6-27-2016

Some Results Concerning Permutation Polynomials over Finite Fields

Stephen Lappano
University of South Florida, slappano@mail.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

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

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 unqiuely represented by a polynomial, f_ϕ of degree $< q$. If the map $x \mapsto f_\phi(x)$ induces a permutation on the underlying field we say f_ϕ 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.

1 Introduction

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 $\phi : \mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial. Further, if we require the degree of this polynomial to be less than q, the polynomial representation of ϕ is unique. Given a function $\phi : \mathbb{F}_q \to \mathbb{F}_q$, the unique polynomial of degree less than q representing ϕ, f_ϕ, is given by

$$f_\phi(\mathtt{x}) = \sum_{a \in \mathbb{F}_q} \phi(a) \left(1 - (\mathtt{x} - a)^{q-1}\right). \tag{1.0.1}$$

The fact that $\mathbb{F}_q$ is polynomally 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 polynomally complete are the finite fields; Heisler [33] obtained the same result without the assumption of commutativity.

A polynomial $f \in \mathbb{F}_q[\mathtt{x}]$ 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 $f \in \mathbb{F}_q[\mathtt{x}]$ 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 $\dfrac{f(\mathtt{x}) - f(\mathtt{y})}{\mathtt{x} - \mathtt{y}} \in \mathbb{F}_q[\mathtt{x}, \mathtt{y}]$ *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* $f \in \mathbb{F}_q[\mathtt{x}]$ *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* $f(\mathtt{x})^s \pmod{(x^q - x)}$ *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 $f \in \mathbb{F}_q[\mathrm{x}]$. Then f is a permutation polynomial of $\mathbb{F}_q$ if and only if*

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

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 λ 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 polynmomial representing this permutation using (1.0.1). In general the study of permutation polynomials is concerned with polynomials that have an especially simple algebraic appearence, 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, $\mathtt{x}, \mathtt{y}, \mathtt{z}$ are reserved for indeterminants, while letters in standard font x, y, z are reserved for elements of a given finite field. We write N_{q^e/q^j} and T_{q^e/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 $\mathtt{x}_1\mathtt{x}_2$ and $\mathtt{x}_1 + \mathtt{x}_2$ generate the ring of symmetric polynomials in $\mathbb{Z}[\mathtt{x}_1, \mathtt{x}_2]$ so there is a unique polynomial $D_n(\mathtt{x}_1, \mathtt{x}_2) \in \mathbb{Z}[\mathtt{x}_1, \mathtt{x}_2]$ such that

$$\mathtt{x}_1^n + x_2^n = D_n(\mathtt{x}_1 + \mathtt{x}_2, \mathtt{x}_1\mathtt{x}_2).$$

The explicit form of $D_n(\mathtt{x}_1, \mathtt{x}_2)$ is given by Warings formula [64], we have

$$D_n(\mathtt{x}_1, \mathtt{x}_2) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-\mathtt{x}_2)^j \mathtt{x}_1^{n-2j}. \tag{1.1.2}$$

For a fixed $a \in \mathbb{F}_q$, $D_n(\mathtt{x}, a)$ 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 $T_n(\mathtt{x}) = \cos(n \arccos(\mathtt{x}))$; in fact $D_n(2\mathtt{x}a, a^2) = 2a^n T_n(\mathtt{x})$. Notice by (1.1.2) we have

$$D_n(\mathtt{x}, ab^2) = \sum_{j=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-a)^j b^k b^{-(k-2j)} \mathtt{x}^{k-2j} = b^k D_n(b^{-1}\mathtt{x}, a).$$

Thus if q is even then every Dickson polynomial $D_n(\mathtt{x}, a), a \in \mathbb{F}_q^*$ over $\mathbb{F}_q$ can be expressed in terms of $D_n(\mathtt{x}, 1)$; if q is odd then every Dickson polynomial $D_n(\mathtt{x}, a), a \in \mathbb{F}_q^*$ can be expressed in terms of $D_n(\mathtt{x}, 1)$ and $D_n(\mathtt{x}, c)$ for a fixed non square $c \in \mathbb{F}_q^*$. Also notice $D_n(\mathtt{x}, 0) = \mathtt{x}^n$.

The permutation behavior of the Dickson polynomials, $D_n(\mathtt{x}, a)$, over $\mathbb{F}_q$ is completely known. If $a = 0$, then $D_n(\mathtt{x}, a) = \mathtt{x}^n$ so $D_n(\mathtt{x}, a)$ 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 $D_n(\mathtt{x}, a), a \in \mathbb{F}_q^*$, 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 $f \in \mathbb{Z}[\mathtt{x}]$ that is a permutation polynomial of $\mathbb{F}_p$ for infinitely many primes p must be a composition of binomials of the form $a\mathtt{x}^n + b$ 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 conncection 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:*

$$\mathtt{x}^n \textit{ is APN on } \mathbb{F}_{p^{2e}} \Rightarrow D_n(1, \mathtt{x}) \textit{ is a PP of } \mathbb{F}_{p^e} \Rightarrow \mathtt{x}^n \textit{ is APN on } \mathbb{F}_{p^e}.$$

For the reversed Dickson polynomial we have

$$D_n(0, \mathtt{x}) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ 2(-\mathtt{x})^k & \text{if } n = 2k, \end{cases}$$

so $D_n(0,\mathtt{x})$ 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

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

so we only need to consider $D_n(1,\mathtt{x})$. 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 $1\le n\le p^2-1$. Then, $D_n(1,\mathtt{x})$ is a PP on $\mathbb{F}_p$ if and only if*

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

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

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

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

X. Hou [39] introduced the polynomial $g_{n,q}\in\mathbb{F}_p[\mathtt{x}]$ (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

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

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 $\mathtt{x}^d h(\mathtt{x}^{(q-1)/t})$, where $t \mid q-1,\ 1 \leq d \leq (q-1)/t$ and $h \in \mathbb{F}_q[\mathtt{x}]$, 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 μ_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 $f = \mathtt{x}^d h(\mathtt{x}^{\frac{q-1}{t}})$, where $h \in \mathbb{F}_q[\mathtt{x}]$. Then, f is a PP of $\mathbb{F}_q$ if and only if*

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

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

The above theorem is actually a special case of Theorem 1.0.4, with $A = \mathbb{F}_q,\ S = \overline{S} = \mu_t,\ \lambda = \overline{\lambda} = \mathtt{x}^{(q-1)/t}$ and $\overline{f} = \mathtt{x}^d h(\mathtt{x})^{(q-1)/t}$. The key step in applying Theorem 1.2.1 is verifying that $\mathtt{x}^d h(\mathtt{x})^{\frac{q-1}{t}}$ 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 monomail mapping of $\mathbb{F}_q$ is completely understood, $\mathtt{x} \mapsto \mathtt{x}^n$ 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

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

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 $f = a\mathtt{x}^n + \mathtt{x}^m \in \mathbb{F}_q[\mathtt{x}]$, 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 $f = a\mathtt{x}^n + \mathtt{x}^m \in \mathbb{F}_q[\mathtt{x}]$, we can transform f into the form

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

where $t \mid q-1$; (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 $\mathtt{x}(a + \mathtt{x}^{r(q-1)}) \in \mathbb{F}_{q^2}[\mathtt{x}]$. In this case, condition *(ii)* of Theorem 1.2.1 is precisely verifying that the map $\mathtt{x} \mapsto \mathtt{x}(a + \mathtt{x}^r)^{q-1}$ is a permutation on μ_{q+1}. In this special case, a method of M. Zieve can be used to construct bijective maps (via degree one rational functions) from $\mu_{q+1} \to \mathbb{F}_q \cup \{\infty\}$. 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 binomails of the form $\mathtt{x}(a+\mathtt{x}^{r(q-1)})$ 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]) *$f = \mathtt{x}^{2^m} + \mathtt{x}^{2^m+2} + \mathtt{x}^{3\cdot 2^m+4}$ 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 $(f(\mathtt{x}+\gamma) + f(\gamma))/\mathtt{x}$ is a permutation polymnomial 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 $\mathtt{x}^{2\alpha+3} + (a\mathtt{x})^{\alpha} - a^2\mathtt{x}$ is a permutation polynomial of $\mathbb{F}_q$.*

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

Theorem 1.2.5 ([21]) *$f = \mathtt{x}^{2^{m+1}+1} + \mathtt{x}^3 + \mathtt{x}$ 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 $\mathtt{x}^d(a + b\mathtt{x}^{q-1} + \mathtt{x}^{r(q-1)})$ 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 refered 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 advesary 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 informtation 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

$$f(\mathtt{x}+a) + f(\mathtt{x}) = b \quad a \in \mathbb{F}_{2^n}^*, \ b \in \mathbb{F}_{2^n}. \tag{1.3.3}$$

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

$$W_f(\lambda, \gamma) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_{2^n/2}(\gamma f(x) + \lambda x)}, \quad \lambda \in \mathbb{F}_{2^n}, \ \gamma \in \mathbb{F}_{2^n}^*. \tag{1.3.4}$$

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 $p(\mathtt{x}) = \sum_{i=0}^{2^n-1} a_i \mathtt{x}^i \in \mathbb{F}_{2^{n/2}}[\mathtt{x}]$ ([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*

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

is called a linearized polynomial over $\mathbb{F}_q$*. Note the map* $\mathtt{x} \mapsto L(\mathtt{x})$ *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, $\mathtt{x}^d$ and attempt to find a linearized polynomial $L(\mathtt{x})$ so the sum $\mathtt{x}^d + L(\mathtt{x})$ is a permutation polynomial. It is quite obvious if the power function $\mathtt{x}^d$ is APN on $\mathbb{F}_{2^n}$, then so is the sum $\mathtt{x}^d + L(\mathtt{x})$. 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 The Polynomial $g_{n,q}$ [*]

2.1 Background

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

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

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

where σ_k is the kth elementary symmetric polynomial in q variables. A comparison of the coefficients of $\mathtt{t}$ on both sides of (2.1.1) tells that

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

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

$$\begin{aligned} \sum_{a\,\in\,\mathbb{F}_q}(\mathtt{x}+a)^n &= \sum_{\alpha(q-1)+\beta q=n}(-1)^\alpha\frac{(\alpha+\beta-1)!n}{\alpha!\beta!}(-1)^\alpha(\mathtt{x}^q-\mathtt{x})^\beta \\ &= \sum_{\frac{n}{q}\leq l\leq\frac{n}{q-1}}\frac{(l-1)!n}{(lq-n)!(n-l(q-1))!}(\mathtt{x}^q-\mathtt{x})^{n-l(q-1)} \qquad (l=\alpha+\beta) \end{aligned}$$

[*] 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.

$$= \sum_{\frac{n}{q} \le l \le \frac{n}{q-1}} \frac{n}{l} \binom{l}{n-l(q-1)} (\mathtt{x}^q - \mathtt{x})^{n-l(q-1)}.$$

Set

$$g_{n,q}(\mathtt{x}) = \sum_{\frac{n}{q} \le l \le \frac{n}{q-1}} \frac{n}{l} \binom{l}{n-l(q-1)} \mathtt{x}^{n-l(q-1)} \in \mathbb{Z}[\mathtt{x}].$$

(Note that the coefficients of $g_{n,q}(\mathtt{x})$ are integers since the coefficients in Waring's formula are integers.) Then in $\mathbb{F}_q[\mathtt{x}]$ we have

$$\sum_{a \,\in\, \mathbb{F}_q} (\mathtt{x} + a)^n = g_{n,q}(\mathtt{x}^q - \mathtt{x}). \tag{2.1.3}$$

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 nth 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 $\mathbb{F}_{q^e}$? With this in mind, we have the following definition:

Definition 2.1.1 (Desirable triple). If $g_{n,q}$ is a permutation polynomial of $\mathbb{F}_{q^e}$, 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 prolems 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 polynomail $g_{n,q}$ satisfies a recurrence relation.

Proposition 2.1.2 ([40]). *The polynomial $g_{n,q}$ satisfies the recurrence relation*

$$\begin{cases} g_{0,q} = \cdots = g_{q-2,q} = 0, \\ g_{q-1,q} = -1, \\ g_{n,q} = \mathtt{x} g_{n-q,q} + g_{n-q+1,q}, \quad n \geq q. \end{cases} \tag{2.1.4}$$

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

$$g_{n,q} = \frac{1}{\mathtt{x}}(g_{n+q,q} - g_{n+1,q}). \tag{2.1.5}$$

For $n < 0$, $g_{n,q} \in \mathbb{F}_p[\mathtt{x}, \mathtt{x}^{-1}]$, the ring of Laurent polynomials in $\mathtt{x}$ 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

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

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 $V \subset \mathbb{F}_{q^{pe}}$. We can choose $\alpha \in \mathbb{F}_{q^e}$ such that $\mathtt{Tr}_{q^e/q}(\alpha) = 1$. Then we have $\mathtt{Tr}_{q^{pe}/q}(\alpha) = \mathtt{Tr}_{q^e/q}(\mathtt{Tr}_{q^{pe}/q^e}(\alpha)) = \mathtt{Tr}_{q^e/q}(p \cdot \alpha) = 0$, so there is some $\beta \in \mathbb{F}_{q^{pe}}$ 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) $g_{pn,q} = g_{n,q}^p$.*

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

Proof.

(i) We have

$$g_{pn,q}(\mathtt{x}^q - \mathtt{x}) = \sum_{a\,\in\,\mathbb{F}_q} (\mathtt{x}+a)^{pn} = \Big(\sum_{a\,\in\,\mathbb{F}_q} (\mathtt{x}+a)^n\Big)^p = [g_{n,q}(\mathtt{x}^q - \mathtt{x})]^p.$$

(ii) For all $x \in \mathbb{F}_{q^{pe}}$, 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., $g_{n_1,q} \equiv g_{n_2,q} \pmod{\mathtt{x}^{q^e} - \mathtt{x}}$.

■

Given two integers $m, n > 0$, we say m and n belong to the same p-cyclotomic coset $(\mathrm{mod}\ q^{pe}-1)$ whenever $m \equiv p^i \cdot n \pmod{q^{pe}-1}$ for some integer $i > 0$. If two integers $m, n > 0$ belong to the same p-cyclotomic coset modulo $q^{pe}-1$, 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*

$$g_{l+q^i,q} = g_{l+1,q} + S_i \cdot g_{l,q}, \tag{2.1.6}$$

where $S_i = \mathtt{x} + \mathtt{x}^q + \cdots + \mathtt{x}^{q^{i-1}}$.

From (2.1.6), we have

$$(S_a - S_b)g_{n,q} = g_{n+q^a,q} - g_{n+q^b,q}, \tag{2.1.7}$$

where $a, b > 0$ are integers. Also note that

$$S_a - S_b \equiv S_{a-b} \pmod{\mathtt{x}^{q^e} - \mathtt{x}} \quad \text{if } b \equiv 0 \text{ or } a \pmod{e}.$$

If $a < 0$, we define $S_a = S_{pe+a}$.

Given integers $d > 1$ and $a = a_0d^0 + \cdots + a_td^t$, $0 \le a_i \le d-1$, the *base d weight* of a is $w_d(a) = a_0 + \cdots + a_t$. Let $n \ge 0$ 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 $n = \alpha_0q^0 + \cdots + \alpha_tq^t$, $0 \le \alpha_i \le q-1$ and $w_q(n)$ be the base q weight of n,*

$$g_{n,q} = \begin{cases} 0 & \text{if } w_q(n) < q-1, \\ -1 & \text{if } w_q(n) = q-1, \\ \alpha_0x^{q^0} + (\alpha_0+\alpha_1)x^{q^1} + \cdots + (\alpha_0 + \cdots + \alpha_{t-1})x^{q^{t-1}} + \delta & \text{if } w_q(n) = q, \end{cases} \tag{2.1.8}$$

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 $a, b \ge 0$. 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,

$$\begin{aligned} g_{q^a-2,q} &= \frac{1}{\mathtt{x}}(g_{q^a+q-2,q} - g_{q^a-1,q}) \\ &= \frac{1}{\mathtt{x}}\Big[-1 - \frac{1}{\mathtt{x}}(g_{q^a+q-1,q} - g_{q^a,q})\Big] \\ &= \frac{1}{\mathtt{x}}\Big(-1 + \frac{S_a}{\mathtt{x}}\Big) \end{aligned}$$

$$= \frac{S_{a-1}^q}{\mathtt{x}^2}$$
$$= \mathtt{x}^{q-2} + \mathtt{x}^{q^2-2} + \cdots + \mathtt{x}^{q^{a-1}-2}. \tag{2.2.9}$$

For which a, e and q is $g_{q^a-2,q}$ a PP of $\mathbb{F}_{q^e}$? 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,

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

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 $f(\mathtt{x})$ and $f(\mathtt{x})/\mathtt{x}$ are permutations of $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^n}^*$ respectively, are exactly of the form $f(x) = ax^{2^k}$ 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 $0 < b < a < pe$.

By (2.1.6), we have

$$\begin{aligned}
S_b \cdot g_{q^a-q^b-1,q} &= g_{q^a-1,q} - g_{q^a-q^b,q} \\
&= g_{q^a-1,q} - (g_{q^{a-b}-1,q})^{q^b} \\
&= -\frac{S_a}{\mathtt{x}} + \Big(\frac{S_{a-b}}{\mathtt{x}}\Big)^{q^b} \\
&= -\frac{S_a - S_{a-b}^{q^b}}{\mathtt{x}} + \Big(\frac{1}{\mathtt{x}^{q^b}} - \frac{1}{\mathtt{x}}\Big) S_{a-b}^{q^b} \\
&= -\frac{S_b}{\mathtt{x}} - \frac{S_b^q - S_b}{\mathtt{x}^{q^b+1}} S_{a-b}^{q^b}.
\end{aligned}$$

So

$$g_{q^a-q^b-1,q} = -\frac{1}{\mathtt{x}} - \frac{(S_b^{q-1}-1)S_{a-b}^{q^b}}{\mathtt{x}^{q^b+1}}. \tag{2.2.10}$$

(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

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

Corollary 2.2.2 *We have*

$$g_{q^2-q-1,q} = -\mathtt{x}^{q-2}.$$

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*

$$g_{q^a-q^b-1,q} \equiv -\mathtt{x}^{q^e-2} \pmod{\mathtt{x}^{q^e} - \mathtt{x}} \tag{2.2.12}$$

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

$$\begin{aligned} g_{q^a-q^b-1,q} &\equiv -\mathtt{x}^{q^e-2} - \mathtt{x}^{q^e-3} a_1 S_e\big((b_1 S_e)^{q-1} - 1\big) \pmod{\mathtt{x}^{q^e} - \mathtt{x}} \\ &= -\mathtt{x}^{q^e-2} - \mathtt{x}^{q^e-3} a_1 S_e (S_e^{q-1} - 1) \\ &= -\mathtt{x}^{q^e-2} - \mathtt{x}^{q^e-3} a_1 (S_e^q - S_e) \\ &\equiv -\mathtt{x}^{q^e-2} \pmod{\mathtt{x}^{q^e} - \mathtt{x}}. \end{aligned} \tag{2.2.13}$$

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

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

For $f \in \mathbb{F}_q[\mathtt{x}]$, denote $\{x \in \overline{\mathbb{F}}_q : f(x) = 0\}$ by $V(f)$, where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$. Then $V(\mathtt{x}^{q^e} - \mathtt{x}) \subset V(\mathtt{x}^{q^b} - \mathtt{x}) \cup V(S_{a-b})$, 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 $0 < a < pe$,

$$S_{a-b} = S_{a_1 e + a_0} \equiv a_1 S_e + S_{a_0} \not\equiv 0 \pmod{\mathtt{x}^{q^e} - \mathtt{x}}.$$

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

$$S_{a_0}(S_e^{q-1} - 1) \equiv 0 \pmod{\mathtt{x}^{q^e} - \mathtt{x}}. \tag{2.2.14}$$

If $a_0 > 0$, then

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

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

$$g_{q^a-q^b-1,q} \equiv -\mathtt{x}^{q^2-2} - \mathtt{x}^{q^2-3}(a_1S_2+\mathtt{x})\big((b_1S_2)^{q-1}-1\big) \pmod{\mathtt{x}^{q^2}-\mathtt{x}}.$$

Then $g_{q^a-q^b-1,q}(x) = 0$ for every $x \in \mathbb{F}_{q^2}$ with $\mathrm{Tr}_{q^2/q}(x) = 0$, 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 $(q^a - q^p - 1, 2; q)$ are abundant. These triples appear so often, we remove them from Table 2.1, for convience 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* $(\mathtt{x} - \mathtt{x}^q)^{q-1} + 1$.

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

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

(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

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

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

$$\begin{aligned} g_{n,q} &\equiv -\mathtt{x}^{q^2-2} - i\mathtt{x}^{q^2-q-2} S_2\Big[\Big(-\frac{1}{2}S_2 + \mathtt{x}\Big)^{q-1} - 1\Big] \pmod{\mathtt{x}^{q^2} - \mathtt{x}} \\ &= -\mathtt{x}^{q^2-2} - i\mathtt{x}^{q^2-q-2}(\mathtt{x} + \mathtt{x}^q)\big[(\mathtt{x} - \mathtt{x}^q)^{q-1} - 1\big]. \end{aligned}$$

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

$$\begin{aligned} g_{n,q}(x) &= -x^{-1} + 2ix^{q^2-q-2}(x + x^q) \\ &= -x^{-1} + 2ix^{q^2-q-1} + 2ix^{q^2-2} \\ &= (2i-1)x^{-1} + 2ix^{-q}. \end{aligned}$$

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

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

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

Therefore, $g_{n,q}$ is a PP of $\mathbb{F}_{q^2}$ if and only if $(2i-1)\mathtt{x}^{-1}+2i\mathtt{x}^{-q}$ is 1-1 on $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$, i.e., if and only if $(2i-1)\mathtt{x}+2i\mathtt{x}^q$ is 1-1 on $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$. So, it remains to show that $(2i-1)\mathtt{x}+2i\mathtt{x}^q$ 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 $(2i-1)\mathtt{x}+2i\mathtt{x}^q$ is a PP of $\mathbb{F}_{q^2}$. Otherwise, there exists $0\neq x\in\mathbb{F}_{q^2}$ such that $(2i-1)x+2ix^q=0$. Then $x^{q-1}=-\frac{2i-1}{2i}$. Hence

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

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 $(2i-1)\mathtt{x}+2i\mathtt{x}^q=2i(\mathtt{x}^q-\mathtt{x})$, which is clearly not 1-1 on $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$.

■

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

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

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

(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

$$\begin{aligned}g_{n,q}&\equiv-\mathtt{x}^{q^2-2}-\mathtt{x}^{q^2-q-2}((i-1)S_2+\mathtt{x}^q)\Big[\Big(-\frac{1}{2}S_2+\mathtt{x}\Big)^{q-1}-1\Big]\pmod{\mathtt{x}^{q^2}-\mathtt{x}}\\&=-\mathtt{x}^{q^2-2}-\mathtt{x}^{q^2-q-2}(i(\mathtt{x}+\mathtt{x}^q)-\mathtt{x})\big[(\mathtt{x}-\mathtt{x}^q)^{q-1}-1\big].\end{aligned}$$

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

$$\begin{aligned} g_{n,q}(x) &= -x^{-1} + 2x^{q^2-q-2}((i-1)x + ix^q) \\ &= -x^{-1} + 2(i-1)x^{q^2-q-1} + 2ix^{q^2-2} \\ &= (2i-1)x^{-1} + (2i-2)x^{-q}. \end{aligned}$$

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

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

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

Therefore, $g_{n,q}$ is a PP of $\mathbb{F}_{q^2}$ if and only if $(2i-1)\mathtt{x}^{-1} + (2i-2)\mathtt{x}^{-q}$ is 1-1 on $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, i.e., if and only if $(2i-1)\mathtt{x} + (2i-2)\mathtt{x}^q$ is 1-1 on $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. So, it remains to show that $(2i-1)\mathtt{x} + (2i-2)\mathtt{x}^q$ 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 $(2i-1)\mathtt{x} + (2i-2)\mathtt{x}^q$ 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

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

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 $(2i-1)\mathtt{x} + (2i-2)\mathtt{x}^q = (2i-2)(\mathtt{x}^q - \mathtt{x})$, which is clearly not 1-1 on $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

■

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

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

$$g_{n,q}(x) = \begin{cases} 0 & \text{if } x = 0, \\ x^{q-2} + \mathrm{Tr}_{q^2/q}(x^{-1}) & \text{if } x \neq 0. \end{cases}$$

(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 $a_0 = 0$, $a_1 = 1$, $b_0 = 1$, $b_1 = 0$),

$$\begin{aligned} g_{n,q}(x) &= x^{-1} + x^{-q-1}S_2(x)(x^{q-1}+1) \\ &= x^{-1} + x^{-q-1}(x+x^q)(x^{q-1}+1) \\ &= x^{-1} + x^{q-2} + x^{-q} \\ &= x^{q-2} + \mathrm{Tr}_{q^2/q}(x^{-1}). \end{aligned}$$

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

$$x^{q-2} + x^{-1} + x^{-q} = c \tag{2.3.15}$$

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

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

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

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

So

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

Hence x is unique.

2° Assume s is even. We show that

$$x^{q-2} + \mathrm{Tr}_{q^2/q}(x^{-1}) = 0 \tag{2.3.16}$$

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 $\mathrm{Tr}_{q^2/q}(x^{-1}) = 0$, and $x^{q-2} = 0$, which is a contradiction.

3° Assume s is odd. We show that (2.3.16) has a solution in $\mathbb{F}_{q^2}^*$. Let $x \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$. Then $x^2 + x + 1 = 0$ and $x^3 = 1$. So

$$\begin{aligned} x^{q-2} + \mathrm{Tr}_{q^2/q}(x^{-1}) &= x^{q-2} + x^{-1} + x^{-q} \\ &= 1 + x^2 + x \qquad \text{(since } q \equiv 2 \pmod 3\text{)} \\ &= 0. \end{aligned}$$

■

The following theorem is particulary 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*

$$g_{q^{2i}-q-1,q} \equiv (i-1)\mathtt{x}^{q^2-q-1} - i\mathtt{x}^{q-2} \pmod{\mathtt{x}^{q^2} - \mathtt{x}}.$$

(ii) Assume that q is odd. Then $\mathtt{x}^{q^2-q-1} + \mathtt{x}^{q-2}$ 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

$$\begin{aligned} g_{q^{2i}-q-1,q} &\equiv -\mathtt{x}^{q^2-2} - \mathtt{x}^{q^2-q-2}\big((i-1)S_2 + \mathtt{x}^q\big)(\mathtt{x}^{q-1} - 1) \pmod{\mathtt{x}^{q^2} - \mathtt{x}} \\ &= -\mathtt{x}^{q^2-2} - \mathtt{x}^{q^2-q-2}\big((i-1)\mathtt{x} + i\mathtt{x}^q\big)(\mathtt{x}^{q-1} - 1) \\ &= -\mathtt{x}^{q^2-2} - \mathtt{x}^{q^2-q-2}\big(-\mathtt{x}^q - (i-1)\mathtt{x} + i\mathtt{x}^{2q-1}\big) \\ &\equiv (i-1)\mathtt{x}^{q^2-q-1} - i\mathtt{x}^{q-2} \pmod{\mathtt{x}^{q^2} - \mathtt{x}}. \end{aligned}$$

(ii) (⇐) Let $f = \mathtt{x}^{q^2-q-1} + \mathtt{x}^{q-2}$. Then

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

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

$$x^{-q} + x^{q-2} = c \tag{2.3.17}$$

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

Assume $x \in \mathbb{F}_{q^2}^*$ is a solution of (2.3.17). Then

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

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

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

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

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

Assume that $x \in \mathbb{F}_{q^2}^*$ 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.

(⇒) Assume to the contrary that $q \equiv -1 \pmod 4$. We show that $x^{-q}+x^{q-2} = 0$ has a solution $x \in \mathbb{F}_{q^2}^*$. Since $4(q-1) \mid q^2-1$, there exists $x \in \mathbb{F}_{q^2}^*$ 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).

■

Theorem 2.3.5 *Let p be an odd prime and q a power of p. Let $0 \le i \le p-2$ and*

$n = q^{p+i+1} - q^{2i+1} - 1$. If

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

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 "$\equiv \pmod{\mathtt{x}^{q^2} - \mathtt{x}}$".

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 $g = g_{q^{p+i+1}-q^{2i+1}-1,q}$.

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

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

$$\begin{aligned} g(x) &= -x^{-1} + \frac{i}{2}x^{-q-1}(x + x^q)\frac{((i+1)x + ix^q)^q - ((i+1)x + ix^q)}{(i+1)x + ix^q} \\ &= -x^{-1} + \frac{i}{2}(x^{-q} + x^{-1})\frac{x^q - x}{(i+1)x + ix^q} \\ &= -x^{-1} + \frac{i}{2}(x^{-q} + x^{-1})\frac{x^{-1} - x^{-q}}{(i+1)x^{-q} + ix^{-1}} \\ &= y + \frac{i}{2}(y^q + y)\frac{y^q - y}{(i+1)y^q + iy} \qquad (y = -x^{-1}) \\ &= \frac{iy^{2q} + 2(i+1)y^{q+1} + iy^2}{2(i+1)y^q + 2iy}. \end{aligned}$$

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

Note: $2(i+1)\mathtt{x}^q + 2i\mathtt{x}$ is a PP of $\mathbb{F}_{q^2}$, and $\dfrac{1}{2(2i+1)}((i+1)\mathtt{x}^q - \mathtt{x})$ is the inverse PP.

So

$$g(x) = \frac{1}{(4i+2)^2}\frac{iu^{2q} + 2(i+1)u^{q+1} + iu^2}{w},$$

where $u = (i+1)w^q - iw$.

The proof will be complete if we can show that for $c \in \mathbb{F}_{q^2}$,

$$\frac{iu^{2q} + 2(i+1)u^{q+1} + iu^2}{w} = c, \tag{2.3.19}$$

i.e.,

$$\frac{i((i+1)w^q - iw)^{2q} + 2(i+1)((i+1)w^q - iw)^{q+1} + i((i+1)w^q - iw)^2}{w} = c \tag{2.3.20}$$

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 $c = 0$. First assume $c \neq 0$. Let $t = wc$. By (2.3.20), $t \in \mathbb{F}_q$. Then (2.3.20) becomes

$$\frac{it^2v^{2q} + 2t^2(i+1)v^{q+1} + it^2v^2}{tc^{-1}} = c,$$

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 $w \in \mathbb{F}_{q^2}^*$. Then

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

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

$$iz^2 + 2(i+1)z + i = 0. \tag{2.3.21}$$

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 $z^2 = z^{q+1} = ((i+1)w^q - iw)^{q^2-1} = 1$. So $z = \pm 1$, which contradicts (2.3.21).

Case 2: i is even.

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

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

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

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

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

$$\begin{aligned} g(x) \ &= -x^{-1} + \frac{1}{2}((i+1)x^{-q} + (i-1)x^{-1})\frac{x^q - x}{(i+1)x+ix^q} \\ &= -x^{-1} + \frac{1}{2}((i+1)x^{-q} + (i-1)x^{-1})\frac{x^{-1} - x^{-q}}{(i+1)x^{-q}+ix^{-1}} \\ &= y + \frac{1}{2}((i+1)y^q + (i-1)y)\frac{y^q - y}{(i+1)y^q+iy} \qquad\qquad (y = -x^{-1}) \\ &= \frac{(i+1)y^{2q} + 2iy^{q+1} + (i+1)y^2}{2(i+1)y^q + 2iy}. \end{aligned}$$

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

Note: $2(i+1)\mathrm{x}^q + 2i\mathrm{x}$ is a PP of $\mathbb{F}_{q^2}$, and $\dfrac{1}{2(2i+1)}((i+1)\mathrm{x}^q - i\mathrm{x})$ 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 $c \in \mathbb{F}_{q^2}$,

$$\frac{(i+1)u^{2q} + 2iu^{q+1} + (i+1)u^2}{w} = c, \tag{2.3.22}$$

i.e.,

$$\frac{(i+1)((i+1)w^q-iw)^{2q}+2i((i+1)w^q-iw)^{q+1}+(i+1)((i+1)w^q-iw)^2}{w}=c \tag{2.3.23}$$

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

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

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

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

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

■

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

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 $f = \mathtt{x}^{q-2} + t\mathtt{x}^{q^2-q-1}$, $t \in \mathbb{F}_q^*$. 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 $f = \mathtt{x}^{q-2} + t\mathtt{x}^{q^2-q-1}$ is a permutation polynomial of $\mathbb{F}_{q^2}$. Noting that the map $\mathtt{x} \mapsto \mathtt{x}^{q^2-q-1}$ is a permutation of $\mathbb{F}_{q^2}$ and substituting $\mathtt{x}^{q^2-q-1}$ for $\mathtt{x}$ 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 $f = t\mathtt{x} + \mathtt{x}^{2q-1}, t \in \mathbb{F}_q^*$. 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 $g_{n,q}(\mathtt{x})$ on $\mathbb{F}_{q^2}$ can be transfered into the form $A\mathtt{x} + B\mathtt{x}^q + C\mathtt{x}^{2q-1}$ 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 $\mathtt{x}^d(a + b\mathtt{x}^{q-1} + \mathtt{x}^{r(q-1)})$ (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 odd, $b \neq p$, $(a, b) \neq (2, 1)$

a	b	a	b	a	b	a	b	a	b	a	b	a	b	a	b
$q = 2$		10	5	24	13	40	7	38	13	50	25	60	37	66	45
–	–	13	11	25	1	40	33	40	7	51	27	61	39	67	47
				25	15	41	35	40	17	52	37	62	1	71	35
$q = 2^2$		**$q = 7^2$**		26	1	42	37	40	31	54	33	63	43	73	59
3	1	6	1	27	19	43	39	41	3	57	7	64	11	74	27
		8	1	28	21	45	13	41	19	58	41	64	45	74	61
$q = 2^3$		8	3	30	25			41	31	59	5	65	49	76	51
–	–	9	3	33	5	**$q = 29$**		42	3	61	47	66	49	76	65
		10	5			15	11	42	21	62	49	67	51	77	67
$q = 2^4$		12	5	**$q = 19$**		21	3	46	29	62	55	69	3	78	9
3	1	12	9	17	9	26	21	49	35	63	39	70	57	78	69
		13	11	23	7	30	1	49	37	64	39	70	65	79	65
$q = 2^5$				25	11	31	19	49	43	64	53	71	59	80	47
–	–	**$q = 11$**		26	13	32	5	50	9	65	7	72	47	80	73
		6	1	30	21	32	27	50	37	67	53	72	61	82	77
$q = 2^6$		10	1	30	23	33	7	51	39	69	63	77	33	83	79
3	1	13	3	31	17	34	5	55	41	70	65	78	73	85	19
		17	13	31	23	34	9	55	47	71	67	80	5	85	59
$q = 3$		18	13	33	17	36	3	57	51	73	71	80	77	85	83
–	–	19	15	34	29	36	13	58	53						
		20	5	35	9	41	23	59	13	**$q = 41$**		**$q = 43$**		**$q = 47$**	
$q = 3^2$		20	17	36	5	42	25	60	5	12	7	20	11	18	3
3	1			36	33	44	1	60	57	31	1	21	11	20	9
4	1	**$q = 13$**		37	35	46	33	61	59	31	5	32	13	24	1
5	1	12	1			46	35			42	1	38	31	29	7
		14	1	**$q = 23$**		47	35	**$q = 37$**		42	33	39	11	37	31
$q = 3^3$		15	3	10	7	52	19	19	15	44	5	46	5	44	21
–	–	18	5	12	1	52	45	29	23	46	5	46	39	45	37
		18	9	21	13	53	23	32	19	46	9	49	11	46	1
$q = 5$		19	5	22	1	54	49	34	21	49	29	51	15	49	3
6	1	22	17	25	3	55	51	36	1	52	21	55	23	50	5
8	1	25	23	26	5	56	5	38	1	53	1	58	29	50	29
				27	21	56	53	38	15	53	23	58	41	51	7
$q = 5^2$		**$q = 17$**		32	17	57	15	39	3	54	25	59	31	54	13
4	1	11	1	34	21			41	7	55	33	60	33	54	51
6	1	15	7	35	31	**$q = 31$**		42	5	57	31	60	39	57	41
7	3	18	1	37	3	22	3	42	9	58	15	61	35	61	27
9	7	18	7	37	11	28	21	43	11	58	33	62	37	62	13
		22	5	37	27	29	21	48	21	59	5	62	53	62	29
$q = 7$		22	9	39	31	35	7	48	45	60	27	65	61	64	33

Table 2.1 (Continued)

a	b	a	b	a	b	a	b	a	b	a	b	a	b	a	b
68	41	58	5	98	19	77	35	115	73	90	39	50	47	110	35
68	57	58	9	98	89	78	37	116	5	90	57	53	47	110	85
70	7	59	11	99	91	83	7	116	113	93	25	70	5	113	91
70	45	59	29	100	67	85	39			94	25	73	17	115	71
73	39	59	37	100	93	85	51	$\boldsymbol{q = 61}$		94	65	74	13	116	29
73	51	60	13	101	95	87	35	38	33	97	73	74	57	116	97
75	55	61	15	102	97	90	61	52	39	98	51	75	15	117	23
76	33	62	17	103	37	90	81	59	51	98	73	77	19	118	23
76	57	63	57	103	55	91	63	60	1	99	75	79	23	118	101
77	59	66	25	103	99	92	65	62	1	100	67	85	35	119	23
77	65	67	43	105	11	94	69	62	49	100	77	85	47	119	61
77	67	68	29			94	71	63	3	101	91	85	69	119	103
79	63	71	11	$\boldsymbol{q = 59}$		95	71	64	5	102	25	87	17	120	13
82	33	72	37	16	13	96	63	64	37	102	81	87	39	120	105
82	69	72	49	20	3	96	73	66	5	103	83	88	13	121	107
83	71	73	5	23	17	97	75	66	9	109	95	88	41	122	63
84	59	75	21	24	15	98	77	67	25	110	97	89	63	122	109
84	73	75	43	30	1	99	79	68	13	111	29	90	45	124	99
85	75	77	47	31	9	101	9	69	15	113	103	90	83	124	113
86	13	78	13	39	27	103	87	71	19	115	101	91	47	126	33
86	77	78	49	50	13	104	89	74	25	115	107	94	53	126	117
87	79	80	1	56	21	104	101	74	55	116	83	95	35	127	113
89	83	81	35	58	1	105	7	75	27	116	109	95	55	129	123
90	85	82	57	61	3	106	51	79	59	117	7	96	57	130	125
91	27	82	79	61	27	106	93	81	39	118	113	97	59	131	127
		83	59	61	33	107	95	82	41	120	5	98	61	133	131
$\boldsymbol{q = 53}$		85	63	63	7	108	83	84	45	120	117	98	77		
27	23	88	13	66	13	108	97	84	79	121	119	99	77	$\boldsymbol{q = 71}$	
32	3	88	69	66	19	109	31	85	47			101	97	36	1
50	21	91	29	67	15	110	25	86	17	$\boldsymbol{q = 67}$		102	31	70	1
51	43	92	23	69	19	110	101	86	49	40	17	102	69	23	3
54	1	92	77	73	27	113	107	87	39	43	11	103	71	53	3
57	7	94	81	76	33	114	109	89	35	48	31	109	83	73	3

Table 2.1 (Continued)

a	b	a	b	a	b	a	b	a	b	a	b	a	b
140	5	111	79	75	3	106	65	108	7	114	69	157	155
131	7	104	81	105	3	107	67	68	9	135	71		
103	11	113	83	119	3	108	69	52	11	95	73	$\boldsymbol{q = 3^4}$	
78	13	113	85	69	5	109	71	85	11	118	77		
95	13	114	85	78	5	92	75	125	11	146	81	3	1
47	15	115	87	98	7	111	75	129	11	121	83	4	1
79	15	120	87	78	9	112	77	43	13	100	85	5	1
80	17	117	91	128	15	113	79	135	13	122	85		
81	19	118	93	137	15	114	81	121	15	123	87	$\boldsymbol{q = 83}$	
121	19	119	95	108	17	116	85	88	17	126	93	42	1
82	21	120	97	123	17	94	87	89	19	126	95	82	1
101	21	131	97	83	19	118	89	55	23	127	95	68	3
41	23	107	103	85	23	119	91	59	23	129	99	85	3
30	27	119	103	86	25	112	97	91	23	136	103	86	5
85	27	123	103	87	27	122	97	121	27	134	109	87	7
88	33	124	105	103	29	137	99	70	29	135	111	127	7
99	35	113	107	104	29	114	103	94	29	136	113	133	7
98	37	119	107	67	31	126	105	95	31	119	115	29	9
97	39	125	107	91	35	135	107	96	33	133	115	151	9
67	41	114	111	46	37	128	109	98	37	134	115	89	11
92	41	127	111	92	37	129	111	100	41	137	115	146	11
93	43	128	113	99	39	126	113	137	41	139	119	90	13
78	47	130	117	81	41	133	119	83	45	152	119	149	15
88	47	131	119	94	41	134	121	110	45	141	123	28	17
62	51	137	131	127	41	135	123	143	45	148	123	69	17
75	51	138	133	118	43	139	125	95	49	153	129	123	17
106	51	139	135	59	49	137	127	137	49	145	131	40	19
98	53	140	137	98	49	142	137	105	51	146	133	43	19
102	61			69	51	145	143	106	53	148	137	136	19
104	65	$\boldsymbol{q = 73}$		101	55			107	55	151	137	80	21
106	69			102	57	$\boldsymbol{q = 79}$		129	55	151	143	95	23
118	69	13	1	113	57			108	57	152	145	34	25
130	69	72	1	119	57	156	5	110	61	154	149	97	27
128	73	74	1	104	61	27	7	113	67	155	151	99	31
109	75	135	1	97	63	54	7	77	69	156	153	72	35

Table 2.1 (Continued)

a	b	a	b	a	b	a	b	a	b	a	b
112	35	142	117	71	17	152	83	174	169	58	45
95	37	128	119	98	17	132	85	176	173	121	47
127	37	143	119	133	17	151	85			122	49
109	39	132	121	155	19	155	85	$\boldsymbol{q = 97}$		152	49
150	39	145	123	77	21	133	87	81	1	164	49
106	45	146	125	100	21	135	91	96	1	124	53
158	49	147	127	133	21	136	93	98	1	140	53
109	51	163	127	102	25	138	97	115	1	178	53
75	53	148	129	77	27	139	99	99	3	147	55
110	53	149	131	35	29	121	101	102	5	60	57
133	55	156	131	163	33	124	103	167	5	76	61
112	57	150	133	109	39	142	105	89	7	128	61
113	59	152	137	46	41	142	107	154	7	130	65
152	59	154	141	141	43	143	107	102	9	150	67
115	63	156	145	112	45	144	109	148	9	117	69
115	69	157	147	113	47	145	111	18	11	122	69
155	69	158	149	165	47	173	111	103	11	77	71
148	71	159	151	173	47	150	121	182	11	134	73
81	73	162	157	114	49	151	123	161	17	135	75
120	73			100	51	156	123	110	25	170	77
121	75	$\boldsymbol{q = 89}$		92	53	159	123	50	27	137	79
95	77	41	1	116	53	149	125	111	27	138	81
126	85	90	1	117	55	152	125	158	27	105	83
127	87	134	1	139	55	132	127	53	29	140	85
154	87	139	1	170	55	154	129	113	31	133	87
110	89	92	5	118	57	155	131	114	33	142	89
128	89	94	5	102	61	156	133	74	35	143	91
131	95	176	5	123	67	154	137	115	35	144	93
149	95	151	7	150	67	159	139	138	35	145	95
132	97	166	7	124	69	169	141	130	37		
133	99	94	9	125	71	168	143	98	39		
134	101	95	11	161	71	166	153	123	39		
115	105	44	13	126	73	168	157	183	41		
136	105	127	13	129	79	170	161	81	43		
139	111	49	15	130	81	173	167	119	43		

3 Permutation Polynomials of the form $f = \mathtt{x}^d(a + b\mathtt{x}^{q-1} + \mathtt{x}^{r(q-1)})$ *

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*

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

where Φ is a permutation of $\mathbb{F}_{q^2}$ and

$$\begin{cases} A = \frac{1}{\beta}(-a_0 b_1 + b_1 + a_1), \\ B = a_0 - \frac{b_1 + 1}{\beta} \\ C = -\frac{1}{\beta}(a_0 b_1 + a_0 + a_1) \end{cases}$$

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 $f = a\mathtt{x} + b\mathtt{x}^q + \mathtt{x}^{2q-1} \in \mathbb{F}_q[\mathtt{x}]$ 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 $f = a\mathtt{x} + b\mathtt{x}^q + \mathtt{x}^{2q-1} \in \mathbb{F}_q[\mathtt{x}]$, 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 $f = a\mathtt{x} + b\mathtt{x}^q + \mathtt{x}^{2q-1} \in \mathbb{F}_q[\mathtt{x}]$, 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) $q > 2, a \neq 1, \mathtt{Tr}_{q/2}\left(\frac{1}{a+1}\right) = 0, b^2 = a^2 + a$.

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

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

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 $f = \mathtt{x}^d(a + b\mathtt{x}^{q-1} + x^{r(q-1)})$. For the remainder of this chapter we focus on the following two questions:

1. When does a binomial of the form $f = \mathtt{x}(a + x^{r(q-1)})$ permute the field $\mathbb{F}_{q^2}$?
2. When does a trinomial of the form $f = \mathtt{x}^3(a + b\mathtt{x}^{q-1} + \mathtt{x}^{2(q-1)})$ 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 $f = \mathtt{x}^d(a + b\mathtt{x}^{q-1} + x^{r(q-1)})$, 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 $f = \mathtt{x}(a + \mathtt{x}^{r(q-1)})$

Consider a binomial of the form $f = a\mathtt{x} + \mathtt{x}^{2q-1} \in \mathbb{F}_q[\mathtt{x}]$, 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, $\mathtt{x}(a + \mathtt{x}^{r(q-1)})$, 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 $f = a\mathtt{x} + \mathtt{x}^{3q-2} \in \mathbb{F}_{q^2}[\mathtt{x}]$, 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* 3*rd root of unity.*

(ii) $q = 5$ *and* a^2 *is a root of* $(\mathtt{x}+1)(\mathtt{x}+2)(\mathtt{x}-2)(\mathtt{x}^2-\mathtt{x}+1)$.

(iii) $q = 2^3$ *and* a^3 *is a root of* $\mathtt{x}^3+\mathtt{x}+1$.

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

(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* $f = a\mathtt{x} + \mathtt{x}^{5q-4} \in \mathbb{F}_{q^2}[\mathtt{x}]$, *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* 5*th root of unity.*

(ii) $q = 3^2$ *and* a^2 *is a root of* $(\mathtt{x}+1)(\mathtt{x}^2+1)(\mathtt{x}^2+\mathtt{x}+2)(\mathtt{x}^2+2\mathtt{x}+2)(\mathtt{x}^4+\mathtt{x}^2+\mathtt{x}+1)(\mathtt{x}^4+\mathtt{x}^3+\mathtt{x}^2+1)(\mathtt{x}^4+2\mathtt{x}^3+\mathtt{x}^2+2\mathtt{x}+1)$.

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

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

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

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

(vii) $q = 2^6$ *and* a^{13} *is a root of* $(\mathtt{x}^2+\mathtt{x}+1)(\mathtt{x}^3+\mathtt{x}+1)$.

Theorem 3.2.4 *Let* $f(\mathtt{x}) = a\mathtt{x} + \mathtt{x}^{7q-6} \in \mathbb{F}_{q^2}[\mathtt{x}]$, *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* $(1+\mathtt{x})(2+\mathtt{x})(3+\mathtt{x})(4+\mathtt{x})(5+\mathtt{x})(6+\mathtt{x})(7+\mathtt{x})(8+\mathtt{x})(9+\mathtt{x})(10+\mathtt{x})(11+\mathtt{x})(12+\mathtt{x}+\mathtt{x}^2)(9+2\mathtt{x}+\mathtt{x}^2)(10+3\mathtt{x}+\mathtt{x}^2)(9+4\mathtt{x}+\mathtt{x}^2)(12+4\mathtt{x}+\mathtt{x}^2)(10+5\mathtt{x}+\mathtt{x}^2)(3+6\mathtt{x}+\mathtt{x}^2)(1+7\mathtt{x}+\mathtt{x}^2)(4+7\mathtt{x}+\mathtt{x}^2)(1+8\mathtt{x}+\mathtt{x}^2)(12+9\mathtt{x}+\mathtt{x}^2)(1+10\mathtt{x}+\mathtt{x}^2)(3+12\mathtt{x}+\mathtt{x}^2)(4+12\mathtt{x}+\mathtt{x}^2)(12+12\mathtt{x}+\mathtt{x}^2)$

(ii) $q = 3^3$ *and* a^4 *is a root of* $(2+\mathtt{x}+\mathtt{x}^2+\mathtt{x}^3)(1+2\mathtt{x}+\mathtt{x}^2+\mathtt{x}^3)(1+\mathtt{x}+2\mathtt{x}^2+\mathtt{x}^3)(2+2\mathtt{x}+2\mathtt{x}^2+\mathtt{x}^3)(1+2\mathtt{x}+\mathtt{x}^2+2\mathtt{x}^3+\mathtt{x}^4+2\mathtt{x}^5+\mathtt{x}^6)$

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

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 $a\mathtt{x}+\mathtt{x}^{5q-4} \in \mathbb{F}_{q^2}[\mathtt{x}]$.

Computations

Let $f = a\mathtt{x}+\mathtt{x}^{5q-4} \in \mathbb{F}_{q^2}[\mathtt{x}]$, where $a \neq 0$, and let $0 \le \alpha, \beta \le q-1$ 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 $f = a\mathtt{x}+\mathtt{x}^{16} \equiv (a+1)\mathtt{x} \pmod{\mathtt{x}^{15}-1}$. In this case, f is clearly a PP if and only if $a \neq 1$.

Now suppose $q \ge 5$. We compute

$$\begin{aligned}\sum_{x\in\mathbb{F}_{q^2}} f(x)^{\alpha+\beta q} &= \sum\nolimits_{x\in\mathbb{F}_{q^2}} (ax+x^{5q-4})^{\alpha}(a^q x^q + x^{5-4q})^{\beta} \\ &= \sum\nolimits_{x\in\mathbb{F}_{q^2}} \sum\nolimits_{i,j} \binom{\alpha}{i}(ax)^{\alpha-i}x^{(5q-4)i}\binom{\beta}{j}(a^q x^q)^{(\beta-j)}x^{(5-4q)j} \\ &= a^{\alpha+\beta q}\sum\nolimits_{i,j}\binom{\alpha}{i}\binom{\beta}{j}a^{-i-jq}\sum\nolimits_{x\in\mathbb{F}_{q^2}} x^{\alpha+\beta q+5(q-1)(i-j)}. \qquad (3.2.1)\end{aligned}$$

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

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

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

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

$$4\alpha + 4 - 5q \leq -\alpha - 1 + 5(i-j) \leq 4\alpha - 1 \tag{3.2.3}$$

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

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

where

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

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

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

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

$$0 = \Lambda(q, 0, a) = \sum_{k=1}^{4} \binom{q-1}{\frac{k(q+1)-1}{5}}^{*} a^{-(\frac{k(q+1)-1}{5})q}$$

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 $\binom{q-1}{\frac{k(q+1)-1}{5}}^{*}$ is nonzero which contradicts (3.2.6). Thus if f is a PP of $\mathbb{F}_{q^2}$ we must have $q + 1 \equiv 0 \pmod 5$.

■

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* $f = a\mathtt{x} + \mathtt{x}^{r(q-1)+1} \in \mathbb{F}_{q^2}[\mathtt{x}]$, *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* $v = a^{-\frac{q+1}{5}q}$, *then*

$$\Lambda(q, \alpha, a) = (-a)^{-\frac{\alpha+1}{5}q} \sum_{i=0}^{\alpha} (-1)^i \binom{\alpha}{i} \sum_{l=0}^{4} \binom{i + \frac{4\alpha-1+l}{5}}{\alpha} v^{5i+l}.$$

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

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

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

$$= (-1)^{\frac{\alpha+1}{5}q} a^{\frac{\alpha+1}{5}q} \sum_{i=0}^{\alpha} \binom{\alpha}{i} \sum_{l=0}^{4} (-1)^i \binom{\frac{1}{5}(l(q+1)-\alpha-1)+i+\alpha}{\alpha} a^{-\frac{q+1}{5}q(l+5i)}$$

$$= (-a)^{\frac{\alpha+1}{5}q} \sum_{i=0}^{\alpha} (-1)^i \binom{\alpha}{i} \sum_{l=0}^{4} \binom{i+\frac{4\alpha-1+l}{5}}{\alpha} v^{5i+l}.$$

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

■

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 $4 \le |\Gamma(q,\alpha)| \le 5$.

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 $q \ge 9$ and $\alpha > 0$ force $k \in \{0,1,2,3\}$. We have the following inequalities

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

Since $4\alpha - 1, 4\alpha + 4 - 5q \equiv 0 \pmod 5$ it follows

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

Since $a \le q-1$ and $0 \le k \le 3$, 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* $y := a^{\frac{q+1}{5}} \neq 1$ *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*

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

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 $K(q+1) = \Gamma(q,\alpha)$. Now we have

$$\begin{aligned} \Lambda(q,\alpha,a) &= \sum_{-\alpha-1+5(i-j)\in\Gamma(q,\alpha)} \binom{\alpha}{i}\binom{q-1-\alpha}{j} a^{-i-jq} \\ &= \sum_{k\in K} \sum_{-\alpha-1+5(i-j)=k(q+1)} \binom{\alpha}{i}\binom{q-1-\alpha}{j} a^{-i+j} \\ &= \sum_{k\in K} a^{-\frac{1}{5}[\alpha+1+k(q+1)]} \sum_{i-j=\frac{1}{5}[\alpha+1+k(q+1)]} \binom{\alpha}{\alpha-i}\binom{q-1-\alpha}{j} \\ &= a^{-\frac{1}{5}(\alpha+1)} \sum_{k\in K} y^{-k} \sum_{\alpha-i+j=\frac{1}{5}[4\alpha-1-k(q+1)]} \binom{\alpha}{\alpha-i}\binom{q-1-\alpha}{j} \\ &= a^{-\frac{1}{5}(\alpha+1)} \sum_{k\in K} y^{-k} \binom{q-1}{\frac{1}{5}[4\alpha-1-k(q+1)]} \\ &= -a^{-\frac{1}{5}(\alpha+1)} \sum_{k\in K} y^{-k} = 0. \end{aligned} \tag{3.2.9}$$

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

$$\Lambda(q,\alpha,a) = -a^{-\frac{1}{5}(\alpha+1)}(y^{-1}+1+y+y^2). \tag{3.2.10}$$

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

$$\Lambda(q, \alpha, a) = -a^{-\frac{1}{5}(\alpha+1)}(1 + y + y^2 + y^3). \tag{3.2.11}$$

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

$$\Lambda(q, \alpha, a) = -a^{-\frac{1}{5}(\alpha+1)}(y^{-2} + y^{-1} + 1 + y). \tag{3.2.12}$$

■

Proof of Theorem 3.2.3

Proof. (⇐) 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).

(⇒) 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 α with the help of a computer algebra system. For a few values of α we find

$$\Lambda(q, \alpha, a) = (-a)^{\frac{\alpha+1}{5}q} v(1+v+v^2+v^3+v^4) \begin{cases} 5^{-4} g_4(v) & \text{if } \alpha = 4, q \geq 24 \\ 5^{-10} g_9(v) & \text{if } \alpha = 9, q \geq 44 \\ 5^{-16} g_{14}(v) & \text{if } \alpha = 14, q \geq 64 \\ 5^{-28} g_{24}(v) & \text{if } \alpha = 24, q \geq 104. \end{cases} \tag{3.2.13}$$

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

$$GCD(R(g_4, g_9), R(g_4, g_{14})) = 2^{15}3^3 5^{197}. \tag{3.2.14}$$

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 $f = a\mathrm{x} + \mathrm{x}^{r(q-1)+1}$ 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 $r > 2$.

3.3 PPs of the form $f = \mathtt{x}^3(a + \mathtt{x}^{2(q-1)})$

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 $f = \mathtt{x}(a + x^{r(q-1)})$ 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 $f = x^3(a + x^{2(q-1)}) \in \mathbb{F}_q[x]$, 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* $q \equiv 1 \pmod 4$

(2) $a = \frac{1}{3}$ *and* $q \equiv -1 \pmod 6$

(3) $a = -\frac{1}{3}$ *and* $q \equiv -1 \pmod{12}$.

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 $\binom{z}{a} = \frac{(z-a+1)_a}{(1)_a}$. If $z \in \mathbb{Q}$, we also define

$$\binom{z}{a}^* = \begin{cases} \binom{z}{a} & \text{if } z \in \mathbb{Z} \\ 0 & \text{otherwise.} \end{cases}$$

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 $\binom{z_1}{a} \equiv \binom{z_2}{a} \pmod p$.*

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*

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

Proof.

$$\begin{aligned} \sum_{x\in\mathbb{F}_{q^2}} f(x)^{\alpha+\beta q} &= \sum_{x\in\mathbb{F}^*_{q^2}} x^{3(\alpha+\beta q)}(a+x^{2(q-1)})^{\alpha}(a+x^{2(1-q)})^{\beta} \\ &= \sum_{x\in\mathbb{F}^*_{q^2}} x^{3(\alpha+\beta q)} \sum_i \binom{\alpha}{i} a^{\alpha-i}x^{2i(q-1)} \sum_j \binom{\beta}{j} a^{(\beta-j)}x^{2j(1-q)} \\ &= a^{\alpha+\beta}\sum_{i,j}\binom{\alpha}{i}\binom{\beta}{j}a^{-(i+j)}\sum_{x\in\mathbb{F}^*_{q^2}} x^{3(\alpha+\beta q)+2(q-1)(i-j)}. \end{aligned}$$

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:

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

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

$$= \sum_{-3(\alpha+1)+2(i-j)=-(q+1),-2(q+1)} \binom{\alpha}{i}\binom{q-1-\alpha}{j} a^{-(i+j)} \tag{3.3.15}$$

$$= \left(\sum_{i-j=\frac{3\alpha-q+2}{2}} + \sum_{i-j=\frac{3\alpha-2q+1}{2}} \right) \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{-(i+j)}$$

$$= \left(\sum_{\alpha-i-j=\frac{3\alpha-q+2}{2}} + \sum_{\alpha-i-j=\frac{3\alpha-2q+1}{2}} \right) \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{-(\alpha-i+j)}$$

$$= \left(\sum_{i+j=\frac{q-\alpha}{2}-1} + \sum_{i+j=q-\frac{\alpha+1}{2}} \right) \binom{\alpha}{i} \binom{\alpha+j}{\alpha} (-1)^j a^{-(\alpha-i+j)} \tag{3.3.16}$$

$$= \sum_i \binom{\alpha}{i} \binom{\frac{q+\alpha}{2}-1-i}{\alpha}^* (-1)^{\frac{q-\alpha}{2}-1-i} a^{2i+1+\frac{\alpha-q}{2}-\alpha} +$$

$$\sum_i \binom{\alpha}{i} \binom{q+\frac{\alpha-1}{2}-i}{\alpha}^* (-1)^{q-\frac{\alpha+1}{2}-i} a^{2i+\frac{\alpha+1}{2}-q-\alpha}$$

$$= (-1)^{\frac{q-\alpha}{2}-1} a^{-\frac{\alpha+q}{2}} \sum_i \binom{\alpha}{i} \binom{\frac{q+\alpha}{2}-1-i}{\alpha}^* (-1)^i a^{2i+1} +$$

$$(-1)^{q-\frac{\alpha+1}{2}} a^{-\frac{\alpha-1}{2}-q} \sum_i \binom{\alpha}{i} \binom{q+\frac{\alpha-1}{2}-i}{\alpha}^* (-1)^i a^{2i}$$

$$= (-1)^{q-\frac{\alpha+1}{2}} a^{-\frac{\alpha-1}{2}-q} \Bigg[(-1)^{\frac{q+1}{2}} a^{\frac{q-1}{2}} \sum_i \binom{\alpha}{i} \binom{\frac{\alpha+q}{2}-1-i}{\alpha}^* (-1)^i a^{2i+1} +$$

$$\sum_i \binom{\alpha}{i} \binom{q+\frac{\alpha-1}{2}-i}{\alpha}^* (-1)^i a^{2i} \Bigg].$$

■

Theorem 3.3.4 *Let $n >$ be a positive interger. Then*

$$\sum_{k \le 2n+1} \binom{2n+1}{k} \left[\prod_{j=1}^{2n+1} (2n+1-2k-2j) \right] (-1)^k \left(\frac{1}{3} \right)^{2k+1} +$$

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

Proof. Define

$$\begin{aligned}
F_1(n,k) &= \binom{2n+1}{k}\left[\prod_{j=1}^{2n+1}(2n+1-2k-2j)\right](-1)^k\left(\frac{1}{3}\right)^{2k+1}\\
F_2(n,k) &= \binom{2n+1}{k}\left[\prod_{j=0}^{2n}(2n-2k-2j)\right](-1)^k\left(\frac{1}{3}\right)^{2k}\\
S_1(n) &= \sum_k F_1(n,k)\\
S_2(n) &= \sum_k F_2(n,k).
\end{aligned}$$

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

$$\begin{aligned}
&27F_1(n+2,k)+8\left(36n^2+126n+113\right)F_1(n+1,k)+192(n+1)^2(2n+3)^2F_1(n,k)\\
&=G_1(n,k+1)-G_1(n,k)
\end{aligned}$$

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

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

Using the same algorithm we see:

$$\begin{aligned}
&27F_2(n+2,k)+8\left(36n^2+126n+113\right)F_2(n+1,k)+192(n+1)^2(2n+3)^2F_2(n,k)\\
&=G_2(n,k+1)-G_2(n,k).
\end{aligned}$$

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

$$R_2(n,k)=\left(\frac{1}{\prod_{j=2}^{5}(2n-k+j)}\right)\cdot(9k(n-k+1)(64(n+1)(2n+3)$$

$$(12n^2+48n+49)k^2-32(n+1)(2n+3)(24n^3+141n^2+285n+200)k$$
$$+32(n+1)(2n+3)(6n^4+42n^3+109n^2+129n+62))).$$

Thus we can conclude both $S_1(n)$ and $S_2(n)$ satisfy the same second order recurrence:

$$27S_1(n+2)+8\left(36n^2+126n+113\right)S_1(n+1)+192(n+1)^2(2n+3)^2S_1(n)=0$$
$$27S_2(n+2)+8\left(36n^2+126n+113\right)S_2(n+1)+192(n+1)^2(2n+3)^2S_2(n)=0.$$

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 remformulation of [Theorem 1.2 [42]].

Proof of Theorem 3.3.1

Proof. (⇒) 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

$$\sum_{x\in\mathbb{F}_{q^2}^*} f(x)^{1+(q-2)q}=\sum_{i=0}^{1}\binom{1}{i}\binom{q-i}{1}(-1)^i a^{2i}=a^2\neq 0.$$

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:

$$
\begin{aligned}
-\sum_{x \in \mathbb{F}_{q^2}} f(x)^{1+(q-2)q} &= \sum_{2(i-j)=-(q+1)+6} \binom{1}{i}\binom{q-2}{j} a^{-(i+j)} + \qquad (3.3.17)\\
&\quad \sum_{2(i-j)=-2(q+1)+6} \binom{1}{i}\binom{q-2}{j} a^{-(i+j)}\\
&= \binom{q-2}{\frac{q-5}{2}} a^{-\frac{q-5}{2}} + \binom{q-2}{\frac{q-3}{2}} a^{-\frac{q-1}{2}} + \binom{q-2}{q-2} a^{-(q-2)}\\
&= (-1)^{\frac{q-5}{2}}(-\frac{3}{2})a^{-\frac{q-5}{2}} + (-1)^{\frac{q-3}{2}}(-\frac{1}{2})a^{-\frac{q-1}{2}} + a\\
&= \frac{1}{2}\left[(-1)^{\frac{q+1}{2}} a^{-\frac{q-1}{2}} \left[3a^2 - 1\right] + 2a\right]
\end{aligned}
$$

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

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

The above takes value 0 only when

$$3a^2 + 2\epsilon a - 1 = (3a - \epsilon)(a + \epsilon) = 0 \qquad (3.3.18)$$

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).

Now suppose $a = \frac{\epsilon}{3}(= \pm\frac{1}{3})$, 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 possibilites:

- $(-1)^{\frac{q+1}{2}} = 1 = \eta(\frac{1}{3})$

  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 $q \equiv \pm 5 \pmod{12} \implies q \equiv 5 \pmod{12} \implies q \equiv -1 \pmod 6$

- Both of these possibilities give case (2).

($\Leftarrow$) 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 α is odd. By (3.3.16) we have:

$$\begin{aligned}
-\sum_{x \in \mathbb{F}_{q^2}} f(x)^{\alpha+\beta q} &= \Big(\sum_{i+j=\frac{q-\alpha}{2}-1} + \sum_{i+j=q-\frac{\alpha+1}{2}}\Big)\binom{\alpha}{i}\binom{q-1-\alpha}{j}a^{-(\alpha-i+j)} \\
&= \binom{q-1}{\frac{q-\alpha}{2}-1} + \binom{q-1}{q-\frac{\alpha+1}{2}} \\
&= (-1)^{\frac{q-\alpha}{2}-1} + (-1)^{q-\frac{\alpha+1}{2}} \\
&= -\Big[(-1)^{\frac{1-\alpha}{2}} + (-1)^{\frac{\alpha+1}{2}}\Big] \\
&= 0.
\end{aligned}$$

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

$$(-1)^{\frac{q+1}{2}}a^{\frac{q-1}{2}}\sum_i \binom{\alpha}{i}\binom{\frac{\alpha+q}{2}-1-i}{\alpha}(-1)^i a^{2i+1} + \sum_i \binom{\alpha}{i}\binom{q+\frac{\alpha-1}{2}-i}{\alpha}(-1)^i a^{2i} = 0.$$

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

$$\sum_i \binom{\alpha}{i}\binom{\frac{\alpha+q}{2}-1-i}{\alpha}(-1)^i\left(\frac{1}{3}\right)^{2i+1}.$$

Now we only have to show that

$$\sum_i \binom{\alpha}{i}\binom{\frac{\alpha+q}{2}-1-i}{\alpha}(-1)^i\left(\frac{1}{3}\right)^{2i+1}+\sum_i \binom{\alpha}{i}\binom{q+\frac{\alpha-1}{2}-i}{\alpha}(-1)^i\left(\frac{1}{3}\right)^{2i}=0$$

in $\mathbb{F}_p$. Write $\alpha = 2n+1$, using Lemma 5.3.5 the LHS of the above becomes

$$\frac{1}{\alpha!2^\alpha}\left[\sum_i \binom{2n+1}{i}\left(\prod_{j=1}^{2n+1}(2n+1-2i-2j)\right)(-1)^i\left(\frac{1}{3}\right)^{2i+1}+\right.$$
$$\left.\sum_i \binom{2n+1}{i}\left(\prod_{j=0}^{2n}(2n-2i-2j)\right)(-1)^i\left(\frac{1}{3}\right)^{2i}\right].$$

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 $f = \mathtt{x}^d(a+\mathtt{x}^{2(q-1)})$ 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 $f = \mathtt{x}^3(a + b\mathtt{x}^{q-1} + \mathtt{x}^{2(q-1)})$

In this section we wish to completely determine PPs of $\mathbb{F}_{q^2}$ of the form $f = \mathtt{x}^3(a + b\mathtt{x}^{q-1} + \mathtt{x}^{2(q-1)}) \in \mathbb{F}_q[\mathtt{x}]$, with $b \neq 0$. Notice if $b = 0$, then f is of the form $f = \mathtt{x}^3(a + x^{2(q-1)}) \in \mathbb{F}_q[\mathtt{x}]$ 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 $f = \mathtt{x}^3(a+b\mathtt{x}^{q-1} + \mathtt{x}^{2(q-1)}) \in \mathbb{F}_q[\mathtt{x}]$. 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* $q \equiv 1 \pmod 4$

(ii) $a = \frac{1}{3}$ *and* $q \equiv -1 \pmod 6$

(iii) $a = -\frac{1}{3}$ *and* $q \equiv -1 \pmod{12}$.

(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

$$\begin{aligned}
&\sum_{x \in \mathbb{F}_{q^2}} f(x)^s \\
&= \sum_{x \in \mathbb{F}_{q^2}^\times} x^{3(\alpha+\beta q)} (a + bx^{q-1} + x^{2(q-1)})^\alpha (a + bx^{1-q} + x^{2(1-q)})^\beta \\
&= \sum_x x^{3(\alpha+\beta q)} \sum_{i,j} \binom{\alpha}{i}\binom{i}{k} a^{\alpha-i} b^{i-k} x^{(q-1)(i-k+2k)} \binom{\beta}{j}\binom{j}{l} a^{\beta-j} b^{j-l} x^{(1-q)(j-l+2l)}
\end{aligned}$$

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

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

$$\begin{aligned}
&= \sum_{i,j} \binom{\alpha}{i}\binom{i}{k}\binom{q-1-\alpha}{j}\binom{j}{l} a^{-i-j} b^{i-k+j-l} \sum_x x^{(q-1)(-3(\alpha+1)+i+k-j-l)} \\
&= - \sum_{-3(\alpha+1)+i+k-j-l \equiv 0 \pmod{q+1}} \binom{\alpha}{i}\binom{i}{k}\binom{q-1-\alpha}{j}\binom{j}{l} a^{-i-j} b^{i-k+j-l} \\
&= -S_q(\alpha, a, b).
\end{aligned}$$

By Hermites 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 $0 \le \alpha \le q-1$.

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 $\mathbb{F}_q^{\times}$. 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

$$y = \left(\frac{y}{t}\right)^3 + b\left(\frac{y}{t}\right)^{q+2} + \left(\frac{y}{t}\right)^{2q+1} = \frac{1}{t^3}\left(y^3 + by^{q+2} + y^{2q+1}\right).$$

Thus t^3 is unique and $(3, q-1) = 1$, so t is unique.

2° 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

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

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 $\mathbb{F}_q$.

1° 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

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

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

2° 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 $x_1 \in \mathbb{F}_{q^2}^*$ with $x_1^{q-1} = -b$. Thus

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

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:

$$\begin{aligned}\sum_{x\in\mathbb{F}_{q^2}} f(x)^{\alpha+\beta q} &= \sum_{x\in\mathbb{F}_{q^2}^*} (x^3(bx^{q-1} + x^{2(q-1)})^{\alpha+\beta q} \\ &= -\sum_{-\alpha+i-j-q-2\equiv 0 \pmod{q+1}} \binom{\alpha}{i}\binom{q-1-\alpha}{j} b^{-(i+j)}. \qquad (3.4.19)\end{aligned}$$

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 $\mathtt{Tr}(z)$ for $\mathtt{Tr}_{q^2/q}(z)$, and $\mathtt{N}(z)$ for $\mathtt{N}_{q^2/q}(z)$.

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

$$a(x - x^q)(x^2 + x^{2q}) + (a + b - 1)(x - x^q)x^{q+1} = 0. \tag{3.4.20}$$

Since $x - x^q \neq 0$, (3.4.20) becomes

$$ax^{2q-2} + (a + b - 1)x^{q-1} + a = 0. \tag{3.4.21}$$

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 $g = a\mathtt{x}^2 + (a+b-1)\mathtt{x} + a$ is reducible over $\mathbb{F}_q$, so $x^{q-1} \in \mathbb{F}_q$. Now we have

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

Since $x \notin \mathbb{F}_q$, 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 $g(\mathbb{F}_{q^2} \setminus \mathbb{F}_q) \subseteq \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

■

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 $\mathtt{Tr}(x)$, and $\mathtt{N}(x)$ are unqiuely determined by y.*

Proof. By definition $g(x) = ax^3 + bx^{q+2} + x^{2q+1}$. Therefore we have

$$\begin{aligned} \mathtt{Tr}(g(x)) &= (ax^3 + bx^{q+2} + x^{2q+1}) + (ax^3 + bx^{q+2} + x^{2q+1})^q \\ &= a\mathtt{Tr}(x^3) + (b + 1)\mathtt{Tr}(x^{q+2}) \qquad (3.4.22) \\ \mathtt{N}(g(x)) &= (ax^3 + bx^{q+2} + x^{2q+1})(ax^3 + bx^{q+2} + x^{2q+1})^q \end{aligned}$$

$$= (a^2+b^2+1)\mathtt{N}(x)^3 + (ab+b)\mathtt{Tr}(x^{4+2q}) + a\mathtt{Tr}(x^{q+5}) \tag{3.4.23}$$

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

$$\begin{cases} \mathtt{Tr}(y) = aTr(x^3) + (b+1)\mathtt{Tr}(x^{q+2}) \\ \mathtt{N}(y) = (a^2+b^2+1)\mathtt{N}(x)^3 + (ab+b)\mathtt{Tr}(x^{4+2q}) + a\mathtt{Tr}(x^{q+5}) \end{cases} \tag{3.4.24}$$

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

$$\mathtt{Tr}(z^3) = \mathtt{Tr}(z)^3 - 2\mathtt{N}(z) \tag{3.4.25}$$

$$\mathtt{Tr}(z^{q+2}) = \mathtt{N}(z)\mathtt{Tr}(z) \tag{3.4.26}$$

$$\mathtt{Tr}(z^{4+2q}) = \mathtt{Tr}(z)^2\mathtt{N}(z)^2 - 2\mathtt{N}(z)^3 \tag{3.4.27}$$

$$\mathtt{Tr}(z^{q+5}) = \mathtt{Tr}(z)^4\mathtt{N}z - 4\mathtt{Tr}(z)^2\mathtt{N}(z)^2 + 2\mathtt{N}(z)^3 \tag{3.4.28}$$

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

$$\begin{cases} a\mathtt{t}^3 - \mathtt{n}(3a-b-1)\mathtt{t} = \mathtt{r} \\ a\mathtt{n}\mathtt{t}^4 + (ab+b-4a)\mathtt{n}^2\mathtt{t}^2 + \mathtt{n}^3(a-b+1)^2 = \mathtt{s} \end{cases} \tag{3.4.29}$$

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

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

1° Assume $\mathtt{r} = 0$. We claim $\mathtt{t} = 0$ as well. If $\mathtt{t} \neq 0$, then we have

$$\frac{\mathtt{t}^2}{\mathtt{n}} = \frac{3a-b-1}{a}.$$

Using the relation $b^2 = 3a+1$, it follows that

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

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

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

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

Therefore we have

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

or equivalently

$$a^2\mathtt{u}^3 - (6a^2 - 2ab - 2a + a\gamma)\mathtt{u}^2 + \left[(3a-b-1)^2 + \gamma(4a-b-ab)\right]\mathtt{u} - (a-b+1)^2\gamma = 0. \tag{3.4.32}$$

Let $p(\mathtt{u}) \in \mathbb{F}_q[\mathtt{u}]$ denote the LHS of (3.4.32). The problem is now reduced to showing $p(\mathtt{u})$ 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

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

where

$$\begin{aligned} h(\gamma) = &-27a^4 + 18a^2b^2 - 18a^2b\gamma + 36a^2b + 18a^2 + 4ab^3\gamma - 8ab^3 - 24ab^2 + 12ab\gamma \\ &-24ab - 4a\gamma^2 + 16a\gamma - 8a + b^4 - 2b^3\gamma + 4b^3 + b^2\gamma^2 - 4b^2\gamma + 6b^2 - 2b\gamma + 4b + 1. \end{aligned}$$

Using the relation $b^2 = 3a + 1$ gives

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

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

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

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

$$\begin{aligned} p(u) &= a^2\mathtt{u}^3 + 3a^2(b - 2)\mathtt{u}^2 + 3a^2(b - 2)^2\mathtt{u} + a^2(b - 2)^3 \\ &= a^2\left(\mathtt{u} + (b - 2)\right)^3 \end{aligned} \tag{3.4.37}$$

Clearly $p(\mathtt{u})$ 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 $\mathtt{Tr}(x)$ and $\mathtt{N}(x)$ are uniquely determined by y, we must have $\mathtt{Tr}(x_1) = \mathtt{Tr}(x)$ and $\mathtt{N}(x_1) = \mathtt{N}(x)$. 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 $x_1 = x$.

■

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

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{q^2}} f(x)^s \\
&= \sum_{x\in\mathbb{F}_{q^2}^{\times}} x^{3(\alpha+\beta q)}(a+bx^{q-1}+x^{2(q-1)})^{\alpha}(a+bx^{1-q}+x^{2(1-q)})^{\beta} \\
&= \sum_{x} x^{3(\alpha+\beta q)} \sum_{i,j} \binom{\alpha}{i}\binom{i}{k} a^{\alpha-i}b^{i-k}x^{(q-1)(i-k+2k)}\binom{\beta}{j}\binom{j}{l}a^{\beta-j}b^{j-l}x^{(1-q)(j-l+2l)} \\
&= \sum_{i,j}\binom{\alpha}{i}\binom{i}{k}\binom{\beta}{j}\binom{j}{l}a^{\alpha+\beta-i-j}b^{i-k+j-l}\sum_{x} x^{3(\alpha+\beta q)+(q-1)(i+k-j-l)}
\end{aligned}$$

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

$$\begin{aligned}
&= \sum_{i,j}\binom{\alpha}{i}\binom{i}{k}\binom{q-1-\alpha}{j}\binom{j}{l}a^{-i-j}b^{i-k+j-l}\sum_{x} x^{(q-1)(-3(\alpha+1)+i+k-j-l)} \\
&= -\sum_{-3(\alpha+1)+i+k-j-l\equiv 0 \pmod{q+1}} \binom{\alpha}{i}\binom{i}{k}\binom{q-1-\alpha}{j}\binom{j}{l}a^{-i-j}b^{i-k+j-l} && (3.4.38) \\
&= -S_q(\alpha,a,b). && (3.4.39)
\end{aligned}$$

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

$$S_q(\alpha,a,b) = 0 \text{ for each } 0 \le \alpha \le q-1.$$

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

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

Therefore the sum in (5.5.45) becomes

$$0 = \sum_{-3-j-l\equiv 0 \pmod{q+1}} \binom{q-1}{j}\binom{j}{j}a^{-j}b^{j-l}$$

$$= \sum_{0 \leq l \leq \frac{q-2}{2}} \binom{q-1}{q-2-l} \binom{q-2-l}{l} a^{-(q-2-l)} b^{q-2-2l}$$
$$= \frac{a}{b} \sum_{0 \leq l \leq \frac{q-2}{2}} \binom{q-2-l}{l} (-1)^{q-2-l} a^{l} b^{-2l}$$

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

$$= -\frac{a}{b} \sum_{0 \leq l \leq \frac{q-2}{2}} \binom{q-2-l}{l} z^{l}$$

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

$$= -\frac{a}{b} \sum_{2 \leq l \leq \frac{q-2}{2}+2} \binom{-l}{l-2} z^{l-2}$$
$$= -\frac{a}{b}(z^{-2}) \sum_{0 \leq l \leq q-1} \binom{-l}{l-2} z^{l}.$$

Thus by lemma 3.5.1, the polynomial $x^2 + x - z$ has two distict 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

$$0 = \sum_{-6+i+k-j-l \equiv 0 \pmod{q+1}} \binom{1}{i} \binom{i}{k} \binom{q-2}{j} \binom{j}{l} a^{-(i+j)} b^{i+j-k-l}$$
$$= \sum_{-6-j-l=-2(q+1),-(q+1)} \binom{q-2}{j} \binom{j}{l} a^{-j} b^{j-l} +$$
$$\sum_{-5-j-l=-(q+1)} \binom{q-2}{j} \binom{j}{l} a^{-1-j} b^{1+j-l} + \sum_{-4-j-l=-(q+1)} \binom{q-2}{j} \binom{j}{l} a^{-1-j} b^{j-l}$$
$$= \binom{q-2}{q-2} \binom{q-2}{q-2} a^{-(q-2)} + \sum_{0 \leq l \leq \frac{q-5}{2}} \binom{q-2}{q-5-l} \binom{q-5-l}{l} a^{-(q-5-l)} b^{q-5-2l}$$
$$+ \sum_{0 \leq l \leq \frac{q-4}{2}} \binom{q-2}{q-4-l} \binom{q-4-l}{l} a^{-(1+q-4-l)} b^{1+q-4-2l}$$

$$+\sum_{0\leq l\leq \frac{q-3}{2}} \binom{q-2}{q-3-l}\binom{q-3-l}{l} a^{-(1+q-3-l)} b^{q-3-2l}$$

$$= a + \sum_{0\leq l\leq \frac{q-5}{2}} (-1)^{q-5-l}(q-4-l)\binom{q-5-l}{l} a^{l+4} b^{-4-2l}$$

$$+\sum_{0\leq l\leq \frac{q-4}{2}} (-1)^{q-4-l}(q-3-l)\binom{q-4-l}{l} a^{l+2} b^{-2l-2} +$$

$$+\sum_{0\leq l\leq \frac{q-3}{2}} (-1)^{q-3-l}(q-2-l)\binom{q-3-l}{l} a^{l+1} b^{-2-2l}$$

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

$$= a + \frac{a^4}{b^4}\sum_{0\leq l\leq \frac{q-5}{2}} (-4-l)\binom{-l-5}{l} z^l + \frac{-a^2}{b^2}\sum_{0\leq l\leq \frac{q-4}{2}} (-l-3)\binom{-l-4}{l} z^l$$

$$+\frac{a}{b^2}\sum_{0\leq l\leq \frac{q-3}{2}} (-l-2)\binom{-l-3}{l} z^l$$

$$= a + \left(\frac{a}{b}\right)^4 (-z^{-5}) \sum_{5\leq l\leq \frac{q-5}{2}+5} (l-1)\binom{-l}{l-5} z^l$$

$$+\left(\frac{a}{b}\right)^2 (z^{-4}) \sum_{4\leq l\leq \frac{q-4}{2}+4} (l-1)\binom{-l}{l-4} z^l + \left(\frac{a}{b^2}\right)(-z^{-3}) \sum_{3\leq l\leq \frac{q-3}{2}+3} (l-1)\binom{-l}{l-3} z^l$$

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

$$= a + \left(\frac{a}{b}\right)^4 (-z^{-5}) \sum_{0\leq l\leq q-1} (l-1)\binom{-l}{l-5} z^l \tag{3.4.40}$$

$$+\left(\frac{a}{b}\right)^2 (z^{-4}) \sum_{0\leq l\leq q-1} (l-1)\binom{-l}{l-4} z^l + \left(\frac{a}{b^2}\right)(-z^{-3}) \sum_{0\leq l\leq q-1} (l-1)\binom{-l}{l-3} z^l$$

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

$$= a + \left(\frac{a}{b}\right)^4 (-z^{-5}) \left(\frac{2z^3(1+3z)}{1+4z}\right) + \left(\frac{a}{b}\right)^2 (z^{-4}) \left(-\frac{z^3}{1+4z}\right)$$

$$+\left(\frac{a}{b^2}\right)\left(-z^{-3}\right)\left(\frac{2z^3}{1+4z}\right)$$
$$=\frac{2(a-1)a\left(3a-b^2+1\right)}{b^2-4a}. \tag{3.4.41}$$

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*

$$\sum_{0\le l\le q-1}\binom{-l}{l-2}z^l = \begin{cases} \frac{1}{8} & \textit{if } r_1 = r_2 \\ 0 & \textit{if } r_1 \ne r_2 \in \mathbb{F}_q \\ z & \textit{if } r_1, r_2 \notin \mathbb{F}_q. \end{cases}$$

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

$$\begin{aligned}
\sum_{0\le l\le q-1}\binom{-l}{l-2}z^l &= \sum_{0\le l<q-1} C\left[\frac{1}{x^{l-2}(1+x)^l}\right]z^l \\
&= \sum_{0\le l\le q-1} C\left[x^2\cdot\left(\frac{z}{x(1+x)}\right)^l\right] \\
&= C\left[\sum_{0\le l\le q-1} x^2\cdot\left(\frac{z}{x(1+x)}\right)^l\right] \\
&= C\left[x^2\cdot\left(\frac{1-\left(\frac{z}{x(1+x)}\right)^q}{1-\frac{z}{x(1+x)}}\right)\right] \\
&= C\left[x^2\cdot\frac{x(1+x)}{x(1+x)-z}\left(1-z\left(\frac{1}{x^q}-\frac{1}{1+x^q}\right)\right)\right] \\
&= C\left[\frac{x^3(1+x)}{x(1+x)-z}\right]+C\left[\frac{-z}{x^{q-2}}\cdot\frac{x(1+x)}{x(1+x)-z}\right]+C\left[\frac{x^3(1+x)}{x(1+x)-z}\cdot\frac{1}{1+x^q}\right] \\
&= C\left[\frac{-z^2}{x^{q-2}}\cdot\left(1+\frac{1}{x^2+x-z}\right)\right]
\end{aligned}$$

$$= C\left[\frac{-z^2}{x^{q-2}}\cdot\left(\frac{1}{x^2+x-z}\right)\right] \tag{3.5.42}$$

Now suppose $r_1 = r_2 (= -\frac{1}{2})$. Then 3.5.42 becomes

$$\begin{aligned}
&= C\left[\frac{-z^2}{x^{q-2}}\cdot\frac{1}{(x-r_1)^2}\right]\\
&= C\left[\frac{-z^2}{r_1^2}\binom{-2}{q-2}\left(-\frac{1}{r_1}\right)^{q-2}\right]\\
&= \frac{-z^2}{r_1^q}(-1)^{q-2}(q-1)(-1)^{q-2} = \frac{z^2}{r_1}\\
&= \frac{1}{8}
\end{aligned}$$

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

$$\begin{aligned}
&= C\left[\frac{-z^2}{x^{q-2}}\left(\frac{1}{(x-r_1)(x-r_2)}\right)\right]\\
&= C\left[\frac{-z^2}{x^{q-2}}\left(\frac{1}{x-r_1}-\frac{1}{x-r_2}\right)\frac{1}{r_1-r_2}\right]\\
&= C\left[\frac{z^2}{r_1-r_2}\cdot\frac{1}{x^{q-2}}\left(\frac{1}{r}\cdot\frac{1}{1-\frac{x}{r_1}}-\frac{1}{r_2}\cdot\frac{1}{1-\frac{x}{r_2}}\right)\right]\\
&= \frac{z^2}{r_1-r_2}\left(\frac{1}{r_1^{q-1}}-\frac{1}{r_2^{q-1}}\right)\\
&= \begin{cases} 0 & \text{if } r_1, r_2 \in \mathbb{F}_q \\ z & \text{if } r_1, r_2 \notin \mathbb{F}_q \end{cases}
\end{aligned}$$

■

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*

$$\sum_{0\leq l\leq q-1}(l-1)\binom{-l}{l-5}z^l = \frac{2z^3(1+3z)}{1+4z} \tag{3.5.43}$$

$$\sum_{0\le l\le q-1}(l-1)\binom{-l}{l-4}z^l = -\frac{z^3}{1+4z} \tag{3.5.44}$$

$$\sum_{0\le l\le q-1}(l-1)\binom{-l}{l-3}z^l = \frac{2z^3}{1+4z}. \tag{3.5.45}$$

Proof. We make use of the following facts:

1. $\displaystyle\sum_{0\le l\le q-1}(l-1)\binom{-l}{l-j}z^l = \sum_{0\le l\le q-1}(l+1)\binom{-l}{l-j}z^l - \sum_{0\le l\le q-1}2\binom{-l}{l-j}z^l$

2. $\displaystyle\binom{-(q-1)}{q-6} \equiv \binom{-(q-1)}{q-5} \equiv \binom{-(q-1)}{q-4} \equiv 0 \pmod p$

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

We proceed as in the previous lemma.

$$\begin{aligned}
\sum_{0\le l\le q-1}(l+1)\binom{-l}{l-5}z^l &= C\left[x^5\sum_{0\le l\le q-1}(l+1)\left(\frac{z}{x(1+x)}\right)^l\right]\\
&= C\left[x^5\frac{1-\left(\frac{z}{x(1+x)}\right)^q}{\left(1-\frac{z}{x(1+x)}\right)^2}\right]\\
&= C\left[x^5\left(\frac{x(1+x)}{x(1+x)-z}\right)^2\left(1-z\left(\frac{1}{x^q}-\frac{1}{1+x^q}\right)\right)\right]\\
&= C\left[\frac{-z}{x^{q-5}}\left(1+\frac{z}{x(1+x)-z}\right)^2\right]\\
&= C\left[\frac{-z}{x^{q-5}}\left(\frac{2z}{(x-r_1)(x-r_2)}+\frac{z^2}{(x-r_1)^2(x-r_2)^2}\right)\right]\\
&= C\left[\frac{-2z^2}{x^{q-5}}\left(\frac{1}{(x-r_1)(x-r_2)}\right)\right]\\
&\quad + C\left[\frac{-z^3}{x^{q-5}}\left(\frac{1}{(x-r_1)(x-r_2)}\right)^2\right]
\end{aligned}$$

For the first term we continue exactly as in the previous lemma to see

$$\begin{aligned}
C\left[\frac{-2z^2}{x^{q-5}}\left(\frac{1}{(x-r_1)(x-r_2)}\right)\right] &= C\left[\frac{-2z^2}{x^{q-5}}\left(\frac{1}{x-r_1}-\frac{1}{x-r_2}\right)\frac{1}{r_1-r_2}\right] \\
&= C\left[\frac{2z^2}{r_1-r_2}\cdot\frac{1}{x^{q-5}}\left(\frac{1}{r_1}\cdot\frac{1}{1-\frac{x}{r_1}}-\frac{1}{r_2}\cdot\frac{1}{1-\frac{x}{r_2}}\right)\right] \\
&= \frac{2z^2}{r_1-r_2}\left(\left(\frac{1}{r_1}\right)^{q-4}-\left(\frac{1}{r_2}\right)^{q-4}\right) \qquad (3.5.46) \\
&= \frac{2z^2}{r_1-r_2}\left(r_1^3-r_2^3\right) \\
&= (2z^2)(r_1^2+r_1r_2+r_2^2) \\
&= 2z^2((r_1+r_2)^2-r_1r_2) \\
&= 2z^2(1+z). \qquad (3.5.47)
\end{aligned}$$

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

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

Again, working like before we have

$$\begin{aligned}
C\left[\frac{1}{x^{q-5}}\left(\frac{1}{x-r_1}-\frac{1}{x-r_2}\right)^2\right] &= C\left[\frac{1}{x^{q-5}}\left((x-r1)^{-2}+(x-r_2)^{-2}-\frac{2}{(x-r_1)(x-r_2)}\right)\right] \\
&= \frac{1}{r_1^2}\binom{-2}{q-5}\left(\frac{-1}{r_1}\right)^{q-5}+\frac{1}{r_2^2}\binom{-2}{q-5}\left(\frac{-1}{r_2}\right)^{q-5} \\
&+\frac{2}{r_1-r_2}(r_1^3-r_2^3) \\
&= (-4)(r_1^2+r_2^2)-2(r_1^2+r_1r_2+r_2^2) \\
&= (-4)(1+2z)+2(1+z) \\
&= -2(1+2z). \qquad (3.5.49)
\end{aligned}$$

Combining (3.5.47), (3.5.48) and (3.5.49) we have

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

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.

■

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

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 subsitution 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 $\mathtt{x}^d$ of $\mathbb{F}_{2^n}$ and to search for a linearized polynomial $L(\mathtt{x})$ such that $\mathtt{x}^d + L(\mathtt{x})$ 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 $\mathtt{x}^d + L(\mathtt{x})$, where d is a positive integer and $L \in \mathbb{F}_{2^n}[\mathtt{x}]$ 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* $L(\mathtt{x}) \in \mathbb{F}_{2^n}[\mathtt{x}]$ *be a nonzero linearized polynomial. Then* $\mathtt{x}^d + L(\mathtt{x})$ *is a permutation polynomial on* $\mathbb{F}_{2^n}$ *if and only if*

$$\frac{L(\mu)}{\mu^d} \notin \{\alpha^d + (\alpha+1)^d | \alpha \in \mathbb{F}_{2^n}\}$$

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

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

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

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

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

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

(ii) If $k = n/3$ *or* $2n/3$ *and* $k \equiv 2 \pmod 3$, *then* $\mathtt{x}^{1+2^k} + (\mathtt{x} + \mathtt{x}^{2^k})^{2^{k+1}}$ *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 $\mathtt{x}^{1+2^k} + (\mathtt{x} + \mathtt{x}^{2k})^{2^{2k+1}}$ and $\mathtt{x}^{1+2^k} + (\mathtt{x} + \mathtt{x}^{2k})^{2^{k+1}}$ are permutation polynomials of $\mathbb{F}_{2^n}$. We confirm this conjecture in the next section.

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

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

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

$$\frac{L(x)}{x^{1+2^k}} \notin \{y^{2k} + y + 1 : y \in \mathbb{F}_2^n\} \tag{4.2.1}$$

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

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

Since $n/k = 3$ we only have to show

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

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

Assume that k is even. We show that

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

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

Notice for $x \in \mathbb{F}_{2^n}$ we have

$$\begin{aligned}
\mathtt{Tr}_{2^n/2^k}\left(\frac{(x+x^{2^k})^{2^{2k+1}}}{x^{1+2^k}}\right) &= \mathtt{Tr}_{2^n/2^k}\left(\frac{x^{2^{2k+1}}+x^2}{x^{1+2^k}}\right) \\
&= \mathtt{Tr}_{2^n/2^k}\left(\frac{x^{2^{2k+1}+2^{2k}}+x^{2+2^{2k}}}{x^{1+2^k+2^{2k}}}\right) \\
&= \frac{\left(\mathtt{Tr}_{2^n/2^k}(x^3+x^{1+2^{k+1}})\right)}{\mathtt{N}_{2^n/2^k}(x)}.
\end{aligned}$$

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

$$\mathtt{Tr}_{2^n/2^k}(x^3+x^{1+2^{k+1}}) + \mathtt{N}_{2^n/2^k}(x) \neq 0 \tag{4.2.4}$$

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 $\mathtt{x}^3 + v \in \mathbb{F}_{2^k}[\mathtt{x}]$ is irreducible. Let α be a root of $\mathtt{x}^3 + v$. It follows that $\mathbb{F}_{2^n} = \mathbb{F}_{2^k}(\alpha)$. Since $\mathtt{x}^3 + v$ is the minimum polynomial of α over $\mathbb{F}_{2^k}$, it is easy to see $\mathtt{Tr}_{2^n/2^k}(\alpha) = 0$ and $\mathtt{N}_{2^n/2^k}(\alpha) = v$. Now since $\alpha^4 = \alpha v$, an induction gives

$$\alpha^{2^k} = v^{1+2^2+\cdots+2^{2\cdot k/2}}\alpha = v^{\frac{1}{3}(2^k-1)}\alpha. \tag{4.2.5}$$

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

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

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

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

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

$$\begin{aligned}
\mathtt{N}_{2^n/2^k}(x) &= (a+b\alpha+c\beta)(a+b\alpha^{\sigma}+c\beta^{\sigma})(a+b\alpha^{\sigma^2}+c\beta^{\sigma^2}) \\
&= a^3 + b^3\mathtt{N}_{2^n/2^k}(\alpha) + c^3\mathtt{N}_{2^n/2^k}(\beta) + a^2b\mathtt{Tr}_{2^n/2^k}(\alpha) + a^2c\mathtt{Tr}_{2^n/2^k}(\beta)
\end{aligned}$$

$$+ b^2a\mathtt{Tr}_{2^n/2^k}(\alpha\alpha^\sigma) + b^2c\mathtt{Tr}_{2^n/2^k}(\alpha\alpha^\sigma\beta^{\sigma^2}) + c^2a\mathtt{Tr}_{2^n/2^k}(\beta\beta^\sigma)$$
$$+ c^2b\mathtt{Tr}_{2^n/2^k}(\beta\beta^\sigma\alpha^{\sigma^2}) + abc\mathtt{Tr}_{2^n/2^k}(\alpha\beta^\sigma + \alpha^\sigma\beta).$$

Observe that we have

$$\mathtt{Tr}_{2^n/2^k}(\alpha\alpha^\sigma) = \mathtt{N}_{2^n/2^k}(\alpha)\mathtt{Tr}_{2^n/2^k}(\frac{1}{\alpha}) = 0,$$

$$\mathtt{Tr}_{2^n/2^k}(\beta\beta^\sigma) = \mathtt{Tr}_{2^n/2^k}(\alpha\alpha^\sigma)^2 = 0,$$

$$\mathtt{Tr}_{2^n/2^k}(\alpha\alpha^\sigma\beta^{\sigma^2}) = \mathtt{N}_{2^n/2^k}(\alpha)\mathtt{Tr}_{2^n/2^k}(\beta) = 0,$$

$$\mathtt{Tr}_{2^n/2^k}(\beta\beta^\sigma\alpha^{\sigma^2}) = \mathtt{N}_{2^n/2^k}(\beta)\mathtt{Tr}_{2^n/2^k}(\frac{1}{\alpha}) = 0,$$

$$\begin{aligned}\mathtt{Tr}_{2^n/2^k}(\alpha\beta^\sigma + \alpha^\sigma\beta) &= \mathtt{Tr}_{2^n/2^k}(\alpha^{\sigma^2}\beta + \alpha^\sigma\beta)\\ &= \mathtt{Tr}_{2^n/2^k}(\beta(\mathtt{Tr}_{2^n/2^k}(\alpha) - \alpha))\\ &= \mathtt{Tr}_{2^n/2^k}(\alpha)\mathtt{Tr}_{2^n/2^k}(\beta) + \mathtt{Tr}_{2^n/2^k}(\alpha\beta)\\ &= v.\end{aligned}$$

Combining the above facts we have

$$\mathtt{N}_{2^n/2^k}(x) = a^3 + b^3v + c^3v^2 + abcv \tag{4.2.7}$$

Proceeding as before we also have

$$\begin{aligned}\mathtt{Tr}_{2^n/2^k}(x^{1+2^{k+1}}) &= \mathtt{Tr}_{2^n/2^k}((a + b\alpha + c\beta)(a^2 + b^2\alpha^2 + c^2\beta^2)^\sigma)\\ &= \mathtt{Tr}_{2^n/2^k}((a + b\alpha + c\beta)(a^2 + c^2v\alpha^\sigma + b^2\beta^\sigma))\\ &= a^3 + bc^2v\mathtt{Tr}_{2^n/2^k}(\alpha\alpha^\sigma) + b^3\mathtt{Tr}_{2^n/2^k}(\alpha\beta^\sigma)\\ &\quad + c^3v\mathtt{Tr}_{2^n/2^k}(\alpha^\sigma\beta) + cb^2\mathtt{Tr}_{2^n/2^k}(\beta\beta^\sigma)\\ &= a^3 + b^3\mathtt{Tr}_{2^n/2^k}(\alpha\beta^\sigma) + c^3v\mathtt{Tr}_{2^n/2^k}(\alpha^\sigma\beta).\end{aligned}$$

Using (4.2.5) we have

$$\mathtt{Tr}_{2^n/2^k}(\alpha\beta^\sigma) = \mathtt{N}_{2^n/2^k}(\alpha)\mathtt{Tr}_{2^n/2^k}(\frac{\alpha}{\alpha^\sigma}) = v^{1-\frac{1}{3}(2^k-1)},$$
$$\mathtt{Tr}_{2^n/2^k}(\alpha^\sigma\beta) = \mathtt{N}_{2^n/2^k}(\alpha)\mathtt{Tr}_{2^n/2^k}(\frac{\alpha^\sigma}{\alpha}) = v^{1+\frac{1}{3}(2^k-1)}.$$

Thus

$$\mathtt{Tr}_{2^n/2^k}(x^{1+2^{k+1}}) = a^3 + b^3v^{1-\frac{1}{3}(2^k-1)} + c^3v^{2+\frac{1}{3}(2^k-1)}. \tag{4.2.8}$$

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

$$\mathtt{Tr}_{2^n/2^k}(x^3 + x^{1+2^{k+1}}) + \mathtt{N}_{2^n/2^k}(x) = abcv + a^3 + b^3v^{1-\frac{1}{3}(2^k-1)} + c^3v^{2+\frac{1}{3}(2^k-1)}.$$

Define

$$a_1 = a, \qquad b_1 = bv^{-\frac{1}{9}(2^k-1)}, \qquad c_1 = cv^{\frac{1}{9}(2^k-1)}.$$

Then

$$\begin{aligned}\mathtt{Tr}_{2^n/2^k}(x^3 + x^{1+2^{k+1}}) + \mathtt{N}_{2^n/2^k}(x) &= a_1b_1c_1v + a_1^3 + b_1^3v + c_1^3v^2 \\ &= \mathtt{N}_{2^n/2^k}(a_1 + b_1\alpha + c_1\alpha^2) \quad \text{(by (4.2.7))} \\ &\neq 0.\end{aligned}$$

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

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

$$\mathtt{Tr}_{2^n/2^k}(x^3 + x^{1+2^{2k+1}}) + \mathtt{N}_{2^n/2^k}(x) \neq 0 \tag{4.2.9}$$

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

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

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

$$
\begin{aligned}
&= \mathtt{Tr}_{2^n/2^k}((a+b\alpha+c\beta)(a^2+c^2v\alpha^{\sigma^2}+b^2\beta^{\sigma^2}))\\
&= a^3+bc^2v\mathtt{Tr}_{2^n/2^k}(\alpha\alpha^{\sigma^2})+b^3\mathtt{Tr}_{2^n/2^k}(\alpha\beta^{\sigma^2})\\
&\quad + c^3v\mathtt{Tr}_{2^n/2^k}(\alpha^{\sigma^2}\beta)+cb^2\mathtt{Tr}_{2^n/2^k}(\beta\beta^{\sigma^2})\\
&= a^3+b^3\mathtt{Tr}_{2^n/2^k}(\alpha\beta^{\sigma^2})+c^3v\mathtt{Tr}_{2^n/2^k}(\alpha^{\sigma^2}\beta).
\end{aligned}
$$

Using (4.2.5) it follows that

$$
\begin{aligned}
\mathtt{Tr}_{2^n/2^k}(\alpha\beta^{\sigma^2}) &= \mathtt{N}_{2^n/2^k}(\alpha)\mathtt{Tr}_{2^n/2^k}(\frac{\alpha^\sigma}{\alpha}) = v^{1+\frac{1}{3}(2^k-1)},\\
\mathtt{Tr}_{2^n/2^k}(\alpha^{\sigma^2}\beta) &= \mathtt{N}_{2^n/2^k}(\alpha)\mathtt{Tr}_{2^n/2^k}(\frac{\alpha}{\alpha^\sigma}) = v^{1-\frac{1}{3}(2^k-1)}.
\end{aligned}
$$

Thus

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

Putting the pieces together we have

$$
\mathtt{Tr}_{2^n/2^k}(x^3+x^{1+2^{2k+1}})+\mathtt{N}_{2^n/2^k}(x) = abcv+a^3+b^3v^{1+\frac{1}{3}(2^k-1)}+c^3v^{2-\frac{1}{3}(2^k-1)}. \tag{4.2.11}
$$

Define

$$
a_2=a, \qquad b_2=bv^{\frac{1}{9}(2^k-1)}, \qquad c_2=cv^{-\frac{1}{9}(2^k-1)}.
$$

Then

$$
\begin{aligned}
\mathtt{Tr}_{2^n/2^k}(x^3+x^{1+2^{2k+1}})+\mathtt{N}_{2^n/2^k}(x) &= a_2b_2c_2v+a_2^3+b_2^3v+c_2^3v^2\\
&= \mathtt{N}_{2^n/2^k}(a_2+b_2\alpha+c_2\beta)\\
&\neq 0
\end{aligned}
$$

Now assume k is odd. For each $x\in\mathbb{F}_{2^n}^*$, by (4.2.9), with n replaced by $2n$ and k replaced by $2k$ we have

$$
\mathtt{Tr}_{2^{2n}/2^{2k}}(x^3+x^{1+2^{2k+1}})+\mathtt{N}_{2^{2n}/2^{2k}}(x)\neq 0. \tag{4.2.12}
$$

For each $z \in \mathbb{F}_{2^n}$, we have

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

as well as

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

Therefore (4.2.12) becomes

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

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

■

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,

$$c'_k n^{1+\frac{2}{3k-3+\epsilon}} \leq g_k(n) \leq c_k n^{1+\frac{1}{k}}, \tag{5.1.1}$$

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]

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

$$p_2 + l_2 = p_1 l_1.$$

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:

$$p_2 + l_2 = p_1 l_1, \;\; p_3 + l_3 = p_1 l_1^2.$$

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:

$$p_2 + l_2 = p_1 l_1, \;\; p_3 + l_3 = p_1 l_1^2, \;\; p_4 + l_4 = p_1 l_1^3, \;\; p_5 + l_5 = p_4 l_1 - 2p_3 l_2 + p_2 l_3.$$

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 $f, g \in \mathbb{F}_q[\mathtt{x}, \mathtt{y}]$. 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 $\Gamma_3(q) = G_q(\mathtt{xy}, \mathtt{xy}^2)$, 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 $G_q(\mathtt{xy}, \mathtt{xy}^2)$. 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 $1 \le k \le q - 1$, let

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

and

$$B_k = \big[(\mathtt{x} + 1)^{2k} - 1\big]\mathtt{x}^{q-1-k} - 2\mathtt{x}^{q-1} \in \mathbb{F}_q[\mathtt{x}]. \tag{5.1.3}$$

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 $G_q(\mathtt{x}\mathtt{y}, \mathtt{x}^k\mathtt{y}^{2k})$, 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*

$$m \le \frac{p-1}{\lfloor (p-1)/\alpha(p) \rfloor}.$$

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 $a \ge 0$ and $x \in \mathbb{F}_q$, $x^a = x^{a^*}$. We always assume that $1 \le k \le q-1$; additional assumptions on k, when they apply, will be included in the context.

Lemma 5.2.1 *For $1 \le s \le q-1$,*

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

Proof. We have

$$\begin{aligned}
\sum_{x \in \mathbb{F}_q} A_k(x)^s &= \sum_{x \in \mathbb{F}_q^*} x^{ks} \left[(x+1)^k - x^k \right]^s \\
&= \sum_{x \in \mathbb{F}_q^*} x^{ks} \sum_i \binom{s}{i} (x+1)^{ki} (-x^k)^{s-i} \\
&= \sum_{x \in \mathbb{F}_q^*} \sum_i (-1)^{s-i} \binom{s}{i} x^{2ks-ki} (x+1)^{(ki)^*} \\
&= \sum_{x \in \mathbb{F}_q^*} \sum_i (-1)^{s-i} \binom{s}{i} x^{2ks-ki} \sum_j \binom{(ki)^*}{j} x^{(ki)^*-j} \\
&= \sum_{i,j} (-1)^{s-i} \binom{s}{i} \binom{(ki)^*}{j} \sum_{x \in \mathbb{F}_q^*} x^{2ks-j}
\end{aligned}$$

$$= (-1)^{s+1}\sum_i (-1)^i \binom{s}{i} \sum_{j\equiv 2ks\,(mod\, q-1)} \binom{(ki)^*}{j}.$$

If $2ks \not\equiv 0 \pmod{q-1}$,

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

If $2ks \equiv 0 \pmod{q-1}$,

$$\begin{aligned}\sum_{x\in\mathbb{F}_q} A_k(x)^s &= (-1)^{s+1}\sum_i (-1)^i \binom{s}{i}\left[\binom{(ki)^*}{0} + \binom{(ki)^*}{q-1}\right]\\ &= (-1)^{s+1}\sum_i (-1)^i \binom{s}{i}\binom{(ki)^*}{(2ks)^*}.\end{aligned}$$

Hence (5.2.4) *always holds.*

■

Lemma 5.2.2 *(i) If q is even,*

$$\sum_{x\in\mathbb{F}_q} B_k(x)^s = \sum_{i=0}^{s}\binom{s}{i}\binom{(2ki)*}{(ks)^*}, \qquad 1 \le s \le q-1. \tag{5.2.5}$$

(ii) If q is odd,

$$\sum_{x\in\mathbb{F}_q} B_k(x)^s = -(-2)^s\sum_{i,j} 2^{-i}(-1)^j\binom{s}{i}\binom{i}{j}\binom{(2kj)*}{(ki)^*}, \qquad 1 \le s \le q-1. \tag{5.2.6}$$

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

$$\begin{aligned}
\sum_{x\in\mathbb{F}_q} B_k(x)^s &= \sum_{x\in\mathbb{F}_q^*} \Big(\big[(x+1)^{2k}+1\big]x^{-k}\Big)^s \\
&= \sum_{x\in\mathbb{F}_q^*} x^{-ks}\big[(x+1)^{2k}+1\big]^s \\
&= \sum_{x\in\mathbb{F}_q^*} x^{-ks} \sum_i \binom{s}{i} (x+1)^{(2ki)^*} \\
&= \sum_{x\in\mathbb{F}_q^*} x^{-ks} \sum_i \binom{s}{i} \sum_j \binom{(2ki)^*}{j} x^j \\
&= \sum_{i,j} \binom{s}{i} \binom{(2ki)^*}{j} \sum_{x\in\mathbb{F}_q^*} x^{j-ks} \\
&= \sum_i \binom{s}{i} \sum_{j\equiv ks \pmod{q-1}} \binom{(2ki)^*}{j}.
\end{aligned}$$

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 $ks \equiv 0 \pmod{q-1}$,

$$\sum_{x\in\mathbb{F}_q} B_k(x)^s = \sum_i \binom{s}{i}\Big[\binom{(2ki)^*}{0} + \binom{(2ki)^*}{q-1}\Big] = \sum_i \binom{s}{i}\binom{(2ki)^*}{(ks)^*}.$$

(ii) We have

$$\begin{aligned}\sum_{x\in\mathbb{F}_q} B_k(x)^s &= \sum_{x\in\mathbb{F}_q^*}\Big(\big[(x+1)^{2k}-1\big]x^{-k}-2\Big)^s \\ &= \sum_{x\in\mathbb{F}_q^*}\sum_i \binom{s}{i}\big[(x+1)^{2k}-1\big]^i x^{-ki}(-2)^{s-i} \\ &= (-2)^s\sum_{x\in\mathbb{F}_q^*}\sum_i(-2)^{-i}\binom{s}{i}x^{-ki}\sum_j\binom{i}{j}(x+1)^{(2kj)^*}(-1)^{i-j} \\ &= (-2)^s\sum_{x\in\mathbb{F}_q^*}\sum_{i,j}2^{-i}(-1)^j\binom{s}{i}\binom{i}{j}x^{-ki}\sum_l\binom{(2kj)^*}{l}x^l \\ &= (-2)^s\sum_{i,j,l}2^{-i}(-1)^j\binom{s}{i}\binom{i}{j}\binom{(2kj)^*}{l}\sum_{x\in\mathbb{F}_q^*}x^{l-ki} \\ &= -(-2)^s\sum_{i,j}\sum_{l\equiv ki\,(\mathrm{mod}\,q-1)}2^{-i}(-1)^j\binom{s}{i}\binom{i}{j}\binom{(2kj)^*}{l}.\end{aligned}$$

Note that if $l \equiv ki \pmod{q-1}$ and $0 \le l \le (2kj)^*$, then either $l = (ki)^*$ or $i = 0$, $j > 0$ and $l = q-1$; in the latter case, $\binom{i}{j} = 0$. Therefore, we have

$$\sum_{x\in\mathbb{F}_q} B_k(x)^s = -(-2)^s\sum_{i,j}2^{-i}(-1)^j\binom{s}{i}\binom{i}{j}\binom{(2kj)^*}{(ki)^*}.$$

■

Theorem 5.2.3 *(i) A_k is a PP of $\mathbb{F}_q$ if and only if* $\gcd(k, q-1) = 1$ *and*

$$\sum_i(-1)^i\binom{s}{i}\binom{(ki)^*}{(2ks)^*} = 0 \quad \text{for all } 1 \le s \le q-2. \tag{5.2.7}$$

(ii) B_k is a PP of $\mathbb{F}_q$ if and only if $\gcd(k, q-1) = 1$ *and*

$$\sum_i(-1)^i\binom{s}{i}\binom{(2ki)^*}{(ks)^*} = (-2)^s \quad \text{for all } 1 \le s \le q-2. \tag{5.2.8}$$

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), $\sum_{x\in\mathbb{F}_q} A_k(x)^s = 0$ for all $1 \le s \le q-2$ 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 $B_k = [(\mathtt{x}+1)^{2k} - 1]\mathtt{x}^{q-1-k}$.

If $q = 2$, then $k = 1$ and $B_k = \mathtt{x}^2$, 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 $1 \le s \le q-2$ 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 $\gcd(k, (q-2)/2) = 1$,

$$\sum_{i,j} 2^{-i}(-1)^j \binom{s}{i}\binom{i}{j}\binom{(2kj)^*}{(ki)^*} = \begin{cases} 0 & \text{for } 1 \le s \le q-2, \\ 1 & \text{for } s = q-1, \end{cases} \tag{5.2.9}$$

if and only if (5.2.8) holds. Set

$$S_i = 2^{-i}\sum_j (-1)^j \binom{i}{j}\binom{(2kj)^*}{(ki)^*}, \qquad 0 \le i \le q-1.$$

Then (5.2.9) is equivalent to

$$\sum_i \binom{s}{i} S_i = \begin{cases} 1 & \text{if } s = 0, \\ 0 & \text{if } 1 \le s \le q-2, \\ 1 & \text{if } s = q-1. \end{cases} \tag{5.2.10}$$

Equation (5.2.10) is a recursion for S_i, which has a unique solution

$$S_i = \begin{cases} (-1)^i & \text{if } 0 \le i \le q-2, \\ 2 & \text{if } i = q-1. \end{cases}$$

Therefore, (5.2.9) is equivalent to

$$\sum_j (-1)^j \binom{i}{j} \binom{(2kj)^*}{(ki)^*} = \begin{cases} (-2)^i & \text{if } 0 \le i \le q-2, \\ 2 & \text{if } i = q-1. \end{cases} \tag{5.2.11}$$

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 $i = q-1$,

$$\begin{aligned} \sum_j (-1)^j \binom{i}{j} \binom{(2kj)^*}{(ki)^*} &= \sum_{j=\frac{q-1}{2},\, q-1} (-1)^j \binom{q-1}{j} \binom{(2kj)^*}{q-1} \\ &= (-1)^{\frac{q-1}{2}} \binom{-1}{\frac{q-1}{2}} + (-1)^{q-1} \binom{-1}{q-1} = 2. \end{aligned}$$

3° 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 concering A_k and B_k

Assume that $q > 2$ and $1 \le k \le q-1$, and let

$$a := \left\lfloor \frac{q-1}{k} \right\rfloor. \tag{5.3.12}$$

When $\gcd(k, q-1) = 1$, let $k', b \in \{1, \dots, q-1\}$ be such that

$$k'k \equiv 1 \pmod{q-1}, \qquad bk \equiv -1 \pmod{q-1}, \tag{5.3.13}$$

and set

$$c := \left\lfloor \frac{q-1}{k'} \right\rfloor. \tag{5.3.14}$$

Note that

$$\frac{q-1}{a+1} < k \le \frac{q-1}{a} \tag{5.3.15}$$

and

$$\frac{q-1}{c+1} < k' \le \frac{q-1}{c}. \tag{5.3.16}$$

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* $1 < k \le q-1$ *and* A_k *is a PP of* $\mathbb{F}_q$*, then*

$$\binom{ka}{q-1-ka} \equiv 0 \pmod{p}, \tag{5.3.17}$$

$$\binom{2c}{c} \equiv 0 \pmod{p}. \tag{5.3.18}$$

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

$$\frac{q-1}{a+1} < k < \frac{q-1}{a}. \tag{5.3.19}$$

Therefore

$$q - 1 < k(a+1) \le 2ka < 2(q-1),$$

which implies that $(2ka)^* = 2ka - q + 1$. By (5.2.7),

$$\begin{aligned} 0 &= \sum_i (-1)^i \binom{a}{i} \binom{(ki)^*}{(2ka)^*} = \sum_{2a - \frac{q-1}{k} \le i \le a} (-1)^i \binom{a}{i} \binom{ki}{2ka - q + 1} \\ &= (-1)^a \binom{ka}{2ka - q + 1} = (-1)^a \binom{ka}{q - 1 - ka}. \end{aligned}$$

(Note: in the above, $2a - (q-1)/k \le i \le a$ 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 $c \le (q-1)/2$. Since $\gcd(k', q-1) = 1$, (5.3.16) becomes

$$\frac{q-1}{c+1} < k' < \frac{q-1}{c}. \tag{5.3.20}$$

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

$$s = q - 1 - ck', \tag{5.3.21}$$

and

$$(2ks)^* = q - 1 - 2c. \tag{5.3.22}$$

By (5.2.7),

$$0 = \sum_i (-1)^i \binom{s}{i} \binom{(ki)^*}{(2ks)^*} = \sum_i (-1)^i \binom{s}{i} \binom{(ki)^*}{q - 1 - 2c}. \tag{5.3.23}$$

For each $0 \le l \le 2c$, let $i(l) \in \{0, \dots, q-1\}$ be such that $(ki(l))^* = q - 1 - l$. Because of (5.3.20), we have

$$i(l) = \begin{cases} q - 1 - lk' & \text{if } 0 \le l \le c, \\ 2(q-1) - lk' & \text{if } c + 1 \le l \le 2c. \end{cases}$$

When $0 \le l < c$,

$$i(l) = q - 1 - lk' > q - 1 - ck' = s.$$

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

$$0 = (-1)^s \binom{q-1-c}{q-1-2c} = (-1)^s \binom{q-1-c}{c} = (-1)^s \binom{-1-c}{c} = (-1)^{s+c} \binom{2c}{c}.$$

■

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 $\mathbb{F}_q$.

■

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 $k'_{e-1}c \le p-1$. It follows that $k'_{e-1} \le (p-1)/c < 2$. Replacing k' with $(p^{e-1-i}k')^*$ (and k with $(p^{1+i}k)^*$), we also have $k'_i < 2$.

■

Lemma 5.3.6 *Assume that q is odd and B_k is a PP of $\mathbb{F}_q$. Then*

$$(-2)^{k-1} \equiv 1 \pmod{p}.$$

Proof. We first claim that $k \ne q-1$. If, to the contrary, $k = q-1$, since $\gcd(k, (q-1)/2) = 1$ (proof of Theorem 5.2.3, Case 2, 1°), we must have $q = 3$ and $k = 2$. But then $B_k = (X+1)^4 - 1 - 2X^2 \equiv 2X(X+1) \pmod{X^3 - X}$, which is not a PP of $\mathbb{F}_3$.

Since B_k is a PP of $\mathbb{F}_q$, $f := [(\mathtt{x}+1)^{2k} - 1]/\mathtt{x}^k$ is one-to-one on $\mathbb{F}_q^*$. Since $B_k(0) = 0$, we have $f(x) \ne 2$ for all $x \in \mathbb{F}_q^*$. Define $f(0) = 2$. Then $f : \mathbb{F}_q \to \mathbb{F}_q$ is a bijection with $f(-2) = 0$. Thus

$$-1 = \prod_{x \in \mathbb{F}_q \setminus \{-2\}} f(x) = 2 \prod_{x \in \mathbb{F}_q \setminus \{0,-2\}} \frac{(x+1)^{2k} - 1}{x^k} = 2^{k+1} \prod_{x \in \mathbb{F}_q \setminus \{\pm 1\}} (x^k + 1)(x^k - 1). \tag{5.3.24}$$

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

$$-1 = 2^{k+1}\Big(-\frac{1}{2}\Big)\frac{1}{2},$$

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

$$\prod_{\alpha\in S}(\mathtt{x}-\alpha)=\mathtt{x}^{(q-1)/2}-1. \tag{5.3.25}$$

Setting $\mathtt{x}=-1$ 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),

$$\prod_{\alpha\in S\setminus\{1\}}(\mathtt{x}+1-\alpha)=\frac{(\mathtt{x}+1)^{(q-1)/2}-1}{\mathtt{x}}=\sum_{i=1}^{(q-1)/2}\binom{(q-1)/2}{i}\mathtt{x}^{i-1}. \tag{5.3.27}$$

Setting $\mathtt{x}=0$ 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),

$$\prod_{x\in\mathbb{F}_q\setminus\{\pm1\}}(x^k+1)=\prod_{x\in\mathbb{F}_q\setminus\{\pm1\}}(x^2+1)=\Big(\prod_{\alpha\in S\setminus\{1\}}(\alpha+1)\Big)^2=1,$$

$$\prod_{x\in\mathbb{F}_q\setminus\{\pm1\}}(x^k-1)=\Big(\prod_{\alpha\in S\setminus\{1\}}(\alpha-1)\Big)^2=\frac{1}{4}.$$

Thus (5.3.24) becomes $2^{k-1}=-1$.

■

Lemma 5.3.7 *Assume that q is odd, $1<k\le q-1$, and B_k is a PP of $\mathbb{F}_q$. Then k is odd, a and c are even, and*

$$2^{k-1}=1, \tag{5.3.29}$$

$$\binom{a}{\frac{a}{2}}=(-1)^{\frac{a}{2}}2^a, \tag{5.3.30}$$

$$\binom{a-1}{\frac{a}{2}}\binom{ka}{k} = (-1)^{\frac{a}{2}-1}2^{a-1}, \tag{5.3.31}$$

$$\binom{b}{\frac{q-1}{2}} = (-1)^{b+\frac{q+1}{2}}2^{b}, \tag{5.3.32}$$

$$\binom{q-1-ck'}{\frac{1}{2}(q-1-ck')} = (-1)^{\frac{c}{2}+\frac{q-1}{2}}2^{-ck'}, \tag{5.3.33}$$

$$(-c+1)\binom{q-1-(c-1)k'}{\frac{1}{2}[q-1-(c-2)k']} = (-1)^{\frac{c}{2}+\frac{q-1}{2}}2^{-(c-1)k'}. \tag{5.3.34}$$

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

$$\sum_i (-1)^i \binom{\frac{q-1}{2}}{i}\binom{(2ki)^*}{q-1} = (-2)^{\frac{q-1}{2}}. \tag{5.3.35}$$

Since $\gcd(2k,q-1)=2$, $(q-1)/2$ is odd. In the above,

$$\binom{\frac{q-1}{2}}{i}\binom{(2ki)^*}{q-1} \neq 0$$

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),

$$\sum_i (-1)^i \binom{a}{i}\binom{(2ki)^*}{ka} = (-2)^a. \tag{5.3.36}$$

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),

$$\sum_i (-1)^i \binom{a-1}{i}\binom{(2ki)^*}{k(a-1)} = (-2)^{a-1}. \tag{5.3.37}$$

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),

$$(-2)^b = \sum_i (-1)^i \binom{b}{i}\binom{(2ki)^*}{(kb)^*} = \sum_i (-1)^i \binom{b}{i}\binom{(2ki)^*}{q-2}. \tag{5.3.38}$$

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

$$\frac{q-1}{c+1} < k' < \frac{q-1}{c}. \tag{5.3.39}$$

Let $s = (cb)^*$. Then we have

$$s = q - 1 - ck',$$
$$(ks)^* = q - 1 - c.$$

By (5.2.8),

$$\sum_i (-1)^i \binom{s}{i} \binom{(2ki)^*}{q-1-c} = (-2)^s. \tag{5.3.40}$$

For $0 \le l \le c/2$, 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 $i \le s$ only if $l = c/2$. In fact, $\frac{1}{2}(q-1) - lk' = i \le s = q - 1 - ck'$ implies that

$$k' \le \frac{q-1}{2(c-l)},$$

which, by (5.3.39), implies that $2(c-l) \le c$, i.e., $l \ge c/2$.

Therefore, the ith 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

$$(-1)^{\frac{1}{2}(q-1-ck')} \binom{q-1-ck'}{\frac{1}{2}(q-1-ck')} = (-2)^{-ck'},$$

which is (5.3.33).

To prove (5.3.34), we choose $s = ((c-1)b)^*$. We have

$$s = q - 1 - (c-1)k',$$
$$(ks)^* = q - 1 - (c-1),$$

and (5.2.8) gives

$$\sum_i (-1)^i \binom{s}{i} \binom{(2ki)^*}{q-1-(c-1)} = (-2)^s. \tag{5.3.41}$$

For $0 \le l \le c/2 - 1$, let $i \in \{0, \dots, q-1\}$ be such that $(2ki)^* = q - 1 - 2l$. Then

$$i = q - 1 - lk' \quad \text{or} \quad \frac{1}{2}(q-1) - lk'.$$

If $i = q-1-lk'$, then $i > s$. If $i = \frac{1}{2}(q-1) - lk'$, then $i \le s$ only if $l = c/2 - 1$. In fact, $i \le s$ implies that

$$k' \le \frac{q-1}{2(c-1-l)},$$

which further implies that $2(c-1-l) \le c$, i.e., $l \ge c/2 - 1$. Therefore, the ith 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

$$\begin{aligned} -2^{-(c-1)k'} &= (-1)^{\frac{c}{2}-1+\frac{q-1}{2}} \binom{q-1-(c-1)k'}{\frac{1}{2}[q-1-(c-2)k']} \binom{q-1-2(\frac{c}{2}-1)}{q-1-(c-1)} \\ &= (-1)^{\frac{c}{2}-1+\frac{q-1}{2}} \binom{q-1-(c-1)k'}{\frac{1}{2}[q-1-(c-2)k']} (-c+1), \end{aligned}$$

which is (5.3.34).

■

For each odd prime p, let

$$\alpha(p) = \min\Big\{u : u \text{ is a positive even integer, } \binom{u}{u/2} \equiv (-1)^{\frac{u}{2}} 2^u \pmod{p}\Big\}. \tag{5.3.42}$$

Remark 5.3.8 Since

$$\binom{p-1}{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

we always have $\alpha(p) \le p-1$.

Lemma 5.3.9 *Assume that q is odd and $1 < k \le q-1$. If B_k is a PP of $\mathbb{F}_q$, then all the base p digits of k are $\le (p-1)/\alpha(p)$.*

Proof. By (5.3.30), $a = \lfloor (q-1)/k \rfloor \ge \alpha(p)$. Let $q = p^e$ and write $k = k_0 p^0 + \cdots + k_{e-1}p^{e-1}$, where $0 \le k_i \le p-1$. We first show that $k_{e-1} \le (p-1)/\alpha(p)$. Assume that

$k_{e-1} > 0$. Since

$$a \le \frac{q-1}{k} \le \frac{p^e-1}{k_{e-1}p^{e-1}},$$

we have

$$k_{e-1}a \le p - \frac{1}{p^{e-1}}.$$

Thus $k_{e-1}a \le p-1$, and hence $k_{e-1} \le (p-1)/a \le (p-1)/\alpha(p)$.

Replacing k with $(p^{e-1-i}k)^*$, we conclude that $k_i \le (p-1)/\alpha(p)$.

■

We include a quick proof for Theorem 5.1.2.

Proof. [Proof of Theorem 5.1.2] Let $q = p^e$. Assume that $1 < k \le q^m - 1$ and B_k is a PP of $\mathbb{F}_{q^m}$. Write $k = k_0q^0 + \cdots + k_{m-1}q^{m-1}$, $0 \le k_i \le q-1$. By Lemma 5.3.9, all the base p digits of k are $\le \lfloor (p-1)/\alpha(p) \rfloor$. Hence

$$k_i \le \left\lfloor \frac{p-1}{\alpha(p)} \right\rfloor \frac{q-1}{p-1}, \qquad 0 \le i \le m-1.$$

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,

$$k_0 + \cdots + k_{m-1} \le m \left\lfloor \frac{p-1}{\alpha(p)} \right\rfloor \frac{q-1}{p-1} \le q-1.$$

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* $\mathrm{gpf}(e) \le p-1$.

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 $1 \le m \le p-1$. 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 $1 \le k \le q^m - 2$. Let $k' \in \{1, \dots, q^m - 2\}$ be such that $k'k \equiv 1 \pmod{q^m - 1}$. It suffices to show that k' is a power of p. Write $k' = k'_0 q^0 + \cdots + k'_{m-1} q^{m-1}$, $0 \le k'_i \le q - 1$. 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 ≤ 1. Hence

$$k'_i \le \frac{q-1}{p-1}, \qquad 0 \le i \le m-1.$$

Therefore,

$$k'_0 + \cdots + k'_{m-1} \le \frac{q-1}{p-1} m \le q - 1. \tag{5.4.44}$$

Combining (5.4.43) and (5.4.44) gives $k'_0 + \cdots + k'_{m-1} = 1$.

■

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 $k \in \{1, \dots, p^e - 1\}$ which is not a power of p. Then with the help of Lemma 5.5.1, $a := \lfloor (p^e - 1)/k \rfloor \equiv 0 \pmod{p}$. However, (5.3.31) dictates that $a \not\equiv 0 \pmod{p}$, hence a contradiction.

Lemma 5.5.1 *Let $p \ge 3$ be a prime. Let i, j, e be integers such that $0 < i < j \le e-1$,* *and let*

$$\begin{aligned}
&k = k_0p^0 + \cdots + k_{i-1}p^{i-1} + p^i + p^j, \quad k_0, \dots, k_{i-1} \in \{0, \dots, p-1\},\\
&a = \Big\lfloor \frac{p^e-1}{k} \Big\rfloor,\\
&u = \Big\lfloor \frac{e-j}{j-i} \Big\rfloor.
\end{aligned}$$

Assume that a is even and

$$\frac{p^e-1}{p^i+p^j} - \frac{p^e-1}{k} \le 1. \tag{5.5.45}$$

Then

$$a = \begin{cases} p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^{u(i-j)}\big] & \textit{if } u \textit{ is odd,} \\ p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^{u(i-j)}\big] - 1 & \textit{if } u \textit{ is even.} \end{cases} \tag{5.5.46}$$

Proof. Write $e - j = u(i-j) + r$, $0 \le r < j - i$. We have

$$\begin{aligned}
\frac{p^e-1}{p^i+p^j} =& p^{e-j}\frac{1}{1+p^{i-j}} - \frac{1}{p^i+p^j}\\
=& p^{e-j}\big[1 - p^{i-j} + p^{2(i-j)} - \cdots\big] - \frac{1}{p^i+p^j}\\
=& p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)}\big]\\
&\quad + (-1)^{u+1}p^{r+i-j}\big[1 - p^{i-j} + p^{2(i-j)} - \cdots\big] - \frac{1}{p^i+p^j}\\
=& p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)}\big] + (-1)^{u+1}p^{r+i-j}\frac{1}{1+p^{i-j}} - \frac{1}{p^i+p^j}\\
=& p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)}\big] + \frac{1}{p^i+p^j}\big[(-1)^{u+1}p^{r+i} - 1\big].
\end{aligned}$$

Since $r + i < j$, we have

$$\begin{aligned}
0 < \frac{1}{p^i+p^j}\big[(-1)^{u+1}p^{r+i} - 1\big] < 1 \quad \text{if } u \text{ is odd},\\
-1 < \frac{1}{p^i+p^j}\big[(-1)^{u+1}p^{r+i} - 1\big] < 0 \quad \text{if } u \text{ is even}.
\end{aligned}$$

Thus

$$\Big\lfloor\frac{p^e-1}{p^i+p^j}\Big\rfloor=\begin{cases}p^{e-j}\big[1-p^{i-j}+\cdots+(-1)^u p^{u(i-j)}\big] & \text{if } u \text{ is odd,}\\ p^{e-j}\big[1-p^{i-j}+\cdots+(-1)^u p^{u(i-j)}\big]-1 & \text{if } u \text{ is even.}\end{cases}\tag{5.5.47}$$

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.

■

Theorem 5.5.2 *Conjecture B is true for $q = p^e$, where p is an odd prime such that $\alpha(p) > (p-1)/2$.*

Proof. Assume to the contrary that there exists $k \in \{1,\dots,p^e-1\}$, which is not a power of p, such that B_k is a PP of $\mathbb{F}_{p^e}$. Write

$$k = k_0p^0+\cdots+k_{e-1}p^{e-1},\quad 0\le k_i\le p-1.$$

Since $\alpha(p) > (p-1)/2$, by Lemma 5.3.9, $k_i \le 1$ for all i. Let

$$a=\Big\lfloor\frac{p^e-1}{k}\Big\rfloor.$$

By Lemma 5.3.7, a is even, and by (5.3.31),

$$\binom{ka}{k}\not\equiv 0\pmod{p}.$$

In particular, $a\not\equiv 0 \pmod p$.

Let d be the distance in $\mathbb{Z}/e\mathbb{Z}$ defined by

$$d([x],[y])=\min\{|x-y|,\, e-|x-y|\},\quad x,y\in\{0,\dots,e-1\}.$$

This is the arc distance with $[0],\dots,[e-1]$ 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 $1\le l<e$. The 1's among $k_0,\dots,k_{e-1}$ 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

$$(k_0, \dots, k_{e-1}) = (\overset{0}{*} \ \cdots \ * \ \overset{i}{1} \ \underbrace{0 \ \cdots \ 0}_{l-1} \ \overset{j}{1} \ \underbrace{0 \ \cdots \ \overset{e-1}{0}}_{l}),$$

where $j = e-1-l$, $i = j-l = e-1-2l$. We have

$$u = \Big\lfloor \frac{e-j}{j-i} \Big\rfloor = \Big\lfloor \frac{l+1}{l} \Big\rfloor = \begin{cases} 2 & \text{if } l = 1, \\ 1 & \text{if } l \geq 2. \end{cases}$$

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

$$\begin{aligned} \frac{p^e-1}{p^i+p^j} - \frac{p^e-1}{k} &= (p^e-1)\Big[\frac{1}{p^i+p^j} - \frac{1}{k_0p^0+\cdots+k_ip^i+p^j}\Big] \\ &< (p^e-1)\left[\frac{1}{p^i+p^j} - \frac{1}{\frac{p^j}{p-1}+p^j}\right] \\ &= (p^e-1)\frac{1}{p^j}\Big[\frac{p}{p+1} - \frac{p-1}{p}\Big] \\ &= \frac{p^e-1}{p^jp(p+1)} < p^{e-j-2} = 1. \end{aligned}$$

Thus by (5.5.46),

$$a = p^{e-j}\big[1 - p^{i-j} + \cdots + (-1)^u p^{u(i-j)}\big] - 1 = p^2(1-p^{-1}) \equiv 0 \pmod{p},$$

which is a contradiction.

Case 2. Assume that $l \geq 2$. Since the distance between the indices of any two consecutive 1's among $k_0, \dots, k_{e-1}$ 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

$$\begin{aligned}\frac{p^e-1}{p^i+p^j}-\frac{p^e-1}{k} &= (p^e-1)\Big[\frac{1}{p^i+p^j}-\frac{1}{k_0p^0+\cdots+k_ip^i+p^j}\Big]\\ &< (p^e-1)\Big[\frac{1}{p^i+p^j}-\frac{1}{\frac{p^l}{p^l-1}p^i+p^j}\Big]\\ &= \frac{p^e-1}{p^l-1}\frac{p^i}{(p^i+p^j)\big(\frac{p^l}{p^l-1}p^i+p^j\big)}\\ &< \frac{p^{e+i}}{p(p^i+p^j)\big(\frac{p^l}{p^l-1}p^i+p^j\big)}\\ &< \frac{p^{e+i}}{p^{2j+1}} = p^{e+e-1-2l-2(e-1-l)-1} = 1.\end{aligned}$$

Therefore by (5.5.46),

$$a = p^{e-j}\big[1-p^{i-j}+\cdots+(-1)^u p^{u(i-j)}\big] = p^{l+1}(1-p^{-l}) \equiv 0 \pmod p,$$

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 $\alpha(p) \le (p-1)/2$; this follows from a symmetry described below.

Note that for integer $m \ge 0$,

$$2^{-2m}\binom{2m}{m} = \frac{(2m)!}{(2^m \cdot m!)^2} = \frac{(2m-1)!!}{(2m)!!}.$$

Thus $\alpha(p)$ is the smallest positive even integer $2m$ ($\le p-1$) such that

$$\frac{(2m-1)!!}{(2m)!!} \equiv (-1)^m \pmod p. \tag{5.5.48}$$

Let $0 \le m \le (p-1)/2$. Since

$$\begin{aligned}
&2^{-2m}\binom{2m}{m}\left[2^{-(p-1-2m)}\binom{p-1-2m}{\frac{p-1}{2}-m}\right]^{-1}\\
&=\frac{(2m-1)!!}{(2m)!!}\cdot\frac{(p-1-2m)!!}{(p-2-2m)!!}=\frac{(p-2)!!}{(p-1)!!}=\prod_{\substack{2\le i\le p-1\\ i\,\text{even}}}\frac{p-i}{i}=(-1)^{\frac{p-1}{2}},
\end{aligned}$$

condition (5.5.48) is symmetric for m and $(p-1)/2-m$.

For integers $i \le j$, denote $i(i+1)\cdots j$ by $[i,j]$. Then we have

$$\begin{aligned}
\binom{2m}{m}&=\frac{[m+1,2m]}{[1,m]},\\
\binom{p-1-2m}{\frac{p-1}{2}-m}&=\frac{[\frac{p+1}{2}-m,p-1-2m]}{[1,\frac{p-1}{2}-m]}=\frac{[2m+1,\frac{p-1}{2}+m]}{[\frac{p+1}{2}+m,p-1]}.
\end{aligned}$$

Hence

$$\begin{aligned}
\binom{2m}{m}\binom{p-1-2m}{\frac{p-1}{2}-m}&=\frac{[m+1,m+\frac{p-1}{2}]}{[1,m][m+\frac{p+1}{2},p-1]}=\frac{[m+1,m+\frac{p-1}{2}]^2}{[1,p-1]}\\
&=-\Big[m+1,m+\frac{p-1}{2}\Big]^2.
\end{aligned}$$

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 $1 \le k \le q-1$ 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 $k \in \{1,\dots,q-1\}$ 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, $1 < k \le q-1$, and both A_k and B_k are PPs of $\mathbb{F}_q$. Then c is even and*

$$2^{-2ck'} = \binom{2(q-1)-2ck'}{q-1-ck'} + (-1)^{\frac{q-1}{2}+\frac{c}{2}+1}\binom{2(q-1)-2ck'}{\frac{1}{2}(q-1)-(\frac{c}{2}-1)k'}\binom{2c}{c+2}. \quad (5.6.49)$$

Proof. By Lemma 5.3.7, c is even. Let $s = (2cb)^*$. Since $2cb \not\equiv 0 \pmod{q-1}$, we have $1 \le s \le q-2$. Clearly, $2ck' > q-1$. (Otherwise, $2c \le (q-1)/k'$, which implies that $2c \le c$, 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 $k' < (q-1)/2 \le 2$, which implies that $k' = 1$, i.e., $k = 1$, which is a contradiction.) Thus

$$(ks)^* = q - 1 - 2c.$$

By (5.2.8),

$$\sum_i (-1)^i \binom{s}{i}\binom{(2ki)^*}{q-1-2c} = (-2)^s. \quad (5.6.50)$$

For each $0 \le l \le c$, let $i \in \{0, \dots, q-1\}$ 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 $0 \le i \le s$.

Case 1. Assume that $i = \frac{3}{2}(q-1) - lk'$. In this case,

$$\begin{aligned} i &\ge \frac{3}{2}(q-1) - ck' > 2(q-1) - 2ck' \qquad (\text{since } 2ck' > q-1) \\ &= s. \end{aligned}$$

Case 2. Assume that $i = q - 1 - lk'$. In this case we always have $i \geq 0$. Moreover,

$$\begin{aligned} i \leq s &\Leftrightarrow q - 1 - lk' \leq 2(q-1) - 2ck' \\ &\Leftrightarrow l \geq 2c - \frac{q-1}{k'} \\ &\Leftrightarrow l \geq c. \end{aligned}$$

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,

$$\begin{aligned} i \leq s &\Leftrightarrow \frac{1}{2}(q-1) - lk' \leq 2(q-1) - 2ck' \\ &\Leftrightarrow l \geq 2c - \frac{3}{2} \cdot \frac{q-1}{k'} \\ &\Rightarrow l > 2c - \frac{3}{2}(c+1) \\ &\Rightarrow l \geq \frac{c}{2} - 1. \end{aligned}$$

Combining the above three cases, we see that (5.6.50) becomes

$$\begin{aligned} 2^{-2ck'} = &\binom{2(q-1) - 2ck'}{q - 1 - ck'} \\ &+ (-1)^{\frac{q-1}{2} + \frac{c}{2} + 1} \binom{2(q-1) - 2ck'}{\frac{1}{2}(q-1) - (\frac{c}{2} - 1)k'} \binom{q - 1 - 2(\frac{c}{2} - 1)}{q - 1 - 2c} \\ &+ (-1)^{\frac{q-1}{2} + \frac{c}{2}} \binom{2(q-1) - 2ck'}{\frac{1}{2}(q-1) - \frac{c}{2}k'} \binom{q - 1 - c}{q - 1 - 2c}. \end{aligned} \tag{5.6.51}$$

In the above,

$$\binom{q - 1 - 2(\frac{c}{2} - 1)}{q - 1 - 2c} = \binom{-c + 1}{2 + c} = \binom{2c}{c + 2},$$

and, by (5.3.18),

$$\binom{q - 1 - c}{q - 1 - 2c} = \binom{-1 - c}{c} = \binom{2c}{c} = 0.$$

Hence (5.6.49) follows from (5.6.51).

■

Theorem 5.6.2 *Conjecture 5.1.1 is true.*

Proof. Assume to the contrary that Conjecture 5.1.1 is false. Then there exists $1 \le k \le q-1$, 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 ≤ 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,

$$\binom{2c}{c+2} = 0. \tag{5.6.52}$$

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

$$\binom{2(q-1)-2ck'}{q-1-ck'} = 0. \tag{5.6.53}$$

Combining (5.6.49), (5.6.52) and (5.6.53), we have a contradiction.

■

6 Conclusion

This dissertation started with the goal of completely characterizing the permutation behavior of the family of polynomials $g_{n,q}$. Unfortunatelty this problem turned quite challenging and still remains an open problem.

Sticking with the theme of "discovering" these naturally occuring 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 polynomails of the form $f = \mathtt{x}^d(a + b\mathtt{x}^{q-1} + \mathtt{x}^{r(q-1)})$ 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

[1] A. Akbary, D. Ghioca, Q. Wang, *On constructing permutations of finite fields*, Finite Fields Appl. **17** (2011), 51 – 67.

[2] S. Ball and M. Zieve, *Symplectic spreads and permutation polynomials*, in: Finite Fields and Applications, in: Lect. Notes. Comput. Sci., vol. **2948**, Springer, Berlin, 2004, pp.79–88.

[3] E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptol. **4** (1991), 3–72

[4] B. Bollobás, *Modern Graph Theory*, Springer-Verlag, New York, 1998.

[5] J. A. Bondy and M. Simonovits, *Cycles of even length in graphs*, J. Combin. Theory, Ser. B **16** (1974), 97 – 105.

[6] J. A. Bondy, *Extremal problems of Paul Erdös on circuits in graphs*, Paul Erdös and His Mathematics. II, Bolyai Society, Mathematical Studies, 11, Budapest, 2002, 135 – 156.

[7] F. Brioschi, *Des substitutions de la forme* $\theta(r) \equiv \varepsilon\big(r^{n-2} + ar^{\frac{n-3}{2}}\big)$ *pour un nombre* n *premier de lettres*, Math. Ann. **2** (1870), 467 – 470.

[8] F. Brioschi, *Un teorema sulla teoria delle sostituzioni*, Rend. Reale Ist. Lombardo Sci. Lett. (2) **12** (1879), 483 – 485.

[9] K. A. Browning, J. F. Dillon, M. T. McQuistan, A. J. Wolfe, *An APN permutation in dimension six*, Finite Fields: Theory and Applications, 33–32, Contempm Math., **518**, Amer. Math. Soc., Providence, RI, 2010

[10] L. Carlitz, *Some theorems on permutation polynomials*, Bull. Amer. Math. Soc. **68** (1962), 120 – 122.

[11] L. Carlitz, *Permutations in finite fields*, Acta Sci. Math. (Szeged) **24** (1963), 196 – 203.

[12] L. Carlitz and C. Wells, *The number of solutions of a special system of equations in a finite field*, Acta Arith **12** (1966/1967), 77 – 84.

[13] P. Charpin and G. M. Kyureghyan, *When does $G(x) + \gamma\, Tr(H(x))$ permute $\mathbb{F}_{p^n}$?* Finite Fields Appl. **15** (2009), 615 – 632.

[14] P. Charpin and G. M. Kyureghyan, *Monomial functions with linear structure and permutation polynomials*, Finite Fields: Theory and Applications, 99 – 111, Contemp. Math., **518**, Amer. Math. Soc., Providence, RI, 2010.

[15] W. Cherowitzo, *α-flocks and hyperovals*, Geom. Dedic. **72** (1998) 221–246

[16] L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. of Math. **15** (1897), 65-120, 161-183.

[17] L. E. Dickson, *Linear Groups: with an Exposition of the Galois Field Theory*, Dover Publications, Inc., New York, 1958.

[18] L. E. Dickson, *History of the Theory of Numbers*, vol. 3, Carnegie Institute, Washington, D.C., 1923, Dover, New York, 2005.

[19] J. F. Dillon, *Geometry, codes and difference sets: exceptional connections*, in: Ohio State Uni. Math. Res. Inst. Publ., vol 10, de Gruyter, Berlin , 2002, pp. 73 – 85.

[20] V. Dmytrenko, F. Lazebnik, J. Williford, *On monomial graphs of girth eight*, Finite Fields Appl. **13** (2007), 828 – 842.

[21] H. Dobberitn, *Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case*, IEEE Trans. Inf. Theory **45** (1999) 1271–1275..

[22] H. Dobbertin, *Almost perfect nonlinear power functions on $GF(2^n)$: a new case for n divisble by 5*, in: Finite Fields and Applications, Springer, Berlin, 2001, pp. 113 – 121.

[23] G. Exoo and R. Jajcay, *Dynamic cage survey*, Electron. J. Combin. (2013), #DS16, 1 – 55.

[24] N. Fernando, X. Hou, *A piecewise construction of permutation polynomials over finite fields*, Finite Fields Appl. **18** (2012), 1184 – 1194.

[25] N. Fernando, X. Hou, S. D. Lappano, *A new approach to permutation polynomials over finite fields,* II, Finite Fields Appl. (2013), Available online 23 January 2013.

[26] N. Fernando, X. Hou, S. D. Lappano, *Permutation polynomials over finite fields involving* $\mathtt{x} + \mathtt{x}^q + \cdots + \mathtt{x}^{q^{a-1}}$, Discrete Mathematics **315-316** (2014) 0–11.

[27] M. Fried, *On a conjecture of Schur*, Michigan Math. J. **17** (1970) 41–55

[28] Z. Füredi and M. Simonovits, *The history of degenerate (bipartite) extremal graph problems*, Erdős centennial, 169 – 264, Bolyai Soc. Math. Stud., 25, János Bolyai Math. Soc., Budapest, 2013.

[29] R. Gold, *Maximal recursive sequences with 3-valued recursive crosscorrelation functions*, IEEE Trans. Inform. Theory 14 (1968), 154 – 156.

[30] X. Gong, *On permutation polynomials of the form $x^{1+2^k} + L(x)$*, preprint, 2014.

[31] A. Grandi, *Un teorema sulla rappresentazione analitica delle sostituzioni sopra un primo di elementi*, Giorn. Mat. Battaglini **19** (1881), 238 – 245.

[32] A. Grandi, *Generalizzazione di un teorema sulla rappresentazione analitica delle sostituzioni*, Rend. Reale Ist. Lombardo Sci. Lett. (2) **16** (1883), 101 – 111.

[33] J. Heisler, *A characterization of finite fields*, Amer. Math. Monthly **74** (1967) 537–538

[34] T. Helleseth and V. Zinoviev, *New Kloosterman sums identities over* $\mathbb{F}_{2^m}$ *for all* m, Finite Fields Appl. **9** (2003), 187 – 193.

[35] C. Hermite, *Sur les fonctions de sept lettres*, C¿ R. Acad. Sci. Paris **57**, 750–757 (1863); Oeuvres, vol. 2,pp. 280–288, Gauthier-Villars, Paris, 1908.

[36] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, The Clarendon Press, Oxford University Press, New York, 1998.

[37] X. Hou, *Solution to a problem of S. Payne*, Proc. Amer. Math. Soc., **132** (2004), 1 – 8.

[38] X. Hou, *Affinity of permutations of* $\mathbb{F}_{2^n}$, Discr. Appl. Math. vol. **154(2)** (2006) 313–325.

[39] X. Hou, *Two classes of permutation polynomials over finite fields*, J. Combin. Theory A, **118** (2011), 448 – 454.

[40] X. Hou, *A new approach to permutation polynomials over finite fields*, Finite Fields Appl. **18** (2012), 492 – 521.

[41] X. Hou, *A Class of Permutation Binomials over Finite Fields*, Journal of Number Theory, **133** (2013), 3549–3558.

[42] X. Hou, *Determination of a type of permutation trinomials over finite fields*, Acta Arith., **166** (2014), 253-278.

[43] X. Hou, *Determination of a type of permutation trinomials over finite fields, II*, Finite Fields Appl. **35** (2015), 16–35.

[44] X. Hou, *Permutation poltynomials of $\mathbb{F}_{q^2}$ of the form $a\mathtt{x} + \mathtt{x}^{r(q-1)+1}$.*, preprint

[45] X. Hou, *Permutation polynomials over finite fields — a survey of recent advances*, Finite Fields Appl. **32** (2015), 82 – 119.

[46] X. Hou, *A survey of permutation binomials and trinomials over finite fields*, Proceedings of the 11th International Conference on Finite Fields and Their Applications, Magdeburg, Germany, 2013, Contemporary Mathematics **632**, 177–191, 2015.

[47] X. Hou and S.D. Lappano, *Determination of a type of permutation binomials over finite fields*, J. Number Theory, **147** (2015), 14-23.

[48] X. Hou, S.D. Lappano and F. Lazebnik, *Proof of a conjecture on monomial graphs*, arXiv:1507.05306 (2015).

[49] X. Hou, G. L. Mullen, J. A. Sellers, J. L. Yucas, *Reversed Dickson polynomials over finite fields*, Finite Fields Appl. **15** (2009), 748 – 773.

[50] X. Hou, T. Ly, *Necessary conditions for reversed Dickson polynomials to be permutational*, Finite Fields Appl. **16** (2010), 436 – 448.

[51] T. Kasami, *The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes*, Inform. and Control 18 (1971), 369 – 394.

[52] B. G. Kronenthal, *Monomial graphs and generalized quadrangles*, Finite Fields Appl. **18** (2012), 674 – 684.

[53] S.D. Lappano, *A note regarding permutation binomials over $\mathbb{F}_{q^2}$*, Finite Fields Appl. **34** (2015), 153–160.

[54] F. Lazebnik and V. A. Ustimenko, *New examples of graphs without small cycles and of large size*, European J. Combin. **14** (1993), 445 – 460.

[55] F. Lazebnik, V.A. Ustimenko and A.J. Woldar, *A new series of dense graphs of high girth*, Bull. Amer. Math. Soc. (N.S.) **32** (1995), 73 – 79.

[56] F. Lazebnik and A. J. Woldar, *General properties of some families of graphs defined by systems of equations*, J. Graph Theory **38** (2001), 65 – 86.

[57] F. Lazebnik and D. Mubayi, *New lower bounds for Ramsey numbers of graphs and hypergraphs*, Adv. in Appl. Math. **28** (2002), 544 – 559.

[58] F. Lazebnik and J. Verstraëte, *On hypergraphs of girth five*, Electron. J. Combin. **10** (2003), R25, 1 – 15.

[59] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory*, Finite Fields Appl. **13** (2007), no. 1, 58 – 70.

[60] H. Lausch and W. Nöbauer, *Algebra of Polynomials*, North-Holland, Amsterdam, 1973.

[61] J. Levine and J. V. Brawley, *Some cryptographic applications of permutation polynomials*, Cryptologia **1**, 76–92 (1997)

[62] Y. Li and M. Wang, *On EA-equivalence of certain permutations to power mappings*, Des. Codes Cryptogr. **58** (2011), 259–269

[63] R. Lidl, G. L. Mullen, G. Turnwald, *Dickson Polynomials*, Longman Scientific and Technical, Essex, United Kingdom, 1993.

[64] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.

[65] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 197 – 240.

[66] I. G. Macdonald, *Symmetric Functions and Orthogonal Polynomials*, American Mathematical Society, Providence, RI, 1998.

[67] M. Matsui, *Linear cryptanalysis method for DES cipher*, Advances in Cryptology–EUROCRYPT'93. LNCS, vol. 765, pp.386-397. Springer-Verlag, Berlin (1993)

[68] J. E. Marcos, *Specific permutation polynomials over finite fields*, Finite Fields Appl. **17** (2011), 105 – 112.

[69] M. Miller and J. Širáň, *Moore graphs and beyond: A survey of the degree/diameter problem*, Electron. J. Combin. (2013), **20** (2), #DS14v2, 1 – 92.

[70] G.L. Mullen, D. Panario, *Handbook of Finite Fields*, Taylor & Francis, Boca Raton, 2013.

[71] H. Niederreiter and K. H. Robinson, *Complete mappings of finite fields*, J. Austral. Math. Soc. Ser. A **33** (1982), 197 – 212.

[72] K. Nyberg, *Differentially uniform mappings for cryptography*, in: Advances in Cryptology-EUROCRYPT '93, Lofthus, 1993, in: Lecture Notes in Comput. Sci., vol. 765, Springer, Berlin, 1994, pp. 55 – 64.

[73] Y.H. Park and J.B. Lee, *Permutation polynomials and group permutation polynomials*, Bull. Aust. Math. Soc. **63** (2001) 67–74

[74] E. Pasalic, *On cryptographically significant mappings over $GF(2^n)$*, Arithmetic of Finite Fields, 189–204, Lecture Notes in Comput. Sci., **5130**, Springer, Berlin, 2008

[75] E. Pasalic and P Charpin, *Some results concerning cryptographically significant mappings over $GF(2^n)$*, Des. Codes Cryptogr. **57** (2010), 257–269

[76] S. E. Payne, *Linear transformations of a finite field*, Amer. Math. Monthly **78** (1971), 659 – 660.

[77] S. E. Payne, *A complete determination of translation ovoids in finite Desarguian planes*, Lincei - Rend. Sc. fis. mat. nat. LI (1971), 328 – 331.

[78] M. Petkovsek, H. Wilf, D. Zeilberger, *A=B*, A. K. Peters, Ltd., Wellesley, MA, 1996.

[79] L. Redei and T. Szele, *Algebraisch-zahlentheoretische Betrachtungen uber Ringe I*, Acta. Math. **79** (1947) 291–320.

[80]

[81] I. Schur, *Uber den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz uber algebraische Funktionen*, Sitzungsber. Preub. Akad. Wiss. Berlin Math.-Naturwiss. Kl. **1923**, 123–134

[82] D. R. Stinson, *Cryptograohy Theory and Practice Third Edition*, Chapman & Hall, Boca Raton, 2006

D. Wan, *Permutation polynomials over finite fields*, Acta. Math. Sin. New Ser. **3** (1987) 1–5.

[83] D. Wan, R. Lidl, *Permutation polynomials of the form* $\mathrm{x}^r f(\mathrm{x}^{(q-1)/d})$ *and their group structure*, Monatshefte Math. **112** (1991) 149–163.

[84] Q. Wang *Cyclotomic mapping permutation polynomials over finite fields*, in: S.W. Golomb, G. Gong, T. Helleseth, H.-Y. Song (Eds.), Sequences, Subsequences, and Consequences, in: Lect. Notes Comput. Sci., vol. **4893**, Springer, Berlin, 2007, pp. 119-128.

[85] J. Yuan, C. Ding, H. Wang, J. Pieprzyk, *Permutation polynomials of the form* $(x^p - x + \delta)^s + L(x)$, Finite Fields Appl. **14** (2008), 482 – 493.

[86] P. Yuan and C. Ding, *Permutation polynomials over finite fields from a powerful lemma*, Finite Fields Appl. **17** (2011), 560 – 574.

[87] Z. Zha and L. Hu, *Two classes of permutation polynomials over finite fields*, Finite Fields Appl. **18** (2012), 781 – 790.

[88] M.E. Zieve, *On some permutation polynomials over* $\mathbb{F}_q$ *of the form* $x^r h(x^{(q-1)/d})$, Proc. Am. Math. Soc. **137** (2009) 2209–2216.

[89] M.E. Zieve, *Permutation polynomials on $\mathbb{F}_q$ induced from Redei function bijections on subgroups of $\mathbb{F}_q^*$*, arXiv:1310.0776, 2013.

[90] M.E. Zieve, *Permutation polynomials over $\mathbb{F}_{q^2}$ induced from novel permutations of the $(q+1)-th$ roots of unity*, preprint.

[91] X. Zeng, X. Zhu, L. Hu, *Two new permutation polynomials with the form $(x^{2^k}+x+\delta)^s+x$ over $\mathbb{F}_{2^n}$*, Appl. Algebra Engrg. Comm. Comput. **21** (2010), 145 – 150.

8 Appendices

8.1 Appendix A - Copyrights and Permissions

ELSEVIER LICENSE
TERMS AND CONDITIONS

Jul 01, 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.

License Number	3900220148493
License date	Jul 01, 2016
Licensed Content Publisher	Elsevier
Licensed Content Publication	Finite Fields and Their Applications
Licensed Content Title	A note regarding permutation binomials over Fq2
Licensed Content Author	Stephen D. Lappano
Licensed Content Date	July 2015
Licensed Content Volume Number	34
Licensed Content Issue Number	n/a
Licensed Content Pages	8
Start Page	153
End Page	160
Type of Use	reuse in a thesis/dissertation
Portion	full article
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
Estimated size (number of pages)	120
Elsevier VAT number	GB 494 6272 12

ELSEVIER LICENSE
TERMS AND CONDITIONS

Jul 01, 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.

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

ELSEVIER LICENSE
TERMS AND CONDITIONS

Jul 01, 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.

License Number	3900220605480
License date	Jul 01, 2016
Licensed Content Publisher	Elsevier
Licensed Content Publication	Discrete Mathematics
Licensed Content Title	Permutation polynomials over finite fields involving x+xq+···+xqa−1
Licensed Content Author	Neranga Fernando,Xiang-dong Hou,Stephen D. Lappano
Licensed Content Date	6 February 2014
Licensed Content Volume Number	315
Licensed Content Issue Number	n/a
Licensed Content Pages	12
Start Page	173
End Page	184
Type of Use	reuse in a thesis/dissertation
Intended publisher of new work	other
Portion	excerpt
Number of excerpts	2
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