January 2013

A Study of Permutation Polynomials over Finite Fields

Neranga Fernando
University of South Florida, wfernand@mail.usf.edu

A Study of Permutation Polynomials over Finite Fields

by

Neranga Fernando

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.
Masahico Saito, Ph.D.

Date of Approval:
March 22, 2013

Keywords: Finite field, Permutation polynomial, Dickson polynomial, Reversed Dickson polynomial, Normal basis

Dedication

This doctoral dissertation is dedicated to my mother, my father, my sister and my late grandmother.

Acknowledgments

I am heavily indebted to my advisor, Dr. Xiang-dong Hou for his inspiration and invaluable support throughout my graduate studies at the University of South Florida. Undeniably, this work would not have been a success without his directions, guidance and immeasurable contribution. It was really a great honor to have been his student.

I would like to thank the members of my committee Dr. Brian Curtin, Dr. Mohamed Elhamdadi, and Dr. Masahico Saito for all their support, useful advice and critique which added value to this work. I am grateful to Dr. Zi-Xia Song for accepting to be the chairperson of my defense. I would also like to thank Dr. Skrzypek, Dr. Rimbey, and all the other faculty members in the Department of Mathematics and Statistics at USF for their support in diverse ways. Appreciation also goes to the administrative staff, Sarina, Mary Ann, Denise, and Beverly for their assistance in my teaching duties.

Warm appreciation also goes to my friends, Niluk John, Solomon Manukure, Yiu Ming Chan, Arbee Hossain, Kasun Perera, Dasmanthie Chin, Emmanuel Appiah, Anfas Hamza, Jonathan Burns, Helen Barclay, Dahomey Kadera, Stephen Lappano, and Xianqi Li for their friendship and comfort in times of need.

Most importantly, I would like to express my deepest gratitude to my mother Kumari Fernando, my father Sanath Fernando, my sister Erandi Fernando and my late grandmother Moril Swaris for their love and unflinching support and encouragement. Without them, I definitely could not have come this far.

Last but not the least, I would like to thank God Almighty for being with me and answering all my prayers.

Table of Contents

List of Tables

Abstract

Let p be a prime and $q = p^k$. The polynomial $g_{n,q} \in \mathbb{F}_p[\mathtt{x}]$ defined by the functional equation

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

gives rise to many permutation polynomials over finite fields. We are interested in triples $(n, e; q)$ for which $g_{n,q}$ is a permutation polynomial of $\mathbb{F}_{q^e}$. In Chapters 2, 3, and 4 of this dissertation, we present many new families of permutation polynomials in the form of $g_{n,q}$. The permutation behavior of $g_{n,q}$ is becoming increasingly more interesting and challenging. As we further explore the permutation behavior of $g_{n,q}$, there is a clear indication that $g_{n,q}$ is a plenteous source of permutation polynomials.

We also describe a piecewise construction of permutation polynomials over a finite field $\mathbb{F}_q$ which uses a subgroup of $\mathbb{F}_q^*$, a "selection" function, and several "case" functions. Chapter 5 of this dissertation is devoted to this piecewise construction which generalizes several recently discovered families of permutation polynomials.

1 Introduction

Let p be a prime and q a power of p. Let $\mathbb{F}_q$ be the finite field with q elements. A polynomial $f \in \mathbb{F}_q[\mathtt{x}]$ is called a *permutation polynomial* of $\mathbb{F}_q$ if the mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$. Every function from $\mathbb{F}_q$ to $\mathbb{F}_q$ can be represented by a polynomial in $\mathbb{F}_q[\mathtt{x}]$. In fact, if $\phi : \mathbb{F}_q \to \mathbb{F}_q$ is an arbitrary function form $\mathbb{F}_q$ to $\mathbb{F}_q$, then there exists a unique polynomial $g \in \mathbb{F}_q[\mathtt{x}]$ with $\deg(g) \leq q-1$ representing ϕ, that is $g(c) = \phi(c)$ for all $c \in \mathbb{F}_q$. The polynomial g can be found by the Lagrange's interpolation method for the function ϕ. If ϕ is already given as a polynomial function, say $\phi : c \mapsto f(c)$ where $f \in \mathbb{F}_q[\mathtt{x}]$, then g can be obtained from f by reduction modulo $\mathtt{x}^q - \mathtt{x}$. We call permutation polynomials of $\mathbb{F}_q$ PPs over $\mathbb{F}_q$. Search for PPs with nice algebraic structures is an important topic in the study of finite fields since they play a central role in both arithmetic and combinatorial aspects of finite fields. PPs have important applications in Coding Theory, Cryptography, Finite Geometry, Combinatorics and Computer Science, among other fields.

In history, the general study of PPs started with Hermite who considered PPs over finite prime fields. L.E. Dickson was the first person to study PPs of arbitrary finite fields; see [9].

Let $n \geq 0$ be an integer. Since the elementary symmetric polynomials $x_1 + x_2$ and $x_1 x_2$ generate the ring of symmetric polynomials in $\mathbb{Z}[x, y]$, there exists a polynomial $D_n(x, y) \in \mathbb{Z}[x, y]$ such that

$$x_1^n + x_2^n = D_n(x_1 + x_2, x_1 x_2);$$

see [31]. The explicit form of $D_n(x, y)$ is given by Waring's formula [30, Theorem

1.76]

$$D_n(x,y) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-y)^i x^{n-2i}.$$

For fixed $a \in \mathbb{F}_q$, $D_n(x,a) \in \mathbb{F}_q[x]$ is the *Dickson polynomial* of degree n and parameter a. Dickson polynomials are closely related to the well-known Chebyshev polynomials $T_n(x)$ over the complex numbers by

$$D_n(2xa, a^2) = 2a^n T_n(x).$$

The permutation property of the Dickson polynomial is completely known. When $a = 0$, $D_n(x,a) = x^n$, which is a PP over $\mathbb{F}_q$ if and only if $(n, q-1) = 1$. When $0 \neq a \in \mathbb{F}_q$, $D_n(x,a)$ is a PP over $\mathbb{F}_q$ if and only if $(n, q^2-1) = 1$; see [30, Theorem 7.16] or [29, Theorem 3.2].

The concept of the reversed Dickson polynomial $D_n(a,x)$ was first introduced by Hou, Mullen, Sellers and Yucas in [24] by reversing the roles of the variable and the parameter in the Dickson polynomial $D_n(x,a)$. When $a = 0$, $D_n(0,x)$ is a PP over $\mathbb{F}_q$ if and only if $n = 2k$ with $(k, q-1) = 1$. When $a \neq 0$,

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

Hence $D_n(a,x)$ is a PP on $\mathbb{F}_q$ if and only if $D_n(1,x)$ is a PP on $\mathbb{F}_q$. The nth *reversed Dickson polynomial* $D_n(1,x) \in \mathbb{Z}[x]$ is defined by

$$D_n(1, x(1-x)) = x^n + (1-x)^n.$$

There is a connection between reversed Dickson polynomials and almost perfect nonlinear (APN) functions which have very important applications in Cryptography [34]. Please refer [24] for more background of the reversed Dickson polynomial.

X. Hou showed in [21] that for each integer $n \geq 0$, there exists a unique

polynomial $g_{n,q} \in \mathbb{F}_p[\mathtt{x}]$ such that

$$\sum_{a \in \mathbb{F}_q} (\mathtt{x}+a)^n = g_{n,q}(\mathtt{x}^q - \mathtt{x}). \tag{1.0.1}$$

The explicit form of $g_{n,q}$ is given by Waring's formula

$$g_{n,q}(\mathtt{x}) = \sum_{\frac{n}{q} \le l \le \frac{n}{q-1}} \frac{n}{l} \binom{l}{n-l(q-1)} \mathtt{x}^{n-l(q-1)}. \tag{1.0.2}$$

The polynomial $g_{n,q}$ was introduced in [21] as a q-ary version of the reversed Dickson polynomial. We describe the context which led to the formation of the polynomial $g_{n,q}$ in Section 1.1. When $q = 2$, $g_{n,2}$ is the nth reversed Dickson polynomial over $\mathbb{F}_2$ since in characteristic 2

$$g_{n,2}(x^2 - x) = x^n + (x+1)^n = x^n + (1-x)^n = D_n(1, x(1-x)) = D_n(1, x^2 - x).$$

Permutation properties of the polynomial $g_{n,q}$ were first studied by X. Hou in [22]. The results of this study indicated that the polynomial $g_{n,q}$ opens the door to many new classes of PPs in a new approach. In [22], several families of PPs were found, but there were still many instances in which there was no theoretic explanation. Chapters 2, 3, and 4 of this dissertation are an attempt to answer those unexplained cases that also deal with questions about $g_{n,q}$ that were not touched in [22].

Constructing PPs of finite fields piecewise has been in discussion in numerous recent articles on permutation polynomials. We also construct several families of PPs in this dissertation that generalize some existing results.

Hence this dissertation focuses on the following:

(i) When is $g_{n,q}$ a permutation polynomial of $\mathbb{F}_{q^e}$?

(ii) A piecewise construction of permutation polynomials over finite fields.

The main question concerning permutation polynomials is how to recognize them. The following two criteria for this purpose have been useful in our study.

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

   (i) $f^{q-1} \pmod{x^q - x}$ has degree $q-1$;

   (ii) for each integer s with $1 \leq s \leq q-2$, $f^s \equiv f_s \pmod{x^q - x}$ for some $f_s \in \mathbb{F}_q[x]$ with $\deg f_s \leq q-2$.

(2) f is a permutation polynomial of $\mathbb{F}_{p^n}$ if and only if $\sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{\mathrm{Tr}_{p^n/p}(cf(x))} = 0$ for all $0 \neq c \in \mathbb{F}_{p^n}$, where $\zeta_p = e^{2\pi i/p}$ and $\mathrm{Tr}_{p^n/p}(x) = x + x^p + \cdots + x^{p^{n-1}}$ is the absolute trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.

Definition 1.0.1 (Desirable triple). If $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$, we say that the triple $(n, e; q)$ is *desirable*.

A desirable triple is considered *categorized* if an infinite class containing it has been found. Here is an overview of the dissertation.

In Chapter 2, we discuss the polynomial $g_{n,q}$ when $q = 2$ and list some known families of PPs of $\mathbb{F}_{2^e}$. The case $e = 1$ is completely explained in Chapter 2. Table 2.1, generated by a computer search contains all desirable triples $(n, e; 3)$ with $e \leq 6$. We also explain two desirable families of the table. The desirable triple $(407, 3; 3)$ is explained in Chapter 2 as a sporadic case.

Chapter 3 discusses the permutation behavior of the polynomial $g_{n,q}$ where n is of the form $n = q^a - q^b - 1$. Our computer results showed that this type of desirable triples seems to occur more frequently. The case $e = 2$ is of more interest since all known desirable triples when $e > 2$ are explained by Corollary 3.1.2 and Theorem 3.1.3, and Conjecture 3.1.4 states that there are no other cases. A table (Table 3.2), generated by a computer search, which contains desirable triples $(q^a - q^b - 1, 2; q)$ for $q \leq 97$, is also presented. Some of the results listed in table are explained by several new classes discovered in this dissertation, but a theoretical explanation has not been found for many of them.

Chapter 4 primarily deals with desirable triples with even q. Numerous classes of desirable triples with $q = 4$ and $e \leq 6$ (see Table 4.1) are explained. Most of the results are also generalized for an even q.

Chapter 5 describes a piecewise construction of permutation polynomials over a finite field $\mathbb{F}_q$. Permutation polynomials obtained by this construction unify and generalize several recently discovered families of permutation polynomials.

There are two appendices. Appendix A contains some useful *Mathematica* codes written to identify the permutation behavior of the polynomial $g_{n,q}$. Appendix B contains computational results used in the proof of Theorem 2.4.1.

In our notation, letters in typewriter typeface, $\mathtt{x}$, $\mathtt{y}$, $\mathtt{t}$, are reserved for indeterminates. The trace function $\mathrm{Tr}_{q^e/q}$ and the norm function $\mathrm{N}_{q^e/q}$ from $\mathbb{F}_{q^e}$ to $\mathbb{F}_q$ are also treated as polynomials, that is, $\mathrm{Tr}_{q^e/q}(\mathtt{x}) = \mathtt{x}+\mathtt{x}^q+\cdots+\mathtt{x}^{q^{e-1}}$, $\mathrm{N}_{q^e/q}(\mathtt{x}) = \mathtt{x}^{1+q+\cdots+q^{e-1}}$. When q is given, we define $S_a = \mathtt{x} + \mathtt{x}^q + \cdots + \mathtt{x}^{q^{a-1}}$ for every integer $a \geq 0$. Note that $\mathrm{Tr}_{q^e/q} = S_e$.

1.1 The Polynomial $g_{n,q}$

In this section, we derive the formula (1.0.1) and recall some basic properties of $g_{n,q}$ that will be used in later chapters. We refer the reader to [22] for proofs and further details of properties of $g_{n,q}$.

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

$$\mathtt{t}^q-\mathtt{t}+\mathtt{x}^q-\mathtt{x} = (\mathtt{t}+\mathtt{x})^q-(\mathtt{t}+\mathtt{x}) = \prod_{a\in\mathbb{F}_q}(\mathtt{t}+\mathtt{x}+a) = \sum_{k=0}^{q}\sigma_k((\mathtt{x}+a)_{a\in\mathbb{F}_q})\mathtt{t}^{q-k}, \quad (1.1.3)$$

where σ_k is the kth elementary symmetric polynomial in q variables. A comparison

of the coefficients of $\mathtt{t}$ on both sides of (1.1.3) tells that

$$\sigma_k((\mathtt{x}+a)_{a\in\mathbb{F}_q}) = \begin{cases} 1 & \text{if } k=0, \\ -1 & \text{if } k=q-1, \\ \mathtt{x}^q-\mathtt{x} & \text{if } k=q, \\ 0 & \text{otherwise.} \end{cases} \tag{1.1.4}$$

Let $n \geq 0$ be an integer. By Waring's formula [30, Theorem 1.76] and (1.1.4), we have

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

Set

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

(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

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

Proposition 1.1.1 ([22]). *The polynomial $g_{n,q}$ satisfies the recurrence relation*

$$\begin{cases} g_{0,q} = \cdots = g_{q-2,q} = 0, \\ g_{q-1,q} = -1, \\ g_{n,q} = \mathtt{x}g_{n-q,q} + g_{n-q+1,q}, \quad n \geq q. \end{cases} \tag{1.1.5}$$

Using the above recurrence relation, $g_{n,q}$ can be defined for $n < 0$:

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

For $n < 0$, $g_{n,q}$ belongs to $\mathbb{F}_p[\mathtt{x}, \mathtt{x}^{-1}]$, the ring of Laurent polynomials in $\mathtt{x}$ over $\mathbb{F}_p$. Hence the functional equation (1.0.1) holds for all $n \in \mathbb{Z}$.

By (1.1.5) we have the generating function of $\{g_{n,q}\}_{n\geq 0}$:

$$\sum_{n\geq 0} g_{n,q}\mathtt{t}^n = \frac{-\mathtt{t}^{q-1}}{1 - \mathtt{t}^{q-1} - \mathtt{x}\mathtt{t}^q}. \tag{1.1.6}$$

Proposition 1.1.2 *(i) We have* $g_{pn,q} = g_{n,q}^p$.

(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., $g_{n_1,q} \equiv g_{n_2,q} \pmod{\mathtt{x}^{q^e} - \mathtt{x}}$.

■

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

$m \sim_{(e,q)} n$. It follows from Proposition 1.1.2 that desirability of triples is preserved under the $\sim$ equivalence.

Given integers $d > 1$ and $a = a_0 d^0 + \cdots + a_t d^t$, $0 \le a_i \le d-1$, 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.

Lemma 1.1.3 ([22]). *Let $n = \alpha_0 q^0 + \cdots + \alpha_t q^t$, $0 \le \alpha_i \le q-1$ and $w_q(n)$ be the base q weight of n,*

$$g_{n,q} = \begin{cases} 0 & \text{if } w_q(n) < q-1, \\ -1 & \text{if } w_q(n) = q-1, \\ \alpha_0 x^{q^0} + (\alpha_0+\alpha_1)x^{q^1} + \cdots + (\alpha_0+\cdots+\alpha_{t-1})x^{q^{t-1}} + \delta & \text{if } w_q(n) = q, \end{cases} \tag{1.1.7}$$

where

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

Definition 1.1.4 An $\mathbb{F}_q$-linearized polynomial (or a q-polynomial) over $\mathbb{F}_{q^e}$ is a polynomial of the form

$$L(x) = \sum_{i=0}^{k} a_i x^{q^i} \in \mathbb{F}_{q^e}[x].$$

It is well known that L is a PP of $\mathbb{F}_{q^e}$ if and only if $L(x)$ only has the root 0 in $\mathbb{F}_{q^e}$. i.e., L is a PP of $\mathbb{F}_{q^e}$ if and only if $\gcd(L(x), x^{q^e} - x) = 1$.

Definition 1.1.5 The polynomials

$$l(x) = \sum_{i=0}^{k} a_i x^i \quad \text{and} \quad L(x) = \sum_{i=0}^{k} a_i x^{q^i}$$

over $\mathbb{F}_{q^e}$ are called *q-associates* of each other. More precisely, $l(x)$ is the *conventional q-associate* of $L(x)$ and $L(x)$ is the *linearized q-associate* of $l(x)$.

Now by [30, Theorem 3.62], the above condition for L to be a PP of $\mathbb{F}_{q^e}$ can be restated as follows. L is a PP of $\mathbb{F}_{q^e}$ if and only if $\gcd(l(x), x^e - 1) = 1$.

So by (1.1.7) and the above fact, we have the following proposition when $w_q(n) = q$.

Proposition 1.1.6 ([22]). *Let* $n = \alpha_0 q^0 + \cdots + \alpha_t q^t$, $0 \leq \alpha_i \leq q-1$, *with* $w_q(n) = q$. *Then* $(n, e; q)$ *is desirable if and only if*

$$\gcd(\alpha_0 + (\alpha_0 + \alpha_1)\mathtt{x} + \cdots + (\alpha_0 + \cdots + \alpha_{t-1})\mathtt{x}^{t-1}, \mathtt{x}^e - 1) = 1.$$

Next lemma considers triples $(n, e; p)$ where n is of the form $n = \alpha(p^{0e} + p^{1e} + \cdots + p^{(p-1)e}) + \beta$, where $\alpha, \beta \in \mathbb{Z}$.

Lemma 1.1.7 ([22]). *Let* $n = \alpha(p^{0e} + p^{1e} + \cdots + p^{(p-1)e}) + \beta$, *where* $\alpha, \beta \in \mathbb{Z}$. *Then for* $x \in \mathbb{F}_{p^e}$,

$$g_{n,p}(x) = \begin{cases} g_{\alpha p+\beta,p}(x) & \text{if } \mathrm{Tr}_{p^e/p}(x) = 0, \\ x^\alpha g_{\beta,p}(x) & \text{if } \mathrm{Tr}_{p^e/p}(x) \neq 0. \end{cases} \tag{1.1.8}$$

Proposition 1.1.8 ([22]). *In the previous lemma,* $(n, e; p)$ *is desirable if the following two conditions are satisfied.*

(i) Both $g_{\alpha p+\beta,p} + \delta$ *and* $x^\alpha g_{\beta,p}$ *are* $\mathbb{F}_p$*- linear on* $\mathbb{F}_{p^e}$ *and are* $1-1$ *on* $\mathrm{Tr}^{-1}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(0) = \{x \in \mathbb{F}_{p^e} : \mathrm{Tr}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(x) = 0\}$.

(ii) $g_{\beta,p}(1) \neq e\delta$.

Proposition 1.1.9 ([22]). *Assume that both* $g_{\alpha p+\beta,p} + \delta$ *and* $x^\alpha g_{\beta,p}$ *are* $\mathbb{F}_p$*- linear on*

$\mathrm{Tr}^{-1}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(0)$ *and write*

$$g_{\alpha p+\beta,p}(\mathtt{x}^p-\mathtt{x})+\delta \equiv \sum_{i=0}^{e-1} a_i \mathtt{x}^{p^i} \pmod{\mathtt{x}^{q^e}-\mathtt{x}},$$
$$(\mathtt{x}^p-\mathtt{x})^\alpha g_{\beta,p}(\mathtt{x}^p-\mathtt{x}) \equiv \sum_{i=0}^{e-1} b_i \mathtt{x}^{p^i} \pmod{\mathtt{x}^{q^e}-\mathtt{x}}.$$

Then $g_{\alpha p+\beta,p}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(0)$ if and only if

$$\gcd\Big(\sum_{i=0}^{e-1} a_i \mathtt{x}^i, \mathtt{x}^e-1\Big)=\mathtt{x}-1;$$

$x^\alpha g_{\beta,p}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(0)$ if and only if

$$\gcd\Big(\sum_{i=0}^{e-1} b_i \mathtt{x}^i, \mathtt{x}^e-1\Big)=\mathtt{x}-1.$$

Lemma 1.1.10 ([22]). *Let l and $i>0$ be integers. Then*

$$g_{l+q^i,q} = g_{l+1,q} + S_i \cdot g_{l,q}, \tag{1.1.9}$$

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

From (1.1.9), we have

$$(S_a - S_b)g_{n,q} = g_{n+q^a,q} - g_{n+q^b,q}, \tag{1.1.10}$$

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 $S_a = S_{pe+a}$.

2 Special Families of Desirable Triples and a Sporadic Case*

In this chapter, we consider some special cases of the polynomial $g_{n,q}$. This chapter is organized as follows: Section 2.1 discusses the polynomial $g_{n,q}$ when $q = 2$. Section 2.2 explains the case $e = 1$ completely. In Section 2.3, we explain two families of desirable triples when $p = 3$. The desirable triple $(407, 3; 3)$ is explained in Section 2.4 as a sporadic case. Table 2.1 contains all desirable triples $(n, e; 3)$ with $e \leq 6$.

2.1 The Polynomial $g_{n,2}$

When $q = 2$, $g_{n,2}$ is the nth reversed Dickson polynomial $D_n(1, x)$ over $\mathbb{F}_2$. Unlike its twin, Dickon polynomial $D_n(x, a)$, reversed Dickon polynomial $D_n(a, x)$ is difficult to describe. Reversed Dickson permutation polynomials (RDPPs) are connected to almost perfect nonlinear (APN) functions, a well-studied class of functions in cryptography [34].

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 $b \in \mathbb{F}_q$, the equation $f(x + a) - f(x) = b$ has at most two solutions in $\mathbb{F}_q$. APN functions were introduced by Nyberg [34].

Because of the connection between RDPPs and APN functions, some classes of reversed Dickon permutation polynomials were obtained from known APN functions. However, not all reversed Dickson permutation polynomials are obtainable from APN functions (see [24, Prop. 5.4]).

*Sections 2.2 and 2.4 of this chapter are taken from [14] which has been published in the journal "Finite Fields and Their Applications".

All known desirable triples $(n, e; 2)$ are covered by four classes listed below and an implicit conjecture states that there are no other classes.

(i) $n = 2^k + 1$, $(k, 2e) = 1$.

(ii) $n = 2^{2k} - 2^k + 1$, $(k, 2e) = 1$.

(iii) $n = 2^e + 2^k + 1$, $k > 0$, e is even, $(k - 1, e) = 1$.

(iv) $n = 2^{8k} + 2^{6k} + 2^{4k} + 2^{2k} - 1$, $e = 5k$.

Classes (i), (ii), and (iv) were obtained from known APN functions. Classes (i) and (ii) were due to Gold [15] and Kasami [26] respectively. Class (iii) appeared in [24] and it was shown that class (iii) is not obtainable from an APN function. In [12], Dobbertin proved that there is a sequence of APN functions when e is a multiple of 5. Class (iv) was obtained from that APN function. Even though Dobbertin's class is known, it is still not well understood. We refer the reader to [24] for a connection between reversed Dickson permutation polynomials and APN functions.

2.2 The Case $e = 1$

In this section, we determine all desirable triples $(n, 1; q)$.

Theorem 2.2.1 *We have*

$$\sum_{n\geq 0} g_{n,q}(\mathtt{x})\mathtt{t}^n \equiv \frac{-(\mathtt{xt})^{q-1}}{1-(\mathtt{xt})^{q-1}-(\mathtt{xt})^q} + (1-\mathtt{x}^{q-1})\frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}} \pmod{\mathtt{x}^q - \mathtt{x}}. \quad (2.2.1)$$

Namely, modulo $\mathtt{x}^q - \mathtt{x}$*,*

$$g_{n,q}(\mathtt{x}) \equiv a_n\mathtt{x}^n + \begin{cases} \mathtt{x}^{q-1} - 1 & \text{if } n > 0,\ n \equiv 0 \pmod{q-1}, \\ 0 & \text{otherwise}, \end{cases} \quad (2.2.2)$$

where

$$\sum_{n\geq 0} a_n\mathtt{t}^n = \frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}-\mathtt{t}^q}. \quad (2.2.3)$$

Proof. From (1.1.6),

$$\sum_{n\geq 0} g_{n,q}\mathtt{t}^n = \frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}-\mathtt{x}\mathtt{t}^q}.$$

Clearly,

$$\frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}-\mathtt{x}\mathtt{t}^q} \equiv \frac{-(\mathtt{x}\mathtt{t})^{q-1}}{1-(\mathtt{x}\mathtt{t})^{q-1}-(\mathtt{x}\mathtt{t})^q} + (1-\mathtt{x}^{q-1})\frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}} \pmod{\mathtt{x}^{q-1}-1},$$

and

$$\frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}-\mathtt{x}\mathtt{t}^q} \equiv \frac{-(\mathtt{x}\mathtt{t})^{q-1}}{1-(\mathtt{x}\mathtt{t})^{q-1}-(\mathtt{x}\mathtt{t})^q} + (1-\mathtt{x}^{q-1})\frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}} \pmod{\mathtt{x}}.$$

Thus (2.2.1) is proved.

■

Corollary 2.2.2 *(i) Assume $q > 2$. Then $(n, 1; q)$ is desirable if and only if* $\gcd(n, q-1) = 1$ *and $a_n \neq 0$ (in $\mathbb{F}_p$).*

(ii) Assume $q = 2$. Then $(n, 1; 2)$ is desirable if and only if $a_n = 0$ (in $\mathbb{F}_2$).

Proof. (i) By (2.2.2), $g_{n,q}(x) = a_n x^n$ for all $x \in \mathbb{F}_q^*$. If $g_{n,q}$ is a PP of $\mathbb{F}_q$, then $a_n \neq 0$ and $\gcd(n, q-1) = 1$. On the other hand, assume $a_n \neq 0$ and $\gcd(n, q-1) = 1$. By (5.2.6), we have $g_{n,q} \equiv a_n \mathtt{x}^n \pmod{\mathtt{x}^q - \mathtt{x}}$, which is a PP of $\mathbb{F}_q$.

(ii) By (2.2.2), $g_{n,2} \equiv a_n\mathtt{x} + \mathtt{x} - 1 \pmod{\mathtt{x}^2 - \mathtt{x}}$. If $a_n = 0$, then $g_{n,2} = \mathtt{x} - 1$ which is clearly a PP of $\mathbb{F}_2$. Now assume $g_{n,2}$ is a PP of $\mathbb{F}_2$. Then $g_{n,2}(0) = 1$ and $g_{n,2}(1) = a_n$. Since $g_{n,2}$ is a PP of $\mathbb{F}_2$, $a_n = 0$.

■

From (2.2.3) one can easily derive an explicit expression for a_n. But that expression does not give any simple pattern of those n with $a_n \neq 0$ (in $\mathbb{F}_p$).

2.3 Two Families of Desirable Triples when $p = 3$

Theorem 2.3.1 *Let $n = 26(3^0 + 3^e + 3^{2e}) + 7$. Then $(n, e; 3)$ is desirable if and only if* $\gcd(1 + x + x^4, x^e - 1) = x - 1$.

Proof. Since $26 \cdot 3 + 7 = 85 = 1 \cdot 3^0 + 1 \cdot 3^1 + 1 \cdot 3^4$, by Lemma 1.1.3 we have

$$g_{26\cdot 3+7}(x) = g_{85,3}(x) = x^{3^0} - x^{3^1} - x^{3^2} - x^{3^3}.$$

Also, $g_{7,3}(x) = x$, so $x^{26} g_{7,3}(x) = x^{27}$. Both $g_{26.3+7}$ and $x^{26} g_{7,3}$ are $\mathbb{F}_3$-linear on $\mathbb{F}_{3^e}$. Moreover, $x^{26} g_{7,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$ and $g_{7,3}(1) = 1 \neq 0$. So by Proposition 1.1.8, $g_{n,3}$ is a PP of $\mathbb{F}_{3^e}$ if and only if $g_{85,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$.
We have, by [22, Eq. 3.4], $-g_{85,3}(x^3 - x) = x^{3^0} + x^{3^1} + x^{3^4}$. So by Proposition 1.1.9, $g_{85,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$ if and only if $\gcd(1 + x + x^4, x^e - 1) = x - 1$.

■

Theorem 2.3.2 *Let* $n = 163(3^0 + 3^e + 3^{2e}) - 162$. *Then* $(n, e; 3)$ *is desirable if and only if* $\gcd(x + x^4 + x^5, x^e - 1) = x - 1$.

Proof. Since $163 \cdot 3 - 162 = 327 = 0.3^0 + 1.3^1 + 0.3^2 + 0.3^3 + 1.3^4 + 1.3^5$,
by Lemma 1.1.3 we have

$$g_{327,3} = x^{3^1} + x^{3^2} + x^{3^3} - x^{3^4}.$$

Also, $g_{-162,3}(x) = \frac{1}{x^{162}}$, so $x^{163} g_{-162,3}(x) = x$. Both $g_{163.3-162}$ and $x^{163} g_{-162,3}$ are $\mathbb{F}_3$-linear on $\mathbb{F}_{3^e}$. Moreover, $x^{163} g_{-162,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$ and $g_{-162,3}(1) = 1 \neq 0$. So by Proposition 1.1.8, $g_{n,3}$ is a PP of $\mathbb{F}_{3^e}$ if and only if $g_{327,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$.
We have, by [22, Eq. 3.4], $-g_{327,3}(x^3 - x) = x^{3^1} + x^{3^4} + x^{3^5}$. So by Proposition 1.1.9, $g_{327,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$ if and only if $\gcd(x + x^4 + x^5, x^e - 1) = x - 1$.

■

2.4 A Sporadic Case

The second unexplained case of desirable triple in Table 3 of [22] is $(407, 3; 3)$, where $407 = 2 \cdot 3^0 + 2 \cdot 3^4 + 3^5$. Theorem 2.4.1 suggests that this might be a sporadic case.

By (1.1.9) and Lemma 1.1.3, we have

$$
\begin{aligned}
&g_{407,3}(\mathtt{x})\\
=&\, g_{2\cdot 3^0+2\cdot 3^4+3^5,3}\\
=&\, g_{3+2\cdot 3^4,3}+S_5\cdot g_{2+2\cdot 3^4,3}\\
=&\, g_{3+2\cdot 3^4,3}+S_5\cdot (g_{3+3^4,3}+S_4\cdot g_{2+3^4,3})\\
=&\, \mathtt{x}^3+\mathtt{x}^{3^2}+\mathtt{x}^{3^3}+S_5\cdot(-1+S_4\cdot(-\mathtt{x}-\mathtt{x}^3-\mathtt{x}^{3^2}-\mathtt{x}^{3^3}))\\
\equiv&\, \mathrm{Tr}_{3^3/3}(\mathtt{x})-S_5(1+S_4^2) \pmod{\mathtt{x}^{3^3}-\mathtt{x}}\\
\equiv&\, \mathrm{Tr}_{3^3/3}(\mathtt{x})+S_4^{3^2}(1+S_4^2) \pmod{\mathtt{x}^{3^3}-\mathtt{x}} \qquad (S_5\equiv -S_4^{3^2} \pmod{\mathtt{x}^{3^3}-\mathtt{x}})\\
\equiv&\, \mathrm{Tr}_{3^3/3}(\mathtt{y})+\mathtt{y}^{3^2}(1+\mathtt{y}^2) \pmod{\mathtt{x}^{3^3}-\mathtt{x}},
\end{aligned}
$$

where $\mathtt{y}=S_4(\mathtt{x})$, which is a PP of $\mathbb{F}_{3^3}$. We can further write

$$
\begin{aligned}
g_{407,3}(\mathtt{x}) &\equiv \mathrm{Tr}_{3^3/3}(\mathtt{y})+\mathtt{y}^8\big(\mathrm{Tr}_{3^3/3}(\mathtt{y})-\mathtt{y}^{3^2}\big) \pmod{\mathtt{x}^{3^3}-\mathtt{x}}\\
&= (1+\mathtt{y}^8)\mathrm{Tr}_{3^3/3}(\mathtt{y})-\mathtt{y}^{17}.
\end{aligned}
$$

For $x'\in\mathbb{F}_{3^3}^*$, $y=S_4(x')$, we have

$$
g_{407,3}(x')=(1+y^8)\mathrm{Tr}_{3^3/3}(y)-y^{17}=(1+x^2)\mathrm{Tr}_{3^3/3}\Big(\frac{1}{x}\Big)-x,
$$

where $x=y^{-9}=S_4(x')^{-9}$. So the fact that $g_{407,3}$ is a PP of $\mathbb{F}_{3^3}$ is equivalent to the fact that the function

$$
h(x)=(1+x^2)\mathrm{Tr}_{3^3/3}(\frac{1}{x})-x \tag{2.4.4}
$$

is a permutation of $\mathbb{F}_{3^3}^*$. In the next theorem (and its proof), we investigate some peculiar properties of h in (2.4.4) as a function defined on $\mathbb{F}_{q^3}^*$.

Theorem 2.4.1 *Let h be as in* (2.4.4). *h is a permutation of $\mathbb{F}_{q^3}^*$ if and only if $q=3$.*

Proof.

($\Leftarrow$) We will show that for every $z \in \mathbb{F}_{3^3}^*$, there exists an $x \in \mathbb{F}_{3^3}^*$ such that

$$(1+x^2)\mathrm{Tr}_{3^3/3}\Big(\frac{1}{x}\Big) - x = z. \tag{2.4.5}$$

If $\mathrm{Tr}_{3^3/3}(\frac{1}{z}) = 0$, $x = -z$ is the solution. If $\mathrm{Tr}_{3^3/3}(\frac{1}{z}) \neq 0$, we may assume $\mathrm{Tr}_{3^3/3}(\frac{1}{z}) = 1$. Then

$$z - 1 = az^2(z+b), \quad (a,b) = (1,0),\ (1,1),\ (-1,1). \tag{2.4.6}$$

We show that one of the following systems has a solution $x \in \mathbb{F}_{3^3}^*$:

$$\begin{cases} x^2 - x + 1 - z = 0, \\ \mathrm{Tr}_{3^3/3}\Big(\frac{1}{x}\Big) = 1; \end{cases} \tag{2.4.7}$$

$$\begin{cases} x^2 + x + 1 + z = 0, \\ \mathrm{Tr}_{3^3/3}\Big(\frac{1}{x}\Big) = -1. \end{cases} \tag{2.4.8}$$

The solutions of the quadratic equation in (2.4.7) are $x = -1 + w$, where $w^2 = z$; the solutions of the quadratic equation in (2.4.8) are $x = 1 + u$, where $u^2 = -z$.

Case 1. Assume $(a,b) = (1,0)$. Then $z - 1 = z^3$, from which we have $-z = (\frac{z-1}{z+1})^2$. Let $u = \frac{z-1}{z+1}$. Then $x = 1 + u = -\frac{z}{z+1}$ is a solution of the quadratic equation in (2.4.8), and $\mathrm{Tr}_{3^3/3}(\frac{1}{x}) = \mathrm{Tr}_{3^3/3}(-1 - \frac{1}{z}) = -1$.

Case 2. Assume $(a,b) = (1,1)$. Then $z - 1 = z^2(z+1)$, from which we have $(-z)^3 = (z+1)^2$. Let $u^3 = -(z+1)$. Then $x = 1 + u$ is a solution of the quadratic equation in (2.4.8), and

$$\mathrm{Tr}_{3^3/3}\Big(\frac{1}{x}\Big) = \mathrm{Tr}_{3^3/3}\Big(\frac{1}{x^3}\Big) = \mathrm{Tr}_{3^3/3}\Big(\frac{1}{1-u^3}\Big) = \mathrm{Tr}_{3^3/3}\Big(-\frac{1}{z}\Big) = -1.$$

Case 3. Assume $(a,b) = (-1,1)$. Then $z - 1 = -z^2(z+1)$, from which we have $z = (\frac{1}{z-1})^2$. Let $w = -\frac{1}{z-1}$. Then $x = -1 + w = \frac{-z}{z-1}$ is a solution of the quadratic

equation in (2.4.7), and $\mathrm{Tr}_{3^3/3}(\frac{1}{x}) = \mathrm{Tr}_{3^3/3}(-1+\frac{1}{z}) = 1$.

($\Rightarrow$) We show that if $q \neq 3$, then h is a not a permutation of $\mathbb{F}_{q^3}^*$.

In general,

$$\begin{aligned} h(x) &= (1+x^2)(x^{-1}+x^{-q}+x^{-q^2}) - x, \\ &= x^{-1}+x^{-q}+x^{-q^2}+x^{2-q}+x^{2-q^2} \\ &= y+y^q+y^{q^2}+y^{q-2}+y^{q^2-2} \\ &= g(y), \end{aligned} \tag{2.4.9}$$

where $y = x^{-1} \in \mathbb{F}_{q^3}^*$, and $g(\mathtt{y}) = \mathtt{y}+\mathtt{y}^q+\mathtt{y}^{q^2}+\mathtt{y}^{q-2}+\mathtt{y}^{q^2-2}$.

First assume $q = 2$. We have

$$g(y) = y^4+y+1, \qquad y \in \mathbb{F}_{2^3}^*.$$

It is obvious that g is not 1-1 on $\mathbb{F}_{2^3}^*$.

Now Assume $q > 3$. We show that g is not a PP of $\mathbb{F}_{q^3}$. (Since $g(0) = 0$, it follows from (2.4.9) that h is not a permutation of $\mathbb{F}_{q^3}^*$.)

Case 1. Assume $q > 3$ is odd. We have

$$g(\mathtt{y})^{2q^2+2} \equiv 8\mathtt{y}^{q^3-1} + \text{terms of lower degree} \pmod{\mathtt{y}^{q^3}-\mathtt{y}}.$$

(The complete expression of $g^{2q^2+2} \pmod{\mathtt{y}^{q^3}-\mathtt{y}}$ is given in Appendix B.) By Hermite's criterion, g is not a PP of $\mathbb{F}_{q^3}$.

Case 2. Assume $q > 3$ is even. We have

$$g(\mathtt{y})^{2q^2+q+3} \equiv \mathtt{y}^{q^3-1} + \text{terms of lower degree} \pmod{\mathtt{y}^{q^3}-\mathtt{y}}.$$

(The complete expression of $g^{2q^2+q+3} \pmod{\mathtt{y}^{q^3}-\mathtt{y}}$ is given in Appendix B.) By Hermite's criterion, g is not a PP of $\mathbb{F}_{q^3}$.

■

Table 2.1: Desirable triples $(n, e; 3)$, $e \leq 6$, $w_3(n) > 3$

e	n	3-adic digits of n	reference
1	17	2 2 1	[22] Prop 3.1
2	71	2 2 1 2	[22] Prop 3.2 (i)
2	95	2 1 1 0 1	[22] Table 2 No.2
2	101	2 0 2 0 1	[22] Table 2 No.2
2	103	1 1 2 0 1	[22] Table 2 No.2
2	119	2 0 1 1 1	[22] Table 2 No.2
2	151	1 2 1 2 1	[22] Table 2 No.5
2	197	2 2 0 1 2	[22] Prop 3.2 (ii)
2	485	2 2 2 2 2 1	[22] Prop 3.1
3	101	2 0 2 0 1	[14] Thm 4.1
3	407	2 0 0 0 2 1	Thm 2.4.1
3	475	1 2 1 2 2 1	
3	605	2 0 1 1 1 2	
3	619	1 2 2 1 1 2	
3	671	2 1 2 0 2 2	
3	701	2 2 2 1 2 2	[22] Prop 3.2 (i)
3	761	2 1 0 1 0 0 1	[22] Table 2 No.2
3	769	1 1 1 1 0 0 1	[22] Table 2 No.2
3	775	1 0 2 1 0 0 1	[22] Table 2 No.2
3	779	2 1 2 1 0 0 1	
3	785	2 0 0 2 0 0 1	[22] Table 2 No.2
3	787	1 1 0 2 0 0 1	[22] Table 2 No.2
3	827	2 2 1 0 1 0 1	
3	839	2 0 0 1 1 0 1	[22] Table 2 No.2
3	847	1 0 1 1 1 0 1	[22] Table 2 No.2
3	925	1 2 0 1 2 0 1	[22] Table 2 No.5
3	1003	1 1 0 1 0 1 1	[22] Table 2 No.2
3	1007	2 2 0 1 0 1 1	[22] Thm 3.10
3	1009	1 0 1 1 0 1 1	[22] Table 2 No.2
3	1097	2 2 1 1 1 1 1	
3	1175	2 1 1 1 2 1 1	
3	1247	2 1 0 1 0 2 1	
3	1423	1 0 2 1 2 2 1	
3	1519	1 2 0 2 0 0 2	[22] Table 2 No.4
3	1739	2 0 1 1 0 1 2	
3	1753	1 2 2 1 0 1 2	
3	1915	1 2 2 1 2 1 2	
3	2021	2 1 2 2 0 2 2	[22] Thm 3.9
3	2117	2 0 1 0 2 2 2	
3	2131	1 2 2 0 2 2 2	[22] Prop 3.2 (ii)

Table 2.1 (Continued)

e	n	3-adic digits of n	reference
3	2537	2 2 2 0 1 1 0 1	
3	2723	2 1 2 1 0 2 0 1	
3	2819	2 0 1 2 1 2 0 1	
3	2897	2 2 0 2 2 2 0 1	
3	3137	2 1 0 2 2 0 1 1	
3	3317	2 1 2 2 1 1 1 1	
3	3361	1 1 1 1 2 1 1 1	
3	3517	1 2 0 1 1 2 1 1	
3	3551	2 1 1 2 1 2 1 1	
3	3559	1 1 2 2 1 2 1 1	
3	3833	2 2 2 0 2 0 2 1	
3	4019	2 1 2 1 1 1 2 1	
3	4253	2 1 1 1 1 2 2 1	
3	4261	1 1 2 1 1 2 2 1	
3	5093	2 2 1 2 2 2 0 2	
3	5507	2 2 2 2 1 1 1 2	
3	5557	1 1 2 1 2 1 1 2	
3	5665	1 1 2 2 0 2 1 2	
3	5719	1 1 2 1 1 2 1 2	
3	13121	2 2 2 2 2 2 2 2 1	[22] Prop 3.1
4	173	2 0 1 0 2	[22] Table 2 No.3
4	1477	1 0 2 0 0 0 2	[22] Table 2 No.3
4	6479	2 2 2 2 1 2 2 2	[22] Prop 3.2 (i)
4	6647	2 1 0 0 1 0 0 0 1	[22] Table 2 No.2
4	6653	2 0 1 0 1 0 0 0 1	[22] Table 2 No.2
4	6655	1 1 1 0 1 0 0 0 1	[22] Table 2 No.2
4	6661	1 0 2 0 1 0 0 0 1	[22] Table 2 No.2
4	6671	2 0 0 1 1 0 0 0 1	[22] Table 2 No.2
4	6679	1 0 1 1 1 0 0 0 1	[22] Table 2 No.2
4	6725	2 0 0 0 2 0 0 0 1	[22] Table 2 No.2
4	6727	1 1 0 0 2 0 0 0 1	[22] Table 2 No.2
4	6733	1 0 1 0 2 0 0 0 1	[22] Table 2 No.2
4	6751	1 0 0 1 2 0 0 0 1	[22] Table 2 No.2
4	6887	2 0 0 0 1 1 0 0 1	[22] Table 2 No.2
4	6895	1 0 1 0 1 1 0 0 1	[22] Table 2 No.2
4	7135	1 2 0 0 1 2 0 0 1	[22] Table 2 No.5
4	7373	2 0 0 0 1 0 1 0 1	[22] Table 2 No.2
4	7375	1 1 0 0 1 0 1 0 1	[22] Table 2 No.2
4	7381	1 0 1 0 1 0 1 0 1	[22] Table 2 No.2
4	7399	1 0 0 1 1 0 1 0 1	[22] Table 2 No.2
4	8119	1 0 2 0 1 0 2 0 1	[22] Table 2 No.5
4	8831	2 0 0 0 1 0 0 1 1	[22] Table 2 No.2

Table 2.1 (Continued)

e	n	3-adic digits of n	reference
4	8839	1 0 1 0 1 0 0 1 1	[22] Table 2 No.2
4	8855	2 2 2 0 1 0 0 1 1	[22] Thm 3.10
4	11071	1 0 0 2 1 0 0 2 1	[22] Table 2 No.5
4	17717	2 1 0 2 2 0 0 2 2	[22] Thm 3.9
4	19519	1 2 2 2 0 2 2 2 2	[22] Prop 3.2 (ii)
4	26725	1 1 2 2 2 1 0 0 1 1	
4	28669	1 1 2 2 2 0 0 1 1 1	
4	29525	2 1 1 1 1 1 1 1 1 1	[14] Thm 3.2
4	36997	1 2 0 2 0 2 2 1 2 1	
4	43933	1 1 0 1 2 0 0 2 0 2	
4	53149	1 1 1 0 2 2 0 0 2 2	[14] Thm 3.2
4	57575	2 0 1 2 2 2 0 2 2 2	Thm 2.2.1
4	84965	2 1 2 2 1 1 2 2 0 1 1	[14] Thm 3.6
4	88655	2 1 1 1 2 1 1 1 1 1 1	[14] Thm 3.5
4	90815	2 1 1 0 2 1 1 2 1 1 1	[14] Thm 3.1
4	91525	1 1 2 2 1 1 2 2 1 1 1	[14] 4.3
4	107765	2 2 0 1 1 2 0 1 1 2 1	[14] Thm 3.8
4	133079	2 1 2 2 1 1 2 0 2 0 2	
4	148415	2 1 2 0 2 1 2 1 1 1 2	[14] Rmk 3.3
4	167173	1 2 1 2 2 0 1 1 1 2 2	
4	265805	2 2 1 1 2 1 1 1 1 1 1 1	[14] Thm 3.5
4	267935	2 1 1 2 1 1 1 2 1 1 1 1	[14] Thm 3.1
4	272375	2 2 2 1 2 1 1 1 2 1 1 1	[14] Thm 3.1
4	272615	2 1 2 1 2 2 1 1 2 1 1 1	[14] Thm 3.1
4	273095	2 2 1 1 2 1 2 1 2 1 1 1	[14] Thm 3.1
4	354293	2 2 2 2 2 2 2 2 2 2 2 1	[22] Prop 3.1
5	515	2,0,0,1,0,2	[22] Table 2 No.3
5	569	2,0,0,0,1,2	[22] Table 2 No.3
5	2675	2,0,0,0,0,2,0,1	[22] Table 2 No.3
5	4393	1,0,2,0,0,0,0,2	[22] Table 2 No.3
5	13177	1,0,0,2,0,0,0,0,2	[22] Table 2 No.3
5	20171	2,0,0,0,0,2,0,0,0,1	[22] Table 2 No.3
5	58805	2,2,2,2,2,1,2,2,2,2	[22] Prop 3.2 (i)
5	59297	2,1,0,0,0,1,0,0,0,0,1	[14] Thm 3.1
5	59303	2,0,1,0,0,1,0,0,0,0,1	[14] Thm 3.1
5	59305	1,1,1,0,0,1,0,0,0,0,1	[14] Thm 3.1
5	59311	1,0,2,0,0,1,0,0,0,0,1	[14] Thm 3.1
5	59321	2,0,0,1,0,1,0,0,0,0,1	[14] Thm 3.1
5	59323	1,1,0,1,0,1,0,0,0,0,1	[14] Thm 3.1
5	59329	1,0,1,1,0,1,0,0,0,0,1	[14] Thm 3.1
5	59347	1,0,0,2,0,1,0,0,0,0,1	[14] Thm 3.1
5	59375	2,0,0,0,1,1,0,0,0,0,1	[14] Thm 3.1

Table 2.1 (Continued)

e	n	3-adic digits of n	reference
5	59377	1,1,0,0,1,1,0,0,0,0,1	[14] Thm 3.1
5	59383	1,0,1,0,1,1,0,0,0,0,1	[14] Thm 3.1
5	59401	1,0,0,1,1,1,0,0,0,0,1	[14] Thm 3.1
5	59455	1,0,0,0,2,1,0,0,0,0,1	[14] Thm 3.1
5	59537	2,0,0,0,0,2,0,0,0,0,1	[14] Thm 3.1
5	59539	1,1,0,0,0,2,0,0,0,0,1	[14] Thm 3.1
5	59545	1,0,1,0,0,2,0,0,0,0,1	[14] Thm 3.1
5	59563	1,0,0,1,0,2,0,0,0,0,1	[14] Thm 3.1
5	59617	1,0,0,0,1,2,0,0,0,0,1	[14] Thm 3.1
5	60023	2,0,0,0,0,1,1,0,0,0,1	[14] Thm 3.1
5	60031	1,0,1,0,0,1,1,0,0,0,1	[14] Thm 3.1
5	60049	1,0,0,1,0,1,1,0,0,0,1	[14] Thm 3.1
5	60103	1,0,0,0,1,1,1,0,0,0,1	[14] Thm 3.1
5	60757	1,2,0,0,0,1,2,0,0,0,1	[22] Table 2 No.5
5	61481	2,0,0,0,0,1,0,1,0,0,1	[14] Thm 3.1
5	61483	1,1,0,0,0,1,0,1,0,0,1	[14] Thm 3.1
5	61489	1,0,1,0,0,1,0,1,0,0,1	[14] Thm 3.1
5	61507	1,0,0,1,0,1,0,1,0,0,1	[14] Thm 3.1
5	61561	1,0,0,0,1,1,0,1,0,0,1	[14] Thm 3.1
5	63685	1,0,2,0,0,1,0,2,0,0,1	[22] Table 2 No.5
5	65855	2,0,0,0,0,1,0,0,1,0,1	[14] Thm 3.1
5	65857	1,1,0,0,0,1,0,0,1,0,1	[14] Thm 3.1
5	65863	1,0,1,0,0,1,0,0,1,0,1	[14] Thm 3.1
5	65881	1,0,0,1,0,1,0,0,1,0,1	[14] Thm 3.1
5	65935	1,0,0,0,1,1,0,0,1,0,1	[14] Thm 3.1
5	72469	1,0,0,2,0,1,0,0,2,0,1	[22] Table 2 No.5
5	78977	2,0,0,0,0,1,0,0,0,1,1	[14] Thm 3.1
5	78979	1,1,0,0,0,1,0,0,0,1,1	[14] Thm 3.1
5	78985	1,0,1,0,0,1,0,0,0,1,1	[14] Thm 3.1
5	79003	1,0,0,1,0,1,0,0,0,1,1	[14] Thm 3.1
5	79055	2,2,2,2,0,1,0,0,0,1,1	[22] Thm 3.10
5	79057	1,0,0,0,1,1,0,0,0,1,1	[14] Thm 3.1
5	98821	1,0,0,0,2,1,0,0,0,2,1	Thm 2.2.2
5	118591	1,2,0,0,0,2,0,0,0,0,2	[22] Table 2 No.4
5	158117	2,1,0,0,2,2,0,0,0,2,2	[14] Thm 3.2
5	176659	1,2,2,2,2,0,2,2,2,2,2	[22] Prop 3.2 (ii)
5	474349	1,1,1,0,0,2,2,0,0,0,2,2	[14] Thm 3.2
5	513875	2,0,1,0,2,2,2,0,0,2,2,2	Thm 2.2.1
5	766661	2,1,2,2,2,1,1,2,2,2,0,1,1	[14] Thm 3.6
5	1121443	1,2,2,2,2,0,2,2,2,2,0,0,2	[14] Thm 3.2
5	1541623	1,1,0,1,0,2,2,2,0,0,2,2,2	[14] Thm 3.2
5	9565937	2,2,2,2,2,2,2,2,2,2,2,2,2,2,1	[22] Prop 3.1

Table 2.1 (Continued)

e	n	3-adic digits of n	reference
6	530711	2,2,2,2,2,2,1,2,2,2,2,2	[22] Prop 3.2 (i)
6	532175	2,1,0,0,0,0,1,0,0,0,0,0,1	[14] Thm 3.1
6	532183	1,1,1,0,0,0,1,0,0,0,0,0,1	[14] Thm 3.1
6	532189	1,0,2,0,0,0,1,0,0,0,0,0,1	[14] Thm 3.1
6	532199	2,0,0,1,0,0,1,0,0,0,0,0,1	[14] Thm 3.1
6	532253	2,0,0,0,1,0,1,0,0,0,0,0,1	[14] Thm 3.1
6	532261	1,0,1,0,1,0,1,0,0,0,0,0,1	[14] Thm 3.1
6	532279	1,0,0,1,1,0,1,0,0,0,0,0,1	[14] Thm 3.1
6	532423	1,0,1,0,0,1,1,0,0,0,0,0,1	[14] Thm 3.1
6	532495	1,0,0,0,1,1,1,0,0,0,0,0,1	[14] Thm 3.1
6	532901	2,0,0,0,0,0,2,0,0,0,0,0,1	[14] Thm 3.1
6	532903	1,1,0,0,0,0,2,0,0,0,0,0,1	[14] Thm 3.1
6	532927	1,0,0,1,0,0,2,0,0,0,0,0,1	[14] Thm 3.1
6	532981	1,0,0,0,1,0,2,0,0,0,0,0,1	[14] Thm 3.1
6	534359	2,0,0,0,0,0,1,1,0,0,0,0,1	[14] Thm 3.1
6	534367	1,0,1,0,0,0,1,1,0,0,0,0,1	[14] Thm 3.1
6	536551	1,2,0,0,0,0,1,2,0,0,0,0,1	[22] Table 2 No.5
6	538735	1,1,0,0,0,0,1,0,1,0,0,0,1	[14] Thm 3.1
6	538741	1,0,1,0,0,0,1,0,1,0,0,0,1	[14] Thm 3.1
6	538813	1,0,0,0,1,0,1,0,1,0,0,0,1	[14] Thm 3.1
6	538975	1,0,0,0,0,1,1,0,1,0,0,0,1	[14] Thm 3.1
6	551855	2,0,0,0,0,0,1,0,0,1,0,0,1	[14] Thm 3.1
6	551935	1,0,0,0,1,0,1,0,0,1,0,0,1	[14] Thm 3.1
6	571591	1,0,0,2,0,0,1,0,0,2,0,0,1	[22] Table 2 No.5
6	591221	2,0,0,0,0,0,1,0,0,0,1,0,1	[14] Thm 3.1
6	591229	1,0,1,0,0,0,1,0,0,0,1,0,1	[14] Thm 3.1
6	591247	1,0,0,1,0,0,1,0,0,0,1,0,1	[14] Thm 3.1
6	591463	1,0,0,0,0,1,1,0,0,0,1,0,1	[14] Thm 3.1
6	650431	1,0,0,0,2,0,1,0,0,0,2,0,1	Thm 2.2.2
6	709327	1,0,1,0,0,0,1,0,0,0,0,1,1	[14] Thm 3.1
6	709399	1,0,0,0,1,0,1,0,0,0,0,1,1	[14] Thm 3.1
6	709559	2,2,2,2,2,0,1,0,0,0,0,1,1	[22] Thm 3.10
6	1419125	2,1,0,0,0,2,2,0,0,0,0,2,2	[14] Thm 3.2
6	1592863	1,2,2,2,2,2,0,2,2,2,2,2,2	[22] Prop 3.2 (ii)
6	4612151	2,0,1,0,0,2,2,2,0,0,0,2,2,2	Thm 2.2.1
6	6905813	2,1,2,2,2,2,1,1,2,2,2,2,0,1,1	[14] Thm 3.6
6	10095919	1,2,2,2,2,2,0,2,2,2,2,2,0,0,2	[14] Thm 3.2
6	19657477	1,0,2,2,2,2,0,0,2,2,2,2,0,0,1,1	[14] Thm 3.2
6	258280325	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,1	[22] Prop 3.1

3 Desirable Triples of the Form $(q^a - q^b - 1, e; q)$[†]

In this chapter, we study desirable triples $(n, e; q)$, where n is of the form $q^a - q^b - 1$. From our initial computer search we noticed that $g_{n,q}$ is always a PP of $\mathbb{F}_{q^2}$ when base q digits of n are $(q-1, q-1, q-2, q-1)$. These observations motivated us to discover all desirable triples $(n, 2; 5)$ where the base 5 digits of n are all 4 except only one being 3. Table 3.1 contains all such desirable triples when $q = 5$ and $e = 2$ with their corresponding a and b values.

Table 3.1: Desirable triples $(5^a - 5^b - 1, 2; q)$, $a, b \geq 0$

n	base 5 digits of n	a	b
599	4 4 3 4	4	2
14999	4 4 4 4 3 4	6	4
15599	4 4 3 4 4 4	6	2
15619	4 3 4 4 4 4	6	1
74999	4 4 4 4 4 3 4	7	5
374999	4 4 4 4 4 4 3 4	8	6
389999	4 4 4 4 3 4 4 4	8	4
390599	4 4 3 4 4 4 4 4	8	2
390619	4 3 4 4 4 4 4 4	8	1
1949999	4 4 4 4 4 3 4 4 4	9	5
7812499	4 4 4 4 4 4 4 4 4 3	10	9

These results clearly indicated that the form $n = q^a - q^b - 1$ is special. As a result, a seperate computer search was conducted for this type of desirable triples only.

[†]Portions of this chapter are taken from [14] which has been published in the journal "Finite Fields and Their Applications".

This chapter is organized as follows: In Section 3.1, we discuss the case $b = 0$ and present results that explain desirable triples when $e > 2$. Section 3.2 focuses on desirable triples $(q^a - q^b - 1, 2; q)$. All desirable triples $(q^a - q^b - 1, 2; q)$, $q \leq 97$, $0 < b < a < 2p$, that are not covered by Corollary 3.1.2 and Theorems 3.1.3, 3.2.1, 3.2.2 are included in Table 3.2 that can be found at the end of this chapter. Theorem 3.2.7 explains some desirable triples in Table 3.2. But in many other cases, no theoretic explanation of the computer results in known.

Three conjectures are stated in this chapter. Conjecture 3.1.1 is related to Payne's Theorem when q is even. Conjecture 3.1.4 states that there are no other cases when $e > 2$ except the cases explained by Corollary 3.1.2 and Theorem 3.1.3. Conjecture 3.2.6 predicts several classes of permutation binomials of $\mathbb{F}_{q^2}$.

Recall that $S_a = \mathtt{x} + \mathtt{x}^q + \cdots + \mathtt{x}^{q^{a-1}}$ for every integer $a \geq 0$.

3.1 The Polynomial $g_{q^a-q^b-1,q}$

Assume $n > 0$ and $n \equiv q^a - q^b - 1 \pmod{q^{pe} - 1}$ for some integers $a, b \geq 0$. If $a = 0$ or b, then $n \sim_{(e,q)} q^{pe} - 2$, where $(q^{pe-2}, e; q)$ is desirable if and only if $q > 2$ [22, Proposition 3.2 (i)]. If $b = 0$ and $a > 0$, we have $n \equiv q^a - 2 \pmod{q^{pe} - 1}$. By Proposition 1.1.1 and Lemma 1.1.3,

$$\begin{aligned} g_{q^a-2,q} &= \frac{1}{\mathtt{x}}(g_{q^a+q-2,q} - g_{q^a-1,q}) \\ &= \frac{1}{\mathtt{x}}\Big[-1 - \frac{1}{\mathtt{x}}(g_{q^a+q-1,q} - g_{q^a,q})\Big] \\ &= \frac{1}{\mathtt{x}}\Big(-1 + \frac{S_a}{\mathtt{x}}\Big) \\ &= \frac{S_{a-1}^q}{\mathtt{x}^2} \\ &= \mathtt{x}^{q-2} + \mathtt{x}^{q^2-2} + \cdots + \mathtt{x}^{q^{a-1}-2}. \end{aligned} \tag{3.1.1}$$

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 3.1.1 *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 $f(x)$ and $f(x)/x$ are permutations of $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^n}^*$ respectively, are exactly of the form $f(x) = ax^{2^k}$ with $a \in \mathbb{F}_{2^n}^*$ and $\gcd(k, n) = 1$ [19, §8.5], [20, 35, 36].

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 (1.1.9), we have

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

So

$$g_{q^a-q^b-1,q} = -\frac{1}{\mathtt{x}} - \frac{(S_b^{q-1}-1)S_{a-b}^{q^b}}{\mathtt{x}^{q^b+1}}. \tag{3.1.2}$$

(Note that (3.1.2) also holds for $b = 0$; see (3.1.1).) 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 (3.1.2) we have

$$g_{q^a-q^b-1,q} \equiv -\mathtt{x}^{q^e-2} - \mathtt{x}^{q^e-q^{b_0}-2}(a_1 S_e + S_{a_0}^{q^{b_0}})\big((b_1 S_e + S_{b_0})^{q-1} - 1\big) \pmod{\mathtt{x}^{q^e} - \mathtt{x}}. \tag{3.1.3}$$

Corollary 3.1.2 *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 (3.1.2). ∎

The following theorem is a generalization of [22, Proposition 3.2 (i)].

Theorem 3.1.3 *Assume* $e \geq 2$. *Let* $0 < b < a < pe$. *Then*

$$g_{q^a-q^b-1,q} \equiv -\mathtt{x}^{q^e-2} \pmod{\mathtt{x}^{q^e} - \mathtt{x}} \tag{3.1.4}$$

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 (3.1.3), we have $a_0 = b_0 = 0$ and $0 < b_1 < p$. So

$$\begin{aligned} g_{q^a-q^b-1,q} &\equiv -\mathtt{x}^{q^e-2} - \mathtt{x}^{q^e-3} a_1 S_e\big((b_1 S_e)^{q-1} - 1\big) \pmod{\mathtt{x}^{q^e} - \mathtt{x}} \\ &= -\mathtt{x}^{q^e-2} - \mathtt{x}^{q^e-3} a_1 S_e (S_e^{q-1} - 1) \\ &= -\mathtt{x}^{q^e-2} - \mathtt{x}^{q^e-3} a_1 (S_e^q - S_e) \\ &\equiv -\mathtt{x}^{q^e-2} \pmod{\mathtt{x}^{q^e} - \mathtt{x}}. \end{aligned} \tag{3.1.5}$$

($\Rightarrow$) Assume (3.1.4) holds. Then by (3.1.2),

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

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 $0<a<pe$,

$$S_{a-b}=S_{a_1e+a_0}\equiv a_1S_e+S_{a_0}\not\equiv 0 \pmod{\mathtt{x}^{q^e}-\mathtt{x}}.$$

So we must have $\mathbb{F}_{q^e}\subset\mathbb{F}_{q^b}$. Hence $b\equiv 0 \pmod e$. Now by (3.1.3) and the calculation in (3.1.5), we have

$$S_{a_0}(S_e^{q-1}-1)\equiv 0 \pmod{\mathtt{x}^{q^e}-\mathtt{x}}. \tag{3.1.6}$$

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 (3.1.6). 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 (3.1.3), 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 3.1.2 and Theorem 3.1.3.

Conjecture 3.1.4 *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) $a \equiv b \equiv 0 \pmod{e}$.

3.2 Desirable Triples of the Form $(q^a - q^b - 1, 2; q)$

While Corollary 3.1.2 and Theorem 3.1.3 cover all known desirable triples $(q^a - q^b - 1, e; q)$ when $e \geq 3$, Conjecture 3.1.4 states that there are no other cases. In contrast the case $e = 2$ seems to be chaotic, and of course very interesting too; see Table 3.2. For the rest of this chapter, we will focus on desirable triples of the form $(q^a - q^b - 1, 2; q)$, $0 < b < a < 2p$.

3.2.1 The Case $b = p$

Theorem 3.2.1 *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 $0 < i \leq \frac{1}{2}(p-1)$ *and* $n = q^{p+2i} - q^p - 1$. *Then*

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

(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 (3.1.3), $a_0 = 0$, $a_1 = i$, $b_0 = 1$, $b_1 = \frac{p-1}{2}$. 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 3.2.2 *Let p be an odd prime and q a power of p.*

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

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

(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 (3.1.3), $a_0 = 1$, $a_1 = i - 1$, $b_0 = 1$, $b_1 = \frac{p-1}{2}$. 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 $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

■

Proposition 3.2.3 *Let p be an odd prime and $q = p^k$. Let $i > 0$. If i is even,*

$$g_{q^{p+i}-q^p-1,q} \equiv -\mathtt{x}^{q^2-2} - i\mathtt{x}^{q-2} \sum_{j=0}^{q-2} \mathtt{x}^{(q-1)j} \pmod{\mathtt{x}^{q^2} - \mathtt{x}}.$$

If i is odd,

$$g_{q^{p+i}-q^p-1,q} \equiv -\mathtt{x}^{q^2-q-1} - i\mathtt{x}^{q-2} \sum_{j=0}^{q-2} \mathtt{x}^{(q-1)j} \pmod{\mathtt{x}^{q^2} - \mathtt{x}}.$$

Proof. Let $n = q^{p+i} - q^p - 1$. Throughout the proof, "$\equiv$" means "$\equiv \pmod{\mathtt{x}^{q^2} - \mathtt{x}}$".

Case 1. Assume that i is even. Let $e = 2$, $a = p + i$, $b = p$. In the notation of (3.1.3), $a_0 = 0$, $a_1 = \frac{i}{2}$, $b_0 = 1$, $b_1 = \frac{p-1}{2}$. By (3.1.3), we have

$$\begin{aligned} g_{n,q} &\equiv -\mathtt{x}^{q^2-2} - \mathtt{x}^{q^2-q-2}\,\frac{i}{2}S_2 \cdot \Big[\Big(-\frac{1}{2}S_2 + S_1\Big)^{q-1} - 1\Big] \\ &= -\mathtt{x}^{q^2-2} - \frac{i}{2}\mathtt{x}^{q^2-q-2}(\mathtt{x} + \mathtt{x}^q)\big((\mathtt{x} - \mathtt{x}^q)^{q-1} - 1\big) \\ &= -\mathtt{x}^{q^2-2} - \frac{i}{2}\mathtt{x}^{q^2-q-1}(1 + \mathtt{x}^{q-1})\big(\mathtt{x}^{q-1}(1 - \mathtt{x}^{q-1})^{q-1} - 1\big). \end{aligned}$$

Note that

$$(1 - \mathtt{x}^{q-1})^{q-1} = \frac{1 - \mathtt{x}^{(q-1)q}}{1 - \mathtt{x}^{q-1}} = \sum_{j=0}^{q-1} \mathtt{x}^{(q-1)j}.$$

So

$$\begin{aligned} g_{n,q} &\equiv -\mathtt{x}^{q^2-2} - \frac{i}{2}\mathtt{x}^{q^2-q-1}(1 + \mathtt{x}^{q-1})\Big[\mathtt{x}^{q-1}\sum_{j=0}^{q-1}\mathtt{x}^{(q-1)j} - 1\Big] \\ &= -\mathtt{x}^{q^2-2} - \frac{i}{2}\mathtt{x}^{q^2-q-1}\Big[\sum_{j=1}^{q}\mathtt{x}^{(q-1)j} + \sum_{j=2}^{q+1}\mathtt{x}^{(q-1)j} - 1 - \mathtt{x}^{q-1}\Big] \\ &= -\mathtt{x}^{q^2-2} - \frac{i}{2}\mathtt{x}^{q^2-q-1} \cdot 2\sum_{j=2}^{q}\mathtt{x}^{(q-1)j} \\ &= -\mathtt{x}^{q^2-2} - i\mathtt{x}^{q-2}\sum_{j=0}^{q-2}\mathtt{x}^{(q-1)j}. \end{aligned}$$

Case 2. Assume that i is odd. In the notation of (3.1.3), $a_0 = 1$, $a_1 = \frac{i-1}{2}$, $b_0 = 1$, $b_1 = \frac{p-1}{2}$. By (3.1.3),

$$\begin{aligned} g_{n,q} \equiv & -\mathtt{x}^{q^2-2} - \mathtt{x}^{q^2-q-2}\Big(\frac{i-1}{2}S_2 + S_1^q\Big)\Big[\Big(-\frac{1}{2}S_2 + S_1\Big)^{q-1} - 1\Big] \\ = & -\mathtt{x}^{q^2-2} - \mathtt{x}^{q^2-q-2}\Big(-\frac{1}{2}S_2 + S_1^q\Big)\Big[\Big(-\frac{1}{2}S_2 + S_1\Big)^{q-1} - 1\Big] \\ & - \frac{i}{2}\mathtt{x}^{q^2-q-2}S_2 \cdot \Big[\Big(-\frac{1}{2}S_2 + S_1\Big)^{q-1} - 1\Big]. \end{aligned}$$

In the above,

$$\begin{aligned}
&- \mathtt{x}^{q^2-2} - \mathtt{x}^{q^2-q-2}\Big(-\frac{1}{2}S_2 + S_1^q\Big)\Big[\Big(-\frac{1}{2}S_2 + S_1\Big)^{q-1} - 1\Big] \\
&= - \mathtt{x}^{q^2-2} - \mathtt{x}^{q^2-q-2}\,\frac{1}{2}\,(\mathtt{x}^q - \mathtt{x})\big((\mathtt{x} - \mathtt{x}^q)^{q-1} - 1\big) \\
&= - \mathtt{x}^{q^2-2} - \frac{1}{2}\mathtt{x}^{q^2-q-2}\big((\mathtt{x}^q - \mathtt{x})^q - (\mathtt{x}^q - \mathtt{x})\big) \\
&\equiv - \mathtt{x}^{q^2-2} - \frac{1}{2}\mathtt{x}^{q^2-q-2} \cdot 2(\mathtt{x} - \mathtt{x}^q) \\
&= - \mathtt{x}^{q^2-q-1},
\end{aligned}$$

and, by the calculation in Case 1,

$$-\frac{i}{2}\mathtt{x}^{q^2-q-2}S_2 \cdot \Big[\Big(-\frac{1}{2}S_2 + S_1\Big)^{q-1} - 1\Big] \equiv -i\mathtt{x}^{q-2}\sum_{j=0}^{q-2}\mathtt{x}^{(q-1)j}.$$

So

$$g_{n,q} \equiv -\mathtt{x}^{q^2-q-1} - i\mathtt{x}^{q-2}\sum_{j=0}^{q-2}\mathtt{x}^{(q-1)j}.$$

■

3.2.2 The Case $b = 1$

Theorem 3.2.4 *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 (3.1.3) (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

$$x^{q-2} + x^{-1} + x^{-q} = c \tag{3.2.7}$$

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

Assume that $x \in \mathbb{F}_{q^2}^*$ is a solution of (3.2.7). 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 (3.2.7), 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

$$x^{q-2} + \mathrm{Tr}_{q^2/q}(x^{-1}) = 0 \tag{3.2.8}$$

has no solution in $\mathbb{F}_{q^2}^*$. Assume to the contrary that $x \in \mathbb{F}_{q^2}^*$ is a solution of (3.2.8). 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 (3.2.8) 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

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

■

Theorem 3.2.5 *(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 (3.1.3), 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) ($\Leftarrow$) 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

$$x^{-q} + x^{q-2} = c \tag{3.2.9}$$

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

Assume $x \in \mathbb{F}_{q^2}^*$ is a solution of (3.2.9). 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 (3.2.9) 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.

($\Rightarrow$) 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).

■

We conclude this section with a conjecture that grew out of Theorem 3.2.5.

Conjecture 3.2.6 *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) $t = 3$, $q \equiv -1 \pmod 6$.

3.2.3 The Case $a = p + i + 1$ and $b = 2i + 1$

Theorem 3.2.7 *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*

$$\left(\frac{2i+1}{q}\right) = \begin{cases} 1 & \text{if } i \text{ is odd,} \\ (-1)^{\frac{q-1}{2}} & \text{if } i \text{ is even,} \end{cases} \tag{3.2.10}$$

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 (3.1.3), $a_0 = 0, a_1 = \frac{p-i}{2}, b_0 = 1, b_1 = i$.

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 $x \in \mathbb{F}_{q^2}^*$,

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

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

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

Let $w = 2(i+1)y^q + 2iy$. Then $y = \dfrac{1}{2(2i+1)}((i+1)w^q - iw)$. (Here $2(i+1)x^q + 2ix$ is a PP of $\mathbb{F}_{q^2}$, and $\dfrac{1}{2(2i+1)}((i+1)x^q - ix)$ is its 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 $c \in \mathbb{F}_{q^2}$,

$$\frac{iu^{2q} + 2(i+1)u^{q+1} + iu^2}{w} = c, \tag{3.2.11}$$

i.e.,

$$\frac{i((i+1)w^q - iw)^{2q} + 2(i+1)((i+1)w^q - iw)^{q+1} + i((i+1)w^q - iw)^2}{w} = c \tag{3.2.12}$$

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 (3.2.12), $t \in \mathbb{F}_q$. Then (3.2.12) 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 (3.2.12) 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

$$iz^2 + 2(i+1)z + i = 0. \tag{3.2.13}$$

Since i is odd $2i+1$ is a square in $\mathbb{F}_q$. So (3.2.13) 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 (3.2.13).

Case 2: i is even.

In the notation of (3.1.3), $a_0 = 1, a_1 = \frac{p-i-1}{2}, b_0 = 1, b_1 = i$.

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

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

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

Let $w = 2(i+1)y^q + 2iy$. Then $y = \frac{1}{2(2i+1)}((i+1)w^q - iw)$. (Here $2(i+1)x^q + 2ix$ is a PP of $\mathbb{F}_{q^2}$, and $\frac{1}{2(2i+1)}((i+1)x^q - ix)$ is its 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 $c \in \mathbb{F}_{q^2}$,

$$\frac{(i+1)u^{2q} + 2iu^{q+1} + (i+1)u^2}{w} = c, \tag{3.2.14}$$

i.e.,

$$\frac{(i+1)((i+1)w^q - iw)^{2q} + 2i((i+1)w^q - iw)^{q+1} + (i+1)((i+1)w^q - iw)^2}{w} = c \tag{3.2.15}$$

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 (3.2.15), $t' \in \mathbb{F}_q$. Then (3.2.15) 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 (3.2.15) 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

$$(i+1)z^2 + 2iz + (i+1) = 0. \tag{3.2.16}$$

Since i is even $\left(\frac{2i+1}{q}\right) = (-1)^{\frac{q-1}{2}}$, i.e. $-(2i+1)$ is a square in $\mathbb{F}_q$. So (3.2.16) 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 (3.2.16).

■

Table 3.2: 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
$\boldsymbol{q = 2}$		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
$\boldsymbol{q = 2^2}$		$\boldsymbol{q = 7^2}$		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
$\boldsymbol{q = 2^3}$		8	3	30	25			41	31	59	5	65	49	76	51
–	–	9	3	33	5	$\boldsymbol{q = 29}$		42	3	61	47	66	49	76	65
		10	5			15	11	42	21	62	49	67	51	77	67
$\boldsymbol{q = 2^4}$		12	5	$\boldsymbol{q = 19}$		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
$\boldsymbol{q = 2^5}$				25	11	31	19	49	43	64	53	71	59	80	47
–	–	$\boldsymbol{q = 11}$		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
$\boldsymbol{q = 2^6}$		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
$\boldsymbol{q = 3}$		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	$\boldsymbol{q = 41}$		$\boldsymbol{q = 43}$		$\boldsymbol{q = 47}$	
$\boldsymbol{q = 3^2}$		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	$\boldsymbol{q = 13}$		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	$\boldsymbol{q = 23}$		47	35	$\boldsymbol{q = 37}$		42	33	39	11	37	31
$\boldsymbol{q = 3^3}$		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
$\boldsymbol{q = 5}$		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
$\boldsymbol{q = 5^2}$		$\boldsymbol{q = 17}$		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	$\boldsymbol{q = 31}$		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
$\boldsymbol{q = 7}$		22	9	39	31	35	7	48	45	60	27	65	61	64	33

Table 3.1 (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 3.1 (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 3.1 (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		

4 The Polynomial $g_{n,q}$ when q is Even[†]

This chapter is organized as follows: Section 4.1 mostly discusses the case when the base q weight of n is $q+1$. We recall that for given integers $d > 1$ and $a = a_0 d^0 + \cdots + a_t d^t$, $0 \leq a_i \leq d-1$, the *base d weight* of a is $w_d(a) = a_0 + \cdots + a_t$. In Section 4.2, we further study the permutation behavior of $g_{n,q}$ in even characteristic when the base q weight of n is arbitrary. Examples are given in each section that explain many desirable triples in Table 4.1 that can be found at the end of this chapter which contains all desirable triples $(n, e; 4)$ with $e \leq 6$ and $w_4(n) > 4$.

Even though this chapter primarily deals with the case of even characteristic we point out to the reader that in Lemmas 4.2.1, 4.2.5, 4.2.17 and Theorem 4.2.6, 4.2.11, 4.2.12, 4.2.19 the characteristic is assumed to be arbitrary.

4.1 Families of Desirable Triples with $w_q(n) = q+1$

Theorem 4.1.1 *Let $q \geq 4$ be even, and let*

$$n = 1 + q^{a_1} + q^{b_1} + \cdots + q^{a_{q/2}} + q^{b_{q/2}},$$

where $a_i, b_i \geq 0$ are integers. Then

$$g_{n,q} = \sum_i S_{a_i} S_{b_i} + \sum_{i<j} (S_{a_i} + S_{b_i})(S_{a_j} + S_{b_j}).$$

[†]Portions of this chapter are taken from [14] which has been published in the journal "Finite Fields and Their Applications".

Proof. We write g_n for $g_{n,q}$. By (1.1.10) we have

$$\begin{aligned}
g_n &= g_{1+2q^{a_1}+q^{a_2}+q^{b_2}+\cdots+q^{a_{q/2}}+q^{b_{q/2}}} + (S_{b_1} - S_{a_1}) g_{1+q^{a_1}+q^{a_2}+q^{b_2}+\cdots+q^{a_{q/2}}+q^{b_{q/2}}} \\
&= g_{1+2q^{a_1}+q^{a_2}+q^{b_2}+\cdots+q^{a_{q/2}}+q^{b_{q/2}}} \\
&\quad + (S_{a_1} + S_{b_1})(S_{a_1} + S_{a_2} + S_{b_2} + \cdots + S_{a_{q/2}} + S_{b_{q/2}}) \\
&= \cdots\cdots \\
&= g_{1+2q^{a_1}+\cdots+2q^{a_{q/2}}} + \sum_{i=1}^{q/2} (S_{a_i} + S_{b_i}) \Big(S_{a_i} + \sum_{j=i+1}^{q/2} (S_{a_j} + S_{b_j}) \Big) \\
&= S_{a_1}^2 + \cdots + S_{a_{q/2}}^2 + \sum_{i=1}^{q/2} (S_{a_i} + S_{b_i}) \Big(S_{a_i} + \sum_{j=i+1}^{q/2} (S_{a_j} + S_{b_j}) \Big) \\
&= \sum_i S_{a_i} S_{b_i} + \sum_{i<j} (S_{a_i} + S_{b_i})(S_{a_j} + S_{b_j}).
\end{aligned}$$

■

Corollary 4.1.2 *Let $q \geq 4$ be even, and let*

$$n = t_0 + 2t_1 q^{a_1} + \cdots + 2t_k q^{a_k},$$

where $t_0, \ldots, t_k$ and $a_1, \ldots, a_k$ are nonnegative integers with $t_0 + 2t_1 + \cdots + 2t_k = q+1$. Then

$$g_{n,q} = (t_1 S_{a_1} + \cdots + t_k S_{a_k})^2.$$

In particular, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$ if and only if

$$\gcd\Big(\sum_{i=1}^{k} t_i (1 + \mathtt{x} + \cdots + \mathtt{x}^{a_i - 1}),\ \mathtt{x}^e - 1 \Big) = 1.$$

Proof. By Theorem 4.1.1,

$$g_{n,q} = t_1 S_{a_1}^2 + \cdots + t_k S_{a_k}^2 = (t_1 S_{a_1} + \cdots + t_k S_{a_k})^2.$$

The rest is obvious.

■

In Theorem 4.1.1, the mapping $g_{n,q} : \mathbb{F}_{q^e} \to \mathbb{F}_{q^e}$ is quadratic in the multivariate sense, i.e., with the identification $\mathbb{F}_{q^e} \cong \mathbb{F}_q^e$. In general, it is difficult to tell whether a quadratic mapping is bijective. However, in some cases, such as Corollary 4.1.2, $g_{n,q}$ can be reduced to a suitable form which allows a quick determination whether it is a PP. Here are some additional examples of Theorem 4.1.1:

Example 4.1.3 Let $q = 2^s$, $s > 1$, $e > 1$ odd, $n = q^0 + (q-1)q^1 + q^2$. Then

$$g_{n,q} = S_1^2 + S_1 S_2 = \mathtt{x}^{q+1},$$

which is a PP of $\mathbb{F}_{q^e}$.

Example 4.1.4 Let $q = 4$, $e > 1$, $n = q^0 + q^1 + q^e + q^{e+1} + q^a$, $a \geq 0$. Then

$$\begin{aligned} g_{n,q} &= S_1 S_a + S_e S_{e+1} + (S_1 + S_a)(S_e + S_{e+1}) \\ &\equiv S_1 S_a + S_e S_{e+1} + (S_1 + S_a) S_1 \pmod{\mathtt{x}^{q^e} - \mathtt{x}} \\ &= S_1^2 + S_e S_{e+1} \\ &= \mathtt{x}^2 + \mathtt{x}\mathrm{Tr}_{q^e/q}(\mathtt{x}) + \mathrm{Tr}_{q^e/q}(\mathtt{x})^2. \end{aligned}$$

We claim that when e is odd, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Assume to the contrary that there exist $x, y \in \mathbb{F}_{q^e}$, $x \neq y$, such that $g_{n,q}(x) = g_{n,q}(y)$. From $\mathrm{Tr}_{q^e/q}(g_{n,q}(x)) = \mathrm{Tr}_{q^e/q}(g_{n,q}(y))$, we derive that $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y) = c$. Then the equation $g_{n,q}(x) = g_{n,q}(y)$ becomes

$$(x + y + c)(x + y) = 0.$$

So $x + y + c = 0$. Thus $c = \mathrm{Tr}_{q^e/q}(c) = \mathrm{Tr}_{q^e/q}(x + y) = 0$. Hence $(x + y)^2 = 0$, which is a contradiction.

Example 4.1.5 Let $q = 4$, $e > 1$, $n = q^0 + 2q^1 + q^e + q^{e+1}$. Then by Theorem 4.1.1,

$$\begin{aligned} g_{q^0+2\cdot q^1+q^e+q^{e+1}} &= S_1S_1 + S_eS_{e+1} \\ &\equiv \mathtt{x}^2 + \mathtt{x}\mathrm{Tr}_{q^e/q}(\mathtt{x}) + \mathrm{Tr}_{q^e/q}(\mathtt{x})^2 \pmod{\mathtt{x}^{q^e} - \mathtt{x}}. \end{aligned}$$

We claim that when e is odd, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.
Assume that there exist $x, a \in \mathbb{F}_{q^e}$ such that $g(x) = g(x + a)$. Then

$$x^2 + x\mathrm{Tr}_{q^e/q}(x) + \mathrm{Tr}_{q^e/q}(x)^2 = (x+a)^2 + (x+a)\mathrm{Tr}_{q^e/q}(x+a) + \mathrm{Tr}_{q^e/q}(x+a)^2. \quad (4.1.1)$$

It leads to

$$a^2 + x\mathrm{Tr}_{q^e/q}(a) + a\mathrm{Tr}_{q^e/q}(x) + a\mathrm{Tr}_{q^e/q}(a) + \mathrm{Tr}_{q^e/q}(a)^2 = 0. \quad (4.1.2)$$

By taking traces on both sides of (4.1.2) we get $\mathrm{Tr}_{q^e/q}(a) = 0$.
By (4.1.2), $a(a + \mathrm{Tr}_{q^e/q}(x)) = 0$.
If $\mathrm{Tr}_{q^e/q}(x) = a$, taking traces on both sides gives $e\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(a) = 0$. Since e is odd $\mathrm{Tr}_{q^e/q}(x) = 0$, which is a contradiction. Therefore $a = 0$.

Example 4.1.6 Let $q = 4$, $e > 1$, $n = q^0 + q^1 + 2q^{e-1} + q^e$. Then by Theorem 4.1.1,

$$\begin{aligned} g_{q^0+q^1+2q^{e-1}+q^e} &= S_1S_e + S_{e-1}S_{e-1} \\ &= \mathtt{x}\mathrm{Tr}_{q^e/q}(\mathtt{x}) + \mathrm{Tr}_{q^e/q}(\mathtt{x})^2 + \mathtt{x}^{2q^{e-1}}. \end{aligned}$$

We claim that when e is odd, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.
Assume that there exist $x, a \in \mathbb{F}_{q^e}$ such that $g(x) = g(x + a)$. Then

$$x\mathrm{Tr}_{q^e/q}(x) + \mathrm{Tr}_{q^e/q}(x)^2 + x^{2q^{e-1}} = (x+a)\mathrm{Tr}_{q^e/q}(x+a) + \mathrm{Tr}_{q^e/q}(x+a)^2 + (x+a)^{2q^{e-1}}. \quad (4.1.3)$$

It leads to

$$x\mathrm{Tr}_{q^e/q}(a) + a\mathrm{Tr}_{q^e/q}(x) + a\mathrm{Tr}_{q^e/q}(a) + \mathrm{Tr}_{q^e/q}(a)^2 + a^{2q^{e-1}} = 0. \quad (4.1.4)$$

By taking traces on both sides we get $\mathrm{Tr}_{q^e/q}(a) = 0$. By (4.1.4),

$$a\mathrm{Tr}_{q^e/q}(x) + a^{2q^{e-1}} = 0. \tag{4.1.5}$$

If $\mathrm{Tr}_{q^e/q}(x) = 0$, $a = 0$.
If $\mathrm{Tr}_{q^e/q}(x) = 1$, $a + a^{2q^{e-1}} = 0$. Squaring both sides gives $a(a+1) = 0$. If $a = 1$, then since e is odd, it contradicts the fact that $\mathrm{Tr}_{q^e/q}(a) = 0$. Therefore $a = 0$.
If $\mathrm{Tr}_{q^e/q}(x) \neq 0, 1$, squaring both sides of (4.1.5) gives $a(a\mathrm{Tr}_{q^e/q}(x)^2 + 1) = 0$. If $a\mathrm{Tr}_{q^e/q}(x)^2 + 1 = 0$, taking traces on both sides gives $e = 0$. It contradicts the fact that e is odd. Therefore $a = 0$.

Example 4.1.7 Let $q = 4$, $e > 2$, $n = q^0 + 2q^{e-2} + 2q^{e-1}$. Then by Theorem 4.1.1,

$$g_{q^0+2q^{e-2}+2q^{e-1}} = S_{e-2}^2 + S_{e-1}^2 = \mathtt{x}^{2q^{e-2}}.$$

Since $\gcd(2q^{e-2}, q^e - 1) = 1$, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Example 4.1.8 Let $q = 4$, $e > 2$, $n = q^0 + 2q^1 + 2q^2$. Then by Theorem 4.1.1,

$$g_{q^0+2q^1+2q^2} = S_1^2 + S_2^2 = \mathtt{x}^{2q}.$$

Since $\gcd(2q, q^e - 1) = 1$, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Example 4.1.9 Let $q = 4$, $e \geq 2$, $n = 3q^0 + 2q^1$. Then by Theorem 4.1.1,

$$g_{3q^0+2q^1} = S_0^2 + S_1^2 = \mathtt{x}^2.$$

Since $\gcd(2, q^e - 1) = 1$, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Example 4.1.10 Let $q = 2^s$, $s > 1$, $e > 1$, $n = (q-1)q^0 + 2q^{e-1}$. Then by Theorem 4.1.1,

$$\begin{aligned} g_{(q-1)q^0+2q^{e-1}} &= S_0^2 + S_{e-1}^2 \\ &= S_e^2 + \mathtt{x}^{2q^{e-1}}. \end{aligned}$$

We claim that when e is even, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.
Assume that there exist $x, a \in \mathbb{F}_{q^e}$ such that $g(x) = g(x+a)$. Then we have

$$\mathrm{Tr}_{q^e/q}(x)^2 + x^{2q^{e-1}} = \mathrm{Tr}_{q^e/q}(x+a)^2 + (x+a)^{2q^{e-1}}. \tag{4.1.6}$$

It leads to

$$\mathrm{Tr}_{q^e/q}(a)^2 + a^{2q^{e-1}} = 0. \tag{4.1.7}$$

If we raise both sides to the $(q/2)^{\text{th}}$ power, we get $\mathrm{Tr}(a) + a^{q^e} = 0$. By taking traces on both sides we get $(e+1)\mathrm{Tr}_{q^e/q}(a) = 0$. Since e is even $\mathrm{Tr}_{q^e/q}(a) = 0$.
By (4.1.7), $a = 0$.

Example 4.1.11 Let $q = 2^s$, $s > 1$, $e > 1$, $n = (q-1)q^0 + 2q^{e-2}$. Then by Theorem 4.1.1,

$$\begin{aligned} g_{(q-1)q^0+2q^{e-2}} &= S_0^2 + S_{e-2}^2 \\ &= S_e^2 + \mathtt{x}^{2q^{e-2}} + \mathtt{x}^{2q^{e-1}}. \end{aligned}$$

We claim that when e is odd, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.
Assume that there exist $x, a \in \mathbb{F}_{q^e}$ such that $g(x) = g(x+a)$. Then we have

$$\mathrm{Tr}_{q^e/q}(x)^2 + x^{2q^{e-2}} + x^{2q^{e-1}} = \mathrm{Tr}_{q^e/q}(x+a)^2 + (x+a)^{2q^{e-2}} + (x+a)^{2q^{e-1}}. \tag{4.1.8}$$

It leads to

$$\mathrm{Tr}_{q^e/q}(a)^2 + a^{2q^{e-2}} + a^{2q^{e-1}} = 0. \tag{4.1.9}$$

By taking traces on both sides we get $\mathrm{Tr}_{q^e/q}(a) = 0$.
By (4.1.9), $a^{2\cdot q^{e-2}} + a^{2\cdot q^{e-1}} = 0$.
Raising both sides to the $(q/2)^{\text{th}}$ power gives $a(a^{q^{e-2}} + 1) = 0$.
If $a^{q^{e-2}} + 1 = 0$, $\mathrm{Tr}_{q^e/q}(a) = 1$, since e is odd, which is a contradiction.
So $a = 0$.

Example 4.1.12 Let $q = 4$, $e > 2$, $n = q^0 + 2q^1 + 2q^e$. Then by Theorem 4.1.1,

$$\begin{aligned} g_{q^0+2q^1+2q^e} &= S_1^2 + S_e^2 \\ &= \mathtt{x}^2 + S_e^2. \end{aligned}$$

We claim that when e is even, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.
Assume that there exist $x, a \in \mathbb{F}_{q^e}$ such that $g(x) = g(x + a)$. Then we have

$$x^2 + \mathrm{Tr}_{q^e/q}(x)^2 = (x + a)^2 + \mathrm{Tr}_{q^e/q}(x + a)^2. \tag{4.1.10}$$

It leads to

$$\mathrm{Tr}_{q^e/q}(a)^2 + a^2 = 0. \tag{4.1.11}$$

Since e is even, by taking traces on both sides we get $\mathrm{Tr}_{q^e/q}(a) = 0$.
Then by (4.1.11), $a = 0$.

4.2 More Families of Desirable Triples with Even q

Lemma 4.2.1 *Let $n = (q-1)q^a + (q-1)q^b$, where $a, b \geq 0$. Then*

$$g_{n,q} = -1 - (S_b - S_a)^{q-1}.$$

Proof. If $a = b$, then $n = (q-2)q^a + q^{a+1}$. By Lemma 1.1.3, $g_{n,q} = -1$.

Now assume $a < b$. We have

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

Thus $g_{n,q} = -1 - (S_b - S_a)^{q-1}$.

■

Theorem 4.2.2 *Let $q = 2^s$, $s > 1$, $e > 0$, and $n = (q-1)q^0 + (q-1)q^e + 2q^a$, $a \geq 0$. Then*

$$g_{n,q} \equiv \mathtt{x}\mathrm{Tr}_{q^e/q}(\mathtt{x}) + \mathrm{Tr}_{q^e/q}(\mathtt{x})^2 + S_a^2 \cdot \left(1 + \mathrm{Tr}_{q^e/q}(\mathtt{x})^{q-1}\right) \pmod{\mathtt{x}^{q^e} - \mathtt{x}},$$

Assume that e is even and $\gcd(a, e) = 1$. Then $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Proof. Write $g_n = g_{n,q}$. We have

$$\begin{aligned} g_n &= g_{q+q^a+(q-1)q^e} + S_a \cdot g_{(q-1)q^0+q^a+(q-1)q^e} \\ &= g_{q+q^{e+1}} + (S_a - S_e)g_{q+(q-1)q^e} + S_a \cdot (g_{q+(q-1)q^e} + S_a \cdot g_{(q-1)q^0+(q-1)q^e}) \\ &\equiv S_e(S_e + S_1) + S_a^2(1 + S_e^{q-1}) \pmod{\mathtt{x}^{q^e} - \mathtt{x}} \qquad \text{(Lemma 4.2.1)} \\ &= \mathtt{x}\mathrm{Tr}_{q^e/q}(\mathtt{x}) + \mathrm{Tr}_{q^e/q}(\mathtt{x})^2 + S_a^2 \cdot \left(1 + \mathrm{Tr}_{q^e/q}(\mathtt{x})^{q-1}\right). \end{aligned}$$

To prove that g_n is a PP of $\mathbb{F}_{q^e}$, we assume that $g_n(x) = g_n(y)$, $x, y \in \mathbb{F}_{q^e}$, and try to show that $x = y$. From $\mathrm{Tr}_{q^e/q}(g_n(x)) = \mathrm{Tr}_{q^e/q}(g_n(y))$, we derive that $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y) = c$. If $c = 0$, the equation $g_n(x) = g_n(y)$ becomes $S_a(x)^2 = S_a(y)^2$, i.e., $S_a(x + y) = 0$. Since $\gcd(1 + \mathtt{x} + \cdots + \mathtt{x}^{a-1}, \mathtt{x}^e + 1) = 1$, we have $x = y$. If $c \neq 0$, the equation $g_n(x) = g_n(y)$ becomes $c(x + y) = 0$, which also gives $x = y$.

■

Example 4.2.3 Let $q = 2^s$, $s > 1$, $e > 1$, $n = (q-1)q^0 + 2q^{e-1} + (q-1)q^e$. Then

$$\begin{aligned} g_{(q-1)q^0+2q^{e-1}+(q-1)q^e} &= g_{q+q^{e-1}+(q-1)q^e} + S_{e-1}g_{(q-1)q^0+q^{e-1}+(q-1)q^e} \\ &= g_{q+q^{e+1}} + (S_{e+1} - S_e)g_{q+(q-1)q^e} + S_{e-1}g_{q+(q-1)q^e} + S_{e-1}g_{(q-1)q^0+(q-1)q^e} \\ &= S_e(S_e - x) + S_{e-1}^2 g_{(q-1)q^0+(q-1)q^e} \end{aligned}$$

Note that

$$\begin{aligned} S_e g_{(q-1)q^0+(q-1)q^e} &= g_{(q-1)q^0+q^{e+1}} - g_{q+(q-1)q^e} \\ &= S_e + x^{q^e} - (S_e - x) \\ &= x^{q^e} - x = S_e^q - S_e, \end{aligned}$$

i.e.,

$$g_{(q-1)q^0+(q-1)q^e} = S_e^{q-1} - 1. \tag{4.2.12}$$

So

$$\begin{aligned} g_{(q-1)q^0+2q^{e-1}+(q-1)q^e} &= S_e^2 - xS_e + S_{e-1}^2(S_e^{q-1} - 1) \\ &= S_e^2 - xS_e + (S_e^2 + x^{2q^{e-1}})(S_e^{q-1} - 1) \\ &= x\mathrm{Tr}_{q^e/q}(x) + \mathrm{Tr}_{q^e/q}(x)^2 + x^{2q^{e-1}} + \mathrm{Tr}_{q^e/q}(x)^{q-1}x^{2q^{e-1}}. \end{aligned}$$

Thus modulo $\mathtt{x}^{q^e} - \mathtt{x}$ we have

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

We claim that when e is even, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Clearly $x^{2q^{e-1}}$ and $x\mathrm{Tr}_{q^e/q}(x) + \mathrm{Tr}_{q^e/q}(x)^2$ map two sets $\{x \in \mathbb{F}_{q^e}; \mathrm{Tr}_{q^e/q}(x) = 0\}$ and $\{x \in \mathbb{F}_{q^e}; \mathrm{Tr}_{q^e/q}(x) \neq 0\}$ to themselves respectively.

Case 1. Let $x, y \in \{x \in \mathbb{F}_{q^e}; \mathrm{Tr}_{q^e/q}(x) = 0\}$.

$g(x) = g(y) \;\Rightarrow\; x^{2\cdot q^{e-1}} = y^{2\cdot q^{e-1}}$. Raising both sides to the $(q/2)^{\text{th}}$ power gives $x = y$.

Case 2. Let $x, y \in \{x \in \mathbb{F}_{q^e}; \mathrm{Tr}_{q^e/q}(x) \neq 0\}$ s.t. $x \neq y$ and $g(x) = g(y)$. Then

$$x\mathrm{Tr}_{q^e/q}(x) + \mathrm{Tr}_{q^e/q}(x)^2 = y\mathrm{Tr}_{q^e/q}(y) + \mathrm{Tr}_{q^e/q}(y)^2. \tag{4.2.13}$$

Since e is even, taking traces on both sides gives $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y)$.

By (4.2.14), $(x - y)\mathrm{Tr}_{q^e/q}(x) = 0$. Since $x \neq y$, $\mathrm{Tr}_{q^e/q}(x) = 0$, a contradiction.

Example 4.2.4 Let $q = 2^s$, $s > 1$, $e > 1$, $n = (q-1)q^0 + 2q^1 + (q-1)q^e$. Then

$$
\begin{aligned}
g_{(q-1)q^0+2q^1+(q-1)q^e} &= g_{2q^1+(q-1)q^e} + S_1 g_{(q-1)q^0+q^1+(q-1)q^e} \\
&= g_{2q^1+(q-1)q^e} + S_1\{g_{q^1+(q-1)q^e} + S_1 g_{(q-1)q^0+(q-1)q^e}\} \\
&= g_{2q^1+(q-1)q^e} + S_1(S_e + x) + S_1^2(S_e^{q-1} - 1) \quad (4.2.12) \\
&= g_{q^0+q^1+(q-1)q^e} + S_1 g_{q^1+(q-1)q^e} + xS_e + x^2 S_e^{q-1} \\
&= g_{2q^0+(q-1)q^e} + S_1 g_{q^0+(q-1)q^e} + S_1(S_e + x) + xS_e + x^2 S_e^{q-1} \\
&= g_{2q^0+(q-1)q^e} + x^2 + xS_e + x^2 S_e^{q-1} \\
&= \mathrm{Tr}_{q^e/q}(x)^2 + x^2 + x\mathrm{Tr}_{q^e/q}(x) + x^2\mathrm{Tr}_{q^e/q}(x)^{q-1}.
\end{aligned}
$$

Thus modulo $\mathtt{x}^{q^e} - \mathtt{x}$ we have

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

We claim that when e is even, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Clearly x^2 and $x\mathrm{Tr}_{q^e/q}(x) + \mathrm{Tr}_{q^e/q}(x)^2$ map two sets $\{x \in \mathbb{F}_{q^e}; \mathrm{Tr}_{q^e/q}(x) = 0\}$ and $\{x \in \mathbb{F}_{q^e}; \mathrm{Tr}_{q^e/q}(x) \neq 0\}$ to themselves respectively.

Case 1. Let $x, y \in \{x \in \mathbb{F}_{q^e}; \mathrm{Tr}_{q^e/q}(x) = 0\}$. Then

$$
g(x) = g(y) \;\Rightarrow\; x^2 = y^2 \;\Rightarrow\; x = y.
$$

Case 2. Let $x, y \in \{x \in \mathbb{F}_{q^e}; \mathrm{Tr}_{q^e/q}(x) \neq 0\}$ s.t. $g(x) = g(y)$. Then

$$
x\mathrm{Tr}_{q^e/q}(x) + \mathrm{Tr}_{q^e/q}(x)^2 = y\mathrm{Tr}_{q^e/q}(y) + \mathrm{Tr}_{q^e/q}(y)^2. \tag{4.2.14}
$$

Since e is even, taking traces on both sides gives $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y)$. Then by (4.2.14), $x = y$.

Lemma 4.2.5 *Let $a_1, \ldots, a_q \geq 0$, and $n = (q-1) + q^{a_1} + \cdots + q^{a_q}$. Then*

$$
g_{n,q} = -S_1 - S_{a_1} - \cdots - S_{a_q} - S_{a_1} \cdots S_{a_q}.
$$

Proof. Write $g_n = g_{n,q}$. We have

$$\begin{aligned} g_n &= g_{q+q^{a_2}+\cdots+q^{a_q}} + S_{a_1} \cdot g_{(q-1)+q^{a_2}+\cdots+q^{a_q}} \\ &= g_{q+q^{a_2}+\cdots+q^{a_q}} + S_{a_1} \cdot (g_{q+q^{a_3}+\cdots+q^{a_q}} + S_{a_2} \cdot g_{(q-1)+q^{a_3}+\cdots+q^{a_q}}) \\ &= g_{q+q^{a_2}+\cdots+q^{a_q}} - S_{a_1} + S_{a_1}S_{a_2} \cdot g_{(q-1)+q^{q_3}+\cdots+q^{a_q}} \\ &= \cdots\cdots \\ &= g_{q+q^{a_2}+\cdots+q^{a_q}} - S_{a_1} + S_{a_1}\cdots S_{a_q} \cdot g_{q-1} \\ &= -S_1 - S_{a_2} - \cdots - S_{a_q} - S_{a_1} - S_{a_1}\cdots S_{a_q}. \end{aligned}$$

■

Theorem 4.2.6 *Let $q = p^s$, $e > 0$, $a > 0$, and $n = (q-1)q^0 + (q-1)q^e + q^a$. Then*

$$g_{n,q} = -\mathtt{x} - S_a + \mathrm{Tr}_{q^e/q}(\mathtt{x}) - S_a \mathrm{Tr}_{q^e/q}(\mathtt{x})^{q-1}. \tag{4.2.15}$$

Assume that

(i) $-2a - 1 + e \not\equiv 0 \pmod{p}$;

(ii) $\gcd(\mathtt{x}^a + \mathtt{x} - 2, \mathtt{x}^e - 1) = \mathtt{x} - 1$;

(iii) $\gcd(2\mathtt{x}^a + \mathtt{x} - 3, \mathtt{x}^e - 1) = \mathtt{x} - 1$.

Then $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Proof. Eq. (4.2.15) follows from Lemma 4.2.5. To prove that $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$ under the given conditions, we assume that $g_{n,q}(x) = g_{n,q}(y)$, $x, y \in \mathbb{F}_{q^e}$, and try to show that $x = y$. From $\mathrm{Tr}_{q^e/q}(g_{n,q}(x)) = \mathrm{Tr}_{q^e/q}(g_{n,q}(y))$, we derive that

$$(-2a - 1 + e)\big(\mathrm{Tr}_{q^e/q}(x) - \mathrm{Tr}_{q^e/q}(y)\big) = 0.$$

Since $-2a - 1 + e \not\equiv 0 \pmod{p}$, we have $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y) = c$.

If $c = 0$, the equation $g_{n,q}(x) = g_{n,q}(y)$ becomes

$$2(x-y) + (x-y)^q + \cdots + (x-y)^{q^{a-1}} = 0.$$

Since

$$\gcd(2 + \mathtt{x} + \cdots + \mathtt{x}^{a-1}, 1 + \mathtt{x} + \cdots + \mathtt{x}^{e-1}) = \frac{1}{\mathtt{x}-1}\gcd(\mathtt{x}^a + \mathtt{x} - 2, \mathtt{x}^e - 1) = 1,$$

we must have $x - y = 0$.

If $c \neq 0$, the equation $g_{n,q}(x) = g_{n,q}(y)$ becomes

$$3(x-y) + 2(x-y)^q + \cdots + 2(x-y)^{q^{a-1}} = 0.$$

Since

$$\gcd(3 + 2\mathtt{x} + \cdots + 2\mathtt{x}^{a-1}, 1 + \mathtt{x} + \cdots + \mathtt{x}^{e-1}) = \frac{1}{\mathtt{x}-1}\gcd(2\mathtt{x}^a + \mathtt{x} - 3, \mathtt{x}^e - 1) = 1,$$

we also have $x - y = 0$.

■

Example 4.2.7 Let $q = 2^s$, $s > 1$, $e > 1$, $n = (q-1)q^0 + q^2 + (q-1)q^e$. Then

$$\begin{aligned} g_{(q-1)q^0+q^2+(q-1)q^e} &= g_{q+(q-1)q^e} + S_2 g_{(q-1)q^0+(q-1)q^e} \\ &= x + \mathrm{Tr}(x) + (x + x^q) g_{(q-1)q^0+(q-1)q^e} \\ &= x + \mathrm{Tr}(x) + (x + x^q)(\mathrm{Tr}_{q^e/q}(x)^{q-1} - 1)(4.2.12) \\ &= x^q + \mathrm{Tr}_{q^e/q}(x) + x^q \mathrm{Tr}_{q^e/q}(x)^{q-1} + x\mathrm{Tr}_{q^e/q}(x)^{q-1}. \end{aligned}$$

Thus modulo $\mathtt{x}^{q^e} - \mathtt{x}$ we have

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

We claim that when e is even, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Clearly x^q and $x + \mathrm{Tr}_{q^e/q}(x)$ map two sets $\{x \in \mathbb{F}_{q^e}; \mathrm{Tr}_{q^e/q}(x) = 0\}$ and $\{x \in \mathbb{F}_{q^e}; \mathrm{Tr}_{q^e/q}(x) \neq 0\}$ to themselves respectively.

Case 1. Let $x, y \in \{x \in \mathbb{F}_{q^e}; \mathrm{Tr}_{q^e/q}(x) = 0\}$. Then

$$g(x) = g(y) \;\Rightarrow\; x^q = y^q \;\Rightarrow\; x = y.$$

Case 2. Let $x, y \in \{x \in \mathbb{F}_{q^e}; \mathrm{Tr}_{q^e/q}(x) \neq 0\}$ s.t. $g(x) = g(y)$. Then

$$x + \mathrm{Tr}_{q^e/q}(x) = y + \mathrm{Tr}_{q^e/q}(y). \tag{4.2.16}$$

Since e is even, taking traces on both sides gives $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y)$. Then by (4.2.16), $x = y$.

Theorem 4.2.8 *Let $q = 2^s$, $s > 1$, $e > 0$, and let $n = (q-1)q^0 + \frac{q}{2}q^{e-1} + \frac{q}{2}q^e$. We have*

$$g_{n,q} = \mathtt{x} + \mathrm{Tr}_{q^e/q}(\mathtt{x}) + \mathtt{x}^{\frac{1}{2}q^e}\mathrm{Tr}_{q^e/q}(\mathtt{x})^{\frac{1}{2}q}.$$

When e is odd, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Proof. By Lemma 4.2.5,

$$\begin{aligned} g_{n,q} &= S_1 + S_{e-1}^{\frac{q}{2}} S_e^{\frac{q}{2}} \\ &= \mathtt{x} + (S_e^{\frac{1}{2}q} + \mathtt{x}^{\frac{1}{2}q^e}) S_e^{\frac{1}{2}q} \\ &= \mathtt{x} + \mathrm{Tr}_{q^e/q}(\mathtt{x}) + \mathtt{x}^{\frac{1}{2}q^e}\mathrm{Tr}_{q^e/q}(\mathtt{x})^{\frac{1}{2}q}. \end{aligned}$$

Assume that e is odd. To prove that $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$, assume to the contrary that there exist $x, y \in \mathbb{F}_{q^e}$, $x \neq y$, such that $g_{n,q}(x) = g_{n,q}(y)$. From $\mathrm{Tr}_{q^e/q}(g_{n,q}(x)) = \mathrm{Tr}_{q^e/q}(g_{n,q}(y))$, we derive that $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y) = a$. If $a = 0$, the equation $g_{n,q}(x) = g_{n,q}(y)$ becomes $x = y$, which is a contradiction. If $a \neq 0$, the equation $g_{n,q}(x) = g_{n,q}(y)$ becomes

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

i.e.,

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

So $x + y = a$. Then $a = \mathrm{Tr}_{q^e/q}(a) = \mathrm{Tr}_{q^e/q}(x+y) = 0$, which is a contradiction.

■

Example 4.2.9 Let $q = 4$, $e > 1$ and Let $n = 3q^0 + 2q^{e-1} + 2q^e$. Then

$$\begin{aligned}
g_{3\cdot q^0+2q^{e-1}+2q^e} &= g_{q+2q^{e-1}+q^e} + S_e g_{3q^0+2q^{e-1}+q^e} \\
&= x + \mathrm{Tr}_{q^e/q}(x) + S_e g_{3q^0+2q^{e-1}+q^e} \\
&= x + \mathrm{Tr}_{q^e/q}(x) + S_e(1 + S_e g_{3q^0+2q^{e-1}}) \\
&= x + \mathrm{Tr}_{q^e/q}(x) + S_e + S_e^2 g_{3q^0+2q^{e-1}} \\
&= x + \mathrm{Tr}_{q^e/q}(x) + S_e + S_e^2 S_{e-1}^2 \\
&= x + S_e^2 S_{e-1}^2 \\
&= x + \mathrm{Tr}_{q^e/q}(x)^2 (\mathrm{Tr}_{q^e/q}(x) + x^{q^{e-1}})^2 \\
&= x + \mathrm{Tr}_{q^e/q}(x) + x^{2q^{e-1}} \mathrm{Tr}_{q^e/q}(x)^2.
\end{aligned}$$

We claim that when e is odd, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$. Assume that there exist $x, a \in \mathbb{F}_{q^e}$ such that $g(x) = g(x+a)$. Then we have
$x + \mathrm{Tr}_{q^e/q}(x) + x^{2q^{e-1}} \mathrm{Tr}_{q^e/q}(x)^2 = (x+a) + \mathrm{Tr}_{q^e/q}(x+a) + (x+a)^{2q^{e-1}} \mathrm{Tr}_{q^e/q}(x+a)^2$.
It leads to

$$a + \mathrm{Tr}_{q^e/q}(a) + \mathrm{Tr}_{q^e/q}(x)^2 a^{2q^{e-1}} + \mathrm{Tr}_{q^e/q}(a)^2 x^{2q^{e-1}} + \mathrm{Tr}_{q^e/q}(a)^2 a^{2q^{e-1}} = 0. \quad (4.2.17)$$

By taking traces on both sides we get $\mathrm{Tr}_{q^e/q}(a) = 0$.
By (4.2.17),

$$a + \mathrm{Tr}_{q^e/q}(x)^2 a^{2q^{e-1}} = 0. \quad (4.2.18)$$

If $\mathrm{Tr}_{q^e/q}(x) = 0$, then (4.2.18) gives $a = 0$.
If $\mathrm{Tr}_{q^e/q}(x) = 1$, then (4.2.18) gives $a + a^{2q^{e-1}} = 0$. Squaring both sides of gives $a(a+1) = 0$. If $a = 1$, since e is odd that contradicts the fact that $\mathrm{Tr}_{q^e/q}(a) = 0$. Therefore $a = 0$.

If $\mathrm{Tr}_{q^e/q}(x) \neq 0, 1$, squaring both sides of (4.2.18) gives $a(a + \mathrm{Tr}_{q^e/q}(x)) = 0$. If $\mathrm{Tr}_{q^e/q}(x) = a$, taking traces on both sides gives $e\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(a) = 0$. Since e is odd $\mathrm{Tr}_{q^e/q}(x) = 0$, which is a contradiction. Therefore $a = 0$.

Theorem 4.2.10 *Let $q = 4$, $e > 2$, and $n = 3q^0 + 2q^{e-2} + 2q^e$. We have*

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

Assume that $e > 2$ is even and $\gcd(1 + \mathtt{x}^2 + \mathtt{x}^{e-3}, \mathtt{x}^e + 1) = 1$. *Then $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.*

Proof. Let $q = 4$, $e > 2$, $n = 3q^0 + 2q^{e-2} + 2q^e$. Then,

$$g_{n,q} = \mathtt{x} + \mathrm{Tr}_{q^e/q}(\mathtt{x}) + (\mathtt{x}^{q^{e-2}} + \mathtt{x}^{q^{e-1}})^2 \mathrm{Tr}_{q^e/q}(\mathtt{x})^2 \pmod{\mathtt{x}^{q^e} - \mathtt{x}}.$$

Assume that e is even and $\gcd(1 + \mathtt{x}^2 + \mathtt{x}^{e-3}, \mathtt{x}^e + 1) = 1$.
To prove that $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$, we assume that $g_{n,q}(x) = g_{n,q}(y)$, $x, y \in \mathbb{F}_{q^e}$, and try to show that $x = y$. From $\mathrm{Tr}_{q^e/q}(g_{n,q}(x)) = \mathrm{Tr}_{q^e/q}(g_{n,q}(y))$ we derive that $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y)$. Let $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y) = a \in \mathbb{F}_q$. If $a = 0$, then $x = y$.
If $a \neq 0$, then $g_{n,q}(x) = g_{n,q}(y)$ becomes

$$z = a^2(z^{2q^{e-2}} + z^{2q^{e-1}}), \tag{4.2.19}$$

where $z = x + y$. Substitute (4.2.19) into itself to find $z^{q^3} = z + z^{q^2}$. Since e is even and $\gcd(1 + \mathtt{x}^2 + \mathtt{x}^{e-3}, \mathtt{x}^e + 1) = 1$, we have $z = 0$.

■

Theorem 4.2.11 *Let $n = 1 + q^{a_1} + \cdots + q^{a_{q+t}}$, where $-1 \leq t \leq q - 4$. Then*

$$g_{n,q} = -\sum_{1 \leq i_1 < \cdots < i_{t+2} \leq q+t} S_{a_{i_1}} \cdots S_{a_{i_{t+2}}}. \tag{4.2.20}$$

Proof. Use induction on t. When $t = -1$, n is a sum of q powers of q, in which case the conclusion is already known. Let $0 \le t \le q-4$. We have

$$\begin{aligned}
g_n &= g_{2+q^{a_2}+\cdots+q^{a_{q+t}}} + S_{a_1} \cdot g_{1+q^{a_2}+\cdots+q^{a_{q+t}}} \\
&= g_{2+q^{a_2}+\cdots+q^{a_{q+t}}} - S_{a_1} \sum_{2\le i_2<\cdots<i_{t+2}\le q+t} S_{a_{i_2}} \cdots S_{a_{i_{t+2}}} \text{(induction hypothesis)} \\
&= g_{3+q^{a_3}+\cdots+q^{a_{q+t}}} + S_{a_2} \cdot g_{2+q^{a_3}+\cdots+q^{a_{q+t}}} - S_{a_1} \sum_{2\le i_2<\cdots<i_{t+2}\le q+t} S_{a_{i_2}} \cdots S_{a_{i_{t+2}}} \\
&= g_{3+q^{a_3}+\cdots+q^{a_{q+t}}} - S_{a_2} \sum_{3\le i_3<\cdots<i_{t+2}\le q+t} S_{a_{i_3}} \cdots S_{a_{i_{t+2}}} \\
&\quad - S_{a_1} \sum_{2\le i_2<\cdots<i_{t+2}\le q+t} S_{a_{i_2}} \cdots S_{a_{i_{t+2}}} \qquad \text{(induction hypothesis)} \\
&= \cdots\cdots \\
&= g_{q+t+1} - \sum_{1\le i_1<\cdots<i_{t+2}\le q+t} S_{a_{i_1}} \cdots S_{a_{i_{t+2}}}.
\end{aligned}$$

Since $w_q(q+t+1)) = t+2 < q-1$, we have $g_{q+t+1} = 0$, which gives (4.2.20).

■

Let q be even and $t = 0$ in (4.2.20). Then

$$g_{n,q} = \sum_{1\le i_1<i_2\le q} S_{a_{i_1}} S_{a_{i_2}} = \sum_i S_{b_i} S_{c_i} + \sum_{i<j} (S_{b_i} + S_{c_i})(S_{b_j} + S_{c_j}),$$

where $(a_1, \ldots, a_q) = (b_1, \ldots, b_{q/2}, c_1, \ldots, c_{q/2})$. This is Theorem 4.1.1. In fact, Theorem 4.2.11 is a generalized version of Theorem 4.1.1.

The next theorem is a generalization of [14, Theorem 6.12].

Theorem 4.2.12 *Let $q = p^2$, $e > 0$, and $n = (p^2-p-1)q^0 + (p-1)q^e + pq^a + q^b$, $a, b \ge 0$. Then*

$$g_{n,q} = -S_a^p - S_b S_e^{p-1}. \tag{4.2.21}$$

Assume that $a+b \not\equiv 0 \pmod{p}$ *and*

$$\gcd\big(\mathtt{x}(\mathtt{x}^a-1)^2-\epsilon(\mathtt{x}^b-1)^2,\,(\mathtt{x}-1)(\mathtt{x}^e-1)\big)=(\mathtt{x}-1)^2,$$

for $\epsilon=0,1$. *Then* $g_{n,q}$ *is a PP of* $\mathbb{F}_{q^e}$.

Proof. Equation (4.2.21) follows from Theorem 4.2.11.

To prove that $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$ under the given conditions, we assume that $g_{n,q}(x)=g_{n,q}(y)$, $x,y\in\mathbb{F}_{q^e}$, and try to show that $x=y$. From $S_e(g_{n,q}(x))=S_e(g_{n,q}(y))$ we derive that

$$(a+b)\big(S_e(x)-S_e(y)\big)^p=0.$$

Since $a+b\not\equiv 0 \pmod{p}$, we have $S_e(x)=S_e(y)=c\in\mathbb{F}_q$. Now the equation $g_{n,q}(x)=g_{n,q}(y)$ becomes

$$S_a(z)^p=-c^{p-1}S_b(z),$$

where $z=x-y$. Thus

$$S_a(z)=\big(-c^{p-1}S_b(z)\big)^{pq^{e-1}}=-c^{q-p}S_b(z^{pq^{e-1}}). \tag{4.2.22}$$

We iterate both sides of (4.2.22) to get

$$(S_a\circ S_a)(z)=-c^{q-p}S_b\Big(\big(-c^{q-p}S_b(z^{pq^{e-1}})\big)^{pq^{e-1}}\Big)=c^{q-1}(S_b\circ S_b)(z^{q^{e-1}}),$$

i.e.,

$$\big[(S_a\circ S_a)(z)\big]^q=c^{q-1}(S_b\circ S_b)(z). \tag{4.2.23}$$

Let $\epsilon=c^{q-1}$, which is 0 or 1. The conventional associates of the q-polynomials $(S_a\circ S_a)^q$ and $S_b\circ S_b$ are $\mathtt{x}(1+\mathtt{x}+\cdots+\mathtt{x}^{a-1})^2$ and $(1+\mathtt{x}+\cdots+\mathtt{x}^{b-1})^2$, respectively

[30, §3.4]. Since

$$\begin{aligned}
&\gcd\big(\mathtt{x}(1+\mathtt{x}+\cdots+\mathtt{x}^{a-1})^2-\epsilon(1+\mathtt{x}+\cdots+\mathtt{x}^{b-1})^2,\, 1+\mathtt{x}+\cdots+\mathtt{x}^{e-1}\big)\\
=&\frac{1}{(\mathtt{x}-1)^2}\gcd\big(\mathtt{x}(\mathtt{x}^a-1)^2-\epsilon(\mathtt{x}^b-1)^2,\,(\mathtt{x}-1)(\mathtt{x}^e-1)\big)\\
=&1,
\end{aligned}$$

it follows from (4.2.23) that $z=0$, i.e., $x=y$.

■

Example 4.2.13 Let $q=4$, $e>3$, $n=q^0+2q^1+q^2+q^e$. Then by Theorem 4.1.1,

$$g_{n,q}\equiv x^2+x\mathrm{Tr}_{q^e/q}(x)+x^q\mathrm{Tr}_{q^e/q}(x)\pmod{\mathtt{x}^{q^e}-\mathtt{x}}.$$

We claim that when $\gcd(1+\mathtt{x}+\mathtt{x}^2,\mathtt{x}^e+1)=1$, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.
To prove that $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$, we assume that $g_{n,q}(x)=g_{n,q}(y)$, $x,y\in\mathbb{F}_{q^e}$, and try to show that $x=y$. From $\mathrm{Tr}_{q^e/q}(g_{n,q}(x))=\mathrm{Tr}_{q^e/q}(g_{n,q}(y))$ we derive that $\mathrm{Tr}_{q^e/q}(x)=\mathrm{Tr}_{q^e/q}(y)$. Let $\mathrm{Tr}_{q^e/q}(x)=\mathrm{Tr}_{q^e/q}(y)=a\in\mathbb{F}_q$.
If $a=0$, then $x=y$.
If $a\neq 0$, then $g_{n,q}(x)=g_{n,q}(y)$ becomes

$$z^2=a(z+z^q),\tag{4.2.24}$$

where $z=x+y$. Substitute (4.2.24) into itself to find $(z^2)^q=(z^2)+(z^2)^{q^2}$. Since $\gcd(1+\mathtt{x}+\mathtt{x}^2,\mathtt{x}^e+1)=1$, we have $z=0$.

Example 4.2.14 Let $q=4$, $e>4$, $n=q^0+2q^1+q^{e-2}+q^e$. Then by Theorem 4.1.1,

$$g_{n,q}\equiv x^2+\mathrm{Tr}_{q^e/q}(x)^2+x^{q^{e-2}}\mathrm{Tr}_{q^e/q}(x)+x^{q^{e-1}}\mathrm{Tr}_{q^e/q}(x)\pmod{\mathtt{x}^{q^e}-\mathtt{x}}.$$

We claim that when $\gcd(1+\mathtt{x}^2+\mathtt{x}^5,\mathtt{x}^e+1)=1$ and e is even, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.
To prove that $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$, we assume that $g_{n,q}(x)=g_{n,q}(y)$, $x,y\in\mathbb{F}_{q^e}$,

and try to show that $x = y$. From $\mathrm{Tr}_{q^e/q}(g_{n,q}(x)) = \mathrm{Tr}_{q^e/q}(g_{n,q}(y))$ we derive that $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y)$. Let $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y) = a \in \mathbb{F}_q$.
If $a = 0$ then $x = y$. If $a \neq 0$, then $g_{n,q}(x) = g_{n,q}(y)$ becomes

$$z^2 = a(z^{q^{e-2}} + z^{q^{e-1}}), \tag{4.2.25}$$

where $z = x + y$. Substitute (4.2.25) into itself to find $(z^2)^{q^5} = (z^2) + (z^2)^{q^2}$. Since $\gcd(1 + \mathtt{x}^2 + \mathtt{x}^5, \mathtt{x}^e + 1) = 1$, we have $z = 0$.

Example 4.2.15 Let $q = 4$, $e > 3$, $n = q^0+q^{e-2}+2q^{e-1}+q^e$. Then by Theorem 4.1.1,

$$g_{n,q} \equiv x^{2q^{e-1}} + x^{q^{e-2}}\mathrm{Tr}_{q^e/q}(x) + x^{q^{e-1}}\mathrm{Tr}_{q^e/q}(x) \pmod{\mathtt{x}^{q^e} - \mathtt{x}}.$$

We claim that when $\gcd(1 + \mathtt{x}^2 + \mathtt{x}^3, \mathtt{x}^e + 1) = 1$, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.
To prove that $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$, we assume that $g_{n,q}(x) = g_{n,q}(y)$, $x, y \in \mathbb{F}_{q^e}$, and try to show that $x = y$. From $\mathrm{Tr}_{q^e/q}(g_{n,q}(x)) = \mathrm{Tr}_{q^e/q}(g_{n,q}(y))$ we derive that $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y)$. Let $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y) = a \in \mathbb{F}_q$.
If $a = 0$ then $x = y$. If $a \neq 0$, then $g_{n,q}(x) = g_{n,q}(y)$ becomes

$$z = a^2(z^{2q^{e-2}} + z^{2q^{e-1}}), \tag{4.2.26}$$

where $z = x + y$. Substitute (4.2.26) into itself to find $z^{q^3} = z + z^{q^2}$. Since $\gcd(1 + \mathtt{x}^2 + \mathtt{x}^3, \mathtt{x}^e + 1) = 1$, we have $z = 0$.

Example 4.2.16 Let $q = 4$, $e > 3$, $n = q^0+q^{e-2}+q^e+2q^{e+1}$. Then by Theorem 4.1.1,

$$g_{n,q} \equiv x^2 + x^{q^{e-2}}\mathrm{Tr}_{q^e/q}(x) + x^{q^{e-1}}\mathrm{Tr}_{q^e/q}(x) \pmod{\mathtt{x}^{q^e} - \mathtt{x}}.$$

We claim that when $\gcd(1 + \mathtt{x}^2 + \mathtt{x}^5, \mathtt{x}^e + 1) = 1$, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.
To prove that $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$, we assume that $g_{n,q}(x) = g_{n,q}(y)$, $x, y \in \mathbb{F}_{q^e}$, and try to show that $x = y$. From $\mathrm{Tr}_{q^e/q}(g_{n,q}(x)) = \mathrm{Tr}_{q^e/q}(g_{n,q}(y))$ we derive that $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y)$. Let $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y) = a \in \mathbb{F}_q$.

If $a = 0$ then $x = y$. If $a \neq 0$, then $g_{n,q}(x) = g_{n,q}(y)$ becomes

$$z^2 = a(z^{q^{e-2}} + z^{q^{e-1}}), \tag{4.2.27}$$

where $z = x + y$. Substitute (4.2.27) into itself to find $z^{q^5} = z + z^{q^2}$. Since $\gcd(1 + \mathtt{x}^2 + \mathtt{x}^5, \mathtt{x}^e + 1) = 1$, we have $z = 0$.

Lemma 4.2.17 *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a function, and assume that there exists $y \in \mathbb{F}_p^n$ such that $f(x + y) - f(x)$ is a nonzero constant for all $x \in \mathbb{F}_p^n$. Then*

$$\sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)} = 0 \qquad (\zeta_p = e^{2\pi i/p}).$$

Proof. Assume $f(x + y) - f(x) = c \in \mathbb{F}_p^*$. We have

$$\sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)} = \sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x+y)} = \sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)+c} = \zeta^c \sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)}.$$

Since $\zeta^c \neq 1$, we have $\sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)} = 0$.

■

Remark 4.2.18 If $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is quadratic, then $\sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)} = 0$ if and only if there exists $y \in \mathbb{F}_p^n$ such that $f(x + y) - f(x)$ is a nonzero constant for all $x \in \mathbb{F}_p^n$. See [10, Ch. VII, VIII], [19, §5.1], [30, §6.2].

Let $f = \sum_{i=0}^{e-1} a_i \mathtt{x}^{p^i} \in \mathbb{F}_{p^e}[\mathtt{x}]$ be a p-linearized polynomial considered as a $\mathbb{F}_p$-linear map from $\mathbb{F}_{p^e}$ to $\mathbb{F}_{p^e}$. The adjoint of f is the $\mathbb{F}_p$-linear map f^* such that

$$\mathrm{Tr}_{p^e/p}(xf(y)) = \mathrm{Tr}_{p^e/p}(f^*(x)y) \quad \text{for all } x, y \in \mathbb{F}_{p^e}.$$

We have $f^* = \sum_{i=0}^{e-1} a_{e-i}^{p^i} \mathtt{x}^{p^i}$, where the subscript is taken modulo e. For $0 \leq k \leq e$, we have

$$(f^{p^k})^*(\mathtt{x}) \equiv f^*(\mathtt{x}^{p^{e-k}}) \pmod{\mathtt{x}^{p^e} - \mathtt{x}}.$$

(Here f^{p^k} means product, not composition.) In fact, since $f^{p^k} = \sum_i a_i^{p^k} \mathtt{x}^{p^{i+k}} = \sum_i a_{i-k}^{p^k} \mathtt{x}^{p^i}$, we have

$$(f^{p^k})^* = \sum_i (a_{e-i-k}^{p^k})^{p^i} \mathtt{x}^{p^i} = \sum_i a_{e-(k+i)}^{p^{k+i}} \mathtt{x}^{p^i} = \sum_i a_{e-i}^{p^i} \mathtt{x}^{p^{i-k}} \equiv f^*(\mathtt{x}^{p^{e-k}}) \pmod{\mathtt{x}^{p^e} - \mathtt{x}}.$$

The following theorem is a generalization of [14, Theorem 6.15].

Theorem 4.2.19 *Let p be a prime and k, n positive integers. Let $A, B \in \mathbb{F}_{p^{kn}}[\mathrm{x}]$ satisfying the following conditions.*

(i) A is a p-linearized polynomial that permutes $\mathbb{F}_{p^k}$.

(ii) $B(x+y) = B(x)$ for all $x \in \mathbb{F}_{p^{kn}}$ and $y \in \mathbb{F}_{p^k}$.

(iii) $B^{p^k} - B$ is a p-linearized polynomial, and all zeros of $(A^{p^k} - A)^* + (B^{p^k} - B)^*$ in $\mathbb{F}_{p^{kn}}$ are contained in $\mathbb{F}_{p^k}$.

Then $A + B$ is a PP of $\mathbb{F}_{p^{kn}}$.

Proof. By [30, Theorem 7.7], it suffices to show that for all $0 \neq a \in \mathbb{F}_{p^{kn}}$,

$$\sum_{x \in \mathbb{F}_{p^{kn}}} \zeta_p^{\mathrm{Tr}(a \cdot (A+B)(x))} = 0,$$

where $\zeta_p = e^{2\pi i/p}$ and $\mathrm{Tr} = \mathrm{Tr}_{p^{kn}/p}$.

Case 1. Assume $\mathrm{Tr}_{p^{kn}/p^k}(a) \neq 0$. By Lemma 4.2.17, It suffices to show that there exists a $y \in \mathbb{F}_{p^{kn}}$ such that $\mathrm{Tr}\big[a \cdot (A+B)(x+y) - a \cdot (A+B)(x)\big]$ is a nonzero constant for all $x \in \mathbb{F}_{p^{kn}}$.

Since $\mathrm{Tr}_{p^{kn}/p^k}(a) \neq 0$ and A permutes $\mathbb{F}_{p^k}$, there exists a $y \in \mathbb{F}_{p^k}$ such that

$\mathrm{Tr}_{p^k/p}\big[A(y)\mathrm{Tr}_{p^{kn}/p^k}(a)\big] \neq 0$. For all $x \in \mathbb{F}_{p^{kn}}$ we have

$$\begin{aligned}
&\mathrm{Tr}\big[a\cdot(A+B)(x+y)-a\cdot(A+B)(x)\big]\\
&=\mathrm{Tr}\big[a\big(A(x+y)+B(x+y)-A(x)-B(x)\big)\big]\\
&=\mathrm{Tr}\big(aA(y)\big) \qquad\qquad (B(x+y)=B(x))\\
&=\mathrm{Tr}_{p^k/p}\big[\mathrm{Tr}_{p^{kn}/p^k}\big(aA(y)\big)\big]\\
&=\mathrm{Tr}_{p^k/p}\big[A(y)\mathrm{Tr}_{p^{kn}/p^k}(a)\big],
\end{aligned}$$

which is a nonzero constant.

Case 2. Assume $\mathrm{Tr}_{p^{kn}/p^k}(a)=0$. Then $a=b^{p^{(n-1)k}}-b$ for some $b\in\mathbb{F}_{p^{kn}}\setminus\mathbb{F}_{p^k}$. For $x\in\mathbb{F}_{p^{kn}}$ we have

$$\begin{aligned}
\mathrm{Tr}\big[a\cdot(A+B)(x)\big] &= \mathrm{Tr}\big[(b^{p^{(n-1)k}}-b)\cdot(A+B)(x)\big]\\
&= \mathrm{Tr}\big[b\big((A+B)^{p^k}(x)-(A+B)(x)\big)\big]\\
&= \mathrm{Tr}\big[b\big((A^{p^k}-A)(x)+(B^{p^k}-B)(x)\big)\big]\\
&= \mathrm{Tr}\big[x\big((A^{p^k}-A)^*(b)+(B^{p^k}-B)^*(b)\big)\big].
\end{aligned}$$

Condition (iii) implies that for $z\in\mathbb{F}_{p^{kn}}$,

$$(A^{p^k}-A)^*(z)+(B^{p^k}-B)^*(z)=0 \Leftrightarrow z\in\mathbb{F}_{p^k}.$$

Since $b\notin\mathbb{F}_{p^k}$, we have $(A^{p^k}-A)^*(b)+(B^{p^k}-B)^*(b)\neq 0$. Therefore

$$\sum_{x\in\mathbb{F}_{p^{kn}}}\zeta_p^{\mathrm{Tr}[a\cdot(A+B)(x)]}=\sum_{x\in\mathbb{F}_{p^{kn}}}\zeta_p^{\mathrm{Tr}[x((A^{p^k}-A)^*(b)+(B^{p^k}-B)^*(b))]}=0.$$

■

Corollary 4.2.20 *Let $e=3k$, $k\geq 1$, $q=2^s$, $s\geq 2$, and $n=(q-3)q^0+2q^1+q^{2k}+q^{4k}$. Then*

$$g_{n,q}\equiv \mathtt{x}^2+S_{2k}S_{4k} \pmod{\mathtt{x}^{q^e}-\mathtt{x}},$$

and $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Proof. We write g_n for $g_{n,q}$. We have

$$\begin{aligned} g_n &= g_{(q-2)q^0+2q^1+q^{2k}} + S_{4k} \cdot g_{(q-3)q^0+2q^1+q^{2k}} \\ &= g_{(q-1)q^0+2q^1} + S_{2k} \cdot g_{(q-2)q^0+2q^1} + S_{4k}S_{2k} \\ &= g_{2q^1} + S_1 \cdot g_{(q-1)q^0+q^1} + S_{4k}S_{2k} \\ &= \mathtt{x}^2 + S_{4k}S_{2k}. \end{aligned}$$

It follows from Theorem 4.2.19 that g_n is a PP of $\mathbb{F}_{q^e}$.

■

Conjecture 4.2.21 *Let $q = 4$, $e = 3k$, $k \geq 1$, and $n = 3q^0 + 3q^{2k} + q^{4k}$. It is easy to see that*

$$g_{n,q} \equiv \mathtt{x} + S_{2k} + S_{4k} + S_{4k}S_{2k}^3 \equiv \mathtt{x} + S_{2k}^{q^{2k}} + S_{2k}^{q^k+3} \pmod{\mathtt{x}^{q^e} - \mathtt{x}}.$$

We conjecture that $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

The conjecture has been verified for $e \leq 12$.

Table 4.1: Desirable triples $(n, e; 4)$, $e \leq 6$, $w_4(n) > 4$

e	n	base 4 digits of n	reference
2	59	3,2,3	Thm 3.2.4 (ii)
2	127	3,3,3,1	[22] Prop 3.1
3	29	1,3,1	Exmp 4.1.3
3	101	1,1,2,1	Thm 4.2.12
3	149	1,1,1,2	
3	163	3,0,2,2	[14] Thm 6.10
3	281	1,2,1,0,1	Cor 4.2.20
3	307	3,0,3,0,1	
3	329	1,2,0,1,1	Exmp 4.1.4
3	341	1,1,1,1,1	Exmp 4.1.4
3	2047	3,3,3,3,3,1	[22] Prop 3.1
4	281	1,2,1,0,1	Thm 4.2.12
4	307	3,0,3,0,1	
4	401	1,0,1,2,1	Thm 4.2.12
4	547	3,0,2,0,2	[14] Thm 6.10
4	779	3,2,0,0,3	Thm 4.2.2
4	787	3,0,1,0,3	Thm 4.2.6
4	817	1,0,3,0,3	
4	899	3,0,0,2,3	Thm 4.2.2
4	1469	1,3,3,2,1,1	
4	2201	1,2,1,2,0,2	
4	2317	1,3,0,0,1,2	
4	2321	1,0,1,0,1,2	Thm 4.2.12
4	2377	1,2,0,1,1,2	
4	2441	1,2,0,2,1,2	
4	4387	3,0,2,0,1,0,1	
4	32767	3,3,3,3,3,3,3,1	[22] Prop 3.1
5	29	1,3,1	Exmp 4.1.3
5	1049	1,2,1,0,0,1	Thm 4.2.12
5	1061	1,1,2,0,0,1	Thm 4.2.12
5	1169	1,0,1,2,0,1	Thm 4.2.12
5	1289	1,2,0,0,1,1	Thm 4.2.12
5	1409	1,0,0,2,1,1	Thm 4.2.12
5	1541	1,1,0,0,2,1	Thm 4.2.12
5	1601	1,0,0,1,2,1	Thm 4.2.12
5	2083	3,0,2,0,0,2	[14] Thm 6.10
5	2563	3,0,0,0,2,2	Thm 4.2.8

Table 4.1 (Continued)

e	n	base 4 digits of n	reference
5	4229	1,1,0,2,0,0,1	Thm 4.2.12
5	4289	1,0,0,3,0,0,1	
5	4387	3,0,2,0,1,0,1	
5	5129	1,2,0,0,0,1,1	Exmp 4.1.4
5	5141	1,1,1,0,0,1,1	Exmp 4.1.4
5	5189	1,1,0,1,0,1,1	Exmp 4.1.4
5	5249	1,0,0,2,0,1,1	Thm 4.2.12
5	5381	1,1,0,0,1,1,1	Exmp 4.1.4
5	8713	1,2,0,0,2,0,2	
5	9281	1,0,0,1,0,1,2	Thm 4.2.12
5	17429	1,1,1,0,0,1,0,1	
5	17441	1,0,2,0,0,1,0,1	Thm 4.2.12
5	17489	1,0,1,1,0,1,0,1	
5	17681	1,0,1,0,1,1,0,1	
5	524287	3,3,3,3,3,3,3,3,3,1	[22] Prop 3.1
6	4361	1,2,0,0,1,0,1	Thm 4.2.12
6	6161	1,0,1,0,0,2,1	Thm 4.2.12
6	6401	1,0,0,0,1,2,1	Thm 4.2.12
6	8227	3,0,2,0,0,0,2	[14] Thm 6.10
6	8707	3,0,0,0,2,0,2	Thm 4.2.10
6	12299	3,2,0,0,0,0,3	Thm 4.2.2
6	12307	3,0,1,0,0,0,3	Thm 4.2.6
6	14339	3,0,0,0,0,2,3	Thm 4.2.2
6	37121	1,0,0,0,1,0,1,2	Thm 4.2.12
6	65801	1,2,0,0,1,0,0,0,1	Cor 4.2.20
6	65921	1,0,0,2,1,0,0,0,1	
6	66307	3,0,0,0,3,0,0,0,1	
6	135209	1,2,2,0,0,0,1,0,2	
6	135217	1,0,3,0,0,0,1,0,2	
6	135457	1,0,2,0,1,0,1,0,2	
6	137249	1,0,2,0,0,2,1,0,2	
6	8388607	3,3,3,3,3,3,3,3,3,3,3,1	[22] Prop 3.1

5 A Piecewise Construction of Permutation Polynomials over Finite Fields[‡]

5.1 Introduction

Let p be a prime and $q = p^n$, where n is a positive integer. Let $k \mid q-1$ and let $\omega \in \mathbb{F}_q^*$ be an element of order k. We shall define $\omega^\infty = 0$ and $0^0 = 0$. Let $f_\infty, f_0, \ldots, f_{k-1} \in \mathbb{F}_q[x]$ and let $\theta : \mathbb{F}_q \to \{\omega^i : i = \infty, 0, \ldots, k-1\}$. Define

$$F(x) = f_\infty(x)\big(1-\theta(x)^{q-1}\big) + \frac{1}{k}\sum_{i=0}^{k-1}\big[\omega^{-0i}f_0(x) + \cdots + \omega^{-(k-1)i}f_{k-1}(x)\big]\theta(x)^i, \quad x \in \mathbb{F}_q. \tag{5.1.1}$$

Note that

$$F(x) = f_i(x) \quad \text{if } \theta(x) = \omega^i,\ i \in \{\infty, 0, \ldots, k-1\}. \tag{5.1.2}$$

We shall call the functions f_i, $i = \infty, 0, \ldots, k-1$, the *case* functions of F and the function θ the *selection* function of F. We have

Proposition 5.1.1 *The function in* (5.1.1) *is a permutation of* $\mathbb{F}_q$ *if and only if*

(i) f_i *is 1-1 on* $\theta^{-1}(\omega^i)$ *for each* $i \in \{\infty, 0, \ldots, k-1\}$, *and*

(ii) $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$ *for all* $i, j \in \{\infty, 0, \ldots, k-1\}$, $i \neq j$.

The idea of constructing permutation polynomials (PPs) of finite fields piecewise is not new; it has appeared in literature, at least implicitly. PPs of the form

[‡]This chapter consists of the paper [13] which has been published in the journal "Finite Fields and Their Applications".

$x^{m+1} + ax$, where $m \mid q-1$, were considered in [4, 5, 6, 28, 33]. (In the notation of (5.1.1), one has $k = \frac{q-1}{m}$, $\theta(x) = x^m$, $f_\infty(x) = 0$, $f_i(x) = (a + \omega^i)x$, $0 \le i \le k-1$.) PPs of the forms $x^{p-1-s} + ax^{(p-1-2s)/2}$ and $x^{p-s} + ax^{(p-s+1)/2} + bx$ were studied in [2, 3, 16, 17]. (In the notation of (5.1.1), $q = p$, $k = 2$ and $\theta(x) = x^{\frac{p-1}{2}}$.)

Several recent articles on permutation polynomials suggest that the piecewise approach has more to offer. In [21], it was shown that the *reversed Dickson polynomial* $D_{3^n+5}(1, x) = (1 - y - y^2)y^{\frac{3^n+1}{2}} - 1 - y + y^2$, where $y = 1 - x$, is a PP over $\mathbb{F}_{3^n}$ for even n. This particular PP was generalized by Zha and Hu in [39] in a formulation similar to (5.1.1). Also presented in [39] were several families of PPs of the form $(x^{p^l} - x + \delta)^s + L(x)$, where L is a linearized polynomial; PPs of this form had been explored by different authors in several previous papers [18, 37, 40]. In [1, 38], new PPs were constructed through certain commutative diagrams. Such PPs can also be viewed as piecewise functions (see [1, Lemma 1.1] or [38, Lemma 2.4]) although they are not necessarily of the form (5.1.1).

Returning to Proposition 5.1.1, the challenge is to choose simple functions θ and f_i ($i = \infty, 0, \ldots, k-1$) such that conditions (i) and (ii) are satisfied. The next proposition provides a way to check condition (ii) when θ is related to f_i.

Proposition 5.1.2 *Let $i, j \in \{\infty, 0, \ldots, k-1\}$, $i \neq j$. Assume that there exist functions h_i and h_j from $\mathbb{F}_q$ to $\mathbb{F}_q$ such that the following two conditions hold.*

(i) $[(h_i \circ f_i)(x)]^{\frac{1}{k}(q-1)} = \theta(x)$ *if* $\theta(x) = \omega^i$; $[(h_j \circ f_j)(x)]^{\frac{1}{k}(q-1)} = \theta(x)$ *if* $\theta(x) = \omega^j$.

(ii) If $b \in f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j))$, *then* $\left(h_i(b)^{\frac{1}{k}(q-1)}, h_j(b)^{\frac{1}{k}(q-1)}\right) \neq (\omega^i, \omega^j)$.

Then $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$.

Proof. Assume to the contrary that there exists $b \in f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j))$. Then $b = f_i(x) = f_j(y)$ for some $x \in \theta^{-1}(\omega^i)$ and $y \in \theta^{-1}(\omega^j)$. By (i), $h_i(b)^{\frac{1}{k}(q-1)} = [(h_i \circ f_i)(x)]^{\frac{1}{k}(q-1)} = \omega^i$. In the same way, $h_j(b)^{\frac{1}{k}(q-1)} = \omega^j$. So we have a contradiction.

■

We will construct several families of PPs of the form (5.1.1) by choosing the selection function θ to be $\theta(x) = \big(L(x)+\delta\big)^{\frac{1}{k}(q-1)}$, where $L(x)$ is a linearized polynomial, or $\theta(x) = x^{\frac{1}{k}(q-1)}$. The PPs obtained in this paper unify and generalize several existing results, mostly from [39].

5.2 PPs with $\theta(x) = \big(L(x)+\delta\big)^{\frac{1}{k}(q-1)}$

Theorem 5.2.1 *Let $k \mid q-1$ and let $\omega \in \mathbb{F}_q^*$ be an element of order k. Let $\mathbb{F}_r \subset \mathbb{F}_q$ and $\sigma_0, \ldots, \sigma_{k-1} \in \mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_r)$ such that $\sigma_i(\omega^i)$, $0 \le i \le k-1$, are all distinct. Let L and g be r-linearized polynomials over $\mathbb{F}_r$ with $L(1)=0$, $g(1)=1$ and g a PP of $\mathbb{F}_q$. Let $\delta_\infty, \delta_0, \ldots, \delta_{k-1}, \delta \in \mathbb{F}_r$. Then*

$$F(x) = \big(g(x)+\delta_\infty\big)\big[1-(L(x)+\delta)^{q-1}\big] + \frac{1}{k}\sum_{i=0}^{k-1}\Big[\omega^{-0i}\big(\sigma_0(x)+\delta_0\big)+\cdots+\omega^{-(k-1)i}\big(\sigma_{k-1}(x)+\delta_{k-1}\big)\Big]\big(L(x)+\delta\big)^{\frac{i}{k}(q-1)}.$$

is a PP of $\mathbb{F}_q$.

Proof. Let $\theta(x) = (L(x)+\delta)^{\frac{1}{k}(q-1)}$, $f_\infty(x) = g(x)+\delta_\infty$, $f_i(x) = \sigma_i(x)+\delta_i$, $0 \le i \le k-1$. We use Proposition 5.1.2 to show that $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$ for all $i, j \in \{\infty, 0, \ldots, k-1\}$, $i \ne j$. Let $h_\infty(x) = g^{-1}(L(x))+\delta$ and $h_i(x) = \sigma_i^{-1}(L(x))+\delta$, $x \in \mathbb{F}_q$. Then

$$(h_\infty \circ f_\infty)(x) = g^{-1}\big(L(g(x)+\delta_\infty)\big)+\delta = L(x)+\delta.$$

(Note that $L(\delta_\infty)=0$ and $L\circ g = g \circ L$.) In the same way, $(h_i \circ f_i)(x) = L(x)+\delta$, $0 \le i \le k-1$. Thus

$$\big[(h_i \circ f_i)(x)\big]^{\frac{1}{k}(q-1)} = \big(L(x)+\delta\big)^{\frac{1}{k}(q-1)} = \theta(x), \quad i \in \{\infty, 0, \ldots, k-1\}.$$

Let $b \in \mathbb{F}_q$. For $0 \le i \le k-1$ we have

$$\begin{aligned} h_i(b)^{\frac{1}{k}(q-1)} &= \left[\sigma_i^{-1}(L(b)) + \delta\right]^{\frac{1}{k}(q-1)} = \left[\sigma_i^{-1}\big(L(b)+\delta\big)\right]^{\frac{1}{k}(q-1)} \\ &= \sigma_i^{-1}\big((L(b)+\delta)^{\frac{1}{k}(q-1)}\big) = \sigma_i^{-1}(\theta(b)). \end{aligned}$$

(Note that $\sigma_i^{-1}(\delta) = \delta$.) Since $g^{-1}(\delta) = \delta$, we also have

$$h_\infty(b) = g^{-1}(L(b)) + \delta = g^{-1}(L(b)+\delta).$$

Now for $i, j \in \{0, \ldots, k-1\}$, $i \ne j$, we have

$$\Big(h_i(b)^{\frac{1}{k}(q-1)},\ h_j(b)^{\frac{1}{k}(q-1)}\Big) = \big(\sigma_i^{-1}(\theta(b)),\ \sigma_j^{-1}(\theta(b))\big) \ne (\omega^i, \omega^j)$$

since $\sigma_i(\omega^i) \ne \sigma_j(\omega^j)$. Also,

$$\Big(h_\infty(b)^{\frac{1}{k}(q-1)},\ h_i(b)^{\frac{1}{k}(q-1)}\Big) = \Big(\big(g^{-1}(L(b)+\delta)\big)^{\frac{1}{k}(q-1)},\ \sigma_i^{-1}(\theta(b))\Big) \ne (0, \omega^i)$$

since $g^{-1}(L(b)+\delta) = 0$ implies $L(b)+\delta = 0$, which implies $\theta(b) = 0$. By Proposition 5.1.2, we have $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$ for all $i, j \in \{\infty, 0, \ldots, k-1\}$, $i \ne j$.

■

Remark 5.2.2 In Theorem 5.2.1, $\delta \in \mathbb{F}_r$ can be replaced with an arbitrary function from $\mathbb{F}_q$ to $\mathbb{F}_r$. Also, each σ_i can be replaced with $\sigma_i + \beta_i$, where $\beta_i : \mathbb{F}_q \to \ker_{\mathbb{F}_q} L$ is any function such that $\sigma_i + \beta_i$ is a PP of $\mathbb{F}_q$.

Remark 5.2.3 In Theorem 5.2.1, if we drop the assumption that $\sigma_i(\omega^i)$, $0 \le i \le k-1$, are all distinct, and maintain others, then we can describe a necessary and sufficient condition on $\sigma_0, \ldots, \sigma_{k-1}$ for F to be a PP of $\mathbb{F}_q$. It is clear that F is a PP of $\mathbb{F}_q$ if and only if $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$ for all $i, j \in \{\infty, 0, \ldots, k-1\}$ with $i \ne j$. From the proof of Theorem 5.2.1, we always have $f_\infty(\theta^{-1}(0)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$ for $j \in \{0, \ldots, k-1\}$. For $0 \le i < j \le k-1$, $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) \ne \emptyset$ if and

only if the following system has a solution $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$:

$$\begin{cases} \big(L(x)+\delta\big)^{\frac{1}{k}(q-1)} = \omega^i, \\ \big(L(y)+\delta\big)^{\frac{1}{k}(q-1)} = \omega^j, \\ \sigma_i(x)+\delta_i = \sigma_j(y)+\delta_j. \end{cases} \tag{5.2.3}$$

Apply σ_i to the first equation of (5.2.3) and σ_j to the second. We see that (5.2.3) is equivalent to

$$\begin{cases} \big(L(u)+\delta\big)^{\frac{1}{k}(q-1)} = \sigma_i(\omega^i), \\ \big(L(v)+\delta\big)^{\frac{1}{k}(q-1)} = \sigma_j(\omega^j), \\ u+\delta_i = v+\delta_j, \end{cases} \tag{5.2.4}$$

where $u = \sigma_i(x)$, $v = \sigma_j(y)$. The third equation of (5.2.4) implies that $L(u) = L(v)$. Therefore, (5.2.4) has a solution $(u, v) \in \mathbb{F}_q \times \mathbb{F}_q$ if and only if $\sigma_i(\omega^i) = \sigma_j(\omega^j)$ and $\big(L(\mathbb{F}_q)+\delta\big) \cap \big(\sigma_i(\gamma^i) \cdot \langle\gamma^k\rangle\big) \neq \emptyset$, where γ is a primitive element of $\mathbb{F}_q$ such that $\omega = \gamma^{\frac{1}{k}(q-1)}$. We conclude that F is a PP of $\mathbb{F}_q$ if and only if for each pair of distinct integers $i, j \in \{0, \ldots, k-1\}$, either $\sigma_i(\omega^i) \neq \sigma_j(\omega^j)$ or $\big(L(\mathbb{F}_q)+\delta\big) \cap \big(\sigma_i(\gamma^i) \cdot \langle\gamma^k\rangle\big) = \emptyset$.

The construction in Theorem 5.2.1 calls for a sequence $\sigma_0, .., \sigma_{k-1} \in \mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_r)$ such that $\sigma_i(\omega^i)$, $0 \leq i \leq k-1$, are all distinct. All such sequences can be determined by the following method: Write $q = r^m$, and let $\sigma \in \mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_r)$ be given by $\sigma(x) = x^r$.

1. Partition $\{0, 1, \ldots, k-1\}$ into r-cyclotomic classes modulo k.
2. For each r-cyclotomic class $[i] = \{ir^0, ir^1, \ldots, ir^{s-1}\}$, choose any permutation β of $\{0, 1, \ldots, s-1\}$, choose $e_j \in \mathbb{Z}_m$, $0 \leq j \leq s-1$, such that $e_j \equiv \beta(j) - j \pmod{s}$, and choose
$$\sigma_{ir^j} = \sigma^{e_j}, \quad 0 \leq j \leq s-1.$$

Note that $\sigma_{ir^j}(\omega^{ir^j}) = \omega^{ir^j \cdot r^{e_j}} = \omega^{ir^{j+e_j}}$, where $j + e_j$, $0 \leq j \leq s-1$, is a permutation of $0, 1, \ldots, s-1$.

Theorem 5.2.1 allows several variations.

Theorem 5.2.4 *Let $k \mid q-1$ and let $\omega \in \mathbb{F}_q^*$ be an element of order k. Let $\mathbb{F}_r \subset \mathbb{F}_q$, $\sigma_0, \ldots, \sigma_{k-1} \in \mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_r)$, L an r-linearized polynomial over $\mathbb{F}_r$, and*

$$F(x) = \frac{1}{k} \sum_{i=0}^{k-1} \big[\omega^{-0i}\sigma_0(x) + \cdots + \omega^{-(k-1)i}\sigma_{k-1}(x)\big] L(x)^{\frac{i}{k}(q-1)}.$$

Then F is a PP of $\mathbb{F}_q$ if and only if L is a PP of $\mathbb{F}_q$ and $\sigma_i(\omega^i)$, $0 \le i \le k-1$, are all distinct.

Proof. ($\Leftarrow$) Let $\theta(x) = L(x)^{\frac{1}{k}(q-1)}$, $f_\infty(x) = 0$ and $f_i(x) = \sigma_i(x)$, $0 \le i \le k-1$. Note that $\theta^{-1}(0) = 0$. One only has to verify $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$ for $0 \le i < j \le k-1$, which follows from the proof of Theorem 5.2.1.

($\Rightarrow$) Since F has only one root in $\mathbb{F}_q$, L must be a PP of $\mathbb{F}_q$. Assume to the contrary that $\sigma_i(\omega^i) = \sigma_j(\omega^j)$ for some $0 \le i < j \le k-1$. Let γ be a primitive element of $\mathbb{F}_q$ such that $\omega = \gamma^{\frac{1}{k}(q-1)}$. Then

$$\Big(\frac{\sigma_i(\gamma^i)}{\sigma_j(\gamma^j)}\Big)^{\frac{q-1}{k}} = \frac{\sigma_i(\omega^i)}{\sigma_j(\omega^j)} = 1.$$

Hence we can write $\frac{\sigma_i(\gamma^i)}{\sigma_j(\gamma^j)} = \sigma_i(\gamma^l)^k$ for some $l \in \mathbb{Z}$. Thus $\sigma_i(\gamma^{i-lk}) = \sigma_j(\gamma^j)$. Let $x = L^{-1}(\gamma^{i-lk})$ and $y = L^{-1}(\gamma^j)$. Then $\theta(x) = L\big(L^{-1}(\gamma^{i-lk})\big)^{\frac{1}{k}(q-1)} = \omega^i$ and $\theta(y) = L\big(L^{-1}(\gamma^j)\big)^{\frac{1}{k}(q-1)} = \omega^j$. We have

$$F(x) = \sigma_i(x) = L^{-1}\big(\sigma_i(\gamma^{i-lk})\big) = L^{-1}\big(\sigma_j(\gamma^j)\big) = \sigma_j(y) = F(y),$$

which is a contradiction.

■

Theorem 5.2.5 *Let $k \mid q-1$ and let $\omega \in \mathbb{F}_q^*$ be an element of order k. Let $\mathbb{F}_r \subset \mathbb{F}_q$ and $\sigma_0, \ldots, \sigma_{k-1} \in \mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_r)$ such that $\sigma_i(\omega^i)$, $0 \le i \le k-1$, are all distinct. Let L be an r-linearized polynomial over $\mathbb{F}_r$ and let $\delta_0, \ldots, \delta_{k-1} \in \mathbb{F}_q$ and $\delta \in \mathbb{F}_q \setminus L(\mathbb{F}_q)$*

such that $L(\delta_i) - \sigma_i(\delta)$, $0 \le i \le k-1$, *are all equal. Then*

$$F(x) = \frac{1}{k}\sum_{i=0}^{k-1}\big[\omega^{-0i}\big(\sigma_0(x)+\delta_0\big) + \cdots + \omega^{-(k-1)i}\big(\sigma_{k-1}(x)+\delta_{k-1}\big)\big]\big(L(x)+\delta\big)^{\frac{i}{k}(q-1)}$$

is a PP of $\mathbb{F}_q$.

Proof. Let $\theta(x) = \big(L(x)+\delta\big)^{\frac{1}{k}(q-1)}$ and $f_i(x) = \sigma_i(x) + \delta_i$, $0 \le i \le k-1$. It suffices to show that $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$ for $0 \le i < j \le k-1$.

Let $h_i(x) = \sigma_i^{-1}\big(L(x-\delta_i)\big) + \delta$, $0 \le i \le k-1$. Then

$$\big[(h_i \circ f_i)(x)\big]^{\frac{1}{k}(q-1)} = \big[(\sigma_i^{-1} \circ L \circ \sigma_i)(x) + \delta\big]^{\frac{1}{k}(q-1)} = \big[L(x)+\delta\big]^{\frac{1}{k}(q-1)} = \theta(x).$$

For each $b \in \mathbb{F}_q$ we have

$$h_i(b) = \sigma_i^{-1}\big(L(b-\delta_i)\big) + \delta = \sigma_i^{-1}\big(L(b) - L(\delta_i) + \sigma_i(\delta)\big) = \sigma_i^{-1}(c),$$

where $c = L(b) - L(\delta_i) + \sigma_i(\delta)$ is independent of i. So for $0 \le i < j \le k-1$,

$$\Big(h_i(b)^{\frac{1}{k}(q-1)},\ h_j(b)^{\frac{1}{k}(q-1)}\Big) = \Big(\sigma_i^{-1}\big(c^{\frac{1}{k}(q-1)}\big),\ \sigma_j^{-1}\big(c^{\frac{1}{k}(q-1)}\big)\Big) \ne (\omega^i,\ \omega^j)$$

since $\sigma_i(\omega^i) \ne \sigma_j(\omega^j)$. By Proposition 5.1.2, $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$.

■

Given $\sigma_0, \ldots, \sigma_{k-1} \in \mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_r)$ and an r-linearized polynomial L over $\mathbb{F}_r$, the construction in Theorem 5.2.5 calls for solutions $(\delta_0, \ldots, \delta_{k-1}, \delta) \in \mathbb{F}_q^k \times (\mathbb{F}_q \setminus L(\mathbb{F}_q))$ of the system

$$L(\delta_i) - \sigma_i(\delta) = L(\delta_0) - \sigma_0(\delta), \quad 1 \le i \le k-1. \tag{5.2.5}$$

Let $x_i = \delta_i - \delta_0$, $1 \le i \le k-1$, and $x_k = \sigma_0(\delta)$. Then (5.2.5) becomes

$$L(x_i) = \sigma_i\sigma_0^{-1}(x_k) - x_k, \quad 1 \le i \le k-1, \tag{5.2.6}$$

and we seek its solutions $(x_1, \ldots, x_{k-1}, x_k) \in \mathbb{F}_q^{k-1} \times (\mathbb{F}_q \setminus L(\mathbb{F}_q))$. Write $q = r^m$, and let $\sigma \in \mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_r)$ be given by $\sigma(x) = x^r$. Write $\sigma_i \sigma_0^{-1} = \sigma^{e_i}$, $1 \le i \le k-1$, and $L = f(\sigma)$, where $f = a_0 + \cdots + a_{m-1}x^{m-1} \in \mathbb{F}_r[x]$. Then (5.2.6) becomes

$$f(\sigma)(x_i) = (\sigma^{e_i} - \sigma^0)(x_k), \quad 1 \le i \le k-1. \tag{5.2.7}$$

All solutions $(x_1, \ldots, x_{k-1}, x_k) \in \mathbb{F}_q^{k-1} \times (\mathbb{F}_q \setminus L(\mathbb{F}_q))$ of (5.2.7) can be generated by the following method: Let $\epsilon \in \mathbb{F}_q$ such that $\sigma^0(\epsilon), \ldots, \sigma^{m-1}(\epsilon)$ is a normal basis of $\mathbb{F}_q$ over $\mathbb{F}_r$.

1. Choose $g \in \mathbb{F}_r[x]$ such that $\deg g \le m-1$, $\gcd(f, x^m - 1) \nmid g$, and $\gcd(f, x^m - 1) \mid (x^{e_i} - 1)g$ for all $1 \le i \le k-1$. (If such g does not exist, (5.2.7) has no solution $(x_1, \ldots, x_{k-1}, x_k) \in \mathbb{F}_q^{k-1} \times (\mathbb{F}_q \setminus L(\mathbb{F}_q))$.) Set

$$x_k = g(\sigma)(\epsilon).$$

2. Write $\gcd(f, x^m - 1) \equiv uf \pmod{x^m - 1}$, $u \in \mathbb{F}_r[x]$, and let

$$h_i = u \cdot \frac{(x^{e_i} - 1)g}{(f, x^m - 1)}, \quad 1 \le i \le k-1.$$

   Set

$$x_i = h_i(\epsilon), \quad 1 \le i \le k-1.$$

Remark.

(i) In Theorem 5.2.5, let q be odd, $k = 2$, σ a generator of $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_r)$, $L(x) = \sigma(x) - x$, $\delta \in \mathbb{F}_q$ with $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(\delta) \neq 0$, $\sigma_0 = \sigma$, $\delta_0 = \frac{\delta}{2}$, $\sigma_1 = \mathrm{id}$, $\delta_1 = -\frac{\delta}{2}$. Then $F(x) = \frac{1}{2}\big[(\sigma(x) - x + \delta)^{\frac{1}{2}(q+1)} + \sigma(x) + x\big]$, which is the PP in [39, Theorem 1].

(ii) In Theorem 5.2.1 and Remark 5.2.2, let $q = 3^{3l}$, $r = 3^l$, $k = 2$, σ a generator of $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_r)$, $L = \sigma - \mathrm{id}$, $\delta \in \mathbb{F}_r$, $g = \mathrm{id}$, $\delta_\infty = 0$, $\sigma_0 = \sigma$, $\beta_0(x) = 0$, $\delta_0 = \delta$, $\sigma_1 = \sigma^2$, $\beta_1(x) = -\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(x)$, $\delta_1 = -\delta$. (Note that $\sigma_1 + \beta_1 = \sigma^2 - \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}$ is a

PP of $\mathbb{F}_q$ and $L \circ \beta_1 = 0$ on $\mathbb{F}_q$.) Then $F(x) = \big(\sigma(x) - x + \delta\big)^{\frac{1}{2}(q+1)} + x$ is a PP of $\mathbb{F}_q$.

Let $g = \sigma$, $\delta_\infty = 0$, $\sigma_0 = \sigma^2$, $\beta_0(x) = -\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(x)$, $\delta_0 = \delta$, $\sigma_1 = \mathrm{id}$, $\beta_1(x) = 0$, $\delta_1 = -\delta$. Then $F(x) = \big(\sigma(x) - x + \delta\big)^{\frac{1}{2}(q+1)} + \sigma(x)$ is a PP of $\mathbb{F}_q$.

Let $g = \sigma^2$, $\delta_\infty = 0$, $\sigma_0 = \mathrm{id}$, $\beta_0(x) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(x)$, $\delta_0 = \delta$, $\sigma_1 = \sigma$, $\beta_1(x) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(x)$, $\delta_1 = -\delta$. Then $F(x) = \big(\sigma(x) - x + \delta\big)^{\frac{1}{2}(q+1)} + \sigma^2(x)$ is a PP of $\mathbb{F}_q$.

These are the PPs in [39, Theorem 2].

5.3 PPs with $\theta(x) = x^{\frac{1}{k}(q-1)}$

Theorem 5.3.1 *Let $k \mid q-1$ and let $\omega \in \mathbb{F}_q^*$ be an element of order k. Let*

$$F(x) = \frac{1}{k} \sum_{i=0}^{k-1} \big[\omega^{-0i} x^{a_0} + \cdots + \omega^{-(k-1)i} x^{a_{k-1}}\big] x^{\frac{i}{k}(q-1)}, \tag{5.3.8}$$

where $a_0, \ldots, a_{k-1} \in \mathbb{Z}_{q-1}$. Then F is a PP of $\mathbb{F}_q$ if and only if $\gcd\big(a_i, \frac{1}{k}(q-1)\big) = 1$ for all $0 \le i \le k-1$ and ia_i, $0 \le i \le k-1$, are all distinct in $\mathbb{Z}_k$.

Proof. ($\Leftarrow$) Let $\theta(x) = x^{\frac{1}{k}(q-1)}$, $f_\infty = 0$, and $f_i(x) = x^{a_i}$, $0 \le i \le k-1$.

First we show that f_i is 1-1 on $\theta^{-1}(\omega^i)$. Let $x_1, x_2 \in \theta^{-1}(\omega^i)$ such that $f_i(x_1) = f_i(x_2)$. Then $(\frac{x_1}{x_2})^{a_i} = 1$. Also,

$$\Big(\frac{x_1}{x_2}\Big)^{\frac{1}{k}(q-1)} = \frac{x_1^{\frac{1}{k}(q-1)}}{x_2^{\frac{1}{k}(q-1)}} = \frac{\omega^i}{\omega^i} = 1.$$

Since $\gcd\big(a_i, \frac{1}{k}(q-1)\big) = 1$, we have $\frac{x_1}{x_2} = 1$.

Now we show that $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$ for $0 \le i < j \le k-1$. Assume to the contrary that there exists $b \in f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j))$. Then $b = f_i(x) = f_j(y)$ for some $x \in \theta^{-1}(\omega^i)$ and $y \in \theta^{-1}(\omega^j)$. We have

$$b^{\frac{q-1}{k}} = \big(x^{a_i}\big)^{\frac{q-1}{k}} = \big(x^{\frac{q-1}{k}}\big)^{a_i} = \omega^{ia_i}.$$

In the same way $b^{\frac{q-1}{k}} = \omega^{ja_j}$. Thus $ia_i = ja_j$ in $\mathbb{Z}_k$, which is a contradiction.

($\Rightarrow$) First assume that $\gcd\big(a_i, \frac{1}{k}(q-1)\big) = l > 1$ for some $0 \le i \le k-1$. Let $\epsilon \in \mathbb{F}_q^*$ such that $o(\epsilon) = l$. Then for any $x \in \theta^{-1}(\omega^i)$, we have $\epsilon x \in \theta^{-1}(\omega^i)$ and $(\epsilon x)^{a_i} = x^{a_i}$. Thus $F(x) = F(\epsilon x)$, where $x \neq \epsilon x$, which is a contradiction.

Next assume that $ia_i = ja_j$ in $\mathbb{Z}_k$ for some $0 \le i < j \le k-1$. Let γ be a primitive element of $\mathbb{F}_q$ such that $\omega = \gamma^{\frac{1}{k}(q-1)}$. Then $\gamma^i \in \theta^{-1}(\omega^i)$, $\gamma^j \in \theta^{-1}(\omega^j)$, and $(\gamma^i)^{a_i} = (\gamma^j)^{a_j}$. Hence $F(\gamma^i) = F(\gamma^j)$, which is a contradiction.

■

For $k \mid q-1$, let $A_{q,k}$ denote the set of all sequences $(a_0, \ldots, a_{k-1}) \in \mathbb{Z}_{q-1}^k$ such that $\gcd\big(a_i, \frac{1}{k}(q-1)\big) = 1$ for all $0 \le i \le k-1$, and ia_i, $0 \le i \le k-1$, are all distinct in $\mathbb{Z}_k$. For each $d \mid k$, let $\pi_d : \mathbb{Z}_{q-1} \to \mathbb{Z}_{k/d}$ be the canonical homomorphism. Each element of $A_{q,k}$ is generated exactly once through the following steps.

1. For each $d \mid k$, choose a permutation τ_d of $\mathbb{Z}_{k/d}^*$.
2. For each $0 \le i \le k-1$, let
$$\alpha_i = \Big(\frac{i}{(i,k)}\Big)^{-1} \tau_{(i,k)}\Big(\frac{i}{(i,k)}\Big) \in \mathbb{Z}_{k/(i,k)}^*.$$
(Note that in $\mathbb{Z}_k$, $i\alpha_i = (i,k)\tau_{(i,k)}(\frac{i}{(i,k)})$, $0 \le i \le k-1$, which are all distinct.)
3. For each $0 \le i \le k-1$, choose $a_i \in \pi_{(i,k)}^{-1}(\alpha_i)$ such that $\gcd(a_i, \frac{q-1}{k}) = 1$.

The number of choices in Step 1 is $\prod_{d|k} \phi(\frac{k}{d})! = \prod_{d|k} \phi(d)!$. Counting the number of choices in Step 3 requires some effort.

For positive integers $m \mid n$ define

$$h(m,n) = \big|\big\{x \in \mathbb{Z}_{\frac{n}{m}} : \gcd(1+mx, n) = 1\big\}\big|.$$

This function can be explicitly determined in terms of the prime factorizations of m and n.

Lemma 5.3.2 *Let $n = p_1^{e_1} \cdots p_s^{e_s}$, $m = p_1^{f_1} \cdots p_s^{f_s}$, where $p_1, \ldots, p_s$ are distinct primes and $e_i > 0$, $0 \le f_i \le e_i$. Without loss of generality, assume $f_1 = \cdots = f_t = 0$, $f_{t+1}, \ldots, f_s > 0$. Then*

$$h(m,n) = \frac{n}{m}\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_t}\Big).$$

Proof. For $1 \le i_1 < \cdots < i_l \le t$, we have

$$\big|\big\{x \in \mathbb{Z}_{\frac{n}{m}} : 1 + mx \equiv 0 \pmod{p_{i_1} \cdots p_{i_l}}\big\}\big| = \frac{n}{m} \cdot \frac{1}{p_{i_1} \cdots p_{i_l}}.$$

By the inclusion-exclusion formula,

$$h(m,n) = \frac{n}{m} \sum_{l=0}^{t} (-1)^l \sum_{1 \le i_1 < \cdots < i_l \le t} \frac{1}{p_{i_1} \cdots p_{i_l}} = \frac{n}{m}\Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_t}\Big).$$

■

It is quite clear that for any two positive integers m and n and $\alpha \in \mathbb{Z}_n^*$,

$$\big|\big\{x \in \mathbb{Z}_{\frac{n}{(m,n)}} : \gcd(\alpha + mx, n) = 1\big\}\big| = h\big((m,n),\, n\big).$$

Using this notation, we see that in the above Step 3, for each $0 \le i \le k-1$, the number of choices for a_i is

$$\begin{aligned}
&\Big|\Big\{x \in \mathbb{Z}_{\frac{1}{k}(q-1)(i,k)} : \gcd\Big(\alpha_i + \frac{k}{(i,k)}x,\ \frac{q-1}{k}\Big) = 1\Big\}\Big| \\
&= \Big|\Big\{x \in \mathbb{Z}_{\frac{q-1}{k}/(\frac{k}{(i,k)}, \frac{q-1}{k})} : \gcd\Big(\alpha_i + \frac{k}{(i,k)}x,\ \frac{q-1}{k}\Big) = 1\Big\}\Big|(i,k)\Big(\frac{k}{(i,k)},\ \frac{q-1}{k}\Big) \\
&= \Big(k,\ \frac{q-1}{k}(i,k)\Big) h\Big(\Big(\frac{k}{(i,k)},\ \frac{q-1}{k}\Big),\ \frac{q-1}{k}\Big).
\end{aligned}$$

Therefore the total number of choices in Step 3 is

$$\begin{aligned}
&\prod_{0\le i\le k-1}\Big(k,\ \frac{q-1}{k}(i,k)\Big)h\Big(\Big(\frac{k}{(i,k)},\ \frac{q-1}{k}\Big),\ \frac{q-1}{k}\Big)\\
&=\prod_{d|k}\Big[\Big(k,\ \frac{q-1}{k}d\Big)h\Big(\Big(\frac{k}{d},\ \frac{q-1}{k}\Big),\ \frac{q-1}{k}\Big)\Big]^{\phi(\frac{k}{d})}\\
&=\prod_{d|k}\Big[\Big(k,\ \frac{q-1}{d}\Big)h\Big(\Big(d,\ \frac{q-1}{k}\Big),\ \frac{q-1}{k}\Big)\Big]^{\phi(d)}.
\end{aligned}$$

Thus

$$|A_{q,k}|=\prod_{d|k}\Big[\Big(k,\ \frac{q-1}{d}\Big)h\Big(\Big(d,\ \frac{q-1}{k}\Big),\ \frac{q-1}{k}\Big)\Big]^{\phi(d)}\phi(d)!.$$

Denote the function in (5.3.8) by F_f, where $f:\mathbb{Z}_k\to\mathbb{Z}_{q-1}$, $f(i)=a_i$. Let $\mathcal{F}=\{f:\mathbb{Z}_k\to\mathbb{Z}_{q-1}:(f(0),\dots,f(k-1))\in A_{q,k}\}$. Then $G:=\{F_f:f\in\mathcal{F}\}$ is a subgroup of the symmetric group $\mathrm{Sym}(\mathbb{F}_q)$. The composition in G is given by

$$F_g\circ F_f=F_h,$$

where

$$h(i)=f(i)g\big(i\,\overline{f(i)}\big),\quad i\in\mathbb{Z}_k,$$

and $\overline{f(i)}$ is the image of $f(i)$ in $\mathbb{Z}_k$.

Now we determine the order of G. Note that $\theta^{-1}(\omega^j)=\{x\in\mathbb{F}_q:x^{\frac{1}{k}(q-1)}=\omega^j\}=\{\alpha^{j+kl}:0\le l<\frac{1}{k}(q-1)\}$, where α is a primitive element of $\mathbb{F}_q$ such that $\omega=\alpha^{\frac{1}{k}(q-1)}$. For $a,a'\in\mathbb{Z}_{q-1}$, we have

$$\begin{aligned}
&x^a=x^{a'}\text{ for all }x\in\theta^{-1}(\omega^j)\\
\Leftrightarrow\ &(a-a')(j+kl)\equiv 0\pmod{q-1}\quad\text{for all }0\le l<\frac{1}{k}(q-1)\\
\Leftrightarrow\ &(a-a')j\equiv(a-a')k\equiv 0\pmod{q-1}\\
\Leftrightarrow\ &(a-a')(j,k)\equiv 0\pmod{q-1}\\
\Leftrightarrow\ &a-a'\equiv 0\pmod{\frac{q-1}{(j,k)}}.
\end{aligned}$$

It is clear that the mapping

$$\begin{aligned} \mathcal{F} &\longrightarrow G \\ f &\longmapsto F_f \end{aligned}$$

is $\prod_{j=0}^{k-1}(j,k)$ to 1. Thus

$$\begin{aligned} |G| &= \frac{|\mathcal{F}|}{\prod_{j=0}^{k-1}(j,k)} = \frac{|A_{q,k}|}{\prod_{d|k} d^{\phi(k/d)}} = \frac{|A_{q,k}|}{\prod_{d|k}(\frac{k}{d})^{\phi(d)}} \\ &= \prod_{d|k}\Big[\Big(d, \frac{q-1}{k}\Big)h\Big(\Big(d, \frac{q-1}{k}\Big), \frac{q-1}{k}\Big)\Big]^{\phi(d)}\phi(d)!. \end{aligned}$$

In Theorem 5.3.1, one can replace each x^{a_i} with $c_i x^{a_i}$, where $c_i \in \mathbb{F}_q^*$ is a kth power. The following theorem offers a more substantial extension of Theorem 5.3.1.

Theorem 5.3.3 *Let $q, k, \omega, a_0, \ldots, a_{k-1}$ be as in Theorem 5.3.1. For each $0 \le i \le k-1$, let r_i be a power of p such that $k \mid r_i - 1$ and $b_i \in \mathbb{F}_q^*$ such that $(-b_i)^{\frac{q-1}{k}} \ne \omega^{ia_i}$. Then*

$$F(x) = \frac{1}{k}\sum_{i=0}^{k-1}\big[\omega^{-0i}x^{a_0}(x^{a_0}+b_0)^{r_0-1} + \cdots + \omega^{-(k-1)i}x^{a_{k-1}}(x^{a_{k-1}}+b_{k-1})^{r_{k-1}-1}\big]x^{\frac{i}{k}(q-1)} \tag{5.3.9}$$

is a PP of $\mathbb{F}_q$.

Proof. Let $\theta(x) = x^{\frac{1}{k}(q-1)}$, $f_i(x) = x^{a_i}(x^{a_i}+b_i)^{r_i-1}$, $0 \le i \le k-1$. By the proof of Theorem 5.3.1, we have $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$ for $0 \le i < j \le k-1$. It remains to show that f_i is 1-1 on $\theta^{-1}(\omega^i)$. Assume to the contrary that there exist $x, y \in \theta^{-1}(\omega^i)$, $x \ne y$, such that

$$x^{a_i}(x^{a_i}+b_i)^{r_i-1} = y^{a_i}(y^{a_i}+b_i)^{r_i-1}.$$

Write $r = r_i$, $u = \frac{x^{a_i}}{b_i}$, $v = \frac{y^{a_i}}{b_i}$. Then we have

$$u(u+1)^{r-1} = v(v+1)^{r-1}.$$

Thus

$$(v+1)u(u+1)^r - (u+1)v(v+1)^r = 0.$$

The left side of the above equation equals

$$(u-v)(v+1)\big[u(u-v)^{r-1} + (v+1)^{r-1}\big].$$

Note that $v+1 \neq 0$ since otherwise, $\frac{y^{a_i}}{b_i} = v = -1$, which implies that $(-b_i)^{\frac{q-1}{k}} = (y^{a_i})^{\frac{q-1}{k}} = (y^{\frac{q-1}{k}})^{a_i} = \omega^{ia_i}$, which is a contradiction. (This is perhaps an overkill. Since $u \neq v$, we may assume that one of u and v, say v, is not -1.) Now we have

$$u(u-v)^{r-1} + (v+1)^{r-1} = 0,$$

i.e.,

$$-u = \Big(\frac{v+1}{u-v}\Big)^{r-1}.$$

It follows that

$$\Big(-\frac{x^{a_i}}{b_i}\Big)^{\frac{q-1}{k}} = (-u)^{\frac{q-1}{k}} = \Big(\frac{v+1}{u-v}\Big)^{(r-1)\frac{q-1}{k}} = 1.$$

Thus $(-b_i)^{\frac{q-1}{k}} = (x^{\frac{q-1}{k}})^{a_i} = \omega^{ia_i}$, which is a contradiction.

■

Remark.

(i) In Theorem 5.3.1, let q be odd, $k = 2$, $a_0 = t + l$, $a_1 = l$, where $\gcd(l, q-1) = 1$ and $\gcd\big(t+l, \frac{1}{2}(q-1)\big) = 1$. The result is [39, Theorem 8].

(ii) In Theorem 5.3.1, let q be a power of a prime p with $3 \mid q-1$. Let $k = 3$, $a_0 = 1$, $a_1 = 3 + \frac{2}{3}(q-1)$, $a_2 = p + \frac{1}{3}(q-1)$, and assume that $p \equiv 1 \pmod 3$ and $q \equiv 4 \pmod 9$, or $p \equiv 2 \pmod 3$ and $q \equiv 7 \pmod 9$. The result is [39, Theorem 9].

(iii) In Theorem 5.3.1 let q be a power of a prime p such that $q \equiv 1 \pmod 9$. Let $k = 3$, $a_0 = 1$, $a_1 = p^i + \frac{2}{3}(q-1)$, $a_2 = p + \frac{1}{3}(q-1)$, and assume $p^{i-1} \equiv 1 \pmod 3$. The result is [39, Theorem 10].

(iv) In Theorem 5.3.1, let q be a power of a prime p with $p \equiv 1 \pmod{k}$, $q \equiv 1 \pmod{k^2}$, and let $a_i = p^i - \frac{q-1}{k}$, $0 \leq i \leq k-1$. The result is [39, Theorem 11].

(v) In Theorem 5.3.3, let $q = 3^n$, n even, $k = 2$, $a_0 = 3$, $r_0 = 1$, $a_1 = 1$, $r_1 = 3$, $b_1 = 1$. The result is [21, Theorem 2.1].

(vi) In Theorem 5.3.3, let $q = 3^n$, $k = 2$, $a_0 = t$, where $\gcd\big(t, \frac{1}{2}(q-1)\big) = 1$, $r_0 = 1$, $a_1 = 1$, $r_1 = 3$, $b_1 = -\epsilon$, where ϵ is a square of $\mathbb{F}_q^*$. The result is [39, Proposition 1].

6 Conclusion

One of the goals of this dissertation was to explore the permutation behavior of the polynomial $g_{n,q}$ further and answer many questions about $g_{n,q}$ that were not discussed in [22]. Many articles on permutation polynomials introduce necessary and sufficient conditions to construct permutation polynomials. In Chapters 2, 3 and 4, we explained the naturally existing families of permutation polynomials in the form of $g_{n,q}$.

In Chapter 2, we explained the case $e = 1$ and several unexplained desirable triples in [22]. There are still many uncategorized cases in Table 2.1 and most of them occur when $e = 3$ and a few with $e = 4$. All desirable triples are categorized when $e = 5, 6$. Perhaps this is an indication that permutation property of $g_{n,q}$ is easier to understand when e is large. However, we still do not know if the triple $(407, 3; 3)$ belongs to a family. For the time being, we believe that it is a sporadic case.

In Chapter 3, we were in new fronts and answered many questions about $g_{n,q}$ where n is of the form $n = q^a - q^b - 1$. There are still many desirable triples in Table 3.2 for which no theoretic explanation has been found. Conjecture 3.1.1, and 3.1.4 are of more interest in future research in the polynomial $g_{n,q}$. Conjecture 3.2.6 has recently been proved in [23] and its proof has led to the discovery of a hypergeometric identity.

In Chapter 4, we found many categorized cases that explained almost all desirable triples in Table 4.1. Conjecture 4.2.21 is clearly an indication that the unexplained cases in even characteristic seem to be more interesting and challenging.

One of the challenges among the remaining problems of $g_{n,q}$ is to find a criterion for $g_{m,q}$ and $g_{n,q}$ to represent the same function on $\mathbb{F}_{q^e}$, i.e., $g_{m,q} \equiv g_{n,q} \pmod{\mathtt{x}^{q^e} - \mathtt{x}}$.

When $q = 2$, this problem has been answered in [24]. For the general case, there have only been some partial results; see [22, §4].

Computer search results have been a major tool in our effort to find new families of desirable triples of $g_{n,q}$. For example, the conjectures stated in this dissertation would not have been possible without computer search results.

Constructing permutation polynomials has been in literature for some time now and the piecewise construction had been the main focus in several recently published articles. The piecewise approach that we explained in Chapter 5 generalized several recently discovered families of permutation polynomials.

References

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

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

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

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

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

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

[14] 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.

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

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

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

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

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

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

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

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

[23] X. Hou, *A Class of Permutation Binomials over Finite Fields*, arXiv:1210.0881v1, http://arxiv.org/.

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

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

[26] 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.

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

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

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

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

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

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

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

[34] 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.

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

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

[37] 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.

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

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

[40] 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.

APPENDICES

Appendix A - Mathematica Codes for $g_{n,q}$

Here we present some useful Mathematica codes used to identify the permutation behavior of the polynomial $g_{n,q}$. Run the following command each time before you execute each code.

```
Clear["Global`*"]
```

Mathematica Code 1

The following program code, called the Fast Algorithm Code, generates the polynomial $g_{n,q}$ for any given n, e, and q in a very short time.

```
q = ; (* input q *)
list = Flatten[FactorInteger[q]];
p = list[[1]];
e = ; (* input e*)
n = ; (* input n *)
list = {};
m = Length[IntegerDigits[n, q]];
a = IntegerDigits[n, q];
nk = a[[1]];
For[u = 0, u <= q - 1, u++,
   If[u == q - 1, g[u] = -1, g[u] = 0];
  ];
For[t = q, t <= 2 q, t++,
 g[t] =
    PolynomialMod[x* g[t - q] + g[t - q + 1], x^q^e - x, Modulus -> p];
  ];
For[ k = 1, k <= m - 1, k++,
For[i = 0, i <= q - 1, i++,
   g[q*nk + i*q] =
```

```
     PolynomialMod[ g[nk + i]^q, x^q^e - x, Modulus -> p];
   ];
For[j = 1, j <= q - 1, j++,
   For[l = 0, l <= q - 1 - j, l++,
     g[q*nk + j + l*q] =
       PolynomialMod[ (-x* g[q*nk + j - 1 + l*q]) +
         g[q*nk + j - 1 + (l + 1)*q], x^q^e - x, Modulus -> p];
     ];
   ];
For[s = 2, s <= q, s++,
   For[h = 1, h <= s - 1, h++,
     g[q*nk + s*q - h] =
       PolynomialMod[
        x* g[q*nk + s*q - h - q] + g[q*nk + s*q - h - q + 1],
        x^q^e - x, Modulus -> p];
     ];
   ];
nk = q*nk + a[[k + 1]];
 ];
Print["n = ", n];
Print[g[n]];
```

Appendix A (Continued)

Mathematica Code 2

The following code was executed to generate the desirable triples $(n, e; 3)$ in Table 2.1 by changing the values of "e" and list "M" accordingly.

```
e = ; (* input e *)
q = 3^e;
f0 = 0;
f1 = 0;
f2 = 2;
M = {0, 1, 2};
n0 = 2;  (* n0 = last n *)
For [n = 3, n < 3^(3e) - 1, n++,
(* Checking if n is the smallest in the cyclotomic class *)
m = Min[Mod[3^M*n, 3^(3 e) - 1]];
If [n != m, Continue[]];
For[k = n0 + 1, k <= n, k++,
  f = x*f0 + f1;
  f = PolynomialMod[f, x^q - x, Modulus -> 3];
  f0 = f1;
  f1 = f2;
  f2 = f;
  ];
n0 = n;
(* Hermite's criterion *)
IsPP = True;
h = 1;
For [i = 1, i < q - 1, i++,
  h = PolynomialMod[h*f, x^q - x, Modulus -> 3];
  If[Exponent[h, x] > q - 2, IsPP = False; Goto[step3]];
```

```
  ];
 h = PolynomialMod[h*f, x^q - x, Modulus -> 3];
 If[Exponent[h, x] != q - 1, IsPP = False];
 Label[step3];
 If[IsPP, Print [n, " ", IntegerDigits[n, 3]]; Print[f]];];
```

Mathematica Code 3

The following code was executed to generate the desirable triples $(q^a - q^b - 1, 2; q)$, $q \leq 97$, $0 < b < a < 2p$, b odd, $b \neq p$.

```
list1 = {};
list2 = {};
list3 = {};
e = 2;
For[k = 1, k <= 15, k++,
(* Checking if k is prime *)
If[PrimeQ[k] || PrimePowerQ[k], q = k, Continue[]];
list1 = Flatten[FactorInteger[q]];
p = list1[[1]];
Print["q = ", q];
For[b = 1, b < p*e, b++,
   If[! OddQ[b], Continue[]];
   If[b == p, Continue[]]; (* avoid the case b = p *)
For[a = b + 1, a < p*e, a++,
(* finding coefficients a0,a1,b0 and b1*)
    list2 = QuotientRemainder[b, e];
    b0 = list2[[2]];
    b1 = list2[[1]];
    list3 = QuotientRemainder[a - b, e];
```

```
  a0 = list3[[2]];
  a1 = list3[[1]];

  S = Sum[x^q^i, {i, 0, e - 1}];
  S1 = Sum[x^q^i, {i, 0, a0 - 1}];
  S2 = Sum[x^q^i, {i, 0, b0 - 1}];

  g = -x^(q^e - 2) -
    x^(q^e - q^b0 - 2)*(a1*S + S1^q^b0)*((b1*S + S2)^(q - 1) - 1);

  (* Hermite's criterion *)
  IsPP = True;
  f = PolynomialMod[g, x^q^e - x, Modulus -> p];
  h = 1;
  For [i = 1, i < q^e - 1, i++,
   h = PolynomialMod[h*f, x^q^e - x, Modulus -> p];
   If[Exponent[h, x] > q^e - 2, IsPP = False; Goto[step3]];
    ];
  h = PolynomialMod[h*f, x^q^e - x, Modulus -> p];
  If[Exponent[h, x] != q^e - 1 , IsPP = False];
  Label[step3];
  If[IsPP, Print["a = ", a , "     ", "b = ", b]];
  ];
 ];
];
```

Appendix B - Proof of Theorem 2.4.1

When $q > 3$ is odd,

$g(\mathrm{y})^{2q^2+2} \equiv$

$8\mathrm{y}^{-1+q^3}+2\mathrm{y}^{-3+q^3}+\mathrm{y}^{3-4q^2+q^3}+2\mathrm{y}^{q-4q^2+q^3}+4\mathrm{y}^{2+q-4q^2+q^3}+\mathrm{y}^{-3+2q-4q^2+q^3}+6\mathrm{y}^{-1+2q-4q^2+q^3}+$
$5\mathrm{y}^{1+2q-4q^2+q^3}+2\mathrm{y}^{-4+3q-4q^2+q^3}+4\mathrm{y}^{-2+3q-4q^2+q^3}+2\mathrm{y}^{3q-4q^2+q^3}+2\mathrm{y}^{-3q^2+q^3}+2\mathrm{y}^{2-3q^2+q^3}+$
$2\mathrm{y}^{-3+q-3q^2+q^3}+8\mathrm{y}^{-1+q-3q^2+q^3}+6\mathrm{y}^{1+q-3q^2+q^3}+4\mathrm{y}^{-4+2q-3q^2+q^3}+8\mathrm{y}^{-2+2q-3q^2+q^3}+4\mathrm{y}^{2q-3q^2+q^3}$
$+\mathrm{y}^{-3-2q^2+q^3}+2\mathrm{y}^{-1-2q^2+q^3}+\mathrm{y}^{1-2q^2+q^3}+2\mathrm{y}^{3-2q^2+q^3}+2\mathrm{y}^{-4+q-2q^2+q^3}+4\mathrm{y}^{-2+q-2q^2+q^3}+$
$6\mathrm{y}^{q-2q^2+q^3}+6\mathrm{y}^{2+q-2q^2+q^3}+2\mathrm{y}^{-3+2q-2q^2+q^3}+8\mathrm{y}^{-1+2q-2q^2+q^3}+6\mathrm{y}^{1+2q-2q^2+q^3}+2\mathrm{y}^{-4+3q-2q^2+q^3}$
$+4\mathrm{y}^{-2+3q-2q^2+q^3}+2\mathrm{y}^{3q-2q^2+q^3}+4\mathrm{y}^{-q^2+q^3}+6\mathrm{y}^{2-q^2+q^3}+4\mathrm{y}^{-3+q-q^2+q^3}+16\mathrm{y}^{-1+q-q^2+q^3}+$
$12\mathrm{y}^{1+q-q^2+q^3}+6\mathrm{y}^{-4+2q-q^2+q^3}+12\mathrm{y}^{-2+2q-q^2+q^3}+6\mathrm{y}^{2q-q^2+q^3}+\mathrm{y}^{2+2q-4q^2}+2\mathrm{y}^{-1+3q-4q^2}+$
$2\mathrm{y}^{1+3q-4q^2}+\mathrm{y}^{-4+4q-4q^2}+2\mathrm{y}^{-2+4q-4q^2}+\mathrm{y}^{4q-4q^2}+2\mathrm{y}^{-1+2q-3q^2}+2\mathrm{y}^{1+2q-3q^2}+2\mathrm{y}^{-4+3q-3q^2}+$
$4\mathrm{y}^{-2+3q-3q^2}+2\mathrm{y}^{3q-3q^2}+2\mathrm{y}^{3+q-2q^2}+\mathrm{y}^{-4+2q-2q^2}+2\mathrm{y}^{-2+2q-2q^2}+5\mathrm{y}^{2q-2q^2}+6\mathrm{y}^{2+2q-2q^2}+$
$2\mathrm{y}^{-3+3q-2q^2}+8\mathrm{y}^{-1+3q-2q^2}+6\mathrm{y}^{1+3q-2q^2}+2\mathrm{y}^{-4+4q-2q^2}+4\mathrm{y}^{-2+4q-2q^2}+2\mathrm{y}^{4q-2q^2}+4\mathrm{y}^{q-q^2}+$
$6\mathrm{y}^{2+q-q^2}+4\mathrm{y}^{-3+2q-q^2}+16\mathrm{y}^{-1+2q-q^2}+12\mathrm{y}^{1+2q-q^2}+6\mathrm{y}^{-4+3q-q^2}+12\mathrm{y}^{-2+3q-q^2}+6\mathrm{y}^{3q-q^2}+$
$2\mathrm{y}^{-3+q^2}+4\mathrm{y}^{-1+q^2}+4\mathrm{y}^{1+q^2}+4\mathrm{y}^{3+q^2}+2\mathrm{y}^{-4+q+q^2}+6\mathrm{y}^{-2+q+q^2}+14\mathrm{y}^{q+q^2}+12\mathrm{y}^{2+q+q^2}+$
$6\mathrm{y}^{-3+2q+q^2}+18\mathrm{y}^{-1+2q+q^2}+12\mathrm{y}^{1+2q+q^2}+4\mathrm{y}^{-4+3q+q^2}+8\mathrm{y}^{-2+3q+q^2}+4\mathrm{y}^{3q+q^2}+\mathrm{y}^{-2+2q^2}+$
$6\mathrm{y}^{2+2q^2}+6\mathrm{y}^{-3+q+2q^2}+18\mathrm{y}^{-1+q+2q^2}+12\mathrm{y}^{1+q+2q^2}+6\mathrm{y}^{-4+2q+2q^2}+12\mathrm{y}^{-2+2q+2q^2}+6\mathrm{y}^{2q+2q^2}+$
$2\mathrm{y}^{-3+3q^2}+6\mathrm{y}^{-1+3q^2}+4\mathrm{y}^{1+3q^2}+4\mathrm{y}^{-4+q+3q^2}+8\mathrm{y}^{-2+q+3q^2}+4\mathrm{y}^{q+3q^2}+\mathrm{y}^{-4+4q^2}+2\mathrm{y}^{-2+4q^2}+$
$8\mathrm{y}^{-3+q}+20\mathrm{y}^{-1+q}+12\mathrm{y}^{2q}+\mathrm{y}^{4q}+6\mathrm{y}^{2q^2}+\mathrm{y}^{4q^2}+14\mathrm{y}^{1+q}+4\mathrm{y}^{3+q}+6\mathrm{y}^{-4+2q}+13\mathrm{y}^{-2+2q}+$
$6\mathrm{y}^{2+2q}+2\mathrm{y}^{-3+3q}+6\mathrm{y}^{-1+3q}+4\mathrm{y}^{1+3q}+\mathrm{y}^{-4+4q}+2\mathrm{y}^{-2+4q}+6\mathrm{y}^{2}+\mathrm{y}^{4}.$

Appendix B (Continued)

When $q > 3$ is even,

$g(\mathrm{y})^{2q^2+q+3} \equiv$

$\mathrm{y}^{q^3-1} + \mathrm{y}^{q^3-5} + \mathrm{y}^{q^3-q+4} + \mathrm{y}^{q^3-q+2} + \mathrm{y}^{q^3-2q+5} + \mathrm{y}^{q^3-2q+1} + \mathrm{y}^{q^3-2q-1} + \mathrm{y}^{q^3-2q-3}$
$+\mathrm{y}^{q^3-2q-5} + \mathrm{y}^{q^3-q^2+4q-2} + \mathrm{y}^{q^3-q^2+4q-6} + \mathrm{y}^{q^3-q^2+3q-1} + \mathrm{y}^{q^3-q^2+3q-3} + \mathrm{y}^{q^3-q^2+3q-5}$
$+\mathrm{y}^{q^3-q^2+3q-7} + \mathrm{y}^{q^3-q^2+2q} + \mathrm{y}^{q^3-q^2+2q-2} + \mathrm{y}^{q^3-q^2+2q-6} + \mathrm{y}^{q^3-q^2+q+1} + \mathrm{y}^{q^3-q^2+q-1}$
$+\mathrm{y}^{q^3-q^2-4} + \mathrm{y}^{q^3-q^2-q+1} + \mathrm{y}^{q^3-q^2-q-1} + \mathrm{y}^{q^3-q^2-q-3} + \mathrm{y}^{q^3-q^2-q-5} + \mathrm{y}^{q^3-q^2-2q}$
$+\mathrm{y}^{q^3-q^2-2q-4} + \mathrm{y}^{q^3-2q^2+6q-1} + \mathrm{y}^{q^3-2q^2+6q-3} + \mathrm{y}^{q^3-2q^2+6q-5} + \mathrm{y}^{q^3-2q^2+6q-7}$
$+\mathrm{y}^{q^3-2q^2+5q-2} + \mathrm{y}^{q^3-2q^2+5q-6} + \mathrm{y}^{q^3-2q^2+4q-1} + \mathrm{y}^{q^3-2q^2+4q-3} + \mathrm{y}^{q^3-2q^2+3q-2}$
$+\mathrm{y}^{q^3-2q^2+3q-4} + \mathrm{y}^{q^3-2q^2+3q-6} + \mathrm{y}^{q^3-2q^2+2q+3} + \mathrm{y}^{q^3-2q^2+2q+1} + \mathrm{y}^{q^3-2q^2+2q-3}$
$+\mathrm{y}^{q^3-2q^2+q+2} + \mathrm{y}^{q^3-2q^2+q-4} + \mathrm{y}^{q^3-2q^2+3} + \mathrm{y}^{q^3-2q^2-3} + \mathrm{y}^{q^3-2q^2-5} + \mathrm{y}^{q^3-2q^2-q+2}$
$+\mathrm{y}^{q^3-2q^2-q} + \mathrm{y}^{q^3-2q^2-q-2} + \mathrm{y}^{q^3-2q^2-q-4} + \mathrm{y}^{q^3-2q^2-2q+1} + \mathrm{y}^{q^3-2q^2-2q-1} + \mathrm{y}^{q^3-3q^2+2q}$
$+\mathrm{y}^{q^3-3q^2+2q-4} + \mathrm{y}^{q^3-3q^2+q+1} + \mathrm{y}^{q^3-3q^2+q-1} + \mathrm{y}^{q^3-3q^2+q-3} + \mathrm{y}^{q^3-3q^2+q-5}$
$+\mathrm{y}^{q^3-3q^2+2} + \mathrm{y}^{q^3-3q^2} + \mathrm{y}^{q^3-3q^2-4} + \mathrm{y}^{q^3-3q^2-q+3} + \mathrm{y}^{q^3-3q^2-q+1} + \mathrm{y}^{q^3-3q^2-2q+2}$
$+\mathrm{y}^{q^3-4q^2+4q+1} + \mathrm{y}^{q^3-4q^2+4q-1} + \mathrm{y}^{q^3-4q^2+4q-3} + \mathrm{y}^{q^3-4q^2+4q-5} + \mathrm{y}^{q^3-4q^2+3q}$
$+\mathrm{y}^{q^3-4q^2+3q-4} + \mathrm{y}^{q^3-4q^2+2q+1} + \mathrm{y}^{q^3-4q^2+2q-1} + \mathrm{y}^{q^3-4q^2+q} + \mathrm{y}^{q^3-4q^2+q-2}$
$+\mathrm{y}^{q^3-4q^2+q-4} + \mathrm{y}^{q^3-4q^2+5} + \mathrm{y}^{q^3-4q^2+3} + \mathrm{y}^{q^3-4q^2-1} + \mathrm{y}^{q^3-4q^2-q+4} + \mathrm{y}^{q^3-4q^2-q+2}$
$+\mathrm{y}^{q^3-4q^2-2q+3} + \mathrm{y}^{6q^2} + \mathrm{y}^{6q^2-2} + \mathrm{y}^{6q^2-4} + \mathrm{y}^{6q^2-6} + \mathrm{y}^{6q^2-2q} + \mathrm{y}^{6q^2-2q-2} + \mathrm{y}^{6q^2-2q-4}$
$+\mathrm{y}^{6q^2-2q-6} + \mathrm{y}^{5q^2-1} + \mathrm{y}^{5q^2-5} + \mathrm{y}^{5q^2-q} + \mathrm{y}^{5q^2-q-2} + \mathrm{y}^{5q^2-q-4} + \mathrm{y}^{5q^2-q-6}$
$+\mathrm{y}^{5q^2-2q-1} + \mathrm{y}^{5q^2-2q-5} + \mathrm{y}^{4q^2+2q} + \mathrm{y}^{4q^2+2q-2} + \mathrm{y}^{4q^2+2q-4} + \mathrm{y}^{4q^2+2q-6} + \mathrm{y}^{4q^2+q-1}$
$+\mathrm{y}^{4q^2+q-5} + \mathrm{y}^{4q^2+2} + \mathrm{y}^{4q^2-4} + \mathrm{y}^{4q^2-q+1} + \mathrm{y}^{4q^2-q-1} + \mathrm{y}^{4q^2-q-3} + \mathrm{y}^{4q^2-q-5}$
$+\mathrm{y}^{4q^2-2q+2} + \mathrm{y}^{4q^2-2q-4} + \mathrm{y}^{3q^2-3} + \mathrm{y}^{3q^2-q-2} + \mathrm{y}^{3q^2-q-4} + \mathrm{y}^{3q^2-2q-3} + \mathrm{y}^{2q^2+4q}$
$+\mathrm{y}^{2q^2+4q-2} + \mathrm{y}^{2q^2+4q-4} + \mathrm{y}^{2q^2+4q-6} + \mathrm{y}^{2q^2+q-3} + \mathrm{y}^{2q^2+4} + \mathrm{y}^{2q^2+2} + \mathrm{y}^{2q^2-6}$
$+\mathrm{y}^{2q^2-q-1} + \mathrm{y}^{2q^2-q-3} + \mathrm{y}^{2q^2-2q+4} + \mathrm{y}^{2q^2-2q+2} + \mathrm{y}^{2q^2-2q} + \mathrm{y}^{q^2+4q-1} + \mathrm{y}^{q^2+4q-5}$
$+\mathrm{y}^{q^2+3q} + \mathrm{y}^{q^2+3q-2} + \mathrm{y}^{q^2+3q-4} + \mathrm{y}^{q^2+3q-6} + \mathrm{y}^{q^2+2q-3} + \mathrm{y}^{q^2+q} + \mathrm{y}^{q^2+q-6} + \mathrm{y}^{q^2+3}$
$+\mathrm{y}^{q^2-1} + \mathrm{y}^{q^2-3} + \mathrm{y}^{q^2-5} + \mathrm{y}^{q^2-q+4} + \mathrm{y}^{q^2-q+2} + \mathrm{y}^{q^2-2q+3} + \mathrm{y}^{6q} + \mathrm{y}^{6q-2} + \mathrm{y}^{6q-4}$
$+\mathrm{y}^{6q-6} + \mathrm{y}^{5q-1} + \mathrm{y}^{5q-5} + \mathrm{y}^{4q+2} + \mathrm{y}^{4q-4} + \mathrm{y}^{3q+1} + \mathrm{y}^{2q+4} + \mathrm{y}^{2q} + \mathrm{y}^{2q-2} + \mathrm{y}^{2q-4}$
$+\mathrm{y}^{2q-6} + \mathrm{y}^{q+3} + \mathrm{y}^{q+1} + \mathrm{y}^{q-5} + \mathrm{y}^{6} + \mathrm{y}^{2}.$

Appendix C - Copyright and Permissions

For Authors

Home
Rights & responsibilities
Funding body agreements
Open access
Author services
Journal performance
Early career researchers
Book authors
Elsevier Editorial System
Authors' Update

Rights & responsibilities

At Elsevier, we request transfers of copyright, or in some cases exclusive rights, from our journal authors in order to ensure that we have the rights necessary for the proper administration of electronic rights and online dissemination of journal articles. Authors and their employers retain (or are granted/transferred back) significant scholarly rights in their work. We take seriously our responsibility as the steward of the online record to ensure the integrity of scholarly works and the sustainability of journal business models, and we actively monitor and pursue unauthorized and unsubscribed uses and re-distribution (for subscription models).

In addition to authors' scholarly rights, authors have certain responsibilities for their work, particularly in connection with publishing ethics issues.

Rights | FAQ | Responsibilities | Permissions

As a journal author, you have rights for a large range of uses of your article, including use by your employing institute or company. These rights can be exercised without the need to obtain specific permission.

How authors can use their own journal articles

Authors publishing in Elsevier journals have wide rights to use their works for teaching and scholarly purposes without needing to seek permission.

Table of Authors' Rights

	Preprint version (with a few exceptions- see below *)	Accepted Author Manuscript	Published Journal Articles
Use for classroom teaching by author or author's institution and presentation at a meeting or conference and distributing copies to attendees	Yes	Yes with full acknowledgement of final article	Yes with full acknowledgement of final article
Use for internal training by author's company	Yes	Yes with full acknowledgement of final article	Yes with full acknowledgement of final article
Distribution to colleagues for their research use	Yes	Yes	Yes
Use in a subsequent compilation of the author's works	Yes	Yes with full acknowledgement of final article	Yes with full acknowledgement of final article
Inclusion in a thesis or dissertation	Yes	Yes with full acknowledgement of final article	Yes with full acknowledgement of final article
Reuse of portions or extracts from the article in other works	Yes	Yes with full acknowledgement of final article	Yes with full acknowledgement of final article
Preparation of derivative works (other than for commercial purposes)	Yes	Yes with full acknowledgement of final article	Yes with full acknowledgement of final article
Preprint servers	Yes	Yes with the specific written permission of Elsevier	No
Voluntary posting on open web sites operated by author or author's institution for scholarly	Yes (author may later add an appropriate bibliographic citation, indicating subsequent	Yes, with appropriate bibliographic citation and a link to the article once	Only with the specific written permission of Elsevier

Appendix C (Continued)

purposes	publication by Elsevier and journal title)	published	
Mandated deposit or deposit in or posting to subject-oriented or centralized repositories	Yes under specific agreement between Elsevier and the repository	Yes under specific agreement between Elsevier and the repository**	Yes under specific agreement between Elsevier and the repository
Use or posting for commercial gain or to substitute for services provided directly by journal	Only with the specific written permission of Elsevier	Only with the specific written permission of Elsevier	Only with the specific written permission of Elsevier

**Voluntary posting of Accepted Author Manuscripts in the arXiv subject repository is permitted.

Examples of use or posting for commercial gain:

- Posting by companies of employee-authored works for use by customers of those companies (e.g. pharmaceutical companies and physician prescribers)
- Commercial exploitation such as directly associating advertising with posting or charging fees for document delivery or access

***Which journals have different preprint policies?**

If an electronic preprint of an article is placed on a public server prior to its submission to an Elsevier journal, this is not generally viewed by Elsevier as 'prior publication' and will not disqualify the article from further consideration by Elsevier, nor will Elsevier require the removal of that preprint version.

However Cell Press and The Lancet have different preprint policies and will not consider for publication articles that have already been posted publicly. This is a rule agreed upon by The International Committee of Medical Journal Editors. Information on Cell Press policy on preprints is available, as is *The Lancet* preprint policy . There are a number of other journals published by Elsevier (principally journals published on behalf of third party owners) that also have their own preprint policies which will be set out in the Guide for Authors for the relevant journal.

Does Elsevier request a transfer of copyright?

Elsevier requests a transfer of copyright for articles published under subscription-based business models but we generally use different licensing approaches for other publishing models where we offer authors a variety of Creative Commons licenses for some of our author-pays journals and are piloting a range of options. Learn more about Creative Commons licenses.

For subscription-based publishing, we ask for a transfer of copyright for a number of reasons, mainly because:

1. By having the ability to exercise all rights under copyright, Elsevier is able to quickly launch new products and services, and to make agreements with other platforms and services to enrich published content and to make it more accessible and usable. Authors may be based in a number of different countries, which will have their own copyright regimes. Copyright assignments give more legal certainty, particularly in relation to future rights in new technologies.
2. Elsevier uses copyright to protect the integrity of the journal articles in cases of plagiarism, copyright infringement and other third party infringements. The journal subscription business model depends on a substantial body of subscribing customers providing financial support to a particular journal, and "free-riding" infringements diminish this model.
3. An assignment of rights under copyright means that we can more easily show that we own the rights and do not have to seek the participation of the author or obtain power of attorney from the author in order to bring an enforcement action.

Remember, even though we ask for a transfer of copyright, our journal authors retain (or are granted back) significant scholarly rights, as outlined above.

For a more detailed discussion, see the STM Position Paper on the benefits of copyright assignments.

Does Elsevier claim rights in an author's supporting data?

Elsevier supports the general principle that raw research data should be made freely available to all researchers and encourages the public posting of the raw data outputs of research. (Note that this is distinct from charts, tables, etc. which may be included within an article and in which rights would be transferred or licensed to Elsevier as part of the article, in the same way as text, illustrations or photographs). Elsevier therefore does not claim rights in the raw datasets that may be submitted with an article and the author can make these datasets freely available from other (web) locations.

If supported by the author and journal editor, and when a dataset is hosted in a repository that ensures data integrity and supports long-term preservation and inward linking, Elsevier can further support the discoverability of that dataset by connecting it with the published journal article on ScienceDirect through linking from an article or entity or through article interoperability. Click here to review examples of how this could work in practice.

Appendix C (Continued)

For more information on industry positions on this issue supported by Elsevier, view the:

Joint Statement from STM and DataCite on the Linkability and Citability of Research Data, June 2012

Brussels Declaration on STM Publishing , November 2007

STM/ALPSP Statement , June 2006

Can I post my published journal article on open websites?

A published journal article is the definitive final record of published research that appears in the journal and embodies all value-adding publisher activities, including copy editing, formatting and, if relevant, pagination, along with the stewardship of the scholarly record.

You can use your branded and formatted published article for all of the personal and institutional purposes described above. However, in order to safeguard the correct scientific record, Elsevier does not permit the posting of published journal articles (either the pdf provided by Elsevier or HTML files) on any open websites.

As part of its contribution to the stewardship of the scientific literature, Elsevier works with third parties (e.g. national libraries) to preserve its journal articles for posterity and in perpetuity, and invests to drive their usage. Elsevier strictly enforces an absolute guideline on the location of its published journal articles: each branded and formatted published journal article will reside only on a completely controlled site because this is the only way that we as the publisher can guarantee that each published journal article is permanent, authentic and unaltered as part of the 'minutes of science'.

Since Elsevier adds significant value to the final published journal article, we need to take these steps to ensure that this value is maintained, both for Elsevier and for our authors. However, we view preprints and accepted author manuscripts as less formal versions of the article and we therefore take a more liberal approach towards these, as described in more detail on our Article Posting Policies information page.

ABOUT THE AUTHOR

Neranga Fernando was born in Negombo and grew up in Ekala in Sri Lanka. He attended Maris Stella College in Negombo for his high school education. He earned his B.Sc.(special) degree majoring Mathematics from the University of Kelaniya, Sri Lanka in 2007. He then entered the Master's program in Mathematics at the University of South Florida in 2008. After completing his master's in 2009, he entered the Ph.D. program in Mathematics at the University of South Florida in 2010.

Neranga, under the supervision of Dr. Xiang-dong Hou, focused on permutation polynomials over finite fields. He taught several undergraduate courses at USF as a Graduate Teaching Assistant. His research interest lies in Algebra: Finite fields and their applications.

Neranga likes volleyball, soccer, and racquetball.