{q-2} \binom{q-2}{q-2} a^{-(q-2)} + \sum_{0 \leq l \leq \frac{q-5}{2}} \binom{q-2}{q-5-l} \binom{q-5-l}{l} a^{-(q-5-l)} b^{q-5-2l} \]

\[ + \sum_{0 \leq l \leq \frac{q-4}{2}} \binom{q-2}{q-4-l} \binom{q-4-l}{l} a^{-(1+q-4-l)} b^{1+q-4-2l} \]
\[
\begin{align*}
&= a + \sum_{0 \leq l \leq \frac{q-3}{2}} (-1)^{q-5-l}(q-4-l)\left(\frac{q-5-l}{l}\right) a^{l+4} b^{-2l-2} + \\
&+ \sum_{0 \leq l \leq \frac{q-4}{2}} (-1)^{q-4-l}(q-3-l)\left(\frac{q-3-l}{l}\right) a^{l+2} b^{-2l-2} + \\
&+ \sum_{0 \leq l \leq \frac{q-3}{2}} (-1)^{q-3-l}(q-2-l)\left(\frac{q-3-l}{l}\right) a^{l+1} b^{-2l-2} \\
&= a + \frac{a^4}{b^4} \sum_{0 \leq l \leq \frac{q-3}{2}} (-4-l)\left(\frac{-l-5}{l}\right) z^l + \frac{-a^2}{b^2} \sum_{0 \leq l \leq \frac{q-4}{2}} (-l-3)\left(\frac{-l-4}{l}\right) z^l \\
&+ \frac{a}{b^2} \sum_{0 \leq l \leq \frac{q-5}{2}} (-l-2)\left(\frac{-l-3}{l}\right) z^l \\
&= a + \left(\frac{a}{b}\right)^4 (-z^{-5}) \sum_{5 \leq l \leq \frac{q-5}{2} + 5} (l-1)\left(\frac{-l}{l-5}\right) z^l \\
&+ \left(\frac{a}{b}\right)^2 (z^{-4}) \sum_{4 \leq l \leq \frac{q-4}{2} + 4} (l-1)\left(\frac{-l}{l-4}\right) z^l + \left(\frac{a}{b^2}\right) (-z^{-3}) \sum_{3 \leq l \leq \frac{q-3}{2} + 3} (l-1)\left(\frac{-l}{l-3}\right) z^l \\
\end{align*}
\]

We note that \((-l-\frac{i}{k}) = 0\) when \(k < 0\), and \((-l-\frac{i}{l}) \equiv 0 \pmod{p}\) when \(\frac{q-1}{2} + i < l \leq q - 1\), \(i = 3, 4, 5\).

\[
\begin{align*}
&= a + \left(\frac{a}{b}\right)^4 (-z^{-5}) \sum_{0 \leq l \leq q-1} (l-1)\left(\frac{-l}{l-5}\right) z^l \tag{3.4.40} \\
&+ \left(\frac{a}{b}\right)^2 (z^{-4}) \sum_{0 \leq l \leq q-1} (l-1)\left(\frac{-l}{l-4}\right) z^l + \left(\frac{a}{b^2}\right) (-z^{-3}) \sum_{0 \leq l \leq q-1} (l-1)\left(\frac{-l}{l-3}\right) z^l \\
\end{align*}
\]

Making the substitutions (3.5.43), (3.5.44), and (3.5.45) gives

\[
\begin{align*}
&= a + \left(\frac{a}{b}\right)^4 (-z^{-5}) \left(\frac{2z^3(1+3z)}{1+4z}\right) + \left(\frac{a}{b}\right)^2 (z^{-4}) \left(-\frac{z^3}{1+4z}\right) \\
\end{align*}
\]
\[
+ \left( \frac{a}{b^2} \right) (-z^{-3}) \left( \frac{2z^3}{1+4z} \right) \\
= \frac{2(a-1)a(3a-b^2+1)}{b^2-4a}.
\]

(3.4.41)

Thus (5.5.47) shows we must have \( b^2 = 3a + 1 \). Since \( b^2 - 4a = (3a + 1) - 4a = 1 - a \), we can conclude \( 1 - a \) is a square in \( \mathbb{F}_q^* \). This completes the proof of Theorem 3.4.1.

### 3.5 Technical Lemmas

**Lemma 3.5.1** Let \( z \in \mathbb{F}_q^* \). Write \( x^2 + x - z = (x - r_1)(x - r_2) \). Then

\[
\sum_{0 \leq l \leq q-1} \binom{-l}{l-2} z^l = \begin{cases} \\
\frac{1}{8} & \text{if } r_1 = r_2 \\
0 & \text{if } r_1 \neq r_2 \in \mathbb{F}_q \\
z & \text{if } r_1, r_2 \not\in \mathbb{F}_q.
\end{cases}
\]

**Proof.** Let \( C[f(x)] \) denote the constant term in the Laurent series of \( f \) in the indeterminate \( x \). Then we have:

\[
\sum_{0 \leq l \leq q-1} \binom{-l}{l-2} z^l = \sum_{0 \leq l \leq q-1} C \left[ \frac{1}{x^{l-2}(1+x)^l} \right] z^l \\
= \sum_{0 \leq l \leq q-1} C \left[ x^2 \cdot \left( \frac{z}{x(1+x)} \right)^l \right] \\
= C \left\{ \sum_{0 \leq l \leq q-1} x^2 \cdot \left( \frac{z}{x(1+x)} \right)^l \right\} \\
= C \left[ x^2 \cdot \left( \frac{1 - \left( \frac{z}{x(1+x)} \right)^q}{1 - \frac{z}{x(1+x)}} \right) \right] \\
= C \left[ x^2 \cdot \frac{x(1+x)}{x(1+x) - z} \left( 1 - z \left( \frac{1}{x^q} - \frac{1}{1+x^q} \right) \right) \right] \\
= C \left[ \frac{x^3(1+x)}{x(1+x) - z} + C \frac{-z}{x^{q-2}} \cdot \frac{x(1+x)}{x(1+x) - z} \right] + C \left[ \frac{x^3(1+x)}{x(1+x) - z} \cdot \frac{1}{1+x^q} \right] \\
= C \left[ \frac{-z^2}{x^{q-2}} \cdot \left( 1 + \frac{1}{x^2 + x - z} \right) \right]
\]
Now suppose $r_1 = r_2 (= -\frac{1}{2})$. Then 3.5.42 becomes

$$= C \left[ \frac{-z^2}{x^{q-2}} \cdot \frac{1}{(x - r_1)^2} \right]$$

$$= C \left[ \frac{-z^2}{r_1^2} \left( -2 \right) \left( -\frac{1}{r_1} \right)^{q-2} \right]$$

$$= \frac{-z^2}{r_1^q} (-1)^{q-2} (q - 1) (-1)^{q-2} = \frac{z^2}{r_1}$$

$$= \frac{1}{8}$$

If we assume $r_1 \neq r_2$ then 3.5.42 becomes

$$= C \left[ \frac{-z^2}{x^{q-2}} \left( \frac{1}{(x - r_1)(x - r_2)} \right) \right]$$

$$= C \left[ \frac{-z^2}{r_1 - r_2} \cdot \frac{1}{x^{q-2}} \left( \frac{1}{r_1} \frac{1}{1 - \frac{x}{r_1}} - \frac{1}{r_2} \frac{1}{1 - \frac{x}{r_2}} \right) \right]$$

$$= \frac{z^2}{r_1 - r_2} \left( \frac{1}{r_1^{q-1}} - \frac{1}{r_2^{q-1}} \right)$$

$$= \begin{cases} 
0 & \text{if } r_1, r_2 \in \mathbb{F}_q \\
z & \text{if } r_1, r_2 \notin \mathbb{F}_q 
\end{cases}$$

**Lemma 3.5.2** Write $x^2 + x - z = (x - r_1)(x - r_2) \in \mathbb{F}_q[x]$, with $r_1 \neq r_2$. We have the following

$$\sum_{0 \leq l \leq q-1} (l - 1) \binom{-l}{l-5} z^l = \frac{2z^3(1 + 3z)}{1 + 4z}$$  \hspace{1cm} (3.5.43)
\[
\sum_{0 \leq l \leq q-1} (l-1) \left( \frac{-l}{l-4} \right) z^l = -\frac{z^3}{1 + 4z} \quad (3.5.44)
\]

\[
\sum_{0 \leq l \leq q-1} (l-1) \left( \frac{-l}{l-3} \right) z^l = \frac{2z^3}{1 + 4z}. \quad (3.5.45)
\]

**Proof.** We make use of the following facts:

1. \[
\sum_{0 \leq l \leq q-1} (l-1) \left( \frac{-l}{l-j} \right) z^l = \sum_{0 \leq l \leq q-1} (l+1) \left( \frac{-l}{l-j} \right) z^l - \sum_{0 \leq l \leq q-1} 2 \left( \frac{-l}{l-j} \right) z^l
\]

2. \[
\frac{-(q-1)}{q-6} \equiv \frac{-(q-1)}{q-5} \equiv \frac{-(q-1)}{q-4} \equiv 0 \pmod{p}
\]

3. \[
\sum_{0 \leq l \leq q-2} (l+1)y^l = \frac{d}{dy} \left[ \sum_{0 \leq l \leq q-1} y^l \right] = \frac{d}{dy} \left[ \frac{1 - y^q}{1 - y} \right] = \frac{1 - y^q}{(1 - y)^2}
\]

We proceed as in the previous lemma.

\[
\sum_{0 \leq l \leq q-1} (l+1) \left( \frac{-l}{l-5} \right) z^l = C \left[ x^5 \sum_{0 \leq l \leq q-1} (l+1) \left( \frac{z}{x(1+x)} \right)^l \right]
\]

\[
= C \left[ x^5 \frac{1 - \left( \frac{z}{x(1+x)} \right)^q}{1 - \left( \frac{z}{x(1+x)} \right)^2} \right]
\]

\[
= C \left[ x^5 \left( \frac{x(1+x)}{x(1+x)-z} \right)^2 \left( 1 - z \left( \frac{1}{x^q} - \frac{1}{1+x^q} \right) \right) \right]
\]

\[
= C \left[ \frac{-z}{x^{q-5}} \left( 1 + \frac{z}{x(1+x)-z} \right)^2 \right]
\]

\[
= C \left[ \frac{-z}{x^{q-5}} \left( \frac{2z}{(x-r_1)(x-r_2)} + \frac{z^2}{(x-r_1)^2(x-r_2)^2} \right) \right]
\]

\[
= C \left[ \frac{-2z^2}{x^{q-5}} \left( \frac{1}{(x-r_1)(x-r_2)} \right) \right]
\]

\[
+ C \left[ \frac{-z^3}{x^{q-5}} \left( \frac{1}{(x-r_1)(x-r_2)} \right)^2 \right]
\]
For the first term we continue exactly as in the previous lemma to see

\[
C \left[ \frac{-2z^2}{x^{q-5}} \left( \frac{1}{x - r_1}(x - r_2) \right) \right] = C \left[ \frac{-2z^2}{x^{q-5}} \left( \frac{1}{x - r_1} - \frac{1}{x - r_2} \right) \right] = C \left[ \frac{2z^2}{r_1 - r_2} \cdot \frac{1}{x^{q-5}} \left( \frac{1}{r_1} - \frac{1}{r_2} \right) \right] = \frac{2z^2}{r_1 - r_2} \left( \left( \frac{1}{r_1} \right)^{q-4} - \left( \frac{1}{r_2} \right)^{q-4} \right) \quad (3.5.46)
\]

\[
= \frac{2z^2}{r_1 - r_2} (r_3 - r_2)
\]

\[
= (2z^2)(r_1^2 + r_1 r_2 + r_2^2)
\]

\[
= 2z^2 ((r_1 + r_2)^2 - r_1 r_2)
\]

\[
= 2z^2(1 + z). \quad (3.5.47)
\]

For the second term we continue in a similar manner to see

\[
C \left[ \frac{-z^3}{x^{q-5}} \left( \frac{1}{x - r_1}(x - r_2) \right)^2 \right] = C \left[ \frac{-z^3}{(r_1 - r_2)^2} \cdot \frac{1}{x^{q-5}} \left( \frac{1}{x - r_1} - \frac{1}{x - r_2} \right)^2 \right] = \frac{-z^3}{1 + 4z} \cdot C \left[ \frac{1}{x^{q-5}} \left( \frac{1}{x - r_1} - \frac{1}{x - r_2} \right)^2 \right]. \quad (3.5.48)
\]

Again, working like before we have

\[
C \left[ \frac{1}{x^{q-5}} \left( \frac{1}{x - r_1} - \frac{1}{x - r_2} \right)^2 \right] = C \left[ \frac{1}{x^{q-5}} \left( (x - r_1)^{-2} + (x - r_2)^{-2} - \frac{2}{(x - r_1)(x - r_2)} \right) \right] = \frac{1}{r_1^2} \left( -2 \right) \left( \frac{-1}{r_1} \right)^{q-5} + \frac{1}{r_2^2} \left( -2 \right) \left( \frac{-1}{r_2} \right)^{q-5} + \frac{2}{r_1 - r_2} (r_3^2 - r_2^2)
\]

\[
= (-4)(r_1^2 + r_2^2) - 2(r_1^2 + r_1 r_2 + r_2^2)
\]

\[
= (-4)(1 + 2z) + 2(1 + z)
\]

\[
= -2(1 + 2z). \quad (3.5.49)
\]
Combining (3.5.47), (3.5.48) and (3.5.49) we have

\[
\sum_{0 \leq l \leq q-1} (l + 1) \binom{-l}{l - 5} z^l = \frac{2z^2 (1 + 6z + 7z^2)}{1 + 4z}. \tag{3.5.50}
\]

Computing in a similar manner we also have

\[
2 \cdot \sum_{0 \leq l \leq q-1} \binom{-l}{l - 5} z^l = 2(z^2 + z^3). \tag{3.5.51}
\]

Thus combining (3.5.50) and (3.5.51) gives

\[
\sum_{0 \leq l \leq q-1} (l - 1) \binom{-l}{l - 5} z^l = \frac{2z^3(1 + 3z)}{1 + 4z}. \tag{3.5.52}
\]

The identities (3.5.44) and (3.5.45) are proved in the exact same manner. 

\[\square\]
4 Permutation Polynomials of the form $x^{1+2^k} + L(x)$

4.1 Background

Differential cryptanalysis ([3]) together with linear cryptanalysis ([67]) are considered as some of the most efficient tools for block ciphers. The security of modern block ciphers relies on the cryptographic properties of its substitution boxes, which are normally the only source of nonlinearity. These substitution boxes are often constructed by means of power mappings that have desirable cryptographic properties such as high nonlinearity and good differential characteristics. To satisfy these criteria, a cryptographically strong substitution box can be taken from the class of APN functions. For more information on cryptographically significant mappings over finite fields see [74] and [75].

The existence of APN permutations of $\mathbb{F}_{2^n}$, $n$ even, has been a challenging question for quite some time. The only known such APN permutation is the example in $\mathbb{F}_{2^6}$ discovered by Browning, Dillon, McQuistan and Wolfe in 2009 ([9]). As a result there is strong interest in finding APN permutations of $\mathbb{F}_{2^n}$ for even $n \geq 8$. One attempt to construct such functions is to start with a power APN function $x^d$ of $\mathbb{F}_{2^n}$ and to search for a linearized polynomial $L(x)$ such that $x^d + L(x)$ is a permutation of $\mathbb{F}_{2^n}$.

A more general objective has evolved from this line of thought: Determine permutation polynomials of $\mathbb{F}_{2^n}$, of the form $x^d + L(x)$, where $d$ is a positive integer and $L \in \mathbb{F}_{2^n}[x]$ is a linearized polynomial. Several authors have considered the problem (see [62],[74], and [75]), some of the results are gathered below.
Lemma 4.1.1 ([62]) Let $L(x) \in \mathbb{F}_{2^n}[x]$ be a nonzero linearized polynomial. Then $x^d + L(x)$ is a permutation polynomial on $\mathbb{F}_{2^n}$ if and only if

$$\frac{L(\mu)}{\mu^d} \not\in \{\alpha^d + (\alpha + 1)^d | \alpha \in \mathbb{F}_{2^n}\}$$

for all $\mu \in \mathbb{F}_{2^n}^*$.

Theorem 4.1.2 ([62, Theorem 1]) Suppose $\gcd(d, 2^n - 1) = s > 1$ and $\omega_2(\frac{2^n - 1}{s}) = k$, where $\omega_2(t)$ denotes the number of nonzero terms in the base 2 expansion of $t$. If $s \nmid \mu$ for all integers $\mu > 0$ with $\omega_2(\mu) \leq k - 1$, then $x^d + L(x)$ is not a permutation polynomial of $\mathbb{F}_{2^n}$.

Theorem 4.1.3 ([62, Theorem 2]) Let $n$ be odd, $L(x)$ be a nonzero linearized polynomial over $\mathbb{F}_{2^n}$. Then $x^3 + L(x)$ is a permutation polynomial on $\mathbb{F}_{2^n}$ if and only if $L(x) = \alpha^2 x + \alpha x^2$ for some $\alpha \in \mathbb{F}_{2^n}^*$.

Theorem 4.1.4 ([62, Theorem 3]) Suppose $n$ is even and $L(x) \in \mathbb{F}_{2^n}[x]$ is a linearized polynomial. Then $x^3 + L(x)$ is not a permutation polynomial on $\mathbb{F}_{2^n}$.

The previous two theorems can be extended to power functions of the form $x^{1+2^k}$.

Theorem 4.1.5 ([62, Theorem 4]) Suppose $\gcd(k, n) = 1$ and $L(x) \in \mathbb{F}_{2^n}[x]$ is a linearized polynomial. Then $x^{1+2^k} + L(x)$ is a permutation polynomial of $\mathbb{F}_{2^n}$ if and only if $n$ is odd and $L(x) = \alpha^{2^k} x + \alpha x^{2^k}$ for some $\alpha \in \mathbb{F}_{2^n}^*$.

Motivated the above results, Gong considered the same type of polynomials in Theorem 4.1.5 but under the assumption that $\gcd(k, n) > 1$. The following two classes of permutation polynomials were discovered.

Theorem 4.1.6 ([30]) Assume the $3|n$.

(i) If $k = n/3$ or $2n/3$ and $k \equiv 1 \pmod{3}$, then $x^{1+2^k} + (x + x^{2^k})^{2^{k+1}}$ is a permutation polynomial of $\mathbb{F}_{2^n}$.
(ii) If \( k = n/3 \) or \( 2n/3 \) and \( k \equiv 2 \pmod{3} \), then \( x^{1+2^k} + (x + x^{2^k})^{2k+1} \) is a permutation polynomial of \( \mathbb{F}_{2^n} \).

Based on Theorem 4.1.6 and computer search results, Gong conjectured the following: If \( k = n/3 \) and \( k \equiv 0 \pmod{3} \) then both \( x^{1+2^k} + (x + x^{2^k})^{2k+1} \) and \( x^{1+2^k} + (x + x^{2^k})^{2k+1} \) are permutation polynomials of \( \mathbb{F}_{2^n} \). We confirm this conjecture in the next section.

### 4.2 \( L(x) = (x + x^{2^k})^{2k+1} \) or \( L(x) = (x + x^{2^k})^{2k+1} \)

**Theorem 4.2.1** Assume that \( 3|n, k = n/3 \) and \( k \equiv 0 \pmod{3} \). Then \( x^{1+2^k} + (x + x^{2^k})^{2k+1} \) and \( x^{1+2^k} + (x + x^{2^k})^{2k+1} \) are both PPs of \( \mathbb{F}_{2^n} \).

**Proof.** By Lemma 4.1.1, we have \( x^{1+2^k} + L(x) \) is a PP of \( \mathbb{F}_{2^n} \) if and only if

\[
\frac{L(x)}{x^{1+2^k}} \not\in \{y^{2^k} + y + 1 : y \in \mathbb{F}_2^n\} \tag{4.2.1}
\]

for all \( x \in \mathbb{F}_{2^n}^\times \). From (4.2.1) it follows that \( x^{1+2^k} + L(x) \) is a PP of \( \mathbb{F}_{2^n} \) if and only if

\[
\text{Tr}_{2^n/2^k} \left( \frac{L(x)}{x^{1+2^k}} \right) \begin{cases} 0 & \text{if } n/k \text{ is even} \\ 1 & \text{if } n/k \text{ is odd.} \end{cases} \tag{4.2.2}
\]

Since \( n/k = 3 \) we only have to show

\[
\text{Tr}_{2^n/2^k} \left( \frac{L(x)}{x^{1+2^k}} \right) \neq 1.
\]

We first prove that \( x^{1+2^k} + (x + x^{2^k})^{2k+1} \) is a PP of \( \mathbb{F}_{2^n} \) when \( k \) is even.

Assume that \( k \) is even. We show that

\[
\text{Tr}_{2^n/2^k} \left( \frac{(x + x^{2^k})^{2k+1}}{x^{1+2^k}} \right) \neq 1 \tag{4.2.3}
\]

for all \( x \in \mathbb{F}_{2^n} \).
Notice for \( x \in \mathbb{F}_{2^n} \) we have

\[
\text{Tr}_{2^n/2^k} \left( \frac{(x + x^{-2^k}) 2^{k+1}}{x^{1+2^k}} \right) = \text{Tr}_{2^n/2^k} \left( \frac{x^{2^{k+1}} + x^2}{x^{1+2^k}} \right) = \text{Tr}_{2^n/2^k} \left( \frac{x^{2^{k+1} + 2^k} + x^{2+2^k}}{x^{1+2^k+2^k}} \right)
\]

\[
= \left( \frac{\text{Tr}_{2^n/2^k}(x^3 + x^{1+2^k+1})}{\mathbb{N}_{2^n/2^k}(x)} \right)
\]

Therefore, showing (4.2.3) is satisfied is equivalent to showing

\[
\text{Tr}_{2^n/2^k}(x^3 + x^{1+2^k+1}) + \mathbb{N}_{2^n/2^k}(x) \neq 0 \tag{4.2.4}
\]

for all \( x \in \mathbb{F}_{2^n} \).

Since \( 6|n \) by assumption, we have \( 9|2^{k-1} \). Choose \( v \in \mathbb{F}_{2^k} \) such that \( v \) is not a cube in \( \mathbb{F}_{2^k} \). Then \( x^3 + v \in \mathbb{F}_{2^k}[x] \) is irreducible. Let \( \alpha \) be a root of \( x^3 + v \). It follows that \( \mathbb{F}_{2^n} = \mathbb{F}_{2^k}(\alpha) \). Since \( x^3 + v \) is the minimum polynomial of \( \alpha \) over \( \mathbb{F}_{2^k} \), it is easy to see \( \text{Tr}_{2^n/2^k}(\alpha) = 0 \) and \( \mathbb{N}_{2^n/2^k}(\alpha) = v \). Now since \( \alpha^4 = \alpha v \), an induction gives

\[
\alpha^{2^k} = v^{1+2^2+\ldots+2^k/2} \alpha = v^{\frac{1}{2}(2^k-1)} \alpha. \tag{4.2.5}
\]

Write \( x = a + b\alpha + c\alpha^2 \in \mathbb{F}_{2^n}^* \), with \( (a, b, c) \in \mathbb{F}_{2^k}^3 \neq (0, 0, 0) \). We have

\[
\text{Tr}_{2^n/2^k}(x^3) = \text{Tr}_{2^n/2^k}((a + b\alpha + c\alpha^2)(a^2 + b^2\alpha^2 + c^2\alpha^4)).
\]

Combining the fact that \( \text{Tr}_{2^n/2^k}(\alpha) = \text{Tr}_{2^n/2^k}(\alpha^2) = 0 \) and the reduction \( \alpha^3 = v \), we see

\[
\text{Tr}_{2^n/2^k}(x^3) = a^3 + b^3 v + c^3 v^2. \tag{4.2.6}
\]

Let \( \sigma \) denote the Frobenius of \( \mathbb{F}_{2^n}/\mathbb{F}_{2^k} \) and set \( \beta = \alpha^2 \). Then we have

\[
\mathbb{N}_{2^n/2^k}(x) = (a + b\alpha + c\beta)(a + b\alpha^\sigma + c\beta^\sigma)(a + b\alpha^{\sigma^2} + c\beta^{\sigma^2})
\]

\[
= a^3 + b^3 \mathbb{N}_{2^n/2^k}(\alpha) + c^3 \mathbb{N}_{2^n/2^k}(\beta) + a^2 b \text{Tr}_{2^n/2^k}(\alpha) + a^2 c \text{Tr}_{2^n/2^k}(\beta)
\]

75
\[ + b^2 a \text{Tr}_{2^n/2^k}(\alpha \alpha^\sigma) + b^2 c \text{Tr}_{2^n/2^k}(\alpha \alpha^\sigma \beta^\sigma) + c^2 a \text{Tr}_{2^n/2^k}(\beta \beta^\sigma) \\
+ c^2 b \text{Tr}_{2^n/2^k}(\beta \beta^\sigma \alpha^\sigma) + ab \text{Tr}_{2^n/2^k}(\alpha \beta^\sigma + \alpha^\sigma \beta). \]

Observe that we have

\[
\text{Tr}_{2^n/2^k}(\alpha \alpha^\sigma) = N_{2^n/2^k}(\alpha) \text{Tr}_{2^n/2^k}(\frac{1}{\alpha}) = 0, \\
\text{Tr}_{2^n/2^k}(\beta \beta^\sigma) = \text{Tr}_{2^n/2^k}(\alpha \alpha^\sigma)^2 = 0, \\
\text{Tr}_{2^n/2^k}(\alpha \alpha^\sigma \beta^\sigma) = N_{2^n/2^k}(\alpha) \text{Tr}_{2^n/2^k}(\beta) = 0, \\
\text{Tr}_{2^n/2^k}(\beta \beta^\sigma \alpha^\sigma) = N_{2^n/2^k}(\beta) \text{Tr}_{2^n/2^k}(\frac{1}{\alpha}) = 0, \\
\text{Tr}_{2^n/2^k}(\alpha \beta^\sigma + \alpha^\sigma \beta) = \text{Tr}_{2^n/2^k}(\alpha^\sigma^2 \beta + \alpha^\sigma \beta) \\
= \text{Tr}_{2^n/2^k}(\beta(\text{Tr}_{2^n/2^k}(\alpha) - \alpha)) \\
= \text{Tr}_{2^n/2^k}(\alpha) \text{Tr}_{2^n/2^k}(\beta) + \text{Tr}_{2^n/2^k}(\alpha \beta) \\
= v.
\]

Combining the above facts we have

\[
N_{2^n/2^k}(x) = a^3 + b^3 v + c^3 v^2 + abcv \tag{4.2.7}
\]

Proceeding as before we also have

\[
\text{Tr}_{2^n/2^k}(x^{1+2^k+1}) = \text{Tr}_{2^n/2^k}((a + b \alpha + c \beta)(a^2 + b^2 \alpha^2 + c^2 \beta^2)^\sigma) \\
= \text{Tr}_{2^n/2^k}((a + b \alpha + c \beta)(a^2 + c^2 v \alpha^\sigma + b^2 \beta^\sigma)) \\
= a^3 + b c^2 v \text{Tr}_{2^n/2^k}(\alpha \alpha^\sigma) + b^3 \text{Tr}_{2^n/2^k}(\alpha \beta^\sigma) \\
+ c^3 v \text{Tr}_{2^n/2^k}(\alpha^\sigma \beta) + c b^2 \text{Tr}_{2^n/2^k}(\beta \beta^\sigma) \\
= a^3 + b^3 \text{Tr}_{2^n/2^k}(\alpha \beta^\sigma) + c^3 v \text{Tr}_{2^n/2^k}(\alpha^\sigma \beta). 
\]

76
Using (4.2.5) we have

\[
\text{Tr}_{2^{n/2}}(\alpha \beta) = \mathbb{N}_{2^{n/2}}(\alpha) \text{Tr}_{2^{n/2}}(\frac{\alpha}{\beta}) = v^{1-\frac{1}{2}(2^k-1)},
\]

and

\[
\text{Tr}_{2^{n/2}}(\alpha^\sigma \beta) = \mathbb{N}_{2^{n/2}}(\alpha) \text{Tr}_{2^{n/2}}(\frac{\alpha^\sigma}{\alpha}) = v^{1+\frac{1}{2}(2^k-1)}.
\]

Thus

\[
\text{Tr}_{2^{n/2}}(x^{1+2^k+1}) = a^3 + b^3 v^{1-\frac{1}{2}(2^k-1)} + c^3 v^{2+\frac{1}{2}(2^k-1)}.
\]

(4.2.8)

Combining (4.2.6), (4.2.7), and (4.2.8) gives

\[
\text{Tr}_{2^{n/2}}(x^3 + x^{1+2^k+1}) + \mathbb{N}_{2^{n/2}}(x) = abc v + a^3 + b^3 v^{1-\frac{1}{2}(2^k-1)} + c^3 v^{2+\frac{1}{2}(2^k-1)}.
\]

Define

\[
a_1 = a, \quad b_1 = bv^{-\frac{1}{2}(2^k-1)}, \quad c_1 = cv^{\frac{1}{2}(2^k-1)}.
\]

Then

\[
\text{Tr}_{2^{n/2}}(x^3 + x^{1+2^k+1}) + \mathbb{N}_{2^{n/2}}(x) = a_1 b_1 c_1 v + a_1^3 + b_1^3 v + c_1^3 v^2
\]

\[
= \mathbb{N}_{2^{n/2}}(a_1 + b_1 \alpha + c_1 \alpha^2) \quad \text{(by (4.2.7))}
\]

\[
\neq 0.
\]

This completes the proof that \(x^{1+2^k} + (x + x^{2^k})^{2^k+1}\) is a PP of \(F_{2^n}\) when \(k\) is even.

Now we consider \(x^{1+2^k} + (x + x^{2^k})^{2^k+1}\) under the assumption \(k\) is even. We note that to prove that \(x^{1+2^k} + (x + x^{2^k})^{2^k+1}\) is a PP of \(F_{2^n}\), we only need to show

\[
\text{Tr}_{2^{n/2}}(x^3 + x^{1+2^k+1}) + \mathbb{N}_{2^{n/2}}(x) \neq 0 \quad (4.2.9)
\]

for all \(x \in F_{2^n}\).

Equation (4.2.9) can be proved in the same manner as Equation (4.2.4). In fact, we have:

\[
\text{Tr}_{2^{n/2}}(x^{1+2^k+1}) = \text{Tr}_{2^{n/2}}((a + b \alpha + c \beta)(a^2 + b^2 \alpha^2 + c^2 \beta^2)\sigma^2)
\]

77
\[
\begin{align*}
&= \text{Tr}_{2n/2^k}((a + b\alpha + c\beta)(a^2 + c^2\alpha^2 + b^2\beta^2)) \\
&= a^3 + bc^2\nu\text{Tr}_{2n/2^k}(\alpha\alpha^2) + b^3\text{Tr}_{2n/2^k}(\alpha\beta^3) \\
&\quad + c^3\nu\text{Tr}_{2n/2^k}(\alpha\beta^2) + cb^2\nu\text{Tr}_{2n/2^k}(\beta\beta^2) \\
&= a^3 + b^3\text{Tr}_{2n/2^k}(\alpha\beta^3) + c^3\nu\text{Tr}_{2n/2^k}(\alpha\beta^2).
\end{align*}
\]

Using (4.2.5) it follows that
\[
\begin{align*}
\text{Tr}_{2n/2^k}(\alpha\beta^3) &= N_{2n/2^k}(\alpha)\text{Tr}_{2n/2^k}(\frac{\alpha}{\alpha}) = v^{1 + \frac{1}{2}(2^k - 1)}, \\
\text{Tr}_{2n/2^k}(\alpha^2\beta) &= N_{2n/2^k}(\alpha)\text{Tr}_{2n/2^k}(\frac{\alpha}{\alpha}) = v^{1 - \frac{1}{2}(2^k - 1)}.
\end{align*}
\]

Thus
\[
\text{Tr}_{2n/2^k}(x^{1+2^k+1}) = a^3 + b^3v^{1 + \frac{1}{2}(2^k - 1)} + c^3v^{2 - \frac{1}{2}(2^k - 1)}. \tag{4.2.10}
\]

Putting the pieces together we have
\[
\text{Tr}_{2n/2^k}(x^3 + x^{1+2^k+1}) + N_{2n/2^k}(x) = abc^2 + a^3 + b^3v^{1 + \frac{1}{2}(2^k - 1)} + c^3v^{2 - \frac{1}{2}(2^k - 1)}. \tag{4.2.11}
\]

Define
\[
a_2 = a, \quad b_2 = bv^{\frac{1}{2}(2^k - 1)}, \quad c_2 = cv^{\frac{1}{2}(2^k - 1)}.
\]

Then
\[
\begin{align*}
\text{Tr}_{2n/2^k}(x^3 + x^{1+2^k+1}) + N_{2n/2^k}(x) &= a_2b_2c_2v + a_2^3 + b_2^3v + c_2^3v^2 \\
&= N_{2n/2^k}(a_2 + b_2\alpha + c_2\beta) \\
&\neq 0
\end{align*}
\]

Now assume \(k\) is odd. For each \(x \in \mathbb{F}_{2^n}^\ast\), by (4.2.9), with \(n\) replaced by \(2n\) and \(k\) replaced by \(2k\) we have
\[
\text{Tr}_{2^{2n}/2^{2k}}(x^3 + x^{1+2^k+1}) + N_{2^{2n}/2^{2k}}(x) \neq 0. \tag{4.2.12}
\]
For each $z \in \mathbb{F}_{2^n}$, we have

$$\text{Tr}_{2^{2n}/2^k}(z) = z + z^{2^{2k}} + z^{2^{4k}} = z + z^{2^{2k}} + z^{2^k} = \text{Tr}_{2^n/2^k}(z)$$

as well as

$$N_{2^{2n}/2^k}(z) = z \cdot z^{2^{2k}} \cdot z^{2^{4k}} = z \cdot z^{2^{2k}} \cdot z^{2^k} = N_{2^n/2^k}(z).$$

Therefore (4.2.12) becomes

$$\text{Tr}_{2^n/2^k}(x^3 + x^{1+2^{k+1}}) + N_{2^n/2^k}(x) \neq 0.$$

Thus $x^{1+2^k} + (x + x^{2^k})^{2^{k+1}}$ is a PP of $\mathbb{F}_{2^n}$ when $k$ is odd as well. Using the same method, we have $x^{1+2^k} + (x + x^{2^k})^{2^{k+1}}$ is also a PP of $\mathbb{F}_{2^n}$. 

\[\blacksquare\]
5 On Monomials Graphs of Girth Eight∗

5.1 Background

All graphs considered in this chapter are finite, undirected, with no loops or multiple edges. All definitions of graph-theoretic terms that we omit can be found in Bollobás [4]. The order of a graph is the number of its vertices. The degree of a vertex of a graph is the number of vertices adjacent to it. A graph is called \( r \)-regular if degrees of all its vertices are equal to \( r \). A graph is called connected if every pair of its distinct vertices is connected by a path. The distance between two distinct vertices in a connected graph is the length of the shortest path connecting them. The girth of a graph containing cycles is the length of a shortest cycle.

Let \( k \geq 3 \), and \( g_k(n) \) denote the greatest number of edges in a graph of order \( n \) and girth at least \( 2k + 1 \). The function \( g_k(n) \) has been studied extensively; see the surveys by Bondy [6], and by Füredi and Simonovits [28]. It is known that for \( 2 \leq k \neq 5 \), and sufficiently large \( n \),

\[
c_k' n^{1 + \frac{2}{m-k+1}} \leq g_k(n) \leq c_k n^{1 + \frac{1}{k}},
\]

where \( \epsilon = 0 \) if \( k \) is odd, \( \epsilon = 1 \) if \( k \) is even, and \( c_k' \) and \( c_k \) are positive constants depending on \( k \) only. The upper bound was due to Bondy and Simonovits [5], and the lower bound was obtained via an explicit construction by Lazebnik, Ustimenko and Woldar [55]. (For many prior related results see the references in [5, 55].) For \( k = 5 \), a better lower bound is known, and it is of magnitude \( n^{1+1/5} \). The only known

*This chapter is the paper [48]

80
values of $k$ for which the lower bound for $g_k(n)$ is of (maximum) magnitude $n^{1+1/k}$ are $k = 2, 3$, and 5. Several graphs of such extremal magnitude were constructed using polynomials over finite fields as we describe below.

For each $k = 2, 3, 5$, consider a bipartite graph $\Gamma_k(q)$ with vertex partitions $P_k = \mathbb{F}_q^k$ and $L_k = \mathbb{F}_q^k$, and edges defined as follows.

For $k = 2$, a vertex $(p) = (p_1, p_2) \in P_2$ is adjacent to a vertex $[l] = [l_1, l_2] \in L_2$ if and only if

$$p_2 + l_2 = p_1l_1.$$

For $k = 3$, a vertex $(p) = (p_1, p_2, p_3) \in P_3$ is adjacent to a vertex $[l] = [l_1, l_2, l_3] \in L_3$ if and only if the following two equalities hold:

$$p_2 + l_2 = p_1l_1, \quad p_3 + l_3 = p_1l_1^2.$$

For $k = 5$, a vertex $(p) = (p_1, p_2, p_3, p_4, p_5) \in P_5$ is adjacent to a vertex $[l] = [l_1, l_2, l_3, l_4, l_5] \in L_5$ if and only if the following four equalities hold:

$$p_2 + l_2 = p_1l_1, \quad p_3 + l_3 = p_1l_1^2, \quad p_4 + l_4 = p_1l_1^3, \quad p_5 + l_5 = p_4l_1 - 2p_3l_2 + p_2l_3.$$

It can be shown that for $k = 2, 3$ and 5, the graph $\Gamma_k(q)$ is $q$-regular, and it can be shown that the girth of $\Gamma_k(q)$ is $2(k + 1)$ (for $k = 5$ we have to assume that $q$ is odd). For the origins and properties of these constructions, and their relation to generalized polygons, see Lazebnik and Ustimenko [54], [55], Lazebnik and Woldar [56], and the references therein. The graphs described above are also related to Moore graphs and cages; see Miller and Širáň [69] and Exoo and Jajcay [23].

Similar constructions of hypergraphs turned out to be useful for some extremal problems for hypergraphs; see Lazebnik and Mubayi [57] and Lazebnik and Verstraëte [58].

In what follows we concentrate on a generalization of the construction of $\Gamma_3(q)$ above. Let $f, g \in \mathbb{F}_q[x, y]$. The graph $G = G_q(f, g)$ is a bipartite graph
with vertex partitions \( P = \mathbb{F}_q^3 \) and \( L = \mathbb{F}_q^3 \), and edges defined as follows: a vertex \( (p) = (p_1, p_2, p_3) \in P \) is adjacent to a vertex \( [l] = [l_1, l_2, l_3] \in L \) if and only if

\[
p_2 + l_2 = f(p_1, l_1) \quad \text{and} \quad p_3 + l_3 = g(p_1, l_1).
\]

It is clear that \( \Gamma_3(q) = G_q(xy, xy^2) \), and as we already mentioned, the girth of this graph is eight. If \( f \) and \( g \) are monomials, we refer to \( G_q(f, g) \) as a monomial graph.

For certain questions in extremal graph theory and finite geometry, it is desirable to have examples of graphs \( G_q(f, g) \) containing no cycles of length less than eight and not isomorphic to the graph \( G_q(xy, xy^2) \). Do they exist? So far, no such graphs \( G_q(f, g) \) have been found for odd \( q \). For even \( q \), such examples exist, in particular, among monomial graphs. This motivated Dmytrenko, Lazebnik and Wiliford [20] and Kronenthal [52] to study monomial graphs \( G_q(f, g) \) of girth at least eight for odd \( q \). We encourage the interested reader to see these papers for more details and related references.

The results from [20] and [52] suggest that for odd \( q \), monomial graphs of girth at least eight are isomorphic to \( \Gamma_3(q) \). The main conjecture of [20] and [52] is the following.

**Conjecture 5.1.1** Let \( q \) be an odd prime power. Then every monomial graph of girth eight is isomorphic to \( \Gamma_3(q) \).

In an attempt to prove Conjecture 5.1.1, two more related conjectures were proposed in [20] and [52].

For an integer \( 1 \leq k \leq q - 1 \), let

\[
A_k = x^k[(x + 1)^k - x^k] \in \mathbb{F}_q[x]
\]  
(5.1.2)

and

\[
B_k = [(x + 1)^{2k} - 1]x^{q-1-k} - 2x^{q-1} \in \mathbb{F}_q[x].
\]  
(5.1.3)
**Conjecture A.** Let $q$ be a power of an odd prime $p$ and $1 \leq k \leq q - 1$. Then $A_k$ is a PP of $\mathbb{F}_q$ if and only if $k$ is a power of $p$.

**Conjecture B.** Let $q$ be a power of an odd prime $p$ and $1 \leq k \leq q - 1$. Then $B_k$ is a PP of $\mathbb{F}_q$ if and only if $k$ is a power of $p$.

The logical relation between the above three conjectures is as follows. It was proved in [20] that for odd $q$, every monomial graph of girth at least eight is isomorphic to $G_q(xy, x^k y^{2k})$, where $1 \leq k \leq q - 1$ is an integer not divisible by $p$ for which both $A_k$ and $B_k$ are PPs of $\mathbb{F}_q$. In particular, either of Conjectures A and B implies Conjecture 5.1.1.

In [20] and [52], the above conjectures were shown to be true under various additional conditions. The main objective of this chapter is to confirm Conjecture 5.1.1. This is achieved by making progress on Conjectures A and B. Our results fall short of establishing the claims of Conjectures A and B. However, when considered together, these partial results on Conjectures A and B turn out to be sufficient for proving Conjecture 5.1.1.

Throughout this chapter, most equations involving integers should be treated as equations in the characteristic of $\mathbb{F}_q$, i.e., in characteristic $p$.

**Prior Status of Conjecture A**

The proof of [20, Theorem 1] implies that Conjecture A is true for $q = p$.

**Prior Status of Conjecture B**

For each odd prime $p$, let $\alpha(p)$ be the smallest positive even integer $a$ such that

$$
\binom{a}{a/2} \equiv (-1)^{a/2} 2^a \pmod{p}.
$$

The proof of [52, Theorem 4] implies the following.
Theorem 5.1.2 Let \( p \) be an odd prime. If Conjecture B is true for \( q = p^e \), then it is also true for \( q = p^{em} \) whenever

\[
m \leq \frac{p - 1}{[(p - 1)/\alpha(p)]}.
\]

Unfortunately, unlike Conjecture A, Conjecture B has not been established for \( q = p \).

5.2 Power Sums of \( A_k \) and \( B_k \)

Let \( q \) be any prime power (even or odd). For each integer \( a > 0 \), let \( a^* \in \{1, \ldots, q - 1\} \) be such that \( a^* \equiv a \pmod{q - 1} \); we also define \( 0^* = 0 \). Note that for all \( a \geq 0 \) and \( x \in \mathbb{F}_q \), \( x^a = x^{a^*} \). We always assume that \( 1 \leq k \leq q - 1 \); additional assumptions on \( k \), when they apply, will be included in the context.

Lemma 5.2.1 For \( 1 \leq s \leq q - 1 \),

\[
\sum_{x \in \mathbb{F}_q} A_k(x)^s = (-1)^{s+1} \sum_{i=0}^s (-1)^i \binom{s}{i} \frac{(ki)^*}{(2ks)^*}.
\] (5.2.4)

Proof. We have

\[
\sum_{x \in \mathbb{F}_q} A_k(x)^s = \sum_{x \in \mathbb{F}_q^*} \left( (x + 1)^k - x^k \right)^s
\]

\[
= \sum_{x \in \mathbb{F}_q^*} x^{ks} \sum_i \binom{s}{i} (x + 1)^{ki} (-x^k)^{s-i}
\]

\[
= \sum_{x \in \mathbb{F}_q^*} \sum_i (-1)^{s-i} \binom{s}{i} x^{2ks-ki} (x + 1)^{(ki)^*}
\]

\[
= \sum_{x \in \mathbb{F}_q} \sum_i (-1)^{s-i} \binom{s}{i} x^{2ks-ki} \sum_j \binom{(ki)^*}{j} x^{(ki)^* - j}
\]

\[
= \sum_{i,j} (-1)^{s-i} \binom{s}{i} \binom{(ki)^*}{j} \sum_{x \in \mathbb{F}_q^*} x^{2ks-j}
\]
\[
= (-1)^{s+1} \sum_i (-1)^i \left( \begin{array}{c} s \\ i \end{array} \right) \sum_{j \equiv 2ks \pmod{q-1}} \left( \begin{array}{c} (ki)^* \\ j \end{array} \right).
\]

If \(2ks \not\equiv 0 \pmod{q-1}\),
\[
\sum_{x \in \mathbb{F}_q} A_k(x)^s = (-1)^{s+1} \sum_i (-1)^i \left( \begin{array}{c} s \\ i \end{array} \right) \left( \begin{array}{c} (ki)^* \\ (2ks)^* \end{array} \right).
\]

If \(2ks \equiv 0 \pmod{q-1}\),
\[
\sum_{x \in \mathbb{F}_q} A_k(x)^s = (-1)^{s+1} \sum_i (-1)^i \left( \begin{array}{c} s \\ i \end{array} \right) \left[ \left( \begin{array}{c} (ki)^* \\ 0 \end{array} \right) + \left( \begin{array}{c} (ki)^* \\ q-1 \end{array} \right) \right]
\]
\[
= (-1)^{s+1} \sum_i (-1)^i \left( \begin{array}{c} s \\ i \end{array} \right) \left( \begin{array}{c} (ki)^* \\ (2ks)^* \end{array} \right).
\]

Hence (5.2.4) always holds.

\[\]

Lemma 5.2.2  
(i) If \(q\) is even,
\[
\sum_{x \in \mathbb{F}_q} B_k(x)^s = \sum_{i=0}^{s} \left( \begin{array}{c} s \\ i \end{array} \right) \left( \begin{array}{c} (2ki)^* \\ (ks)^* \end{array} \right), \quad 1 \leq s \leq q-1.
\]  \hspace{1cm} (5.2.5)

(ii) If \(q\) is odd,
\[
\sum_{x \in \mathbb{F}_q} B_k(x)^s = -(-2)^s \sum_{i,j} 2^{-i} (-1)^j \left( \begin{array}{c} s \\ i \\ j \end{array} \right) \left( \begin{array}{c} (2kj)^* \\ (ki)^* \end{array} \right), \quad 1 \leq s \leq q-1.
\]  \hspace{1cm} (5.2.6)

Proof.  
(i) If \(k = q-1\),
\[
B_k(x) = (x+1)^{2(q-1)} - 1 = \begin{cases} 
1 & \text{if } x = 1, \\
0 & \text{if } x \in \mathbb{F}_q \setminus \{1\},
\end{cases}
\]
so the left side of (5.2.5) is 1. On the other hand, the right side of (5.2.5) equals

\[ \sum_{i=1}^{s} \binom{s}{i} = 1, \]

and hence (5.2.5) holds.

Now assume that \( 1 \leq k < q - 1 \). The calculation is identical to the proof of Lemma 5.2.1. We have

\[
\sum_{x \in \mathbb{F}_q} B_k(x)^s = \sum_{x \in \mathbb{F}_q^*} \left( [(x + 1)^{2k} + 1] x^{-k} \right)^s \\
= \sum_{x \in \mathbb{F}_q^*} x^{-ks} \left( (x + 1)^{2k} + 1 \right)^s \\
= \sum_{x \in \mathbb{F}_q^*} x^{-ks} \sum_i \left( \binom{s}{i} (x + 1)^{(2ki)^*} \right) \\
= \sum_{x \in \mathbb{F}_q^*} x^{-ks} \sum_i \binom{s}{i} \sum_j \binom{(2ki)^*}{j} x^j \\
= \sum_{i, j} \binom{s}{i} \binom{(2ki)^*}{j} \sum_{x \in \mathbb{F}_q^*} x^j \\
= \sum_{i} \binom{s}{i} \sum_{j \equiv ks \pmod{q-1}} \binom{(2ki)^*}{j}.
\]

If \( ks \not\equiv 0 \pmod{q - 1} \),

\[
\sum_{x \in \mathbb{F}_q} B_k(x)^s = \sum_{i} \binom{s}{i} \binom{(2ki)^*}{(ks)^*}.
\]

If \( ks \equiv 0 \pmod{q - 1} \),

\[
\sum_{x \in \mathbb{F}_q} B_k(x)^s = \sum_{i} \binom{s}{i} \left[ \binom{(2ki)^*}{0} + \binom{(2ki)^*}{q-1} \right] = \sum_{i} \binom{s}{i} \binom{(2ki)^*}{(ks)^*}.
\]
(ii) We have

\[ \sum_{x \in \mathbb{F}_q} B_k(x)^s = \sum_{x \in \mathbb{F}_q} \left( [(x + 1)^{2k} - 1] x^{-k} - 2 \right)^s \]

\[ = \sum_{x \in \mathbb{F}_q} \sum_i \binom{s}{i} [(x + 1)^{2k} - 1]^i x^{-ki} (-2)^{s-i} \]

\[ = (-2)^s \sum_{x \in \mathbb{F}_q} \sum_i (-2)^{-i} \binom{s}{i} x^{-ki} \sum_j \binom{i}{j} (x + 1)^{(2kj)^*} (-1)^{i-j} \]

\[ = (-2)^s \sum_{x \in \mathbb{F}_q} \sum_{i,j} 2^{-i} (-1)^j \binom{s}{i} \binom{i}{j} x^{-ki} \sum_l \binom{(2kj)^*}{l} x^l \]

\[ = (-2)^s \sum_{i,j,l} 2^{-i} (-1)^j \binom{s}{i} \binom{i}{j} \binom{(2kj)^*}{l} \sum_{x \in \mathbb{F}_q} x^{l-ki} \]

\[ = -(-2)^s \sum_{i,j,l} \sum_{t \equiv ki (\text{mod } q-1)} 2^{-i} (-1)^j \binom{s}{i} \binom{i}{j} \binom{(2kj)^*}{l}. \]

Note that if \( l \equiv ki \pmod{q-1} \) and \( 0 \leq l \leq (2kj)^* \), then either \( l = (ki)^* \) or \( i = 0 \), \( j > 0 \) and \( l = q-1 \); in the latter case, \( \binom{i}{j} = 0 \). Therefore, we have

\[ \sum_{x \in \mathbb{F}_q} B_k(x)^s = -(-2)^s \sum_{i,j} 2^{-i} (-1)^j \binom{s}{i} \binom{i}{j} \binom{(2kj)^*}{(ki)^*}. \]

\[ \boxed{} \]

**Theorem 5.2.3**

(i) \( A_k \) is a PP of \( \mathbb{F}_q \) if and only if \( \gcd(k, q-1) = 1 \) and

\[ \sum_i (-1)^i \binom{s}{i} \binom{(ki)^*}{(2ks)^*} = 0 \quad \text{for all} \quad 1 \leq s \leq q-2. \]  \hspace{1cm} (5.2.7)

(ii) \( B_k \) is a PP of \( \mathbb{F}_q \) if and only if \( \gcd(k, q-1) = 1 \) and

\[ \sum_i (-1)^i \binom{s}{i} \binom{(2ki)^*}{(ks)^*} = (-2)^s \quad \text{for all} \quad 1 \leq s \leq q-2. \]  \hspace{1cm} (5.2.8)

We remind the reader that according to our convention, (5.2.7) and (5.2.8) are to be treated as equations in characteristic \( p \).
Proof. [Proof of Theorem 5.2.3] We prove the claims using Hermite’s criterion.

(i) Clearly, 0 is the only root of $A_k$ in $\mathbb{F}_q$ if and only if $\gcd(k, q - 1) = 1$. By (5.2.4),
$$
\sum_{x \in \mathbb{F}_q} A_k(x)^s = 0 \text{ for all } 1 \leq s \leq q - 2 \text{ if and only if (5.2.7) holds.}
$$

(ii) We consider even and odd $q$’s separately.

Case 1. Assume that $q$ is even. We have $B_k = [(x + 1)^{2k} - 1]x^{q-1-k}$.

If $q = 2$, then $k = 1$ and $B_k = x^2$, which is a PP of $\mathbb{F}_2$. In this case, (5.2.8) is vacuously satisfied.

Now assume that $q > 2$. Clearly, 0 is the only root of $B_k$ in $\mathbb{F}_q$ if and only if \( \gcd(k, q - 1) = 1 \). By (5.2.5), \( \sum_{x \in \mathbb{F}_q} B_k(x)^s = 0 \) for all \( 1 \leq s \leq q - 2 \) if and only if (5.2.8) holds.

Case 2. Assume that $q$ is odd.

1° We claim that if $B_k$ is a PP of $\mathbb{F}_q$, then $\gcd(k, (q - 1)/2) = 1$. Otherwise, $\gcd(2k, q - 1) > 2$ and the equation $(x + 1)^{2k} - 1 = 0$ has at least two roots $x_1, x_2 \in \mathbb{F}_q^*$. Then $B_k(x_1) = -2 = B_k(x_2)$, which is a contradiction.

2° We claim that $B_k$ is a PP of $\mathbb{F}_q$ if and only if $\gcd(k, (q - 1)/2) = 1$ and (5.2.8) holds.

By 1° and (5.2.6), we only have to show that under the assumption that $\gcd(k, (q - 2)/2) = 1$,

$$
\sum_{i,j} 2^{-i}(-1)^j \binom{s}{i} \binom{i}{j} \binom{(2k)j}{(ki)^*} = \begin{cases} 0 & \text{for } 1 \leq s \leq q - 2, \\ 1 & \text{for } s = q - 1, \end{cases} \quad (5.2.9)
$$

if and only if (5.2.8) holds. Set

$$
S_i = 2^{-i} \sum_j (-1)^j \binom{i}{j} \binom{(2k)j}{(ki)^*}, \quad 0 \leq i \leq q - 1.
$$
Then (5.2.9) is equivalent to
\[
\sum_i \binom{s}{i} S_i = \begin{cases} 
1 & \text{if } s = 0, \\
0 & \text{if } 1 \leq s \leq q - 2, \\
1 & \text{if } s = q - 1.
\end{cases} \tag{5.2.10}
\]
Equation (5.2.10) is a recursion for \( S_i \), which has a unique solution
\[
S_i = \begin{cases} 
(-1)^i \quad &\text{if } 0 \leq i \leq q - 2, \\
2 \quad &\text{if } i = q - 1.
\end{cases}
\]
Therefore, (5.2.9) is equivalent to
\[
\sum_j (-1)^j \binom{i}{j} \binom{(2kj)^*}{(ki)^*} = \begin{cases} 
(-2)^i \quad &\text{if } 0 \leq i \leq q - 2, \\
2 \quad &\text{if } i = q - 1.
\end{cases} \tag{5.2.11}
\]
It remains to show that when \( i = 0 \) and \( q - 1 \), (5.2.11) is automatically satisfied. When \( i = 0 \), (5.2.11) is clearly satisfied. When \( i = q - 1 \),
\[
\sum_j (-1)^j \binom{i}{j} \binom{(2kj)^*}{(ki)^*} = \sum_{j=q-1}^{q-1} (-1)^j \binom{q-1}{j} \binom{(2kj)^*}{(q-1)}
= (-1)^{q-1} (-1)^{q-1} \binom{q-1}{q-1} = 2.
\]
3\(^{\circ}\) To complete the proof of Case 2, it remains to show that if \( B_k \) is a PP of \( \mathbb{F}_q \), then \( \gcd(k, q - 1) = 1 \), that is, \( k \) must be odd. This is given by Lemma 5.3.7 later.

### 5.3 Facts concerning \( A_k \) and \( B_k \)

Assume that \( q > 2 \) and \( 1 \leq k \leq q - 1 \), and let
\[
a := \left\lfloor \frac{q - 1}{k} \right\rfloor, \tag{5.3.12}
\]
When \( \gcd(k, q - 1) = 1 \), let \( k', b \in \{1, \ldots, q - 1\} \) be such that

\[
k'k \equiv 1 \pmod{q - 1}, \quad bk \equiv -1 \pmod{q - 1},
\]

and set

\[
c := \left\lfloor \frac{q - 1}{k'} \right\rfloor.
\]

Note that

\[
\frac{q - 1}{a + 1} < k < \frac{q - 1}{a},
\]

and

\[
\frac{q - 1}{c + 1} < k' \leq \frac{q - 1}{c}.
\]

The following obvious fact will be used frequently.

**Fact 5.3.1** \( A_k \) is a PP of \( \mathbb{F}_q \) if and only if \( A_{(pk)^*} \) is. The same is true for \( B_k \).

**Lemma 5.3.2** If \( 1 < k \leq q - 1 \) and \( A_k \) is a PP of \( \mathbb{F}_q \), then

\[
\left( \frac{ka}{q - 1 - ka} \right) \equiv 0 \pmod{p},
\]

and

\[
\left( \frac{2c}{c} \right) \equiv 0 \pmod{p}.
\]

**Proof.** 1° We first prove (5.3.17). By Theorem 5.2.3 (i), \( \gcd(k, q - 1) = 1 \), and hence (5.3.15) becomes

\[
\frac{q - 1}{a + 1} < k < \frac{q - 1}{a}.
\]

Therefore

\[
q - 1 < k(a + 1) \leq 2ka < 2(q - 1),
\]
which implies that \((2ka)^* = 2ka - q + 1\). By (5.2.7),

\[
0 = \sum_{i} (-1)^i \binom{a}{i} \binom{(ki)^*}{(2ka)^*} = \sum_{2a - \frac{q+1}{k} \leq i \leq a} (-1)^i \binom{a}{i} \binom{ki}{2ka - q + 1}
\]

\[
= (-1)^a \binom{ka}{2ka - q + 1} = (-1)^a \binom{ka}{q - 1 - ka}.
\]

(Note: in the above, \(2a - (q - 1)/k \leq i \leq a\) implies that \(i = a\).)

2° We now prove (5.3.18). If \(c > (q - 1)/2\), (5.3.18) is automatically satisfied. So we assume that \(c \leq (q - 1)/2\). Since \(\gcd(k', q - 1) = 1\), (5.3.16) becomes

\[
\frac{q - 1}{c + 1} < k < \frac{q - 1}{c}. \quad (5.3.20)
\]

If \(c = (q - 1)/2\), then (5.3.20) implies that \(k' = 1\). It follows that \(k = 1\), which is a contradiction. Thus \(c < (q - 1)/2\). Set \(s = (cb)^*\). Then

\[
s = q - 1 - ck', \quad (5.3.21)
\]

and

\[
(2ks)^* = q - 1 - 2c. \quad (5.3.22)
\]

By (5.2.7),

\[
0 = \sum_{i} (-1)^i \binom{s}{i} \binom{(ki)^*}{(2ks)^*} = \sum_{i} (-1)^i \binom{s}{i} \binom{(ki)^*}{q - 1 - 2c}. \quad (5.3.23)
\]

For each \(0 \leq l \leq 2c\), let \(i(l) \in \{0, \ldots, q - 1\}\) be such that \((ki(l))^* = q - 1 - l\). Because of (5.3.20), we have

\[
i(l) = \begin{cases} 
q - 1 - lk' & \text{if } 0 \leq l \leq c, \\
2(q - 1) - lk' & \text{if } c + 1 \leq l \leq 2c.
\end{cases}
\]

When \(0 \leq l < c\),

\[
i(l) = q - 1 - lk' > q - 1 - ck' = s.
\]
When \( c < l \leq 2c \), we also have

\[
i(l) = 2(q - 1) - lk' > q - 1 - ck' = s.
\]

When \( l = c \), \( i(l) = s \). Therefore (5.3.23) becomes

\[
0 = (-1)^s \binom{q - 1 - c}{q - 1 - 2c} = (-1)^s \left( \frac{q - 1 - c}{c} \right) = (-1)^s \left( -1 - c \right) = (-1)^{s+c} \left( \frac{2c}{c} \right).
\]

\[\blacksquare\]

**Corollary 5.3.3**  
*Conjecture A is true for \( q = p \).*

**Proof.** Let \( 1 < k \leq p - 1 \). Since \( 0 \leq p - 1 - ka \leq ka \leq p - 1 \), we have

\[
\binom{ka}{p - 1 - ka} \not\equiv 0 \pmod{p}.
\]

By Lemma 5.3.2, \( A_k \) is not a PP of \( \mathbb{F}_q \).

\[\blacksquare\]

**Remark 5.3.4** Equation (5.3.17) is contained in [20, Theorem 1], and Corollary 5.3.3 is implied by the proof of [20, Theorem 1].

**Lemma 5.3.5** Assume that \( A_k \) is a PP of \( \mathbb{F}_q \). Then all the base \( p \) digits of \( k' \) are 0 or 1.

**Proof.** We only have to consider the case when \( k \) is not a power of \( p \). By (5.3.18), we have \( c > (p - 1)/2 \). Write \( k' = k'_0 p^0 + \cdots + k'_{e-1} p^{e-1} \), where \( 0 \leq k'_i \leq p - 1 \). Since

\[
c \leq \frac{q - 1}{k'} \leq \frac{p^e - 1}{k'_{e-1} p^{e-1}},
\]

we have

\[
k'_{e-1} c \leq p - \frac{1}{p^{e-1}},
\]
and hence \( k'_e - 1 \leq p - 1 \). It follows that \( k'_e - 1 \leq (p - 1)/c < 2 \). Replacing \( k' \) with \( (p^{e-1}i'k')^* \) (and \( k \) with \( (p^{1+i}k)^* \)), we also have \( k'_i < 2 \).

\[
-1 = \prod_{x \in \mathbb{F}_q \setminus \{-2\}} f(x) = 2 \prod_{x \in \mathbb{F}_q \setminus \{0,-2\}} \frac{(x + 1)^{2k} - 1}{x^k} = 2^{k+1} \prod_{x \in \mathbb{F}_q \setminus \{\pm 1\}} (x^k + 1)(x^k - 1).
\]

(5.3.24)

**Case 1.** Assume that \( k \) is odd. Since \( \gcd(k, (q - 1)/2) = 1 \), we have \( \gcd(k, q - 1) = 1 \). Then,

\[
\prod_{x \in \mathbb{F}_q \setminus \{\pm 1\}} (x^k + 1) = \prod_{y \in \mathbb{F}_q \setminus \{0,2\}} y = -\frac{1}{2},
\]

\[
\prod_{x \in \mathbb{F}_q \setminus \{\pm 1\}} (x^k - 1) = \prod_{y \in \mathbb{F}_q \setminus \{0,-2\}} y = \frac{1}{2}.
\]

Therefore (5.3.24) gives

\[
-1 = 2^{k+1} \left( -\frac{1}{2} \right)^{\frac{1}{2}},
\]

that is, \( 2^{k-1} = 1 \).

**Case 2.** Assume that \( k \) is even. Then \( (q - 1)/2 \) is odd and \( \gcd(k, q - 1) = 2 \).
Let $S$ denote the set of nonzero squares in $\mathbb{F}_q$. We have

$$
\prod_{\alpha \in S} (x - \alpha) = x^{(q-1)/2} - 1. \tag{5.3.25}
$$

Setting $x = -1$ in (5.3.25) gives $\prod_{\alpha \in S} (\alpha + 1) = 2$, that is,

$$
\prod_{\alpha \in S \setminus \{1\}} (\alpha + 1) = 1. \tag{5.3.26}
$$

By (5.3.25),

$$
\prod_{\alpha \in S \setminus \{1\}} (x + 1 - \alpha) = \frac{(x + 1)^{(q-1)/2} - 1}{x} = \sum_{i=1}^{(q-1)/2} \binom{(q-1)/2}{i} x^{i-1}. \tag{5.3.27}
$$

Setting $x = 0$ in (5.3.27) gives

$$
\prod_{\alpha \in S \setminus \{1\}} (\alpha - 1) = \frac{q-1}{2} = -\frac{1}{2}. \tag{5.3.28}
$$

By (5.3.26) and (5.3.28),

$$
\prod_{x \in \mathbb{F}_q \setminus \{\pm 1\}} (x^k + 1) = \prod_{x \in \mathbb{F}_q \setminus \{\pm 1\}} (x^2 + 1) = \left( \prod_{\alpha \in S \setminus \{1\}} (\alpha + 1) \right)^2 = 1,
$$

$$
\prod_{x \in \mathbb{F}_q \setminus \{\pm 1\}} (x^k - 1) = \left( \prod_{\alpha \in S \setminus \{1\}} (\alpha - 1) \right)^2 = \frac{1}{4}.
$$

Thus (5.3.24) becomes $2^{k-1} = -1$.

\[\square\]

**Lemma 5.3.7** Assume that $q$ is odd, $1 < k \leq q - 1$, and $B_k$ is a PP of $\mathbb{F}_q$. Then $k$ is odd, $a$ and $c$ are even, and

$$
2^{k-1} = 1, \tag{5.3.29}
$$

$$
\left( \frac{a}{\frac{q}{2}} \right) = (-1)^{\frac{q}{4}} 2^a. \tag{5.3.30}
$$
\[
\left(\frac{a-1}{\frac{q}{2}}\right)\left(\frac{ka}{k}\right) = (-1)^{\frac{q}{2}-1}2^{a-1}, \tag{5.3.31}
\]
\[
\left(\frac{b}{\frac{q-1}{2}}\right) = (-1)^{b+\frac{q+1}{2}}2^b, \tag{5.3.32}
\]
\[
\left(\frac{q-1-ck'}{\frac{1}{2}(q-1-ck')}\right) = (-1)^{\frac{q+1}{2}+\frac{q-1}{2}}2^{-ck'}, \tag{5.3.33}
\]
\[
(-c+1)\left(\frac{q-1-(c-1)k'}{\frac{1}{2}[q-1-(c-2)k']}\right) = (-1)^{\frac{q+1}{2}+\frac{q-1}{2}}2^{-(c-1)k'}. \tag{5.3.34}
\]

**Proof.** 1° We first show that \(k\) is odd. This will imply (5.3.29) through Lemma 5.3.6 and also complete the proof of Theorem 5.2.3, Case 2, Step 3°. Recall from the proof of Theorem 5.2.3, Case 2, Step 2°, that \(\gcd(k,(q-1)/2) = 1\) and (5.2.8) holds.

Assume to the contrary that \(k\) is even. Equation (5.2.8) with \(s = (q - 1)/2\) gives

\[
\sum_i (-1)^i \left(\frac{\frac{q-1}{2}}{i}\right) \left(\frac{(2ki)^*}{q-1}\right) = (-2)^{\frac{q-1}{2}}. \tag{5.3.35}
\]

Since \(\gcd(2k,q-1) = 2\), \((q - 1)/2\) is odd. In the above,

\[
\left(\frac{\frac{q-1}{2}}{i}\right) \left(\frac{(2ki)^*}{q-1}\right) \neq 0
\]

only if \(i = (q - 1)/2\). Hence (5.3.35) gives \(2^{(q-1)/2} = 1\). So the order of 2 in \(\mathbb{F}_p^*\) is odd. However, by Lemma 5.3.6, \(2^{k-1} = -1\) has order 2, which is a contradiction.

2° We now prove that \(a\) is even and (5.3.30) and (5.3.31) hold. Since \(\gcd(k,(q-1)/2) = 1\) and \(k\) is odd, we have \(\gcd(k,q-1) = 1\). Thus (5.3.15) becomes

\[
\frac{q-1}{a+1} < k < \frac{q-1}{a}.
\]

By (5.2.8),

\[
\sum_i (-1)^i \left(\frac{a}{i}\right) \left(\frac{(2ki)^*}{ka}\right) = (-2)^a. \tag{5.3.36}
\]

In the above, \((2ki)^* \geq ka\) only when \(i \geq a/2\). When \(a/2 < i \leq a\), \((2ki)^* = 2ki - (q -
1) \( < ka \). Therefore, \( a \) must be even and (5.3.36) becomes

\[
(-1)^{\frac{a}{2}} \binom{a}{\frac{a}{2}} = (-2)^a,
\]

which is (5.3.30). Also by (5.2.8),

\[
\sum_i (-1)^i \binom{a-1}{i} \binom{(2ki)^*}{k(a-1)} = (-2)^{a-1}.
\]  

(5.3.37)

In the above, \((2ki)^* \geq k(a-1)\) only when \( i \geq (a-1)/2 \), i.e., \( i \geq a/2 \) (since \( a \) is even). When \( a/2 < i \leq a-1 \), \((2ki)^* = 2ki - (q-1) < k(a-1)\). Hence (5.3.37) becomes

\[
(-1)^{\frac{a}{2}} \binom{a-1}{\frac{a}{2}} \binom{ka}{k(a-1)} = (-2)^{a-1},
\]

which is (5.3.31).

3° Next, we prove (5.3.32). By (5.2.8),

\[
(-2)^b = \sum_i (-1)^i \binom{b}{i} \binom{(2ki)^*}{(kb)^*} = \sum_i (-1)^i \binom{b}{i} \binom{(2ki)^*}{q-2}.
\]  

(5.3.38)

In the above,

\[
\binom{b}{i} \binom{(2ki)^*}{q-2} \neq 0
\]

only if \( i = (q-1)/2 \). Hence (5.3.38) gives

\[
(-2)^b = (-1)^{\frac{q-1}{2}} \binom{b}{\frac{q-1}{2}} \binom{q-1}{q-2} = (-1)^{\frac{q+1}{2}} \binom{b}{\frac{q-1}{2}},
\]

which is (5.3.32).

4° Finally, we prove that \( c \) is even and (5.3.33) and (5.3.13) hold.

In (5.3.16), if \( k' = (q-1)/c \), since \( \gcd(k', q-1) = 1 \), we must have \( k' = 1 \). Then \( k = 1 \), which is a contradiction. Therefore (5.3.16) becomes

\[
\frac{q-1}{c+1} < k' < \frac{q-1}{c}.
\]  

(5.3.39)
Let \( s = (cb)^* \). Then we have

\[
s = q - 1 - ck', \quad (ks)^* = q - 1 - c.
\]

By (5.2.8),

\[
\sum_i (-1)^i \binom{s}{i} \binom{(2ki)^*}{q - 1 - c} = (-2)^s. \tag{5.3.40}
\]

For \( 0 \leq l \leq c/2 \), let \( i \in \{0, \ldots, q - 1\} \) be such that \((2ki)^* = q - 1 - 2l\). By (5.3.39),

\[
i = q - 1 - lk' \quad \text{or} \quad \frac{1}{2}(q - 1) - lk'.
\]

If \( i = q - 1 - lk' \), then \( i > q - 1 - ck' = s \). If \( i = \frac{1}{2}(q - 1) - lk' \), then \( i \leq s \) only if \( l = c/2 \). In fact, \( \frac{1}{2}(q - 1) - lk' = i \leq s = q - 1 - ck' \) implies that

\[
k' \leq \frac{q - 1}{2(c - l)},
\]

which, by (5.3.39), implies that \( 2(c - l) \leq c \), i.e., \( l \geq c/2 \).

Therefore, the \( i \)th term of the sum in (5.3.40) is nonzero only if \( i = \frac{1}{2}(q - 1) - \frac{c}{2}k' \). Hence \( c \) must be even and (5.3.40) gives

\[
(-1)^{\frac{1}{2}(q-1-ck')} \left( \frac{q - 1 - ck'}{\frac{1}{2}(q - 1 - ck')} \right) = (-2)^{-ck'},
\]

which is (5.3.33).

To prove (5.3.34), we choose \( s = ((c - 1)b)^* \). We have

\[
s = q - 1 - (c - 1)k', \quad (ks)^* = q - 1 - (c - 1),
\]

and (5.2.8) gives

\[
\sum_i (-1)^i \binom{s}{i} \binom{(2ki)^*}{q - 1 - (c - 1)} = (-2)^s. \tag{5.3.41}
\]

97
For $0 \leq l \leq c/2 - 1$, let $i \in \{0, \ldots, q - 1\}$ be such that $(2ki)^* = q - 1 - 2l$. Then

$$i = q - 1 - lk' \text{ or } \frac{1}{2}(q - 1) - lk'.$$

If $i = q - 1 - lk'$, then $i > s$. If $i = \frac{1}{2}(q - 1) - lk'$, then $i \leq s$ only if $l = c/2 - 1$. In fact, $i \leq s$ implies that $k' \leq \frac{q - 1}{2(c - 1 - l)}$, which further implies that $2(c - 1 - l) \leq c$, i.e., $l \geq c/2 - 1$. Therefore, the $i$th term of the sum in (5.3.41) is nonzero only if $i = \frac{1}{2}[q - 1 - (c - 2)k']$. Hence (5.3.41) gives

$$-2^{-(c-1)k'} = (-1)^{\frac{c-1}{2}} \left( \frac{q - 1 - (c - 1)k'}{\frac{1}{2}(q - 1 - (c - 2)k')} \right) \left( \frac{q - 1 - 2(c - 1)}{q - 1 - (c - 1)} \right) \left( -c + 1 \right),$$

which is (5.3.34).

Remark 5.3.8 Since

$$\left( \frac{p - 1}{\frac{p - 1}{2}} \right) \equiv (-1)^{\frac{p - 1}{2}} \pmod{p},$$

we always have $\alpha(p) \leq p - 1$.

Lemma 5.3.9 Assume that $q$ is odd and $1 < k \leq q - 1$. If $B_k$ is a PP of $\mathbb{F}_q$, then all the base $p$ digits of $k$ are $\leq (p - 1)/\alpha(p)$.

Proof. By (5.3.30), $a = [(q - 1)/k] \geq \alpha(p)$. Let $q = p^e$ and write $k = k_0p^0 + \cdots + k_{e-1}p^{e-1}$, where $0 \leq k_i \leq p - 1$. We first show that $k_{e-1} \leq (p - 1)/\alpha(p)$. Assume that
Since $k_{e-1} > 0$, we have
\[ a \leq \frac{q-1}{k} \leq \frac{p^e - 1}{k_{e-1}p^{e-1}}, \]
we have
\[ k_{e-1}a \leq p - \frac{1}{p^{e-1}}. \]
Thus $k_{e-1}a \leq p - 1$, and hence $k_{e-1} \leq (p - 1)/a \leq (p - 1)/\alpha(p)$.
Replacing $k$ with $(p^{e-1-i}k)^*$, we conclude that $k_i \leq (p - 1)/\alpha(p)$.

We include a quick proof for Theorem 5.1.2.

**Proof.** [Proof of Theorem 5.1.2] Let $q = p^e$. Assume that $1 < k \leq q^n - 1$ and $B_k$ is a PP of $\mathbb{F}_q$. Write $k = k_0q^0 + \cdots + k_{m-1}q^{m-1}$, $0 \leq k_i \leq q - 1$. By Lemma 5.3.9, all the base $p$ digits of $k$ are $\leq \lfloor (p - 1)/\alpha(p) \rfloor$. Hence
\[ k_i \leq \left\lfloor \frac{p-1}{\alpha(p)} \right\rfloor \frac{q-1}{p-1}, \quad 0 \leq i \leq m - 1. \]
Since Conjecture B is assumed to be true for $q$, by Fact 5.3.1, we may assume that $k \equiv 1 \pmod{q - 1}$, that is,
\[ k_0 + \cdots + k_{m-1} \equiv 1 \pmod{q - 1}. \]
However,
\[ k_0 + \cdots + k_{m-1} \leq m \left\lfloor \frac{p-1}{\alpha(p)} \right\rfloor \frac{q-1}{p-1} \leq q - 1. \]
So we must have $k_0 + \cdots + k_{m-1} = 1$.

### 5.4 A Theorem on $A_k$

**Theorem 5.4.1** Conjecture A is true for $q = p^e$, where $p$ is an odd prime and $\text{gpf}(e) \leq p - 1$.

Theorem 5.4.1 is an immediate consequence of Corollary 5.3.3 and the following lemma.
Lemma 5.4.2 Let \( q \) be a power of an odd prime \( p \) and \( 1 \leq m \leq p-1 \). If Conjecture A is true for \( q \), it is also true for \( q^m \).

Proof. Assume that \( A_k \) is a PP of \( \mathbb{F}_{q^m} \), where \( 1 \leq k \leq q^m-2 \). Let \( k' \in \{1, \ldots, q^m-2\} \) be such that \( k'k \equiv 1 \pmod{q^m-1} \). It suffices to show that \( k' \) is a power of \( p \). Write \( k' = k'_0q^0 + \cdots + k'_{m-1}q^{m-1} \), \( 0 \leq k'_i \leq q-1 \). Since \( A_k \) is a PP of \( \mathbb{F}_q \) and since Conjecture A is true for \( q \), we may assume that \( k' \equiv 1 \pmod{q-1} \), that is,

\[
k'_0 + \cdots + k'_{m-1} \equiv 1 \pmod{q-1}. \tag{5.4.43}
\]

On the other hand, by Lemma 5.3.5, all base \( p \) digits of \( k' \) are \( \leq 1 \). Hence

\[
k'_i \leq \frac{q-1}{p-1}, \quad 0 \leq i \leq m-1.
\]

Therefore,

\[
k'_0 + \cdots + k'_{m-1} \leq \frac{q-1}{p-1} m \leq q-1. \tag{5.4.44}
\]

Combining (5.4.43) and (5.4.44) gives \( k'_0 + \cdots + k'_{m-1} = 1 \).

\[
\boxed{}
\]

Remark 5.4.3 In [52], the author commented that an avenue to improve Theorem ?? is to find a more explicit form for the function \( p_0 \) in that theorem. By Theorem 5.4.1, one can choose \( p_0(r) = r + 1 \).

5.5 A Theorem on \( B_k \)

Our proof of Conjecture B under the condition \( \alpha(p) > (p-1)/2 \) follows a simple line of logic. Assume to the contrary that \( B_k \) is a PP of \( \mathbb{F}_{p^e} \) for some \( k \in \{1, \ldots, p^e-1\} \) which is not a power of \( p \). Then with the help of Lemma 5.5.1, \( a := [(p^e - 1)/k] \equiv 0 \pmod{p} \). However, (5.3.31) dictates that \( a \not\equiv 0 \pmod{p} \), hence a contradiction.

Lemma 5.5.1 Let \( p \geq 3 \) be a prime. Let \( i, j, e \) be integers such that \( 0 < i < j \leq e-1 \),
and let
\[ k = k_0p^0 + \cdots + k_{i-1}p^{i-1} + p^i + p^j, \quad k_0, \ldots, k_{i-1} \in \{0, \ldots, p - 1\}, \]
\[ a = \left\lceil \frac{p^e - 1}{k} \right\rceil, \]
\[ u = \left\lfloor \frac{e - j}{j - i} \right\rfloor. \]

Assume that \( a \) is even and
\[ \frac{p^e - 1}{p^i + p^j} - \frac{p^e - 1}{k} \leq 1. \] (5.5.45)

Then
\[ a = \begin{cases} 
\frac{p^{e-j}}{1} & \text{if } u \text{ is odd}, \\
\frac{p^{e-j}}{1} & \text{if } u \text{ is even}.
\end{cases} \] (5.5.46)

Proof. Write \( e - j = u(i - j) + r, 0 \leq r < j - i \). We have
\[
\frac{p^e - 1}{p^i + p^j} = p^{e-j} \frac{1}{1 + p^{i-j}} - \frac{1}{p^i + p^j}
= p^{e-j} \left[ 1 - p^{i-j} + p^{2(i-j)} - \ldots \right] - \frac{1}{p^i + p^j}
= p^{e-j} \left[ 1 - p^{i-j} + \ldots + (-1)^up^{u(i-j)} \right]
+ (-1)^{u+1}p^{r+i-j} \left[ 1 - p^{i-j} + p^{2(i-j)} - \ldots \right] - \frac{1}{p^i + p^j}
= p^{e-j} \left[ 1 - p^{i-j} + \ldots + (-1)^up^{u(i-j)} \right] + (-1)^{u+1}p^{r+i-j} \left[ 1 + p^{i-j} - \frac{1}{p^i + p^j} \right]
= p^{e-j} \left[ 1 - p^{i-j} + \ldots + (-1)^up^{u(i-j)} \right] + \frac{1}{p^i + p^j} \left[ (-1)^{u+1}p^{r+i} - 1 \right].
\]

Since \( r + i < j \), we have
\[
0 < \frac{1}{p^i + p^j} \left[ (-1)^{u+1}p^{r+i} - 1 \right] < 1 \quad \text{if } u \text{ is odd},
-1 < \frac{1}{p^i + p^j} \left[ (-1)^{u+1}p^{r+i} - 1 \right] < 0 \quad \text{if } u \text{ is even}.
\]
Thus

$$\left\lfloor \frac{p^e - 1}{p^i + p^j} \right\rfloor = \begin{cases}  
p^e - j \left[ 1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)} \right] & \text{if } u \text{ is odd}, \\
p^e - j \left[ 1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)} \right] - 1 & \text{if } u \text{ is even}. \end{cases} \tag{5.5.47}$$

Note that the right side of (5.5.47) is always even. Then (5.5.46) follows from (5.5.45), (5.5.47) and the assumption that $a$ is even.

\begin{proof}
Assume to the contrary that there exists $k \in \{1, \ldots, p^e - 1\}$, which is not a power of $p$, such that $B_k$ is a PP of $\mathbb{F}_{p^e}$. Write

$$k = k_0 p^0 + \cdots + k_{e-1} p^{e-1}, \quad 0 \leq k_i \leq p - 1.$$

Since $\alpha(p) > (p - 1)/2$, by Lemma 5.3.9, $k_i \leq 1$ for all $i$. Let

$$a = \left\lfloor \frac{p^e - 1}{k} \right\rfloor.$$

By Lemma 5.3.7, $a$ is even, and by (5.3.31),

$$\left( \frac{ka}{k} \right) \not\equiv 0 \pmod{p}.$$

In particular, $a \not\equiv 0 \pmod{p}$.

Let $d$ be the distance in $\mathbb{Z}/e\mathbb{Z}$ defined by

$$d([x],[y]) = \min\{|x-y|, e - |x-y|\}, \quad x,y \in \{0,\ldots,e-1\}.$$

This is the arc distance with $[0], \ldots, [e-1]$ evenly placed on a circle in that order. Let $l$ be the shortest distance between two indices $i, j \in \mathbb{Z}/e\mathbb{Z}$ with $k_i = k_j = 1$. Then $1 \leq l < e$. The 1’s among $k_0, \ldots, k_{e-1}$ cannot be evenly spaced. Otherwise,
\[ \gcd(k, p^e - 1) = (p^e - 1)/(p^l - 1) > 1, \] which is a contradiction. Therefore, we may write
\[ (k_0, \ldots, k_{e-1}) = \left( \underbrace{0 \cdots 0}_{l-1} \underbrace{1 0 \cdots 0}_{j} \underbrace{1 0 \cdots 0}_{l} \right) , \]
where \( j = e - 1 - l \), \( i = j - l = e - 1 - 2l \). We have
\[ u = \left\lfloor \frac{e - j}{j - i} \right\rfloor = \left\lfloor \frac{l + 1}{l} \right\rfloor = \begin{cases} 2 & \text{if } l = 1, \\ 1 & \text{if } l \geq 2. \end{cases} \]

**Case 1.** Assume that \( l = 1 \). Since
\[ k_0p^0 + \cdots + k_ip^i \leq p^0 + \cdots + p^i = \frac{p^j - 1}{p - 1} < \frac{p^j}{p - 1}, \]
we have
\[ \frac{p^e - 1}{p^i + p^j} - \frac{p^e - 1}{k} = (p^e - 1) \left[ \frac{1}{p^i + p^j} - \frac{1}{k_{0}p^0 + \cdots + k_ip^i + p^j} \right] < (p^e - 1) \left[ \frac{1}{p^i + p^j} - \frac{1}{\frac{p^j}{p - 1} + p^j} \right] = (p^e - 1) \frac{1}{p^i p(p + 1)} < p^{e-j-2} = 1. \]
Thus by (5.5.46),
\[ a = p^{e-j} \left[ 1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)} \right] - 1 = p^2(1 - p^{-1}) \equiv 0 \quad (\text{mod } p), \]
which is a contradiction.

**Case 2.** Assume that \( l \geq 2 \). Since the distance between the indices of any two consecutive 1’s among \( k_0, \ldots, k_{e-1} \) is \( \geq l \), we have
\[ k_0p^0 + \cdots + k_ip^i < p^i + p^{i-l} + p^{i-2l} + \cdots = p^i \frac{p^l}{p^l - 1}. \]
Hence
\[
\frac{p^e - 1}{p^i + p^j} - \frac{p^e - 1}{k} = (p^e - 1) \left[ \frac{1}{p^i + p^j} - \frac{1}{k_0p^0 + \cdots + k_ip^i + p^j} \right]
\]
\[
< (p^e - 1) \left[ \frac{1}{p^i + p^j} - \frac{1}{\frac{p^j}{p-1}p^i + p^j} \right]
\]
\[
= \frac{p^e - 1}{p^i - 1} \left( \frac{p^i}{p^i + p^j} \right)
\]
\[
< \frac{p^{e+i}}{p(p^i + p^j)} \left( \frac{p^j}{p^i - 1} \right) p^j + p^i \right)
\]
\[
< \frac{p^{e+i}}{p^i+1} = p^{e+e-1-2i-2(e-1)l-1} = 1.
\]

Therefore by (5.5.46),
\[
a = p^{e-j} \left[ 1 - p^{-j} + \cdots + (-1)^u p^{u(i-j)} \right] = p^{i+1} (1 - p^{-i}) \equiv 0 \pmod{p},
\]
which is a contradiction.

Many odd primes $p$ satisfy the condition $\alpha(p) > (p - 1)/2$. Among the first 1000 odd primes $p$, the equation $\alpha(p) = p - 1$ holds with 211 exceptions. The first few exceptions are $\alpha(29) = 10$, $\alpha(31) = 8$, $\alpha(47) = 18$, \ldots. In fact, for any odd prime $p$, either $\alpha(p) = p - 1$ or $\alpha(p) \leq (p - 1)/2$; this follows from a symmetry described below.

Note that for integer $m \geq 0$,
\[
2^{2m} \binom{2m}{m} = \frac{(2m)!}{(2^m \cdot m!)^2} = \frac{(2m - 1)!!}{(2m)!!}.
\]
Thus $\alpha(p)$ is the smallest positive even integer $2m (\leq p - 1)$ such that
\[
\frac{(2m - 1)!!}{(2m)!!} \equiv (-1)^m \pmod{p}. \tag{5.5.48}
\]
Let $0 \leq m \leq (p - 1)/2$. Since

$$2^{-2m} \binom{2m}{m} \left[ 2^{-(p-1-2m)} \left( \frac{p-1-2m}{2} - m \right) \right]^{-1}$$

$$= \frac{(2m - 1)!!}{(2m)!!} \cdot \frac{(p - 1 - 2m)!!}{(p - 2 - 2m)!!} = \frac{(p - 2)!!}{(p - 1)!!} \prod_{2 \leq i \leq p - 1, \text{even}} \frac{p - i}{i} = (-1)^{\frac{p-1}{2}},$$

condition (5.5.48) is symmetric for $m$ and $(p - 1)/2 - m$.

For integers $i \leq j$, denote $i(i + 1) \cdots j$ by $[i, j]$. Then we have

$$\binom{2m}{m} = \frac{[m + 1, 2m]}{[1, m]},$$

$$\binom{p - 1 - 2m}{\frac{p-1}{2} - m} = \frac{[p+1/2 - m, p - 1 - 2m]}{[1, p-1/2 - m]} = \frac{[2m + 1, p-1/2 + m]}{[p+1/2 + m, p - 1]}.$$

Hence

$$\binom{2m}{m} \binom{p - 1 - 2m}{\frac{p-1}{2} - m} = \frac{[m + 1, m + p-1/2]}{[1, m][m + p-1/2, p - 1]} = \frac{[m + 1, m + p-1/2]^2}{[1, p - 1]}$$

$$= - \left[ m + 1, m + \frac{p - 1}{2} \right]^2.$$

Therefore, if (5.5.48) is satisfied, one has

$$\prod_{i=1}^{\frac{p-1}{2}} (m + i)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

### 5.6 A Theorem on monomial graphs of girth eight

We continue to use the notation introduced at the beginning of Section 5.3. For $1 \leq k \leq q - 1$ with $\gcd(k, q - 1) = 1$, the parameters $k'$, $b$ and $c$ are defined in (5.3.13) and (5.3.14).

Assume to the contrary that Conjecture 5.1.1 is false. Then for some $k \in \{1, \ldots, q-1\}$ which is not a power of $p$, both $A_k$ and $B_k$ are PPs of $\mathbb{F}_q$. We will see that the same argument as in the proof of Theorem 5.5.2 gives that $c := \lfloor (q - 1)/k' \rfloor \equiv 0$.
(mod \(p\)). The purpose of the following lemma is to establish an equation that cannot be satisfied when \(c \equiv 0 \pmod{p}\).

**Lemma 5.6.1** Assume that \(q\) is odd, \(1 < k \leq q - 1\), and both \(A_k\) and \(B_k\) are PPs of \(\mathbb{F}_q\). Then \(c\) is even and

\[
2^{-2c'} = \left(\frac{2(q - 1) - 2ck'}{q - 1 - ck'}\right) + (-1)^{\frac{k'}{2} + \frac{2}{3} + 1}\left(\frac{2(q - 1) - 2ck'}{\frac{1}{2}(q - 1) - (\frac{3}{2} - 1)k'}\right)\left(\frac{2c}{c + 2}\right). \tag{5.6.49}
\]

**Proof.** By Lemma 5.3.7, \(c\) is even. Let \(s = (2cb)^*\). Since \(2cb \not\equiv 0 \pmod{q - 1}\), we have \(1 \leq s \leq q - 2\). Clearly, \(2ck' > q - 1\). (Otherwise, \(2c \leq (q - 1)/k'\), which implies that \(2c \leq c\), a contradiction.) It follows that

\[
s = 2(q - 1) - 2ck'.
\]

Note that \(c < (q - 1)/2\). (Otherwise, since \(\gcd(k', q - 1) = 1\), we have \(k' < (q - 1)/2 \leq 2\), which implies that \(k' = 1\), i.e., \(k = 1\), which is a contradiction.) Thus

\[
(ks)^* = q - 1 - 2c.
\]

By (5.2.8),

\[
\sum_i (-1)^i \binom{s}{i} \binom{(2ki)^*}{q - 1 - 2c} = (-2)^s. \tag{5.6.50}
\]

For each \(0 \leq l \leq c\), let \(i \in \{0, \ldots, q - 1\}\) be such that \((2ki)^* = q - 1 - 2l\). Then

\[
i = \frac{3}{2}(q - 1) - lk' \quad \text{or} \quad q - 1 - lk' \quad \text{or} \quad \frac{1}{2}(q - 1) - lk'.
\]

In each of these cases, we determine the necessary conditions on \(l\) such that \(i\) satisfies \(0 \leq i \leq s\).

**Case 1.** Assume that \(i = \frac{3}{2}(q - 1) - lk'\). In this case,

\[
i \geq \frac{3}{2}(q - 1) - ck' > 2(q - 1) - 2ck' \quad \text{(since } 2ck' > q - 1)\]

\[= s.\]
Case 2. Assume that $i = q - 1 - lk'$. In this case we always have $i \geq 0$. Moreover,

\[
i \leq s \iff q - 1 - lk' \leq 2(q - 1) - 2ck' \\
\iff l \geq 2c - \frac{q - 1}{k'} \\
\iff l \geq c.
\]

Case 3. Assume that $i = \frac{1}{2}(q - 1) - lk'$. In this case, $i \geq 0$ if and only if $l \leq c/2$. Moreover,

\[
i \leq s \iff \frac{1}{2}(q - 1) - lk' \leq 2(q - 1) - 2ck' \\
\iff l \geq 2c - \frac{3}{2} \cdot \frac{q - 1}{k'} \\
\Rightarrow l > 2c - \frac{3}{2}(c + 1) \\
\Rightarrow l \geq \frac{c}{2} - 1.
\]

Combining the above three cases, we see that (5.6.50) becomes

\[
2^{-2ck'} = \left(\frac{2(q - 1) - 2ck'}{q - 1 - ck'}\right) \\
+ (-1)^{\frac{q - 1}{2} + \frac{c}{2} + 1} \left(\frac{2(q - 1) - 2ck'}{\frac{1}{2}(q - 1) - (\frac{c}{2} - 1)k'}\right) \left(\frac{q - 1 - 2(\frac{c}{2} - 1)}{q - 1 - 2c}\right) \\
+ (-1)^{\frac{q - 1}{2} + \frac{c}{2}} \left(\frac{2(q - 1) - 2ck'}{\frac{1}{2}(q - 1) - \frac{c}{2}k'}\right) \left(\frac{q - 1 - c}{q - 1 - 2c}\right).
\]

In the above,

\[
\left(\frac{q - 1 - 2(\frac{c}{2} - 1)}{q - 1 - 2c}\right) = \left(-c + 1\right) = \left(\frac{2c}{2 + c}\right) = \left(\frac{c + 2}{c + 2}\right),
\]

and, by (5.3.18),

\[
\left(\frac{q - 1 - c}{q - 1 - 2c}\right) = \left(-\frac{1 - c}{c}\right) = \left(\frac{2c}{c}\right) = 0.
\]

Hence (5.6.49) follows from (5.6.51).

\[\text{Theorem 5.6.2} \ Conjecture 5.1.1 \text{ is true.}\]
**Proof.** Assume to the contrary that Conjecture 5.1.1 is false. Then there exists $1 \leq k \leq q - 1$, which is not a power of $p$, such that both $A_k$ and $B_k$ are PPs of $\mathbb{F}_q$.

By Lemma 5.3.5, all the base $p$ digits of $k'$ are $\leq 1$. By exactly the same argument as in the proof of Theorem 5.5.2, with $k$ and $a$ replaced by $k'$ and $c$, respectively, we conclude that we may assume that $c \equiv 0 \pmod{p}$. Then obviously,

$$\binom{2c}{c+2} = 0. \quad (5.6.52)$$

Since $q - 1 - ck' \equiv p - 1 \pmod{p}$, the sum $(q - 1 - ck') + (q - 1 - ck')$ has a carry in base $p$ at $p^0$, implying that

$$\binom{2(q - 1) - 2ck'}{q - 1 - ck'} = 0. \quad (5.6.53)$$

Combining (5.6.49), (5.6.52) and (5.6.53), we have a contradiction. 

\[\blacksquare\]
This dissertation started with the goal of completely characterizing the permutation behavior of the family of polynomials $g_{n,q}$. Unfortunately this problem turned quite challenging and still remains an open problem.

Sticking with the theme of ”discovering” these naturally occurring permutation polynomials, as opposed to constructing those with desirable properties, leads to a plethora of permutation polynomials over the fields $\mathbb{F}_{q^2}$. In chapter 3 we are able to completely determine the permutation behavior of polynomials of the form $f = x^d(a + bx^{q-1} + x^{r(q-1)})$ for specific values of $d$ and $r$. While a complete classification of permutation binomials and trinomials is still out of hand, we hope that some of the techniques developed in chapter 3 can be used to address other problems involving polynomials over finite fields containing only a few terms.

In chapter 4 we confirm a conjecture of Xin Gong related to construction of a permutation polynomial starting with a non-permuting power function and adding a specific linearized polynomial. Permutation polynomials of this type have applications in cryptography and APN functions.

In chapter 5 we see how a problem relating to combinatorial structures defined over finite fields can be formulated in terms of polynomials of finite fields. While we were able to prove the main conjecture in chapter 5, namely that every monomial graph of girth eight is isomorphic to $\Gamma_3(q)$, the conjectures regarding the polynomials $A_k$ and $B_k$ still remain open.
7 References

References


[7] F. Brioschi, Des substitutions de la forme $\theta(r) \equiv \varepsilon \left( r^{n-2} + ar^{\frac{n-3}{2}} \right)$ pour un nombre $n$ premier de lettres, Math. Ann. 2 (1870), 467 – 470.


[44] X. Hou, *Permutation polynomials of $\mathbb{F}_{q^2}$ of the form $ax + x^{r(q-1)+1}$*, preprint


[90] M.E. Zieve, *Permutation polynomials over $\mathbb{F}_{q^2}$ induced from novel permutations of the $(q + 1)\text{-th}$ roots of unity*, preprint.

8 Appendices

8.1 Appendix A - Copyrights and Permissions
This Agreement between Stephen Lappano ("You") and Elsevier ("Elsevier") consists of your license details and the terms and conditions provided by Elsevier and Copyright Clearance Center.

<table>
<thead>
<tr>
<th><strong>License Number</strong></th>
<th>3900220148493</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>License date</strong></td>
<td>Jul 01, 2016</td>
</tr>
<tr>
<td><strong>Licensed Content Publisher</strong></td>
<td>Elsevier</td>
</tr>
<tr>
<td><strong>Licensed Content Publication</strong></td>
<td>Finite Fields and Their Applications</td>
</tr>
<tr>
<td><strong>Licensed Content Title</strong></td>
<td>A note regarding permutation binomials over Fq2</td>
</tr>
<tr>
<td><strong>Licensed Content Author</strong></td>
<td>Stephen D. Lappano</td>
</tr>
<tr>
<td><strong>Licensed Content Date</strong></td>
<td>July 2015</td>
</tr>
<tr>
<td><strong>Licensed Content Volume Number</strong></td>
<td>34</td>
</tr>
<tr>
<td><strong>Licensed Content Issue Number</strong></td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Licensed Content Pages</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>Start Page</strong></td>
<td>153</td>
</tr>
<tr>
<td><strong>End Page</strong></td>
<td>160</td>
</tr>
<tr>
<td><strong>Type of Use</strong></td>
<td>reuse in a thesis/dissertation</td>
</tr>
<tr>
<td><strong>Portion</strong></td>
<td>full article</td>
</tr>
<tr>
<td><strong>Format</strong></td>
<td>electronic</td>
</tr>
<tr>
<td><strong>Are you the author of this Elsevier article?</strong></td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Will you be translating?</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>Order reference number</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Title of your thesis/dissertation</strong></td>
<td>Some Results Concerning Permutation Polynomials over Finite Fields</td>
</tr>
<tr>
<td><strong>Expected completion date</strong></td>
<td>Aug 2016</td>
</tr>
<tr>
<td><strong>Estimated size (number of pages)</strong></td>
<td>120</td>
</tr>
<tr>
<td><strong>Elsevier VAT number</strong></td>
<td>GB 494 6272 12</td>
</tr>
</tbody>
</table>
This Agreement between Stephen Lappano ("You") and Elsevier ("Elsevier") consists of your license details and the terms and conditions provided by Elsevier and Copyright Clearance Center.

License Number: 3900220415299
License date: Jul 01, 2016
Licensed Content Publisher: Elsevier
Licensed Content Publication: Finite Fields and Their Applications
Licensed Content Title: A new approach to permutation polynomials over finite fields, II
Licensed Content Author: Neranga Fernando, Xiang-dong Hou, Stephen D. Lappano
Licensed Content Date: July 2013
Licensed Content Volume Number: 22
Licensed Content Issue Number: n/a
Licensed Content Pages: 37
Start Page: 122
End Page: 158
Type of Use: reuse in a thesis/dissertation
Intended publisher of new work: other
Portion: excerpt
Number of excerpts: 4
Format: electronic
Are you the author of this Elsevier article?: Yes
Will you be translating?: No
Order reference number: 
Title of your thesis/dissertation: Some Results Concerning Permutation Polynomials over Finite Fields
Expected completion date: Aug 2016
This Agreement between Stephen Lappano ("You") and Elsevier ("Elsevier") consists of your license details and the terms and conditions provided by Elsevier and Copyright Clearance Center.

<table>
<thead>
<tr>
<th>License Number</th>
<th>3900220605480</th>
</tr>
</thead>
<tbody>
<tr>
<td>License date</td>
<td>Jul 01, 2016</td>
</tr>
<tr>
<td>Licensed Content Publisher</td>
<td>Elsevier</td>
</tr>
<tr>
<td>Licensed Content Publication</td>
<td>Discrete Mathematics</td>
</tr>
<tr>
<td>Licensed Content Title</td>
<td>Permutation polynomials over finite fields involving (x + x^q + \cdots + x^{qa-1})</td>
</tr>
<tr>
<td>Licensed Content Author</td>
<td>Neranga Fernando, Xiang-dong Hou, Stephen D. Lappano</td>
</tr>
<tr>
<td>Licensed Content Date</td>
<td>6 February 2014</td>
</tr>
<tr>
<td>Licensed Content Volume Number</td>
<td>315</td>
</tr>
<tr>
<td>Licensed Content Issue Number</td>
<td>n/a</td>
</tr>
<tr>
<td>Start Page</td>
<td>173</td>
</tr>
<tr>
<td>End Page</td>
<td>184</td>
</tr>
<tr>
<td>Type of Use</td>
<td>reuse in a thesis/dissertation</td>
</tr>
<tr>
<td>Intended publisher of new work</td>
<td>other</td>
</tr>
<tr>
<td>Portion</td>
<td>excerpt</td>
</tr>
<tr>
<td>Number of excerpts</td>
<td>2</td>
</tr>
<tr>
<td>Format</td>
<td>electronic</td>
</tr>
<tr>
<td>Are you the author of this Elsevier article?</td>
<td>Yes</td>
</tr>
<tr>
<td>Will you be translating?</td>
<td>No</td>
</tr>
<tr>
<td>Order reference number</td>
<td></td>
</tr>
<tr>
<td>Title of your thesis/dissertation</td>
<td>Some Results Concerning Permutation Polynomials over Finite Fields</td>
</tr>
<tr>
<td>Expected completion date</td>
<td>Aug 2016</td>
</tr>
</tbody>
</table>