January 2013

A Study of Permutation Polynomials over Finite Fields

Neranga Fernando

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

Follow this and additional works at: http://scholarcommons.usf.edu/etd

Part of the Mathematics Commons

Scholar Commons Citation


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

Copyright © 2013, Neranga Fernando
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, Nihuk 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 iii  

Abstract iv  

1 Introduction 1  

1.1 The Polynomial $g_{n,q}$ .................................................. 5  

2 Special Families of Desirable Triples and a Sporadic Case 11  

2.1 The Polynomial $g_{n,2}$ .................................................. 11  

2.2 The Case $e = 1$ ................................................... 12  

2.3 Two Families of Desirable Triples when $p = 3$ ................. 13  

2.4 A Sporadic Case ....................................................... 14  

3 Desirable Triples of the Form $(q^a - q^b - 1, e; q)$ 23  

3.1 The Polynomial $g_{q^a-q^b-1,q}$ ........................................ 24  

3.2 Desirable Triples of the Form $(q^a - q^b - 1, 2; q)$ .......... 28  

3.2.1 The Case $b = p$ .................................................. 28  

3.2.2 The Case $b = 1$ .................................................. 33  

3.2.3 The Case $a = p + i + 1$ and $b = 2i + 1$ ................. 37  

4 The Polynomial $g_{n,q}$ when $q$ is Even 45  

4.1 Families of Desirable Triples with $w_q(n) = q + 1$ .......... 45  

4.2 More Families of Desirable Triples with Even $q$ .......... 51
5 A Piecewise Construction of Permutation Polynomials over Finite Fields 70

5.1 Introduction ................................................................. 70
5.2 PPs with $\theta(x) = (L(x) + \delta)^{\frac{k}{2}(q-1)}$ ................................. 72
5.3 PPs with $\theta(x) = x^{\frac{k}{2}(q-1)}$ ........................................ 78

6 Conclusion 85

References 87

Appendices 91

Appendix A - Mathematica Codes for $g_{n,q}$ ................................. 92
Appendix B - Proof of Theorem 2.4.1 ........................................... 97
Appendix C - Copyright and Permissions ...................................... 99

About the Author  

End Page
### List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Desirable triples ((n, e; 3)), (e \leq 6), (w_3(n) &gt; 3)</td>
<td>18</td>
</tr>
<tr>
<td>3.1</td>
<td>Desirable triples ((5^a - 5^b - 1, 2; q)), (a, b \geq 0)</td>
<td>23</td>
</tr>
<tr>
<td>3.2</td>
<td>Desirable triples ((q^a - q^b - 1, 2; q)), (q \leq 97), (0 &lt; b &lt; a &lt; 2p), (b) odd, (b \neq p), ((a, b) \neq (2, 1))</td>
<td>41</td>
</tr>
<tr>
<td>4.1</td>
<td>Desirable triples ((n, e; 4)), (e \leq 6), (w_4(n) &gt; 4)</td>
<td>68</td>
</tr>
</tbody>
</table>
Let $p$ be a prime and $q = p^k$. The polynomial $g_{n,q} \in \mathbb{F}_p[x]$ defined by the functional equation

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

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.
Let $p$ be a prime and $q$ a power of $p$. Let $\mathbb{F}_q$ be the finite field with $q$ elements. A polynomial $f \in \mathbb{F}_q[x]$ 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 $\mathbb{F}_q[x]$. In fact, if $\phi : \mathbb{F}_q \rightarrow \mathbb{F}_q$ is an arbitrary function form $\mathbb{F}_q$ to $\mathbb{F}_q$, then there exists a unique polynomial $g \in \mathbb{F}_q[x]$ with $\deg(g) \leq q - 1$ representing $\phi$, 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 $\phi$. If $\phi$ is already given as a polynomial function, say $\phi : c \mapsto f(c)$ where $f \in \mathbb{F}_q[x]$, then $g$ can be obtained from $f$ by reduction modulo $x^q - x$. 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 $x_1x_2$ 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

$$x_1^n + x_2^n = D_n(x_1 + x_2, x_1x_2);$$

see [31]. The explicit form of $D_n(x, y)$ is given by Waring’s formula [30, Theorem
1.76]

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

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 \( n \)th 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 non-linear (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 $g_{n,q} \in \mathbb{F}_p[x]$ such that

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

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

$$g_{n,q}(x) = \sum_{\frac{n}{q} \leq l \leq \frac{n}{q - 1}} \frac{n}{l} \left( n - l(q - 1) \right) x^{n - l(q - 1)}. \quad (1.0.2)$$

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 $n$th 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 $F_q$ be of characteristic $p$. Then $f \in F_q[x]$ is a permutation polynomial of $F_q$ 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 $f_s \in F_q[x]$ with deg $f_s \leq q - 2$.

(2) $f$ is a permutation polynomial of $F_{p^n}$ if and only if

$$\sum_{x \in F_{p^n}} \zeta_p^{\text{Tr}_{p^n/p}(cf(x))} = 0$$

for all $0 \neq c \in F_{p^n}$, where $\zeta_p = e^{2\pi i/p}$ and $\text{Tr}_{p^n/p}(x) = x + x^p + \cdots + x^{p^{n-1}}$ is the absolute trace function from $F_{p^n}$ to $F_p$.

**Definition 1.0.1** (Desirable triple). If $g_{n,q}$ is a PP of $F_q^e$, 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 $F_2^e$. 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, \( x, y, t \), are reserved for indeterminates. The trace function \( \text{Tr}_{q^e/q} \) and the norm function \( N_{q^e/q} \) from \( \mathbb{F}_{q^e} \) to \( \mathbb{F}_q \) are also treated as polynomials, that is, \( \text{Tr}_{q^e/q}(x) = x + x^q + \cdots + x^{q^{e-1}}, \ N_{q^e/q}(x) = x^1 + x^q + \cdots + x^{q^{e-1}} \).

When \( q \) is given, we define \( S_a = x + x^q + \cdots + x^{q^{a-1}} \) for every integer \( a \geq 0 \). Note that \( \text{Tr}_{q^e/q} = S_e \).

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

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

where \( \sigma_k \) is the \( k \)th elementary symmetric polynomial in \( q \) variables. A comparison
of the coefficients of $t$ on both sides of (1.1.3) tells that

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

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

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

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

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

Set

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

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

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

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

$$\begin{cases} 
g_{0,q} = \cdots = g_{q-2,q} = 0, \\
g_{q-1,q} = -1, \\
g_{n,q} = x g_{n-q,q} + g_{n-q+1,q}, \quad n \geq q.
\end{cases} \quad (1.1.5)$$
Using the above recurrence relation, \( g_{n,q} \) can be defined for \( n < 0 \):

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

For \( n < 0 \), \( g_{n,q} \) belongs to \( \mathbb{F}_p[x, x^{-1}] \), the ring of Laurent polynomials in \( x \) 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 \( \{g_{n,q}\}_{n \geq 0} \):

\[
\sum_{n \geq 0} g_{n,q} t^n = \frac{-t^{q-1}}{1 - t^{q-1} - xt^q}.
\] (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 \( g_{n_1,q} \equiv g_{n_2,q} \pmod{x^{q^e} - x} \).

**Proof.**

(i) We have

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

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

\[ \square \]

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 \( a = a_0d^0 + \cdots + a_td^t \), \( 0 \leq a_i \leq d - 1 \), the base \( d \) weight of \( a \) is \( w_d(a) = a_0 + \cdots + a_t \).

Let \( n \geq 0 \) be any integer and \( w_q(n) \) denote the base \( q \) weight of \( n \).

**Lemma 1.1.3** ([22]). Let \( n = \alpha_0q^0 + \cdots + \alpha_tq^t \), \( 0 \leq \alpha_i \leq q - 1 \) and \( w_q(n) \) be the base \( q \) weight of \( n \),

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

**Definition 1.1.4** An \( F_q \)-linearized polynomial (or a \( q \)-polynomial) over \( F_q^e \) is a polynomial of the form

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

It is well known that \( L \) is a PP of \( F_{q^e} \) if and only if \( L(x) \) only has the root 0 in \( F_{q^e} \). i.e., \( L \) is a PP of \( F_{q^e} \) 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

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

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 $x \in \mathbb{F}_{p^e}$,

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

**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 $\text{Tr}_{p^e/\mathbb{F}_p}^{-1}(0) = \{x \in \mathbb{F}_{p^e} : \text{Tr}_{p^e/\mathbb{F}_p}(x) = 0\}$.

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

\[
\gcd\left(\sum_{i=0}^{e-1} a_ix^i, x^e - 1\right) = x - 1;
\]

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

\[
\gcd\left(\sum_{i=0}^{e-1} b_ix^i, x^e - 1\right) = x - 1.
\]

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

\[
g_{t+q^i,q} = g_{t+1,q} + S_i \cdot g_{t,q}; \tag{1.1.9}
\]

where \( S_i = x + x^q + \cdots + x^{q^{i-1}} \).

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

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

If \( a < 0 \), we define \( S_a = S_{p+1-a} \).
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 \( n \)th reversed Dickson polynomial \( D_n(1, x) \) over \( \mathbb{F}_2 \). Unlike its twin, Dickson polynomial \( D_n(x, a) \), reversed Dickson 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 \( f : \mathbb{F}_q \rightarrow \mathbb{F}_q \) 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 Dickson 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

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

Namely, modulo \(x^q - x\),

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

where

\[
\sum_{n \geq 0} a_n t^n = \frac{-t^{q-1}}{1 - t^{q-1} - t^q}. \tag{2.2.3}
\]
Proof. From (1.1.6),
\[
\sum_{n \geq 0} g_{n,q} t^n = \frac{-t^{q-1}}{1 - t^{q-1} - xt^q}.
\]
Clearly,
\[
\frac{-t^{q-1}}{1 - t^{q-1} - xt^q} \equiv \frac{-(xt)^{q-1}}{1 - (xt)^{q-1} - (xt)^q} + (1 - x^{q-1}) \frac{-t^{q-1}}{1 - t^{q-1}} \pmod{x^{q-1} - 1},
\]
and
\[
\frac{-t^{q-1}}{1 - t^{q-1} - xt^q} \equiv \frac{-(xt)^{q-1}}{1 - (xt)^{q-1} - (xt)^q} + (1 - x^{q-1}) \frac{-t^{q-1}}{1 - t^{q-1}} \pmod{x}.
\]
Thus (2.2.1) is proved.

Corollary 2.2.2  
(i) Assume $q > 2$. Then $(n, 1; q)$ is desirable if and only if 
\[
gcd(n, q - 1) = 1 \quad \text{and} \quad a_n \neq 0 \quad \text{(in $\mathbb{F}_p$)}.
\]
(ii) Assume $q = 2$. Then $(n, 1; 2)$ is desirable if and only if $a_n = 0$ \quad \text{(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 $g_{n,q} \equiv a_n x^n \pmod{x^q - x}$, which is a PP of $\mathbb{F}_q$.

(ii) By (2.2.2), $g_{n,2} \equiv a_n x + x - 1 \pmod{x^2 - x}$. If $a_n = 0$, then $g_{n,2} = x - 1$ 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 $a_n \neq 0$ \quad \text{(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

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

Also, $g_{7,3}(x) = x$, so $x^{26} g_{7,3}(x) = x^{27}$. Both $g_{26 \cdot 3 + 7}$ and $x^{26} g_{7,3}$ are $\mathbb{F}_3$-linear on $\mathbb{F}_3$.

Moreover, $x^{26} g_{7,3}$ is 1-1 on $\text{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$ 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 $\text{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$.

We have, by [22, Eq. 3.4], $-g_{85,3}(x^3 - x) = x^{30} + x^{31} + x^{34}$. So by Proposition 1.1.9, $g_{85,3}$ is 1-1 on $\text{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$ 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

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

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 $\mathbb{F}_3$. Moreover, $x^{163} g_{-162,3}$ is 1-1 on $\text{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$ 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 $\text{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$.

We have, by [22, Eq. 3.4], $-g_{327,3}(x^3 - x) = x^{31} + x^{34} + x^{33}$. So by Proposition 1.1.9, $g_{327,3}$ is 1-1 on $\text{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$ 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

\[ g_{407,3}(x) \]
\[ = g_{2,3^0+2,3^4+3^5,3} \]
\[ = g_{3+2,3^4,3} + S_5 \cdot g_{2+2,3^4,3} \]
\[ = g_{3+2,3^4,3} + S_5 \cdot (g_{3+3,3^4,3} + S_4 \cdot g_{2+3,3^4,3}) \]
\[ = x^3 + x^3^2 + x^3^3 + S_5 \cdot (-1 + S_4 \cdot (-x - x^3 - x^3^2 - x^3^3)) \]
\[ \equiv \operatorname{Tr}_{3^3/3}(x) - S_5(1 + S_4^2) \pmod{x^3^3 - x} \]
\[ \equiv \operatorname{Tr}_{3^3/3}(x) + S_4^3(1 + S_4^2) \pmod{x^3^3 - x} \quad (S_5 \equiv -S_4^2 \pmod{x^3^3 - x}) \]
\[ \equiv \operatorname{Tr}_{3^3/3}(y) + y^2(1 + y^2) \pmod{x^3^3 - x}, \]

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

\[ g_{407,3}(x) \equiv \operatorname{Tr}_{3^3/3}(y) + y^8(\operatorname{Tr}_{3^3/3}(y) - y^{32}) \pmod{x^3^3 - x} \]
\[ = (1 + y^8)\operatorname{Tr}_{3^3/3}(y) - y^{17}. \]

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

\[ g_{407,3}(x') = (1 + y^8)\operatorname{Tr}_{3^3/3}(y) - y^{17} = (1 + x^2)\operatorname{Tr}_{3^3/3}\left(\frac{1}{x}\right) - x, \]

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

\[ h(x) = (1 + x^2)\operatorname{Tr}_{3^3/3}\left(\frac{1}{x}\right) - x \quad (2.4.4) \]

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

\[
(1 + x^2) \text{Tr}_{3^3/3} \left( \frac{1}{x} \right) - x = z. \tag{2.4.5}
\]

If \( \text{Tr}_{3^3/3} \left( \frac{1}{z} \right) = 0 \), \( x = -z \) is the solution. If \( \text{Tr}_{3^3/3} \left( \frac{1}{z} \right) \neq 0 \), we may assume \( \text{Tr}_{3^3/3} \left( \frac{1}{z} \right) = 1 \). 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 \( x \in \mathbb{F}_{3^3}^* \):

\[
\begin{cases}
x^2 - x + 1 - z = 0, \\
\text{Tr}_{3^3/3} \left( \frac{1}{x} \right) = 1;
\end{cases} \tag{2.4.7}
\]

\[
\begin{cases}
x^2 + x + 1 + z = 0, \\
\text{Tr}_{3^3/3} \left( \frac{1}{x} \right) = -1.
\end{cases} \tag{2.4.8}
\]

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 \( \text{Tr}_{3^3/3} \left( \frac{1}{z} \right) = \text{Tr}_{3^3/3} \left( -1 - \frac{1}{z} \right) = -1 \).

**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

\[
\text{Tr}_{3^3/3} \left( \frac{1}{x} \right) = \text{Tr}_{3^3/3} \left( \frac{1}{x^3} \right) = \text{Tr}_{3^3/3} \left( \frac{1}{1 - u^3} \right) = \text{Tr}_{3^3/3} \left( -\frac{1}{z} \right) = -1.
\]

**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 (2.4.8), and

\[
\text{Tr}_{3^3/3} \left( \frac{1}{x} \right) = \text{Tr}_{3^3/3} \left( \frac{1}{x^3} \right) = \text{Tr}_{3^3/3} \left( \frac{1}{1 - w^3} \right) = \text{Tr}_{3^3/3} \left( -\frac{1}{z} \right) = -1.
\]
equation in (2.4.7), and \( \text{Tr}_{3^3/3}(\frac{1}{x}) = \text{Tr}_{3^3/3}(-1 + \frac{1}{x}) = 1 \).

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

In general,

\[
\begin{align*}
    h(x) &= (1 + x^2)(x^{-1} + x^{-q} + x^{-q^2}) - x, \\
    &= x^{-1} + x^{-q} + x^{-q^2} + x^{2-q} + x^{2-q^2} \\
    &= y + y^q + y^{q^2} + y^{q^2-2} + y^{q^2-2} \\
    &= g(y),
\end{align*}
\]

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

First assume \( q = 2 \). We have

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

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

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

(The complete expression of \( g^{2q^2+2} \pmod{y^{q^3} - y} \) 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

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

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

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

<table>
<thead>
<tr>
<th>(e)</th>
<th>(n)</th>
<th>3-adic digits of (n)</th>
<th>reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>17</td>
<td>2 2 1</td>
<td>[22] Prop 3.1</td>
</tr>
<tr>
<td>2</td>
<td>71</td>
<td>2 2 1 2</td>
<td>[22] Prop 3.2 (i)</td>
</tr>
<tr>
<td>2</td>
<td>95</td>
<td>2 1 1 0 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>2</td>
<td>101</td>
<td>2 0 2 0 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>2</td>
<td>103</td>
<td>1 1 2 0 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>2</td>
<td>119</td>
<td>2 0 1 1 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>2</td>
<td>151</td>
<td>1 2 1 2 1</td>
<td>[22] Table 2 No.5</td>
</tr>
<tr>
<td>2</td>
<td>197</td>
<td>2 0 1 2</td>
<td>[22] Prop 3.2 (ii)</td>
</tr>
<tr>
<td>2</td>
<td>485</td>
<td>2 2 2 2 1</td>
<td>[22] Prop 3.1</td>
</tr>
<tr>
<td>3</td>
<td>101</td>
<td>2 0 2 0 1</td>
<td>[14] Thm 4.1</td>
</tr>
<tr>
<td>3</td>
<td>407</td>
<td>2 0 0 0 2 1</td>
<td>Thm 2.4.1</td>
</tr>
<tr>
<td>3</td>
<td>475</td>
<td>1 2 1 2 1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>605</td>
<td>2 0 1 1 1 2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>619</td>
<td>1 2 2 1 1 2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>671</td>
<td>2 1 2 0 2 2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>701</td>
<td>2 2 2 1 2 2</td>
<td>[22] Prop 3.2 (i)</td>
</tr>
<tr>
<td>3</td>
<td>761</td>
<td>2 1 0 1 0 0 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>3</td>
<td>769</td>
<td>1 1 1 1 0 0 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>3</td>
<td>775</td>
<td>1 0 2 1 0 0 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>3</td>
<td>779</td>
<td>2 1 2 1 0 0 1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>785</td>
<td>2 0 0 2 0 0 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>3</td>
<td>787</td>
<td>1 1 0 2 0 0 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>3</td>
<td>827</td>
<td>2 2 1 0 1 0 1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>839</td>
<td>2 0 0 1 1 0 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>3</td>
<td>847</td>
<td>1 0 1 1 1 0 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>3</td>
<td>925</td>
<td>1 2 0 1 2 0 1</td>
<td>[22] Table 2 No.5</td>
</tr>
<tr>
<td>3</td>
<td>1003</td>
<td>1 1 0 1 0 1 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>3</td>
<td>1007</td>
<td>2 2 0 1 0 1 1</td>
<td>[22] Thm 3.10</td>
</tr>
<tr>
<td>3</td>
<td>1009</td>
<td>1 0 1 1 0 1 1</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>3</td>
<td>1097</td>
<td>2 2 1 1 1 1 1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1175</td>
<td>2 1 1 1 2 1 1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1247</td>
<td>2 1 0 1 0 2 1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1423</td>
<td>1 0 2 1 2 2 1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1519</td>
<td>1 2 0 2 0 0 2</td>
<td>[22] Table 2 No.4</td>
</tr>
<tr>
<td>3</td>
<td>1739</td>
<td>2 0 1 1 0 1 2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1753</td>
<td>1 2 2 1 0 1 2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1915</td>
<td>1 2 2 1 2 1 2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2021</td>
<td>2 1 2 2 0 2 2</td>
<td>[22] Thm 3.9</td>
</tr>
<tr>
<td>3</td>
<td>2117</td>
<td>2 0 1 0 2 2 2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2131</td>
<td>1 2 2 0 2 2 2</td>
<td>[22] Prop 3.2 (ii)</td>
</tr>
</tbody>
</table>
Table 2.1 (Continued)

<table>
<thead>
<tr>
<th>$e$</th>
<th>$n$</th>
<th>3-adic digits of $n$</th>
<th>reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2537</td>
<td>$22201101$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2723</td>
<td>$21210201$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2819</td>
<td>$20121201$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2897</td>
<td>$22022201$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3137</td>
<td>$21022011$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3317</td>
<td>$21221111$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3361</td>
<td>$11112111$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3517</td>
<td>$12011211$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3551</td>
<td>$21121211$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3559</td>
<td>$11221211$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3833</td>
<td>$22202021$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4019</td>
<td>$21211121$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4253</td>
<td>$21111221$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4261</td>
<td>$11211221$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5093</td>
<td>$22122202$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5507</td>
<td>$22221112$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5557</td>
<td>$11212112$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5665</td>
<td>$11220212$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5719</td>
<td>$11211212$</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>13121</td>
<td>$222222221$</td>
<td>[22] Prop 3.1</td>
</tr>
<tr>
<td>4</td>
<td>173</td>
<td>$20102$</td>
<td>[22] Table 2 No.3</td>
</tr>
<tr>
<td>4</td>
<td>1477</td>
<td>$1020002$</td>
<td>[22] Table 2 No.3</td>
</tr>
<tr>
<td>4</td>
<td>6479</td>
<td>$22221222$</td>
<td>[22] Prop 3.2 (i)</td>
</tr>
<tr>
<td>4</td>
<td>6647</td>
<td>$210010001$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>6653</td>
<td>$201010001$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>6655</td>
<td>$111010001$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>6661</td>
<td>$102010001$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>6671</td>
<td>$200110001$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>6679</td>
<td>$101110001$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>6725</td>
<td>$200020001$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>6727</td>
<td>$110020001$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>6733</td>
<td>$101020001$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>6751</td>
<td>$100120001$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>6887</td>
<td>$200011001$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>6895</td>
<td>$101011001$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>7135</td>
<td>$120012001$</td>
<td>[22] Table 2 No.5</td>
</tr>
<tr>
<td>4</td>
<td>7373</td>
<td>$200010101$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>7375</td>
<td>$110010101$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>7381</td>
<td>$101010101$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>7399</td>
<td>$100110101$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>8119</td>
<td>$102010201$</td>
<td>[22] Table 2 No.5</td>
</tr>
<tr>
<td>4</td>
<td>8831</td>
<td>$200010011$</td>
<td>[22] Table 2 No.2</td>
</tr>
<tr>
<td>$e$</td>
<td>$n$</td>
<td>3-adic digits of $n$</td>
<td>reference</td>
</tr>
<tr>
<td>-----</td>
<td>-----------</td>
<td>----------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>4</td>
<td>8839</td>
<td>1 0 1 0 1 0 0 1 1</td>
<td>22 Table 2 No.2</td>
</tr>
<tr>
<td>4</td>
<td>8855</td>
<td>2 2 0 1 0 0 1 1</td>
<td>22 Thm 3.10</td>
</tr>
<tr>
<td>4</td>
<td>11071</td>
<td>1 0 0 2 1 0 0 2 1</td>
<td>22 Table 2 No.5</td>
</tr>
<tr>
<td>4</td>
<td>17717</td>
<td>2 1 0 2 2 0 0 2 2</td>
<td>22 Thm 3.9</td>
</tr>
<tr>
<td>4</td>
<td>19519</td>
<td>1 2 2 0 2 2 2 2 2</td>
<td>22 Prop 3.2 (ii)</td>
</tr>
<tr>
<td>4</td>
<td>26725</td>
<td>1 1 2 2 1 0 0 1 1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>28669</td>
<td>1 1 2 2 0 0 1 1 1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>29525</td>
<td>2 1 1 1 1 1 1 1 1 1</td>
<td>14 Thm 3.2</td>
</tr>
<tr>
<td>4</td>
<td>36997</td>
<td>1 2 0 2 0 2 2 1 2 1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>43933</td>
<td>1 1 0 1 2 0 0 2 0 2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>5149</td>
<td>1 1 1 0 2 2 0 0 2 2</td>
<td>14 Thm 3.2</td>
</tr>
<tr>
<td>4</td>
<td>57575</td>
<td>2 0 1 2 2 2 0 2 2 2</td>
<td>Thm 2.2.1</td>
</tr>
<tr>
<td>4</td>
<td>84965</td>
<td>2 1 2 1 1 2 2 0 1 1</td>
<td>14 Thm 3.6</td>
</tr>
<tr>
<td>4</td>
<td>88655</td>
<td>2 1 1 1 2 1 1 1 1 1</td>
<td>14 Thm 3.5</td>
</tr>
<tr>
<td>4</td>
<td>90815</td>
<td>2 1 1 0 2 1 1 2 1 1 1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>4</td>
<td>91525</td>
<td>1 1 2 2 1 1 1 2 1 1 1</td>
<td>14 4.3</td>
</tr>
<tr>
<td>4</td>
<td>107765</td>
<td>2 2 0 1 1 2 0 1 1 2</td>
<td>14 Thm 3.8</td>
</tr>
<tr>
<td>4</td>
<td>133079</td>
<td>2 1 2 1 1 2 0 2 0 2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>148415</td>
<td>2 1 2 0 2 1 2 1 1 1 2</td>
<td>14 Rmk 3.3</td>
</tr>
<tr>
<td>4</td>
<td>167173</td>
<td>1 2 1 2 2 0 1 1 2 2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>265805</td>
<td>2 2 1 1 2 1 1 1 1 1 1</td>
<td>14 Thm 3.5</td>
</tr>
<tr>
<td>4</td>
<td>267935</td>
<td>2 1 1 2 1 1 2 1 1 1 1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>4</td>
<td>272375</td>
<td>2 2 1 2 1 1 1 2 1 1 1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>4</td>
<td>272615</td>
<td>2 1 2 1 2 1 1 1 2 1 1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>4</td>
<td>273095</td>
<td>2 2 1 1 2 1 2 1 1 1 1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>4</td>
<td>354293</td>
<td>2 2 2 2 2 2 2 2 2 2 2 2 2</td>
<td>22 Prop 3.1</td>
</tr>
<tr>
<td>5</td>
<td>515</td>
<td>2,0,0,1,0,2</td>
<td>22 Table 2 No.3</td>
</tr>
<tr>
<td>5</td>
<td>569</td>
<td>2,0,0,0,1,2</td>
<td>22 Table 2 No.3</td>
</tr>
<tr>
<td>5</td>
<td>2675</td>
<td>2,0,0,0,0,2,0,1</td>
<td>22 Table 2 No.3</td>
</tr>
<tr>
<td>5</td>
<td>4393</td>
<td>1,0,2,0,0,0,0,2</td>
<td>22 Table 2 No.3</td>
</tr>
<tr>
<td>5</td>
<td>13177</td>
<td>1,0,0,2,0,0,0,0,2</td>
<td>22 Table 2 No.3</td>
</tr>
<tr>
<td>5</td>
<td>20171</td>
<td>2,0,0,0,0,2,0,0,0,1</td>
<td>22 Table 2 No.3</td>
</tr>
<tr>
<td>5</td>
<td>58805</td>
<td>2,2,2,2,2,1,2,2,2,2</td>
<td>22 Prop 3.2 (i)</td>
</tr>
<tr>
<td>5</td>
<td>59297</td>
<td>2,1,0,0,0,1,0,0,0,0,1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59303</td>
<td>2,0,1,0,0,1,0,0,0,0,1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59305</td>
<td>1,1,1,0,0,1,0,0,0,0,1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59311</td>
<td>1,0,2,0,0,1,0,0,0,0,1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59321</td>
<td>2,0,0,1,0,1,0,0,0,0,1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59323</td>
<td>1,1,0,1,0,1,0,0,0,0,1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59329</td>
<td>1,0,1,1,0,1,0,0,0,0,1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59347</td>
<td>1,0,0,2,0,1,0,0,0,0,1</td>
<td>14 Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59375</td>
<td>2,0,0,0,1,1,0,0,0,0,1</td>
<td>14 Thm 3.1</td>
</tr>
</tbody>
</table>

20
Table 2.1 (Continued)

<table>
<thead>
<tr>
<th>$e$</th>
<th>$n$</th>
<th>3-adic digits of $n$</th>
<th>reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>59377</td>
<td>1,1,0,0,1,1,0,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59383</td>
<td>1,0,1,0,1,1,0,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59401</td>
<td>1,0,0,1,1,1,0,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59455</td>
<td>1,0,0,2,1,0,0,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59537</td>
<td>2,0,0,0,0,2,0,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59539</td>
<td>1,1,0,0,0,2,0,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59545</td>
<td>1,0,1,0,0,2,0,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59563</td>
<td>1,0,0,1,0,2,0,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>59617</td>
<td>1,0,0,1,2,0,0,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>60023</td>
<td>2,0,0,0,0,1,1,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>60031</td>
<td>1,0,1,0,0,1,1,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>60049</td>
<td>1,0,0,1,0,1,1,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>60103</td>
<td>1,0,0,0,1,1,1,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>60757</td>
<td>1,2,0,0,0,1,2,0,0,0,1</td>
<td>[22] Table 2 No.5</td>
</tr>
<tr>
<td>5</td>
<td>61481</td>
<td>2,0,0,0,0,1,0,1,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>61483</td>
<td>1,1,0,0,0,1,0,1,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>61489</td>
<td>1,0,1,0,0,1,0,1,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>61507</td>
<td>1,0,0,1,0,1,0,1,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>61561</td>
<td>1,0,0,0,1,1,0,1,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>63685</td>
<td>1,0,2,0,0,1,0,2,0,0,1</td>
<td>[22] Table 2 No.5</td>
</tr>
<tr>
<td>5</td>
<td>65855</td>
<td>2,0,0,0,0,1,0,0,1,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>65857</td>
<td>1,1,0,0,0,1,0,0,1,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>65863</td>
<td>1,0,1,0,0,1,0,0,1,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>65881</td>
<td>1,0,0,1,0,1,0,0,1,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>65935</td>
<td>1,0,0,0,1,1,0,0,1,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>72469</td>
<td>1,0,0,2,0,1,0,0,2,0,1</td>
<td>[22] Table 2 No.5</td>
</tr>
<tr>
<td>5</td>
<td>78977</td>
<td>2,0,0,0,0,1,0,0,0,1,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>78979</td>
<td>1,1,0,0,0,1,0,0,0,1,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>78985</td>
<td>1,0,1,0,0,1,0,0,0,1,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>79003</td>
<td>1,0,0,1,0,1,0,0,0,1,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>79055</td>
<td>2,2,2,2,0,1,0,0,0,1,1</td>
<td>[22] Thm 3.10</td>
</tr>
<tr>
<td>5</td>
<td>79057</td>
<td>1,0,0,0,1,1,0,0,0,1,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>5</td>
<td>98821</td>
<td>1,0,0,2,1,0,0,0,2,1</td>
<td>Thm 2.2.2</td>
</tr>
<tr>
<td>5</td>
<td>118591</td>
<td>1,2,0,0,0,2,0,0,0,0,2</td>
<td>[22] Table 2 No.4</td>
</tr>
<tr>
<td>5</td>
<td>158117</td>
<td>2,1,0,0,2,2,0,0,0,0,2</td>
<td>[14] Thm 3.2</td>
</tr>
<tr>
<td>5</td>
<td>176659</td>
<td>1,2,2,2,2,2,2,2,2,2</td>
<td>[22] Prop 3.2 (ii)</td>
</tr>
<tr>
<td>5</td>
<td>474349</td>
<td>1,1,1,0,0,2,2,0,0,0,2</td>
<td>[14] Thm 3.2</td>
</tr>
<tr>
<td>5</td>
<td>513875</td>
<td>2,0,1,0,2,2,0,0,0,2,2</td>
<td>Thm 2.2.1</td>
</tr>
<tr>
<td>5</td>
<td>766661</td>
<td>2,1,2,2,2,1,1,2,2,0,1,1</td>
<td>[14] Thm 3.6</td>
</tr>
<tr>
<td>5</td>
<td>112143</td>
<td>1,2,2,2,0,2,2,2,2,0,0,2</td>
<td>[14] Thm 3.2</td>
</tr>
<tr>
<td>5</td>
<td>154163</td>
<td>1,1,0,1,0,2,2,0,0,2,2,2</td>
<td>[14] Thm 3.2</td>
</tr>
<tr>
<td>5</td>
<td>9565937</td>
<td>2,2,2,2,2,2,2,2,2,2,2,2</td>
<td>[22] Prop 3.1</td>
</tr>
<tr>
<td>$e$</td>
<td>$n$</td>
<td>3-adic digits of $n$</td>
<td>reference</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>----------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>6</td>
<td>530711</td>
<td>2,2,2,2,2,1,2,2,2,2</td>
<td>[22] Prop 3.2 (i)</td>
</tr>
<tr>
<td>6</td>
<td>532175</td>
<td>2,1,0,0,0,1,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>532183</td>
<td>1,1,0,0,0,1,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>532189</td>
<td>1,0,2,0,0,1,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>532199</td>
<td>2,0,0,1,0,0,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>532253</td>
<td>2,0,0,0,1,0,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>532261</td>
<td>2,0,1,0,1,0,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>532279</td>
<td>1,0,0,1,1,0,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>532423</td>
<td>1,0,1,0,1,1,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>532495</td>
<td>1,0,0,1,1,1,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>532901</td>
<td>2,0,0,0,0,2,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>532903</td>
<td>1,1,0,0,0,2,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>532927</td>
<td>1,0,0,1,0,2,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>532981</td>
<td>1,0,0,1,0,2,0,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>534359</td>
<td>2,0,0,0,0,1,1,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>534367</td>
<td>1,0,1,0,0,1,1,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>536551</td>
<td>1,2,0,0,0,1,2,0,0,0</td>
<td>[22] Table 2 No.5</td>
</tr>
<tr>
<td>6</td>
<td>538735</td>
<td>1,1,0,0,0,1,0,1,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>538741</td>
<td>1,0,1,0,0,1,0,1,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>538813</td>
<td>1,0,0,1,0,1,0,1,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>538975</td>
<td>1,0,0,0,1,1,0,1,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>551855</td>
<td>2,0,0,0,0,1,0,0,1,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>551935</td>
<td>1,0,0,1,0,1,0,1,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>571591</td>
<td>1,0,2,0,0,1,0,0,2,0</td>
<td>[22] Table 2 No.5</td>
</tr>
<tr>
<td>6</td>
<td>591221</td>
<td>2,0,0,0,0,1,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>591229</td>
<td>1,0,1,0,0,1,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>591247</td>
<td>1,0,0,1,0,1,0,0,1,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>591463</td>
<td>1,0,0,0,1,1,0,0,1,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>650431</td>
<td>1,0,0,0,2,0,1,0,0,2</td>
<td>Thm 2.2</td>
</tr>
<tr>
<td>6</td>
<td>709327</td>
<td>1,0,1,0,0,0,1,0,0,0</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>709399</td>
<td>1,0,0,1,0,1,0,0,0,1</td>
<td>[14] Thm 3.1</td>
</tr>
<tr>
<td>6</td>
<td>709559</td>
<td>2,2,2,2,2,0,1,0,0,0</td>
<td>[22] Thm 3.10</td>
</tr>
<tr>
<td>6</td>
<td>1419125</td>
<td>2,1,0,0,2,0,0,0,0,2</td>
<td>[14] Thm 3.2</td>
</tr>
<tr>
<td>6</td>
<td>1592863</td>
<td>1,2,2,2,2,0,2,2,2,2</td>
<td>[22] Prop 3.2 (ii)</td>
</tr>
<tr>
<td>6</td>
<td>4612151</td>
<td>2,0,1,0,0,2,2,0,0,2</td>
<td>Thm 2.2</td>
</tr>
<tr>
<td>6</td>
<td>6905813</td>
<td>2,1,2,2,2,2,1,2,2,2,0</td>
<td>[14] Thm 3.6</td>
</tr>
<tr>
<td>6</td>
<td>10095919</td>
<td>1,2,2,2,2,0,2,2,2,2,0</td>
<td>[14] Thm 3.2</td>
</tr>
<tr>
<td>6</td>
<td>19657477</td>
<td>1,0,2,2,2,0,0,2,2,2,0,0</td>
<td>[14] Thm 3.2</td>
</tr>
<tr>
<td>6</td>
<td>258280325</td>
<td>2,2,2,2,2,2,2,2,2,2,2</td>
<td>[22] Prop 3.1</td>
</tr>
</tbody>
</table>

Table 2.1 (Continued)
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 \((5^a - 5^b - 1, 2; q)\), \(a, b \geq 0\)

<table>
<thead>
<tr>
<th>(n)</th>
<th>base 5 digits of (n)</th>
<th>(a)</th>
<th>(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>599</td>
<td>4 4 3 4</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>14999</td>
<td>4 4 4 4 3 4</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>15599</td>
<td>4 4 3 4 4 4</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>15619</td>
<td>4 3 4 4 4 4</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>74999</td>
<td>4 4 4 4 4 3 4</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>374999</td>
<td>4 4 4 4 4 4 3 4</td>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>389999</td>
<td>4 4 4 4 3 4 4 4</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>390599</td>
<td>4 4 3 4 4 4 4 4</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>390619</td>
<td>4 3 4 4 4 4 4 4</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>19499999</td>
<td>4 4 4 4 4 3 4 4 4</td>
<td>9</td>
<td>5</td>
</tr>
<tr>
<td>78124999</td>
<td>4 4 4 4 4 4 4 4 4 4 3 4 4</td>
<td>10</td>
<td>9</td>
</tr>
</tbody>
</table>

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

\(^\dagger\)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 is 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 $\mathbb{F}_{q^e}$.

Recall that $S_a = x + x^q + \cdots + x^{q^{a-1}}$ 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,

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

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

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

$$= \frac{S_a^q}{x^2}$$

$$= x^{q-2} + x^{q^2-2} + \cdots + x^{q^{a-1}-2}. \tag{3.1.1}$$

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,

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

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

$$S_bg_{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}{x} + \left(\frac{S_{a-b}}{x}\right)^{q^b}\]

$$= -\frac{S_a - S_{a-b}}{x} + \left(\frac{1}{x^{q^b}} - \frac{1}{x}\right)S_{a-b}^{q^b}\]

$$= -\frac{S_b}{x} - \frac{S_{b}^{q^b} - S_{b}S_{a-b}^{q^b}}{x^{q^b+1}}S_{a-b}.$$
So
\[ g_{q^a-q^b-1,q} = -\frac{1}{x} - \frac{(S_a^{q-1} - 1)S_b^q}{x^{q+1}}. \] (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
\[ g_{q^a-q^b-1,q} \equiv -x^{q^e-2} - x^{q^e-\phi(q)-2}(a_1S_e + S_{a_0}^q)(b_1S_e + S_{b_0})^{q-1} - 1) \pmod{x^{q^e} - x}. \] (3.1.3)

**Corollary 3.1.2** We have
\[ g_{q^2-q-1,q} = -x^{q^2-2}. \]
In particular, \( (q^2 - q - 1, e; q) \) is desirable if and only if \( q > 2 \) and \( \gcd(q-2, q^e-1) = 1 \).

**Proof.** It follows from (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
\[ g_{q^a-q^b-1,q} \equiv -x^{q^e-2} \pmod{x^{q^e} - x} \] (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
\[ g_{q^a-q^b-1,q} \equiv -x^{q^e-2} - x^{q^e-3}a_1S_e((b_1S_e)^{q-1} - 1) \pmod{x^{q^e} - x} \]
\[ = -x^{q^e-2} - x^{q^e-3}a_1S_e(q^{q-1} - 1) \]
\[ = -x^{q^e-2} - x^{q^e-3}a_1(S_e^{q-1} - 1) \]
\[ = -x^{q^e-2} \quad \text{(mod } x^{q^e} - x). \] (3.1.5)
Assume (3.1.4) holds. Then by (3.1.2),

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

For \(f \in \mathbb{F}_q[x]\), 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 \(V(x^q - x) \subset V(x^q - x) \cup V(S_{a-b})\), i.e., \(\mathbb{F}_{q^e} \subset \mathbb{F}_{q^e} \cup V(S_{a-b})\). Since \(V(S_{a-b})\) is a vector space over \(\mathbb{F}_q\), we must have \(\mathbb{F}_{q^e} \subset \mathbb{F}_{q^e} \) or \(\mathbb{F}_{q^e} \subset V(S_{a-b})\). However, since \(0 < a < pe\),

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

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

\[S_{a_0}(S_{e^{-1}}^{q^e} - 1) \equiv 0 \pmod{x^q - x}. \tag{3.1.6}
\]

If \(a_0 > 0\), then

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

which is a contradiction to (3.1.6). So we must have \(a_0 = 0\), i.e., \(a \equiv 0 \pmod{e}\).

\[\square\]

**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

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

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

The results of our computer search suggest that when \(e \geq 3\), the only desirable triples \((q^a - q^b - 1, e; q)\), \(0 < b < a < pe\), are those given by Corollary 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 \((x - x^q)^{q-1} + 1.\)

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

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

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

**Proof.** (i) We have

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

Hence the claim.
(ii) Let $e = 2$, $a = p + 2i$, $b = p$. In the notation of (3.1.3), $a_0 = 0$, $a_1 = i$, $b_0 = 1$, $b_1 = \frac{p-1}{2}$. Thus

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

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

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

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

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

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

\[
= -x^{-1} + 2ix^{q-2} + 2ix^{q^2-2}
\]

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

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

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

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

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

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

Hence

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

So $(2i - 1)^2 \equiv (2i)^2 \pmod{p}$, i.e., $4i - 1 \equiv 0 \pmod{p}$, which is a contradiction.
(⇒) Assume $4i \equiv 1 \pmod{p}$. Then $(2i - 1)x + 2ix^q = 2i(x^q - x)$, which is clearly not 1-1 on $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

\textbf{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

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

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

\textbf{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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

\[\blacksquare\]

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

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

If \(i\) is odd,

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

**Proof.** Let \(n = q^{p+i} - q^p - 1\). Throughout the proof, “\(\equiv\)” means “\(\equiv \pmod{x^{q^2} - x}\)”. 

31
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

\[
g_{n,q} \equiv -x^{q^2-2} - x^{q^2-q-2} \frac{i}{2} S_2 \cdot \left[ \left( -\frac{1}{2} S_2 + S_1 \right)^{q-1} - 1 \right]
\]

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

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

Note that

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

So

\[
g_{n,q} \equiv -x^{q^2-2} - \frac{i}{2} x^{q^2-q-1} (1 + x^q-1) \left[ x^{q-1} \sum_{j=0}^{q-1} x^{(q-1)j} - 1 \right]
\]

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

\[
= -x^{q^2-2} - \frac{i}{2} x^{q^2-q-1} \cdot 2 \sum_{j=2}^{q} x^{(q-1)j}
\]

\[
= -x^{q^2-2} - i x^{q-2} \sum_{j=0}^{q-2} x^{(q-1)j}.
\]

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),

\[
g_{n,q} \equiv -x^{q^2-2} - x^{q^2-q-2} \left( \frac{i-1}{2} S_2 + S_1 \right) \left[ \left( -\frac{1}{2} S_2 + S_1 \right)^{q-1} - 1 \right]
\]

\[
= -x^{q^2-2} - x^{q^2-q-2} \left( -\frac{1}{2} S_2 + S_1 \right) \left[ \left( -\frac{1}{2} S_2 + S_1 \right)^{q-1} - 1 \right]
\]

\[
- \frac{i}{2} x^{q^2-q-2} S_2 \cdot \left[ \left( -\frac{1}{2} S_2 + S_1 \right)^{q-1} - 1 \right].
\]
In the above,
\[
-x^{q^2-2} - x^{q^2-q-2} \left( -\frac{1}{2} S_2 + S_1^q \right) \left( -\frac{1}{2} S_2 + S_1 \right)^{q-1} - 1 \\
= -x^{q^2-2} - x^{q^2-q-2} \frac{1}{2} (x^{q} - x)(x - x^q)^{q-1} - 1 \\
= -x^{q^2-2} - \frac{1}{2} x^{q^2-q-2} (x^{q} - x)^q - (x^q - x) \\
\equiv -x^{q^2-2} - \frac{1}{2} x^{q^2-q-2} \cdot 2(x - x^q) \\
= -x^{q^2-q-1},
\]
and, by the calculation in Case 1,
\[
-\frac{i}{2} x^{q^2-q-2} S_2 \cdot \left( -\frac{1}{2} S_2 + S_1 \right)^{q-1} - 1 \equiv -ix^{q^2-2} \sum_{j=0}^{q-2} x^{(q-1)j}.
\]
So
\[
g_{n,q} \equiv -x^{q^2-q-1} - ix^{q^2-2} \sum_{j=0}^{q-2} x^{(q-1)j}.
\]

3.2.2 The Case \( b = 1 \)

**Theorem 3.2.4** Let \( q = 2^s \), \( n = q^3 - q - 1 \).

(i) For \( x \in \mathbb{F}_{q^2} \),
\[
g_{n,q}(x) = \begin{cases} 
0 & \text{if } x = 0, \\
\cdot x^{q-2} + \text{Tr}_{q^2/q}(x^{-1}) & \text{if } x \neq 0.
\end{cases}
\]

(ii) \( g_{n,q} \) is a PP of \( \mathbb{F}_{q^2} \) if and only if \( s \) is even.
Proof. (i) It is obvious that \( g(0) = 0 \). Let \( 0 \neq x \in \mathbb{F}_{q^2} \). By (3.1.3) (with \( a_0 = 0, a_1 = 1, b_0 = 1, b_1 = 0 \)),

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

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

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

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

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

Let \( t = c^{-q}x = (cx^{-q})^{-q} \in \mathbb{F}_q^* \). Then \( x = tc^q \). Making this substitution in (3.2.7), we have

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

So

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

Hence \( x \) is unique.

2° Assume \( s \) is even. We show that

\[
x^{q-2} + \text{Tr}_{q^2/q}(x^{-1}) = 0 \tag{3.2.8}
\]

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 \( \text{Tr}_{q^2/q}(x^{-1}) = 0 \), and \( x^{q-2} = 0 \), which is a contradiction.
Assume $s$ is odd. We show that (3.2.8) has a solution in $\mathbb{F}_{q^2}^*$. Let $x \in \mathbb{F}_{2^2}\backslash\mathbb{F}_2$.

Then $x^2 + x + 1 = 0$ and $x^3 = 1$. So

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

$$= 1 + x^2 + x \quad \text{(since } q \equiv 2 \pmod{3})$$

$$= 0.$$

\[\square\]

**Theorem 3.2.5**

(i) Assume $q > 2$. We have

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

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

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

**Proof.** In the notation of (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

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

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

$$= -x^{q^2-2} - x^{q^2-q-2}(-x^q - (i - 1)x + i2^{q-1})$$

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

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

$$f(x) = \begin{cases} 
0 & \text{if } x = 0, \\
-x^q + x^{q-2} & \text{if } x \in \mathbb{F}_{q^2}^*.
\end{cases}$$
We show that for every $c \in \mathbb{F}_{q^2}^*$, the equation
\[ x^{-q} + x^{q-2} = c \]  \hspace{1cm} (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
\[ cx^{-q} = x^{-2q} + x^{-2} = \text{Tr}_{q^2/q}(x^{-2}) \in \mathbb{F}_q. \]
Let $t = c^{-q}x = (cx^{-q})^{-q} \in \mathbb{F}_q^*$. Then $x =tc^q$. So (3.2.9) becomes
\[ \frac{1}{t}(c^{-1} + c^{q(q-2)}) = c. \]
Thus $t = c^{-2} + c^{-2q}$. Hence $x$ is unique.

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

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 $f = x^{q-2} + tx^{q^2-q-1}$, $t \in \mathbb{F}_q^*$. 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) $t = 3$, $q \equiv -1 \pmod{6}$. 

36
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 \( 0 \leq i \leq p - 2 \) and \( n = q^{p+i+1} - q^{2i+1} - 1 \). If

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

(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 “\( \equiv (\mod x^q - x) \)”.

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

\[
g \equiv -x^{q^2-2} - x^{q^2-2}(\frac{p-i}{2} - S_2)((iS_2 + S_1)^{q-1} - 1) \quad (\mod x^q - x)
\]

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

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

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

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

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

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

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

\[
y = -x^{-1}
\]

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

37
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

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

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

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

$$i((i+1)w^q - iw)^{2q} + 2(i+1)((i+1)w^q - iw)^{q+1} + i((i+1)w^q - iw)^2 = c$$  \hspace{1cm} (3.2.11)

i.e.,

$$\frac{i((i+1)w^q - iw)^{2q} + 2(i+1)((i+1)w^q - iw)^{q+1} + i((i+1)w^q - iw)^2}{w} = c$$  \hspace{1cm} (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), \( a_0 = 1, a_1 = \frac{p-i-1}{2}, b_0 = 1, b_1 = i \).

\[
g \equiv -x^{q^2-2} - x^{q^2-2} \left( \frac{p-i-1}{2} S_2 + S_1^q \right) ((iS_2 + x)q^{-1} - 1)
\]

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

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

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

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

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

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

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

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

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

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

where \( u = (i + 1)w^q - iw \).
The proof will be complete if we can show that for $c \in \mathbb{F}_{q^2}$,

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

i.e.,

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

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

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

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

$$(i + 1)z^2 + 2iz + (i + 1) = 0.$$

(3.2.16)

Since $i$ is even $\binom{2i + 1}{q} = (-1)^{\frac{q+1}{2}}$, 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 \((q^a - q^b - 1, 2; q), q \leq 97, 0 < b < a < 2p, b \text{ odd, } b \neq p, (a, b) \neq (2, 1)\)

<table>
<thead>
<tr>
<th>(a)</th>
<th>(b)</th>
<th>(a)</th>
<th>(b)</th>
<th>(a)</th>
<th>(b)</th>
<th>(a)</th>
<th>(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(q = 2)</td>
<td>10 5</td>
<td>24 13</td>
<td>40 7</td>
<td>38 13</td>
<td>50 25</td>
<td>60 37</td>
<td>66 45</td>
</tr>
<tr>
<td>(-)</td>
<td>13 11</td>
<td>25 1</td>
<td>40 33</td>
<td>40 7</td>
<td>51 27</td>
<td>61 39</td>
<td>67 47</td>
</tr>
<tr>
<td>(-)</td>
<td>25 15</td>
<td>41 35</td>
<td>40 17</td>
<td>52 37</td>
<td>62 1</td>
<td>71 35</td>
<td></td>
</tr>
<tr>
<td>(-)</td>
<td>6 1</td>
<td>27 19</td>
<td>43 30</td>
<td>41 3</td>
<td>57 7</td>
<td>64 11</td>
<td>74 27</td>
</tr>
<tr>
<td>(q = 2^2)</td>
<td>8 1</td>
<td>28 21</td>
<td>45 13</td>
<td>41 9</td>
<td>58 41</td>
<td>64 45</td>
<td>74 61</td>
</tr>
<tr>
<td>(q = 2^3)</td>
<td>8 3</td>
<td>30 25</td>
<td>41 31</td>
<td>59 5</td>
<td>65 49</td>
<td>76 51</td>
<td></td>
</tr>
<tr>
<td>(-)</td>
<td>9 3</td>
<td>33 5</td>
<td>(q = 29)</td>
<td>42 3</td>
<td>61 47</td>
<td>66 49</td>
<td>76 65</td>
</tr>
<tr>
<td>(-)</td>
<td>10 5</td>
<td>15 11</td>
<td>42 21</td>
<td>62 49</td>
<td>67 51</td>
<td>77 67</td>
<td></td>
</tr>
<tr>
<td>(q = 2^4)</td>
<td>12 5</td>
<td>(q = 19)</td>
<td>21 3</td>
<td>46 29</td>
<td>62 55</td>
<td>69 3</td>
<td>78 9</td>
</tr>
<tr>
<td>(q = 2^5)</td>
<td>12 9</td>
<td>17 9</td>
<td>26 21</td>
<td>49 35</td>
<td>63 39</td>
<td>70 57</td>
<td>78 69</td>
</tr>
<tr>
<td>(-)</td>
<td>13 11</td>
<td>23 7</td>
<td>30 1</td>
<td>49 37</td>
<td>64 39</td>
<td>70 65</td>
<td>79 65</td>
</tr>
<tr>
<td>(-)</td>
<td>6 1</td>
<td>30 21</td>
<td>32 27</td>
<td>50 37</td>
<td>67 53</td>
<td>72 61</td>
<td>82 77</td>
</tr>
<tr>
<td>(q = 2^6)</td>
<td>10 1</td>
<td>30 23</td>
<td>33 7</td>
<td>51 39</td>
<td>69 63</td>
<td>77 33</td>
<td>83 79</td>
</tr>
<tr>
<td>(-)</td>
<td>10 1</td>
<td>30 23</td>
<td>33 7</td>
<td>51 39</td>
<td>69 63</td>
<td>77 33</td>
<td>83 79</td>
</tr>
<tr>
<td>(q = 2^7)</td>
<td>18 13</td>
<td>33 17</td>
<td>36 3</td>
<td>57 51</td>
<td>73 71</td>
<td>80 77</td>
<td>85 83</td>
</tr>
<tr>
<td>(-)</td>
<td>19 15</td>
<td>34 29</td>
<td>36 13</td>
<td>58 53</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(q = 3^2)</td>
<td>20 17</td>
<td>36 5</td>
<td>42 25</td>
<td>60 5</td>
<td>12 7</td>
<td>20 11</td>
<td>18 3</td>
</tr>
<tr>
<td>(-)</td>
<td>31 17</td>
<td>44 1</td>
<td>60 57</td>
<td>31 1</td>
<td>21 11</td>
<td>20 9</td>
<td></td>
</tr>
<tr>
<td>(-)</td>
<td>4 1</td>
<td>(q = 13)</td>
<td>37 35</td>
<td>46 33</td>
<td>61 59</td>
<td>31 5</td>
<td>32 13</td>
</tr>
<tr>
<td>(-)</td>
<td>5 1</td>
<td>12 1</td>
<td>46 35</td>
<td>42 1</td>
<td>38 31</td>
<td>29 7</td>
<td></td>
</tr>
<tr>
<td>(q = 3^3)</td>
<td>14 1</td>
<td>(q = 23)</td>
<td>47 35</td>
<td>(q = 37)</td>
<td>42 33</td>
<td>39 11</td>
<td>37 31</td>
</tr>
<tr>
<td>(-)</td>
<td>15 5</td>
<td>10 7</td>
<td>52 19</td>
<td>19 15</td>
<td>44 5</td>
<td>46 5</td>
<td>44 21</td>
</tr>
<tr>
<td>(-)</td>
<td>18 9</td>
<td>21 13</td>
<td>53 23</td>
<td>32 19</td>
<td>46 9</td>
<td>49 11</td>
<td>46 1</td>
</tr>
<tr>
<td>(-)</td>
<td>19 5</td>
<td>22 1</td>
<td>54 49</td>
<td>34 21</td>
<td>49 29</td>
<td>51 15</td>
<td>49 3</td>
</tr>
<tr>
<td>(-)</td>
<td>22 7</td>
<td>25 3</td>
<td>55 51</td>
<td>36 1</td>
<td>52 21</td>
<td>55 23</td>
<td>50 5</td>
</tr>
<tr>
<td>(-)</td>
<td>25 23</td>
<td>26 5</td>
<td>56 5</td>
<td>38 1</td>
<td>53 1</td>
<td>58 29</td>
<td>50 29</td>
</tr>
<tr>
<td>(-)</td>
<td>(q = 17)</td>
<td>32 17</td>
<td>57 15</td>
<td>39 3</td>
<td>54 25</td>
<td>59 31</td>
<td>54 13</td>
</tr>
<tr>
<td>(-)</td>
<td>4 1</td>
<td>11 1</td>
<td>34 21</td>
<td>41 7</td>
<td>55 33</td>
<td>60 33</td>
<td>54 51</td>
</tr>
<tr>
<td>(-)</td>
<td>6 1</td>
<td>15 7</td>
<td>35 31</td>
<td>(q = 31)</td>
<td>42 5</td>
<td>57 31</td>
<td>60 39</td>
</tr>
<tr>
<td>(-)</td>
<td>7 3</td>
<td>18 1</td>
<td>37 3</td>
<td>22 3</td>
<td>42 9</td>
<td>58 15</td>
<td>61 35</td>
</tr>
<tr>
<td>(-)</td>
<td>9 7</td>
<td>18 1</td>
<td>37 11</td>
<td>28 21</td>
<td>43 11</td>
<td>58 33</td>
<td>62 37</td>
</tr>
<tr>
<td>(-)</td>
<td>22 5</td>
<td>37 27</td>
<td>29 21</td>
<td>48 21</td>
<td>59 5</td>
<td>62 53</td>
<td>62 29</td>
</tr>
<tr>
<td>(-)</td>
<td>22 9</td>
<td>39 31</td>
<td>35 7</td>
<td>48 45</td>
<td>60 27</td>
<td>65 61</td>
<td>64 33</td>
</tr>
</tbody>
</table>
### Table 3.1 (Continued)

<table>
<thead>
<tr>
<th>(a)</th>
<th>(b)</th>
<th>(a)</th>
<th>(b)</th>
<th>(a)</th>
<th>(b)</th>
<th>(a)</th>
<th>(b)</th>
<th>(a)</th>
<th>(b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>68</td>
<td>41</td>
<td>58</td>
<td>9</td>
<td>77</td>
<td>35</td>
<td>115</td>
<td>73</td>
<td>90</td>
<td>39</td>
</tr>
<tr>
<td>68</td>
<td>57</td>
<td>58</td>
<td>9</td>
<td>98</td>
<td>19</td>
<td>77</td>
<td>35</td>
<td>90</td>
<td>57</td>
</tr>
<tr>
<td>70</td>
<td>7</td>
<td>59</td>
<td>11</td>
<td>83</td>
<td>7</td>
<td>116</td>
<td>113</td>
<td>93</td>
<td>25</td>
</tr>
<tr>
<td>70</td>
<td>45</td>
<td>59</td>
<td>29</td>
<td>100</td>
<td>67</td>
<td>85</td>
<td>39</td>
<td>94</td>
<td>25</td>
</tr>
<tr>
<td>73</td>
<td>39</td>
<td>59</td>
<td>37</td>
<td>100</td>
<td>93</td>
<td>85</td>
<td>51</td>
<td>116</td>
<td>73</td>
</tr>
<tr>
<td>73</td>
<td>51</td>
<td>60</td>
<td>13</td>
<td>103</td>
<td>99</td>
<td>87</td>
<td>35</td>
<td>38</td>
<td>33</td>
</tr>
<tr>
<td>75</td>
<td>55</td>
<td>61</td>
<td>15</td>
<td>102</td>
<td>97</td>
<td>90</td>
<td>61</td>
<td>52</td>
<td>39</td>
</tr>
<tr>
<td>76</td>
<td>33</td>
<td>62</td>
<td>17</td>
<td>103</td>
<td>37</td>
<td>90</td>
<td>81</td>
<td>59</td>
<td>51</td>
</tr>
<tr>
<td>76</td>
<td>57</td>
<td>63</td>
<td>57</td>
<td>103</td>
<td>55</td>
<td>91</td>
<td>63</td>
<td>60</td>
<td>1</td>
</tr>
<tr>
<td>77</td>
<td>59</td>
<td>66</td>
<td>25</td>
<td>103</td>
<td>99</td>
<td>92</td>
<td>65</td>
<td>62</td>
<td>1</td>
</tr>
<tr>
<td>77</td>
<td>65</td>
<td>67</td>
<td>43</td>
<td>105</td>
<td>11</td>
<td>94</td>
<td>69</td>
<td>62</td>
<td>49</td>
</tr>
<tr>
<td>77</td>
<td>67</td>
<td>68</td>
<td>29</td>
<td>94</td>
<td>71</td>
<td>63</td>
<td>3</td>
<td>101</td>
<td>91</td>
</tr>
<tr>
<td>79</td>
<td>63</td>
<td>71</td>
<td>11</td>
<td>95</td>
<td>71</td>
<td>64</td>
<td>5</td>
<td>102</td>
<td>25</td>
</tr>
<tr>
<td>82</td>
<td>33</td>
<td>72</td>
<td>37</td>
<td>16</td>
<td>13</td>
<td>96</td>
<td>63</td>
<td>64</td>
<td>37</td>
</tr>
<tr>
<td>82</td>
<td>69</td>
<td>72</td>
<td>49</td>
<td>20</td>
<td>3</td>
<td>96</td>
<td>73</td>
<td>66</td>
<td>5</td>
</tr>
<tr>
<td>83</td>
<td>71</td>
<td>73</td>
<td>5</td>
<td>23</td>
<td>17</td>
<td>97</td>
<td>75</td>
<td>66</td>
<td>9</td>
</tr>
<tr>
<td>84</td>
<td>59</td>
<td>75</td>
<td>21</td>
<td>24</td>
<td>15</td>
<td>98</td>
<td>77</td>
<td>67</td>
<td>25</td>
</tr>
<tr>
<td>84</td>
<td>73</td>
<td>75</td>
<td>43</td>
<td>30</td>
<td>1</td>
<td>99</td>
<td>79</td>
<td>68</td>
<td>13</td>
</tr>
<tr>
<td>85</td>
<td>75</td>
<td>77</td>
<td>47</td>
<td>31</td>
<td>9</td>
<td>101</td>
<td>9</td>
<td>69</td>
<td>15</td>
</tr>
<tr>
<td>86</td>
<td>13</td>
<td>78</td>
<td>13</td>
<td>39</td>
<td>27</td>
<td>103</td>
<td>87</td>
<td>71</td>
<td>19</td>
</tr>
<tr>
<td>86</td>
<td>77</td>
<td>78</td>
<td>49</td>
<td>50</td>
<td>13</td>
<td>104</td>
<td>89</td>
<td>74</td>
<td>25</td>
</tr>
<tr>
<td>87</td>
<td>79</td>
<td>80</td>
<td>1</td>
<td>56</td>
<td>21</td>
<td>104</td>
<td>101</td>
<td>74</td>
<td>55</td>
</tr>
<tr>
<td>89</td>
<td>83</td>
<td>81</td>
<td>35</td>
<td>58</td>
<td>1</td>
<td>105</td>
<td>7</td>
<td>75</td>
<td>27</td>
</tr>
<tr>
<td>90</td>
<td>85</td>
<td>82</td>
<td>57</td>
<td>61</td>
<td>3</td>
<td>106</td>
<td>51</td>
<td>79</td>
<td>59</td>
</tr>
<tr>
<td>91</td>
<td>27</td>
<td>82</td>
<td>79</td>
<td>61</td>
<td>27</td>
<td>106</td>
<td>93</td>
<td>81</td>
<td>39</td>
</tr>
<tr>
<td>83</td>
<td>59</td>
<td>61</td>
<td>33</td>
<td>107</td>
<td>95</td>
<td>82</td>
<td>41</td>
<td>120</td>
<td>5</td>
</tr>
<tr>
<td>(q = 53)</td>
<td>85</td>
<td>63</td>
<td>63</td>
<td>3</td>
<td>108</td>
<td>83</td>
<td>84</td>
<td>45</td>
<td>120</td>
</tr>
<tr>
<td>27</td>
<td>23</td>
<td>88</td>
<td>13</td>
<td>66</td>
<td>13</td>
<td>108</td>
<td>97</td>
<td>84</td>
<td>79</td>
</tr>
<tr>
<td>32</td>
<td>3</td>
<td>88</td>
<td>69</td>
<td>66</td>
<td>19</td>
<td>109</td>
<td>31</td>
<td>85</td>
<td>47</td>
</tr>
<tr>
<td>50</td>
<td>21</td>
<td>91</td>
<td>29</td>
<td>67</td>
<td>15</td>
<td>110</td>
<td>25</td>
<td>86</td>
<td>17</td>
</tr>
<tr>
<td>51</td>
<td>43</td>
<td>92</td>
<td>23</td>
<td>69</td>
<td>19</td>
<td>110</td>
<td>101</td>
<td>86</td>
<td>49</td>
</tr>
<tr>
<td>54</td>
<td>1</td>
<td>92</td>
<td>77</td>
<td>73</td>
<td>27</td>
<td>113</td>
<td>107</td>
<td>87</td>
<td>39</td>
</tr>
<tr>
<td>57</td>
<td>7</td>
<td>94</td>
<td>81</td>
<td>76</td>
<td>33</td>
<td>114</td>
<td>109</td>
<td>89</td>
<td>35</td>
</tr>
</tbody>
</table>
Table 3.1 (Continued)

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

$q = 3^4$

$q = 83$

$q = 73$

$q = 79$
Table 3.1 (Continued)

<p>| | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>112</td>
<td>35</td>
<td>142</td>
<td>117</td>
<td>71</td>
<td>17</td>
<td>152</td>
<td>83</td>
<td>174</td>
</tr>
<tr>
<td>95</td>
<td>37</td>
<td>128</td>
<td>119</td>
<td>98</td>
<td>17</td>
<td>132</td>
<td>85</td>
<td>176</td>
</tr>
<tr>
<td>127</td>
<td>37</td>
<td>143</td>
<td>119</td>
<td>133</td>
<td>17</td>
<td>151</td>
<td>85</td>
<td>122</td>
</tr>
<tr>
<td>109</td>
<td>39</td>
<td>132</td>
<td>121</td>
<td>155</td>
<td>19</td>
<td>155</td>
<td>85</td>
<td>q</td>
</tr>
<tr>
<td>150</td>
<td>39</td>
<td>145</td>
<td>123</td>
<td>77</td>
<td>21</td>
<td>133</td>
<td>87</td>
<td>81</td>
</tr>
<tr>
<td>106</td>
<td>45</td>
<td>146</td>
<td>125</td>
<td>100</td>
<td>21</td>
<td>135</td>
<td>91</td>
<td>96</td>
</tr>
<tr>
<td>158</td>
<td>49</td>
<td>147</td>
<td>127</td>
<td>133</td>
<td>21</td>
<td>136</td>
<td>93</td>
<td>98</td>
</tr>
<tr>
<td>109</td>
<td>51</td>
<td>163</td>
<td>127</td>
<td>102</td>
<td>25</td>
<td>138</td>
<td>97</td>
<td>115</td>
</tr>
<tr>
<td>75</td>
<td>53</td>
<td>148</td>
<td>129</td>
<td>77</td>
<td>27</td>
<td>139</td>
<td>99</td>
<td>99</td>
</tr>
<tr>
<td>110</td>
<td>53</td>
<td>149</td>
<td>131</td>
<td>35</td>
<td>29</td>
<td>121</td>
<td>101</td>
<td>102</td>
</tr>
<tr>
<td>133</td>
<td>55</td>
<td>156</td>
<td>131</td>
<td>163</td>
<td>33</td>
<td>124</td>
<td>103</td>
<td>167</td>
</tr>
<tr>
<td>112</td>
<td>57</td>
<td>150</td>
<td>133</td>
<td>109</td>
<td>39</td>
<td>142</td>
<td>105</td>
<td>89</td>
</tr>
<tr>
<td>113</td>
<td>59</td>
<td>152</td>
<td>137</td>
<td>46</td>
<td>41</td>
<td>142</td>
<td>107</td>
<td>154</td>
</tr>
<tr>
<td>152</td>
<td>59</td>
<td>154</td>
<td>141</td>
<td>141</td>
<td>43</td>
<td>143</td>
<td>107</td>
<td>102</td>
</tr>
<tr>
<td>115</td>
<td>63</td>
<td>156</td>
<td>145</td>
<td>112</td>
<td>45</td>
<td>144</td>
<td>109</td>
<td>148</td>
</tr>
<tr>
<td>115</td>
<td>69</td>
<td>157</td>
<td>147</td>
<td>113</td>
<td>47</td>
<td>145</td>
<td>111</td>
<td>18</td>
</tr>
<tr>
<td>155</td>
<td>69</td>
<td>158</td>
<td>149</td>
<td>165</td>
<td>47</td>
<td>173</td>
<td>111</td>
<td>103</td>
</tr>
<tr>
<td>148</td>
<td>71</td>
<td>159</td>
<td>151</td>
<td>173</td>
<td>47</td>
<td>150</td>
<td>121</td>
<td>182</td>
</tr>
<tr>
<td>81</td>
<td>73</td>
<td>162</td>
<td>157</td>
<td>114</td>
<td>49</td>
<td>151</td>
<td>123</td>
<td>161</td>
</tr>
<tr>
<td>120</td>
<td>73</td>
<td></td>
<td></td>
<td>100</td>
<td>51</td>
<td>156</td>
<td>123</td>
<td>110</td>
</tr>
<tr>
<td>121</td>
<td>75</td>
<td>q</td>
<td>89</td>
<td>92</td>
<td>53</td>
<td>159</td>
<td>123</td>
<td>50</td>
</tr>
<tr>
<td>95</td>
<td>77</td>
<td>41</td>
<td>1</td>
<td>116</td>
<td>53</td>
<td>149</td>
<td>125</td>
<td>111</td>
</tr>
<tr>
<td>126</td>
<td>85</td>
<td>90</td>
<td>1</td>
<td>117</td>
<td>55</td>
<td>152</td>
<td>125</td>
<td>158</td>
</tr>
<tr>
<td>127</td>
<td>87</td>
<td>134</td>
<td>1</td>
<td>139</td>
<td>55</td>
<td>132</td>
<td>127</td>
<td>53</td>
</tr>
<tr>
<td>154</td>
<td>87</td>
<td>139</td>
<td>1</td>
<td>170</td>
<td>55</td>
<td>154</td>
<td>129</td>
<td>113</td>
</tr>
<tr>
<td>110</td>
<td>89</td>
<td>92</td>
<td>5</td>
<td>118</td>
<td>57</td>
<td>155</td>
<td>131</td>
<td>114</td>
</tr>
<tr>
<td>128</td>
<td>89</td>
<td>94</td>
<td>5</td>
<td>102</td>
<td>61</td>
<td>156</td>
<td>133</td>
<td>74</td>
</tr>
<tr>
<td>131</td>
<td>95</td>
<td>176</td>
<td>5</td>
<td>123</td>
<td>67</td>
<td>154</td>
<td>137</td>
<td>115</td>
</tr>
<tr>
<td>149</td>
<td>95</td>
<td>151</td>
<td>7</td>
<td>150</td>
<td>67</td>
<td>159</td>
<td>139</td>
<td>138</td>
</tr>
<tr>
<td>132</td>
<td>97</td>
<td>166</td>
<td>7</td>
<td>124</td>
<td>69</td>
<td>169</td>
<td>141</td>
<td>130</td>
</tr>
<tr>
<td>133</td>
<td>99</td>
<td>94</td>
<td>9</td>
<td>125</td>
<td>71</td>
<td>168</td>
<td>143</td>
<td>98</td>
</tr>
<tr>
<td>134</td>
<td>101</td>
<td>95</td>
<td>11</td>
<td>161</td>
<td>71</td>
<td>166</td>
<td>153</td>
<td>123</td>
</tr>
<tr>
<td>115</td>
<td>105</td>
<td>44</td>
<td>13</td>
<td>126</td>
<td>73</td>
<td>168</td>
<td>157</td>
<td>183</td>
</tr>
<tr>
<td>136</td>
<td>105</td>
<td>127</td>
<td>13</td>
<td>129</td>
<td>79</td>
<td>170</td>
<td>161</td>
<td>81</td>
</tr>
<tr>
<td>139</td>
<td>111</td>
<td>49</td>
<td>15</td>
<td>130</td>
<td>81</td>
<td>173</td>
<td>167</td>
<td>119</td>
</tr>
</tbody>
</table>
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 $a = a_0d^0 + \cdots + a_td^t$, $0 \leq a_i \leq d - 1$, 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 $w_q(n) > 4$.

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

$$g_{n,q} = \sum_i S_{a_i}S_{b_i} + \sum_{i<j}(S_{a_i} + S_{b_i})(S_{a_j} + S_{b_j}).$$
Proof. We write \( g \) for \( g_{n,q} \). By (1.1.10) we have

\[
g_n = g_{1+2q^{a_1}+2q^{b_2}+\ldots+q^{a_{q/2}}+q^{b_{q/2}}} + (S_{b_1} - S_{a_1})g_{1+q^{a_1}+q^{b_2}+\ldots+q^{a_{q/2}}+q^{b_{q/2}}} \\
= g_{1+2q^{a_1}+q^{a_2}+\ldots+q^{a_{q/2}}+q^{b_{q/2}}} \\
+ (S_{a_1} + S_{b_1})(S_{a_1} + S_{a_2} + S_{b_2} + \ldots + S_{a_{q/2}} + S_{b_{q/2}}) \\
= \ldots \ldots \\
= g_{1+2q^{a_1}+\ldots+2q^{a_{q/2}}} + \sum_{i=1}^{q/2} (S_{a_i} + S_{b_i}) \left( S_{a_i} + \sum_{j=i+1}^{q/2} (S_{a_j} + S_{b_j}) \right) \\
= S_{a_1}^2 + \ldots + S_{a_{q/2}}^2 + \sum_{i=1}^{q/2} (S_{a_i} + S_{b_i}) \left( S_{a_i} + \sum_{j=i+1}^{q/2} (S_{a_j} + S_{b_j}) \right) \\
= \sum_i S_{a_i}S_{b_i} + \sum_{i<j} (S_{a_i} + S_{b_i})(S_{a_j} + S_{b_j}).
\]

\[
\]

\[
\]

Corollary 4.1.2 Let \( q \geq 4 \) be even, and let

\[
n = t_0 + 2t_1q^{a_1} + \ldots + 2t_kq^{a_k},
\]

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

Then

\[
g_{n,q} = (t_1S_{a_1} + \ldots + t_kS_{a_k})^2.
\]

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

\[
gcd\left(\sum_{i=1}^{k} t_i(1 + x + \ldots + x^{a_i-1}), x^e - 1\right) = 1.
\]

Proof. By Theorem 4.1.1,

\[
g_{n,q} = t_1S_{a_1}^2 + \ldots + t_kS_{a_k}^2 = (t_1S_{a_1} + \ldots + t_kS_{a_k})^2.
\]
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

$$g_{n,q} = S_1^2 + S_1S_2 = x^{q+1},$$

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

$$g_{n,q} = S_1S_a + S_eS_{e+1} + (S_1 + S_a)(S_e + S_{e+1})$$

$$\equiv S_1S_a + S_eS_{e+1} + (S_1 + S_a)S_1 \pmod{x^{q^e} - x}$$

$$= S_1^2 + S_eS_{e+1}$$

$$= x^2 + x\text{Tr}_{q^e/q}(x) + \text{Tr}_{q^e/q}(x)^2.$$

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 $\text{Tr}_{q^e/q}(g_{n,q}(x)) = \text{Tr}_{q^e/q}(g_{n,q}(y))$, we derive that $\text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(y) = c$. Then the equation $g_{n,q}(x) = g_{n,q}(y)$ becomes

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

So $x + y + c = 0$. Thus $c = \text{Tr}_{q^e/q}(c) = \text{Tr}_{q^e/q}(x + y) = 0$. 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,

$$g_{q^0+2q^1+q^e+q^{e+1}} = S_1S_1 + S_eS_{e+1}$$

$$\equiv x^2 + x\text{Tr}_{q^e/q}(x) + \text{Tr}_{q^e/q}(x)^2 \pmod{x^{q^e} - x}.$$

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

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

It leads to

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

By taking traces on both sides of (4.1.2) we get $\text{Tr}_{q^e/q}(a) = 0$.

By (4.1.2), $a(a + \text{Tr}_{q^e/q}(x)) = 0$.

If $\text{Tr}_{q^e/q}(x) = a$, taking traces on both sides gives $e\text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(a) = 0$. Since $e$ is odd $\text{Tr}_{q^e/q}(x) = 0$, 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,

$$g_{q^0+q^1+2q^{e-1}+q^e} = S_1S_e + S_{e-1}S_{e-1}$$

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

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

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

It leads to

$$x\text{Tr}_{q^e/q}(a) + a\text{Tr}_{q^e/q}(x) + a\text{Tr}_{q^e/q}(a) + \text{Tr}_{q^e/q}(a)^2 + a^{2q^{e-1}} = 0. \quad (4.1.4)$$
By taking traces on both sides we get $\text{Tr}_{q^e/q}(a) = 0$. By (4.1.4),

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

If $\text{Tr}_{q^e/q}(x) = 0$, $a = 0$.

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

If $\text{Tr}_{q^e/q}(x) \neq 0, 1$, squaring both sides of (4.1.5) gives $a(a\text{Tr}_{q^e/q}(x)^2 + 1) = 0$. If $a\text{Tr}_{q^e/q}(x)^2 + 1 = 0$, 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,

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

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,

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

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,

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

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,

$$g_{(q-1)q^0+2q^{e-1}} = S_0^2 + S_{e-1}^2$$

$$= S_0^2 + x^{2q^{e-1}}.$$
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

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

It leads to

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

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

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,

$$g_{(q-1)q^0+2q^{e-2}} = S_0^2 + S_{e-2}^2$$

$$= S_e^2 + x^{2q^{e-2}} + x^{2q^{e-1}}. \quad (4.1.8)$$

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

$$\text{Tr}_{q^e/q}(x)^2 + x^{2q^{e-2}} + x^{2q^{e-1}} = \text{Tr}_{q^e/q}(x + a)^2 + (x + a)^{2q^{e-2}} + (x + a)^{2q^{e-1}}. \quad (4.1.9)$$

It leads to

$$\text{Tr}_{q^e/q}(a)^2 + a^{2q^{e-2}} + a^{2q^{e-1}} = 0. \quad (4.1.10)$$

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

By (4.1.9), $a^{2q^{e-2}} + a^{2q^{e-1}} = 0$.

Raising both sides to the $(q/2)^{\text{th}}$ power gives $a(a^{q^{e-2}} + 1) = 0$.

If $a^{q^{e-2}} + 1 = 0$, $\text{Tr}_{q^e/q}(a) = 1$, since $e$ is odd, which is a contradiction.

So $a = 0$. 

50
Example 4.1.12 Let $q = 4$, $e > 2$, $n = q^0 + 2q^1 + 2q^e$. Then by Theorem 4.1.1,

\[ g_{q^0 + 2q^1 + 2q^e} = S_1^2 + S_e^2 \]

\[ = x^2 + S_e^2. \]

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

\[ x^2 + \text{Tr}_{q^e/q}(x)^2 = (x + a)^2 + \text{Tr}_{q^e/q}(x + a)^2. \]

(4.1.10)

It leads to

\[ \text{Tr}_{q^e/q}(a)^2 + a^2 = 0. \]

(4.1.11)

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

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

\[
(S_b - S_a)g_{n,q} = g_{(q-1)q^a+q^{b+1},q} - g_{q^{a+1}+(q-1)q^b,q} \\
= -(x^{q^a} + \cdots + x^{q^b}) - (x^{q^{a+1}} + \cdots + x^{q^{b-1}}) \\
= -(x^{q^a} + \cdots + x^{q^{b-1}}) - (x^{q^a} + \cdots + x^{q^{b-1}})^q \\
= -(S_b - S_a) - (S_b - S_a)^q.
\]

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

51
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

\[
\begin{align*}
g_{n,q} & \equiv x\text{Tr}_{q^e/q}(x) + \text{Tr}_{q^e/q}(x)^2 + S_a^2 \cdot (1 + \text{Tr}_{q^e/q}(x)^{q-1}) \quad (\mod x^e - x),
\end{align*}
\]

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

\[
g_n = g_{q+q^0+(q-1)q^e} + S_a \cdot g_{(q-1)q^0+q^a+(q-1)q^e}
\]

\[
= g_{q+q^e+1} + (S_a - S_e)g_{q+(q-1)q^e} + S_a \cdot (g_{q+(q-1)q^e} + S_a \cdot g_{(q-1)q^0+(q-1)q^e})
\]

\[
\equiv S_e(S_e + S_1) + S_a^2(1 + S_e^{q-1}) \quad (\mod x^e - x) \quad (\text{Lemma 4.2.1})
\]

\[
= x\text{Tr}_{q^e/q}(x) + \text{Tr}_{q^e/q}(x)^2 + S_a^2 \cdot (1 + \text{Tr}_{q^e/q}(x)^{q-1}).
\]

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 \( \text{Tr}_{q^e/q}(g_n(x)) = \text{Tr}_{q^e/q}(g_n(y)), \) we derive that \( \text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(y) = c. \) 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 \( \gcd(1 + x + \cdots + x^{a-1}, x^e + 1) = 1, \) we have \( x = y. \) If \( c \neq 0, \) the equation \( g_n(x) = g_n(y) \) becomes \( c(x + y) = 0, \) which also gives \( x = y. \)

\[
\square
\]

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

\[
g_{(q-1)q^0+2q^{e-1}+(q-1)q^e} = g_{q+q^e-1+(q-1)q^e} + S_e-1g_{(q-1)q^0+q^e-1+(q-1)q^e}
\]

\[
= g_{q+q^e+1} + (S_e+1 - S_e)g_{q+(q-1)q^e} + S_e-1g_{q+(q-1)q^e} + S_e-1g_{(q-1)q^0+(q-1)q^e}
\]

\[
= S_e(S_e - x) + S_e^2 - 1g_{(q-1)q^0+(q-1)q^e}
\]

Note that

\[
S_e g_{(q-1)q^0+(q-1)q^e} = g_{(q-1)q^0+q^e+1} - g_{q+(q-1)q^e}
\]

\[
= S_e + x^{q^e} - (S_e - x)
\]

\[
x^{q^e} - x = S_e^q - S_e,
\]

52
i.e.,
\[ g(q-1)q^0 + (q-1)q^e = S_e^{q-1} - 1. \] (4.2.12)

So
\[
g(q-1)q^0 + 2q^e - 1 + (q-1)q^e = S_2e - xS_e + S_e^{q-1} - 1
\]
\[
= xTr_{q^e/q}(x) + Tr_{q^e/q}(x)^2 + x^{2q^e-1} + Tr_{q^e/q}(x)^{q-1}x^{2q^e-1}.
\]

Thus modulo \( x^{q^e} - x \) we have
\[
g_{n,q}(x) \equiv \begin{cases} 
  x^{2q^e-1} & \text{if } Tr_{q^e/q}(x) = 0, \\
  xTr_{q^e/q}(x) + Tr_{q^e/q}(x)^2 & \text{if } Tr_{q^e/q}(x) \neq 0.
\end{cases}
\]

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

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

**Case 1.** Let \( x, y \in \{ x \in \mathbb{F}_{q^e}; Tr_{q^e/q}(x) = 0 \} \).
\[ g(x) = g(y) \Rightarrow x^{2q^e-1} = y^{2q^e-1}. \] Raising both sides to the \( (q/2) \)th power gives \( x = y \).

**Case 2.** Let \( x, y \in \{ x \in \mathbb{F}_{q^e}; Tr_{q^e/q}(x) \neq 0 \} \) s.t. \( x \neq y \) and \( g(x) = g(y) \). Then
\[
xTr_{q^e/q}(x) + Tr_{q^e/q}(x)^2 = yTr_{q^e/q}(y) + Tr_{q^e/q}(y)^2. \] (4.2.13)

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

By (4.2.14), \( (x - y)Tr_{q^e/q}(x) = 0 \). Since \( x \neq y \), \( Tr_{q^e/q}(x) = 0 \), 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
Lemma 4.2.5

Let \( (4.2.14) \),

\[
g_{(q-1)q^0+2q^1+(q-1)q^e} = g_{2q^1+(q-1)q^e} + S_1 g_{(q-1)q^0+q^1+(q-1)q^e}
\]

\[
= g_{2q^1+(q-1)q^e} + S_1 \{ g_{q^1+(q-1)q^e} + S_1 g_{(q-1)q^0+q^1+(q-1)q^e} \}
\]

\[
= g_{2q^1+(q-1)q^e} + S_1 (S_e + x) + S_1^2 (S_e^{q-1} - 1) \quad (4.2.12)
\]

\[
= g_{q^0+q^1+(q-1)q^e} + S_1 g_{q^1+(q-1)q^e} + x S_e + x^2 S_e^{q-1}
\]

\[
= g_{2q^0+(q-1)q^e} + S_1 g_{q^0+(q-1)q^e} + S_1 (S_e + x) + x S_e + x^2 S_e^{q-1}
\]

\[
= g_{2q^0+(q-1)q^e} + x^2 + x S_e + x^2 S_e^{q-1}
\]

\[
= \text{Tr}_{q^e/q}(x)^2 + x^2 + x \text{Tr}_{q^e/q}(x) + x^2 \text{Tr}_{q^e/q}(x)^{q-1}.
\]

Thus modulo \( x^{q^e} - x \) we have

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

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

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

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

\[
g(x) = g(y) \Rightarrow x^2 = y^2 \Rightarrow x = y.
\]

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

\[
x \text{Tr}_{q^e/q}(x) + \text{Tr}_{q^e/q}(x)^2 = y \text{Tr}_{q^e/q}(y) + \text{Tr}_{q^e/q}(y)^2. \quad (4.2.14)
\]

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

\[
g_n = g_{q^{a_2} + \ldots + q^{a_q}} + S_{a_1} \cdot g(q-1) + q^{a_2} + \ldots + q^{a_q}
\]
\[
= g_{q^{a_2} + \ldots + q^{a_q}} + S_{a_1} \cdot (g_{q^{a_3} + \ldots + q^{a_q}} + S_{a_2} \cdot g(q-1) + q^{a_3} + \ldots + q^{a_q})
\]
\[
= g_{q^{a_2} + \ldots + q^{a_q}} - S_{a_1} + S_{a_1} \cdot S_{a_2} \cdot g(q-1) + q^{a_3} + \ldots + q^{a_q}
\]
\[
= \ldots \ldots
\]
\[
= g_{q^{a_2} + \ldots + q^{a_q}} - S_{a_1} + S_{a_1} \cdots S_{a_q} \cdot g_q - 1
\]
\[
= -S_1 - S_{a_2} - \ldots - S_{a_q} - S_{a_1} - S_{a_1} \cdots S_{a_q}.
\]

\[\blacksquare\]

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

\[
g_{n,q} = -x - S_a + \text{Tr}_{q^e/q}(x) - S_a \text{Tr}_{q^e/q}(x)^{q-1}. \tag{4.2.15}
\]

Assume that

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

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

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

Then \( g_{n,q} \) is a PP of \( F_{q^e} \).

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

\[
(-2a - 1 + e)(\text{Tr}_{q^e/q}(x) - \text{Tr}_{q^e/q}(y)) = 0.
\]

Since \(-2a - 1 + e \not\equiv 0 \pmod{p}\), we have \( \text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(y) = c \).
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
\[
gcd(2 + x + \cdots + x^{a-1}, 1 + x + \cdots + x^{e-1}) = \frac{1}{x - 1} \gcd(x^a + x - 2, x^e - 1) = 1,
\]
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
\[
gcd(3 + 2x + \cdots + 2x^{a-1}, 1 + x + \cdots + x^{e-1}) = \frac{1}{x - 1} \gcd(2x^a + x - 3, x^e - 1) = 1,
\]
we also have $x - y = 0$.

\[\square\]

**Example 4.2.7** Let $q = 2^s$, $s > 1$, $e > 1$, $n = (q - 1)q^0 + q^2 + (q - 1)q^e$. Then
\[
g_{(q-1)q^0+q^2+(q-1)q^e} = g_{q+(q-1)q^e} + S_2g_{(q-1)q^0+(q-1)q^e}
\]
\[
= x + \text{Tr}(x) + (x + x^q)g_{(q-1)q^0+(q-1)q^e}
\]
\[
= x + \text{Tr}(x) + (x + x^q)(\text{Tr}_{q^e/q}(x)^q - 1)(4.2.12)
\]
\[
= x^q + \text{Tr}_{q^e/q}(x) + x^q\text{Tr}_{q^e/q}(x)^q - 1 + x\text{Tr}_{q^e/q}(x)^q.
\]

Thus modulo $x^{q^e} - x$ we have
\[
g_{n,q}(x) \equiv \begin{cases} x^q & \text{if } \text{Tr}_{q^e/q}(x) = 0, \\ x + \text{Tr}_{q^e/q}(x) & \text{if } \text{Tr}_{q^e/q}(x) \neq 0. \end{cases}
\]

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

56
Clearly \( x^q \) and \( x + \text{Tr}_{q^e/q}(x) \) map two sets \( \{ x \in \mathbb{F}_{q^e}; \text{Tr}_{q^e/q}(x) = 0 \} \) and \( \{ x \in \mathbb{F}_{q^e}; \text{Tr}_{q^e/q}(x) \neq 0 \} \) to themselves respectively.

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

\[
g(x) = g(y) \Rightarrow x^q = y^q \Rightarrow x = y.
\]

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

\[
x + \text{Tr}_{q^e/q}(x) = y + \text{Tr}_{q^e/q}(y). \tag{4.2.16}
\]

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

\[
g_{n,q} = x + \text{Tr}_{q^e/q}(x) + x^\frac{1}{2}q^e \text{Tr}_{q^e/q}(x)^{\frac{1}{2}q}.
\]

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

**Proof.** By Lemma 4.2.5,

\[
g_{n,q} = S_1 + S_{e-1}^2 S_e^2
\]

\[
= x + (S_e^\frac{1}{2}q + x^\frac{1}{2}q^e)S_e^\frac{1}{2}q
\]

\[
= x + \text{Tr}_{q^e/q}(x) + x^\frac{1}{2}q^e \text{Tr}_{q^e/q}(x)^{\frac{1}{2}q}.
\]

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 \( \text{Tr}_{q^e/q}(g_{n,q}(x)) = \text{Tr}_{q^e/q}(g_{n,q}(y)) \), we derive that \( \text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(y) = a \). 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

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

57
i.e.,

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

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

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

\[g_{3q^0+2q^{e-1}+2q^e} = g_{q+2q^{e-1}+q^e} + S_q g_{3q^0+2q^{e-1}+q^e}
= x + \text{Tr}_{q^e/q}(x) + S_q g_{3q^0+2q^{e-1}+q^e}
= x + \text{Tr}_{q^e/q}(x) + S_q (1 + S_q g_{3q^0+2q^{e-1}})
= x + \text{Tr}_{q^e/q}(x) + S_q + S_q^2 g_{3q^0+2q^{e-1}}
= x + S_q S_{q-1}
= x + \text{Tr}_{q^e/q}(x)^2(\text{Tr}_{q^e/q}(x) + x_{q^{e-1}}^2)
= x + \text{Tr}_{q^e/q}(x) + x_{q^{e-1}}^2 \text{Tr}_{q^e/q}(x).
\]

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

\[x + \text{Tr}_{q^e/q}(x) + x_{2q^{e-1}} \text{Tr}_{q^e/q}(x)^2 = (x + a) + \text{Tr}_{q^e/q}(x + a) + (x + a)_{2q^{e-1}} \text{Tr}_{q^e/q}(x + a)^2.
\]

It leads to

\[a + \text{Tr}_{q^e/q}(a) + \text{Tr}_{q^e/q}(x)^2 a_{2q^{e-1}} + \text{Tr}_{q^e/q}(a)^2 x_{2q^{e-1}} + \text{Tr}_{q^e/q}(a)^2 a_{2q^{e-1}} = 0. \quad (4.2.17)
\]

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

By (4.2.17),

\[a + \text{Tr}_{q^e/q}(x)^2 a_{2q^{e-1}} = 0. \quad (4.2.18)
\]

If \(\text{Tr}_{q^e/q}(x) = 0\), then (4.2.18) gives \(a = 0\).

If \(\text{Tr}_{q^e/q}(x) = 1\), 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 \(\text{Tr}_{q^e/q}(a) = 0\). Therefore \(a = 0\).

\[58\]
If \( \text{Tr}_{q^{e}/q}(x) \neq 0,1 \), squaring both sides of (4.2.18) gives \( a(a + \text{Tr}_{q^{e}/q}(x)) = 0 \). If \( \text{Tr}_{q^{e}/q}(x) = a \), taking traces on both sides gives \( e\text{Tr}_{q^{e}/q}(x) = \text{Tr}_{q^{e}/q}(a) = 0 \). Since \( e \) is odd \( \text{Tr}_{q^{e}/q}(x) = 0 \), 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

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

Assume that \( e > 2 \) is even and \( \text{gcd}(1 + x^2 + x^{e-3}, x^e + 1) = 1 \). 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,

\[
g_{n,q} = x + \text{Tr}_{q^{e}/q}(x) + (x^{q^{e-2}} + x^{q^{e-1}})^2 \text{Tr}_{q^{e}/q}(x)^2 \quad (\text{mod } x^{q^e} - x).
\]

Assume that \( e \) is even and \( \text{gcd}(1 + x^2 + x^{e-3}, x^e + 1) = 1 \).

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 \( \text{Tr}_{q^{e}/q}(g_{n,q}(x)) = \text{Tr}_{q^{e}/q}(g_{n,q}(y)) \) we derive that \( \text{Tr}_{q^{e}/q}(x) = \text{Tr}_{q^{e}/q}(y) \). Let \( \text{Tr}_{q^{e}/q}(x) = \text{Tr}_{q^{e}/q}(y) = a \in \mathbb{F}_q \). If \( a = 0 \), then \( x = y \).

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

\[
z = a^2(z^{2q^{e-2}} + z^{2q^{e-1}}),
\]

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

\[\blacksquare\]

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

\[
g_{n,q} = -\sum_{1 \leq i_1 < \cdots < i_{t+2} \leq q+t} S_{a_{i_1}} \cdots S_{a_{i_{t+2}}}. \quad (4.2.20)
\]
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 $0 \leq t \leq q - 4$. We have

$$g_n = g_{2+q^2+\ldots+q^t} + S_{a_1} \cdot g_{1+q^2+\ldots+q^t}$$

$$= g_{2+q^2+\ldots+q^t} - S_{a_1} \sum_{2 \leq i_2 < \ldots < i_{t+2} \leq q+t} S_{a_{i_2}} \cdots S_{a_{i_{t+2}}} \quad \text{(induction hypothesis)}$$

$$= g_{3+q^3+\ldots+q^t} + S_{a_2} \cdot g_{2+q^3+\ldots+q^t} - S_{a_1} \sum_{2 \leq i_2 < \ldots < i_{t+2} \leq q+t} S_{a_{i_2}} \cdots S_{a_{i_{t+2}}}$$

$$= g_{3+q^3+\ldots+q^t} - S_{a_2} \sum_{3 \leq i_3 < \ldots < i_{t+2} \leq q+t} S_{a_{i_3}} \cdots S_{a_{i_{t+2}}} \quad \text{(induction hypothesis)}$$

$$= \ldots$$

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

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

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

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 $n = (p^2 - p - 1)q^0 + (p - 1)q^e + pq^a + q^b$, $a, b \geq 0$. Then

$$g_{n,q} = -S_p^0 - S_b S_e^{p-1}. \quad (4.2.21)$$
Assume that \(a + b \not\equiv 0 \pmod{p}\) and

\[
gcd(x(x^a - 1)^2 - \varepsilon(x^b - 1)^2, (x - 1)(x^e - 1)) = (x - 1)^2,
\]

for \(\varepsilon = 0, 1\). 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

\[
(a + b)(S_e(x) - S_e(y))^p = 0.
\]

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

\[
S_a(z)^p = -c^{q-1}S_b(z),
\]

where \(z = x - y\). Thus

\[
S_a(z) = (-c^{q-1}S_b(z))^{pq^{e-1}} = -c^{q-1}S_b(z^{pq^{e-1}}). \tag{4.2.22}
\]

We iterate both sides of (4.2.22) to get

\[
(S_a \circ S_a)(z) = -c^{q-1}S_b(-c^{q-1}S_b(z^{pq^{e-1}})^{pq^{e-1}}) = c^{q-1}(S_b \circ S_b)(z^{q^{e-1}}),
\]

i.e.,

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

Let \(\varepsilon = c^{q-1}\), 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 \(x(1 + x + \cdots + x^{a-1})^2\) and \((1 + x + \cdots + x^{b-1})^2\), respectively.
[30, §3.4]. Since
\[
\gcd(x(1 + x + \cdots + x^{a-1})^2 - \epsilon(1 + x + \cdots + x^{b-1})^2, 1 + x + \cdots + x^{e-1})
\]
\[
= \frac{1}{(x - 1)^2} \gcd(x(x^a - 1)^2 - \epsilon(x^b - 1)^2, (x - 1)(x^e - 1))
\]
\[
= 1,
\]
it follows from (4.2.23) that \( z = 0 \), i.e., \( x = y \).

\begin{flushright}
\textbf{□}
\end{flushright}

**Example 4.2.13** Let \( q = 4, e > 3, n = q^0 + 2q^1 + q^2 + q^e \). Then by Theorem 4.1.1,
\[
g_{n,q} \equiv x^2 + x \text{Tr}_{q^e/q}(x) + x^q \text{Tr}_{q^e/q}(x) \quad (\text{mod } x^e - x).
\]

We claim that when \( \gcd(1 + x + x^2, x^e + 1) = 1 \), \( g_{n,q} \) 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 \( \text{Tr}_{q^e/q}(g_{n,q}(x)) = \text{Tr}_{q^e/q}(g_{n,q}(y)) \) we derive that \( \text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(y) \). Let \( \text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(y) = a \in \mathbb{F}_q \).

If \( a = 0 \), then \( x = y \).

If \( a \neq 0 \), then \( g_{n,q}(x) = g_{n,q}(y) \) becomes
\[
z^2 = a(z + z^q), \quad (4.2.24)
\]

where \( z = x + y \). Substitute (4.2.24) into itself to find \( (z^2)^q = (z^2)^{q^2} \). Since \( \gcd(1 + x + x^2, x^e + 1) = 1 \), 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,
\[
g_{n,q} \equiv x^2 + \text{Tr}_{q^e/q}(x)^2 + x^{q^{e-2}} \text{Tr}_{q^e/q}(x) + x^{q^{e-1}} \text{Tr}_{q^e/q}(x) \quad (\text{mod } x^{q^e} - x).
\]

We claim that when \( \gcd(1 + x^2 + x^5, x^e + 1) = 1 \) 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 \( \text{Tr}_{q^e/q}(g_{n,q}(x)) = \text{Tr}_{q^e/q}(g_{n,q}(y)) \) we derive that 
\[ \text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(y). \]
Let \( \text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(y) = a \in \mathbb{F}_q \).
If \( a = 0 \) then \( x = y \). If \( a \neq 0 \), then \( g_{n,q}(x) = g_{n,q}(y) \) becomes
\[ z^2 = a(z^{q^e-2} + z^{q^e-1}), \quad (4.2.25) \]
where \( z = x + y \). Substitute (4.2.25) into itself to find \( (z^2)^{q^e} = (z^2)^2 + (z^2)^q \). Since \( \gcd(1 + x^2 + x^5, x^e + 1) = 1 \), 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,
\[ g_{n,q} \equiv x^{2q^{e-1}} + x^{q^{e-2}}\text{Tr}_{q^e/q}(x) + x^{q^{e-1}}\text{Tr}_{q^e/q}(x) \pmod{x^{q^e} - x}. \]
We claim that when \( \gcd(1 + x^2 + x^3, x^e + 1) = 1 \), \( g_{n,q} \) 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 \( \text{Tr}_{q^e/q}(g_{n,q}(x)) = \text{Tr}_{q^e/q}(g_{n,q}(y)) \) we derive that 
\[ \text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(y). \]
Let \( \text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(y) = a \in \mathbb{F}_q \).
If \( a = 0 \) then \( x = y \). If \( a \neq 0 \), then \( g_{n,q}(x) = g_{n,q}(y) \) becomes
\[ z = a^2(z^{2q^{e-2}} + z^{2q^{e-1}}), \quad (4.2.26) \]
where \( z = x + y \). Substitute (4.2.26) into itself to find \( z^{q^3} = z + z^q \). Since \( \gcd(1 + x^2 + x^3, x^e + 1) = 1 \), 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,
\[ g_{n,q} \equiv x^2 + x^{q^{e-2}}\text{Tr}_{q^e/q}(x) + x^{q^{e-1}}\text{Tr}_{q^e/q}(x) \pmod{x^{q^e} - x}. \]
We claim that when \( \gcd(1 + x^2 + x^5, x^e + 1) = 1 \), \( g_{n,q} \) 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 \( \text{Tr}_{q^e/q}(g_{n,q}(x)) = \text{Tr}_{q^e/q}(g_{n,q}(y)) \) we derive that 
\[ \text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(y). \]
Let \( \text{Tr}_{q^e/q}(x) = \text{Tr}_{q^e/q}(y) = a \in \mathbb{F}_q \).
If $a = 0$ then $x = y$. If $a \neq 0$, then $g_{n,q}(x) = g_{n,q}(y)$ becomes

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

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

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

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

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

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

**Remark 4.2.18** If $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is quadratic, then $\sum_{x \in \mathbb{F}_p^n} c_{p}^{f(x)} = 0$ 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 $f = \sum_{i=0}^{e-1} a_i x^{p^i} \in \mathbb{F}_{p^e}[x]$ be a $p$-linearized polynomial considered as a $\mathbb{F}_{p^e}$-linear map from $\mathbb{F}_{p^e}$ to $\mathbb{F}_{p^e}$. The adjoint of $f$ is the $\mathbb{F}_{p^e}$-linear map $f^*$ such that

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

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

$$(f^{p^k})^*(x) \equiv f^*(x^{p^{e-k}}) \pmod{x^{p^k} - x}.$$
(Here \( f^p \) means product, not composition.) In fact, since
\[
\sum_i a_i^p x^{p^i} = \sum_i a_i x^{p^i} = \sum_i \frac{a_i x^{p^i}}{x^{p^i}}.
\]
we have
\[
(f^p)^* = \sum_i (a_i^{p^i} x^{p^i})^* = \sum_i a_i^{p^i} x^{p^i} = \sum_i a_i^{p^i - k} x^{p^i - k} \equiv f^*(x^{p^i - k}) \pmod{x^{p^i} - x}.
\]

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 \( A, B \in \mathbb{F}_{p^k}[x] \) 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 \( x \in \mathbb{F}_{p^k} \) 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 \( \mathbb{F}_{p^k} \) are contained in \( \mathbb{F}_{p^k} \).

Then \( A + B \) is a PP of \( \mathbb{F}_{p^k} \).

**Proof.** By [30, Theorem 7.7], it suffices to show that for all \( 0 \neq a \in \mathbb{F}_{p^k} \),
\[
\sum_{x \in \mathbb{F}_{p^k}} \zeta_p \text{Tr}(a \cdot (A + B)(x)) = 0,
\]
where \( \zeta_p = e^{2\pi i/p} \) and \( \text{Tr} = \text{Tr}_{p^k/p} \).

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

Since \( \text{Tr}_{p^k/p}(a) \neq 0 \) and \( A \) permutes \( \mathbb{F}_{p^k} \), there exists a \( y \in \mathbb{F}_{p^k} \) such that
For all $x \in \mathbb{F}_{p^k}$ we have

$$\text{Tr}_{p^k/p}[A(y)\text{Tr}_{p^{kn}/p^k}(a)] \neq 0.$$ 

which is a nonzero constant.

**Case 2.** Assume $\text{Tr}_{p^{kn}/p^k}(a) = 0$. Then $a = b^{p^{(n-1)k}} - b$ for some $b \in \mathbb{F}_{p^k} \setminus \mathbb{F}_p$.

For $x \in \mathbb{F}_{p^k}$ we have

$$\text{Tr}[a \cdot (A + B)(x)] = \text{Tr}[(b^{p^{(n-1)k}} - b) \cdot (A + B)(x)]$$

$$= \text{Tr}[b((A + B)^{p^k}(x) - (A + B)(x))]$$

$$= \text{Tr}[b((A^{p^k} - A)(x) + (B^{p^k} - B)(x))]$$

$$= \text{Tr}[x((A^{p^k} - A)^*(b) + (B^{p^k} - B)^*(b))] .$$

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

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

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

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

\[\blacksquare\]

**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

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

66
and \( g_{n,q} \) is a PP of \( \mathbb{F}_{q^e} \).

**Proof.** We write \( g_n \) for \( g_{n,q} \). We have

\[
g_n = g_{(q-2)q^0+2q^1+q^{2k}} + S_{4k} \cdot g_{(q-3)q^0+2q^1+q^{2k}}
= g_{(q-1)q^0+2q^1} + S_{2k} \cdot g_{(q-2)q^0+2q^1} + S_{4k}S_{2k}
= g_{2q^1} + S_1 \cdot g_{(q-1)q^0+q^1} + S_{4k}S_{2k}
= x^2 + S_{4k}S_{2k}.
\]

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

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

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 \((n, e; 4), e \leq 6, w_4(n) > 4\)

<table>
<thead>
<tr>
<th>(e)</th>
<th>(n)</th>
<th>base 4 digits of (n)</th>
<th>reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>59</td>
<td>3,2,3</td>
<td>Thm 3.2.4 (ii)</td>
</tr>
<tr>
<td>2</td>
<td>127</td>
<td>3,3,3,1</td>
<td>[22] Prop 3.1</td>
</tr>
<tr>
<td>3</td>
<td>29</td>
<td>1,3,1</td>
<td>Exmp 4.1.3</td>
</tr>
<tr>
<td>3</td>
<td>101</td>
<td>1,1,2,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>3</td>
<td>149</td>
<td>1,1,1,2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>163</td>
<td>3,0,2,2</td>
<td>[14] Thm 6.10</td>
</tr>
<tr>
<td>3</td>
<td>281</td>
<td>1,2,1,0,1</td>
<td>Cor 4.2.20</td>
</tr>
<tr>
<td>3</td>
<td>307</td>
<td>3,0,3,0,1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>329</td>
<td>1,2,0,1,1</td>
<td>Exmp 4.1.4</td>
</tr>
<tr>
<td>3</td>
<td>341</td>
<td>1,1,1,1,1</td>
<td>Exmp 4.1.4</td>
</tr>
<tr>
<td>3</td>
<td>2047</td>
<td>3,3,3,3,3,1</td>
<td>[22] Prop 3.1</td>
</tr>
<tr>
<td>4</td>
<td>281</td>
<td>1,2,1,0,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>4</td>
<td>307</td>
<td>3,0,3,0,1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>401</td>
<td>1,0,1,2,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>4</td>
<td>547</td>
<td>3,0,2,0,2</td>
<td>[14] Thm 6.10</td>
</tr>
<tr>
<td>4</td>
<td>779</td>
<td>3,2,0,0,3</td>
<td>Thm 4.2.2</td>
</tr>
<tr>
<td>4</td>
<td>787</td>
<td>3,0,1,0,3</td>
<td>Thm 4.2.6</td>
</tr>
<tr>
<td>4</td>
<td>817</td>
<td>1,0,3,0,3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>899</td>
<td>3,0,0,2,3</td>
<td>Thm 4.2.2</td>
</tr>
<tr>
<td>4</td>
<td>1469</td>
<td>1,3,3,2,1,1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2201</td>
<td>1,2,1,2,0,2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2317</td>
<td>1,3,0,0,1,2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2321</td>
<td>1,0,1,0,1,2</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>4</td>
<td>2377</td>
<td>1,2,0,1,1,2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2441</td>
<td>1,2,0,2,1,2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4387</td>
<td>3,0,2,0,1,0,1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>32767</td>
<td>3,3,3,3,3,3,3,1</td>
<td>[22] Prop 3.1</td>
</tr>
<tr>
<td>5</td>
<td>29</td>
<td>1,3,1</td>
<td>Exmp 4.1.3</td>
</tr>
<tr>
<td>5</td>
<td>1049</td>
<td>1,2,1,0,0,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>5</td>
<td>1061</td>
<td>1,1,2,0,0,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>5</td>
<td>1169</td>
<td>1,0,1,2,0,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>5</td>
<td>1289</td>
<td>1,2,0,0,1,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>5</td>
<td>1409</td>
<td>1,0,0,2,1,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>5</td>
<td>1541</td>
<td>1,1,0,0,2,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>5</td>
<td>1601</td>
<td>1,0,0,1,2,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>5</td>
<td>2083</td>
<td>3,0,2,0,0,2</td>
<td>[14] Thm 6.10</td>
</tr>
<tr>
<td>5</td>
<td>2563</td>
<td>3,0,0,0,2,2</td>
<td>Thm 4.2.8</td>
</tr>
<tr>
<td>$e$</td>
<td>$n$</td>
<td>base 4 digits of $n$</td>
<td>reference</td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>---------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>5</td>
<td>4229</td>
<td>1,1,0,2,0,0,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>5</td>
<td>4289</td>
<td>1,0,0,3,0,0,1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>4387</td>
<td>3,0,2,0,1,0,1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5129</td>
<td>1,2,0,0,0,1,1</td>
<td>Exmp 4.1.4</td>
</tr>
<tr>
<td>5</td>
<td>5141</td>
<td>1,1,1,0,0,1,1</td>
<td>Exmp 4.1.4</td>
</tr>
<tr>
<td>5</td>
<td>5189</td>
<td>1,1,0,1,0,1,1</td>
<td>Exmp 4.1.4</td>
</tr>
<tr>
<td>5</td>
<td>5249</td>
<td>1,0,0,2,0,1,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>5</td>
<td>5381</td>
<td>1,1,0,0,1,1,1</td>
<td>Exmp 4.1.4</td>
</tr>
<tr>
<td>5</td>
<td>8713</td>
<td>1,2,0,0,2,0,2</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>9281</td>
<td>1,0,0,1,0,1,2</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>5</td>
<td>17429</td>
<td>1,1,1,0,0,1,0,1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>17441</td>
<td>1,0,2,0,0,1,0,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>5</td>
<td>17489</td>
<td>1,0,1,1,0,1,0,1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>17681</td>
<td>1,0,1,0,1,1,0,1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>524287</td>
<td>3,3,3,3,3,3,3,3,3,3,1</td>
<td>[22] Prop 3.1</td>
</tr>
<tr>
<td>6</td>
<td>4361</td>
<td>1,2,0,0,1,0,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>6</td>
<td>6161</td>
<td>1,0,1,0,0,2,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>6</td>
<td>6401</td>
<td>1,0,0,0,1,2,1</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>6</td>
<td>8227</td>
<td>3,0,2,0,0,0,2</td>
<td>[14] Thm 6.10</td>
</tr>
<tr>
<td>6</td>
<td>8707</td>
<td>3,0,0,0,2,0,2</td>
<td>Thm 4.2.10</td>
</tr>
<tr>
<td>6</td>
<td>12299</td>
<td>3,2,0,0,0,0,3</td>
<td>Thm 4.2.2</td>
</tr>
<tr>
<td>6</td>
<td>12307</td>
<td>3,0,1,0,0,0,3</td>
<td>Thm 4.2.6</td>
</tr>
<tr>
<td>6</td>
<td>14339</td>
<td>3,0,0,0,0,2,3</td>
<td>Thm 4.2.2</td>
</tr>
<tr>
<td>6</td>
<td>37121</td>
<td>1,0,0,0,1,0,1,2</td>
<td>Thm 4.2.12</td>
</tr>
<tr>
<td>6</td>
<td>65801</td>
<td>1,2,0,0,1,0,0,0,1</td>
<td>Cor 4.2.20</td>
</tr>
<tr>
<td>6</td>
<td>65921</td>
<td>1,0,0,2,1,0,0,0,1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>66307</td>
<td>3,0,0,0,3,0,0,0,1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>135209</td>
<td>1,2,2,0,0,0,1,0,2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>135217</td>
<td>1,0,3,0,0,0,1,0,2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>135457</td>
<td>1,0,2,0,1,0,1,0,2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>137249</td>
<td>1,0,2,0,0,2,1,0,2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>8388607</td>
<td>3,3,3,3,3,3,3,3,3,3,1</td>
<td>[22] Prop 3.1</td>
</tr>
</tbody>
</table>
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

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

(5.1.1)

Note that

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

We shall call the functions $f_i, i = \infty, 0, \ldots, k - 1$, the case functions of $F$ and the function $\theta$ 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

\[\text{This chapter consists of the paper [13] which has been published in the journal “Finite Fields and Their Applications”.}\]
$x^{m+1} + ax$, where $m \mid q - 1$, were considered in [4, 5, 6, 28, 33]. (In the notation of (5.1.1), one has $k = \frac{q-1}{m}, \theta(x) = x^m, f_\infty(x) = 0, f_i(x) = (a + \omega^i)x, 0 \leq i \leq k - 1.$) 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 $D_{3^n+5}(1, x) = (1 - y - y^2)y^{3^n+1} - 1 - y + y^2$, 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 $(x^p - x + \delta)^s + L(x)$, 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 $\theta$ 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 $\theta$ 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) $[(h_i \circ f_i)(x)]^{\frac{1}{2}(q-1)} = \theta(x)$ if $\theta(x) = \omega^i$; $[(h_j \circ f_j)(x)]^{\frac{1}{2}(q-1)} = \theta(x)$ if $\theta(x) = \omega^j$.

(ii) If $b \in f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j))$, then $(h_i(b))^{\frac{1}{2}(q-1)}, h_j(b))^{\frac{1}{2}(q-1)} \neq (\omega^i, \omega^j)$.

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), $h_i(b)^{\frac{1}{2}(q-1)} = [(h_i \circ f_i)(x)]^{\frac{1}{2}(q-1)} = \omega^i$. In the same way, $h_j(b)^{\frac{1}{2}(q-1)} = \omega^j$. So we have a contradiction. ■
We will construct several families of PPs of the form (5.1.1) by choosing the selection function \( \theta \) to be \( \theta(x) = (L(x) + \delta)^{\frac{1}{k}(q-1)} \), 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 \( \theta(x) = (L(x) + \delta)^{\frac{1}{k}(q-1)} \)

**Theorem 5.2.1** Let \( k \mid q-1 \) and let \( \omega \in \mathbb{F}_q^* \) be an element of order \( k \). Let \( F_r \subset \mathbb{F}_q \) and \( \sigma_0, \ldots, \sigma_{k-1} \in \text{Aut}(\mathbb{F}_q/F_r) \) such that \( \sigma_i(\omega^j), \ 0 \leq i \leq k-1, \) are all distinct. Let \( f_\infty(x), f_0(x), \ldots, f_{k-1}(x) \) be linearized polynomials over \( F_r \) with \( f(1) = 0, g(1) = 1 \) and \( g \) a PP of \( \mathbb{F}_q \).

Let \( \delta_\infty, \delta_0, \ldots, \delta_{k-1}, \delta \in \mathbb{F}_r \). Then

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

is a PP of \( \mathbb{F}_q \).

**Proof.** Let \( \theta(x) = (L(x) + \delta)^{\frac{1}{k}(q-1)} \), \( f_\infty(x) = g(x) + \delta_\infty \), \( f_i(x) = \sigma_i(x) + \delta_i \), \( 0 \leq i \leq k-1 \). 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 \( i, j \in \{\infty, 0, \ldots, k-1\}, i \neq j \). 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

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

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

\[
[(h_i \circ f_i)(x)]^{\frac{1}{k}(q-1)} = (L(x) + \delta)^{\frac{1}{k}(q-1)} = \theta(x), \quad i \in \{\infty, 0, \ldots, k-1\}.
\]
Let $b \in \mathbb{F}_q$. For $0 \leq i \leq k - 1$ we have

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

(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 $i, j \in \{0, \ldots, k - 1\}$, $i \neq j$, we have

$$\left(h_i(b)^{\frac{1}{k}(q-1)}, h_j(b)^{\frac{1}{k}(q-1)}\right) = (\sigma_i^{-1}(\theta(b)), \sigma_j^{-1}(\theta(b))) \neq (\omega^i, \omega^j)$$

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

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

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 $i, j \in \{\infty, 0, \ldots, k - 1\}$, $i \neq j$.

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 $\sigma_i$ 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 $\sigma_i(\omega^i)$, $0 \leq i \leq k - 1$, 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 $i \neq j$. 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 $0 \leq i < j \leq k - 1$, $f_i(\theta^{-1}(\omega^i)) \cap f_j(\theta^{-1}(\omega^j)) \neq \emptyset$ if and
only if the following system has a solution \((x, y) \in \mathbb{F}_q \times \mathbb{F}_q\):

\[
\begin{align*}
\left( L(x) + \delta \right)^{\frac{1}{k(q-1)}} &= \omega^i, \\
\left( L(y) + \delta \right)^{\frac{1}{k(q-1)}} &= \omega^j, \\
\sigma_i(x) + \delta_i &= \sigma_j(y) + \delta_j.
\end{align*}
\]

(5.2.3)

Apply \(\sigma_i\) to the first equation of (5.2.3) and \(\sigma_j\) to the second. We see that (5.2.3) is equivalent to

\[
\begin{align*}
\left( L(u) + \delta \right)^{\frac{1}{k(q-1)}} &= \sigma_i(\omega^i), \\
\left( L(v) + \delta \right)^{\frac{1}{k(q-1)}} &= \sigma_j(\omega^j), \\
u + \delta_i &= v + \delta_j,
\end{align*}
\]

(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 \((L(\mathbb{F}_q) + \delta) \cap (\sigma_i(\gamma^i) \cdot \langle \gamma^k \rangle) \neq \emptyset\), where \(\gamma\) 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 \((L(\mathbb{F}_q) + \delta) \cap (\sigma_i(\gamma^i) \cdot \langle \gamma^k \rangle) = \emptyset\).

The construction in Theorem 5.2.1 calls for a sequence \(\sigma_0, \ldots, \sigma_{k-1} \in \text{Aut}(\mathbb{F}_q/\mathbb{F}_r)\) 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 \(\sigma \in \text{Aut}(\mathbb{F}_q/\mathbb{F}_r)\) 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 \(\beta\) 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 \(\sigma_{ir^j}(\omega_{ir^j}) = \omega^{ir^j \cdot e_j} = \omega^{ir^j + e_j}\), 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 \( \mathbb{F}_r \subset \mathbb{F}_q \), \( \sigma_0, \ldots, \sigma_{k-1} \in \text{Aut}(\mathbb{F}_q/\mathbb{F}_r) \), \( L \) an \( r \)-linearized polynomial over \( \mathbb{F}_r \), and

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

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

**Proof.** (\( \Leftarrow \)) Let \( \theta(x) = L(x)^{\frac{1}{k}(q-1)} \), \( f_\infty(x) = 0 \) and \( f_i(x) = \sigma_i(x) \), \( 0 \leq i \leq k-1 \). Note that \( \theta^{-1}(0) = 0 \). One only has to verify \( f_i(\theta^{-1}(\omega^j)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset \) for \( 0 \leq i < j \leq k-1 \), 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 \( \sigma_i(\omega^j) = \sigma_j(\omega^j) \) for some \( 0 \leq i < j \leq k-1 \). Let \( \gamma \) be a primitive element of \( \mathbb{F}_q \) such that \( \omega = \gamma^{\frac{1}{k}(q-1)} \). Then

\[
\left( \frac{\sigma_i(\gamma^j)}{\sigma_j(\gamma^j)} \right)^{\frac{q-1}{k}} = \frac{\sigma_i(\omega^j)}{\sigma_j(\omega^j)} = 1.
\]

Hence we can write \( \frac{\sigma_i(\gamma^j)}{\sigma_j(\gamma^j)} = \sigma_i(\gamma^j)^k \) 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 \( \theta(x) = L(L^{-1}(\gamma^{i-lk}))^{\frac{1}{k}(q-1)} = \omega^j \) and \( \theta(y) = L(L^{-1}(\gamma^j))^{\frac{1}{k}(q-1)} = \omega^j \). We have

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

which is a contradiction.

\[\square\]

**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 \( \sigma_0, \ldots, \sigma_{k-1} \in \text{Aut}(\mathbb{F}_q/\mathbb{F}_r) \) such that \( \sigma_i(\omega^i) \), \( 0 \leq i \leq k-1 \), 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 \( \delta \in \mathbb{F}_q \setminus L(\mathbb{F}_q) \)

75
such that \( L(\delta_i) - \sigma_i(\delta) \), \( 0 \leq i \leq k - 1 \), are all equal. Then

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

is a PP of \( \mathbb{F}_q \).

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

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

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

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

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

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

\[
\left( h_i(b)^{\frac{1}{q-1}}, h_j(b)^{\frac{1}{q-1}} \right) = \left( \sigma_i^{-1}(c^{\frac{1}{q-1}}), \sigma_j^{-1}(c^{\frac{1}{q-1}}) \right) \neq (\omega^i, \omega^j)
\]

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

Given \( \sigma_0, \ldots, \sigma_{k-1} \in \text{Aut}(\mathbb{F}_q/\mathbb{F}_r) \) 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

\[
L(\delta_i) - \sigma_i(\delta) = L(\delta_0) - \sigma_0(\delta), \quad 1 \leq i \leq k - 1.
\]

(5.2.5)

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

\[
L(x_i) = \sigma_i\sigma_0^{-1}(x_k) - x_k, \quad 1 \leq i \leq k - 1,
\]

(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 \(\sigma \in \text{Aut}(\mathbb{F}_q/\mathbb{F}_r)\) be given by \(\sigma(x) = x^r\). Write \(\sigma, \sigma^{-1} = \sigma^{\epsilon_i}, 1 \leq i \leq k - 1\), 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

\[
f(\sigma)(x_i) = (\sigma^{\epsilon_i} - \sigma^0)(x_k), \quad 1 \leq i \leq k - 1.
\]

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 \(\text{deg} \, g \leq m - 1\), \(\gcd(f, x^m - 1) \nmid g\), and \(\gcd(f, x^m - 1) \mid (x^{\epsilon_i} - 1)g\) for all \(1 \leq i \leq k - 1\). (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 \(\gcd(f, x^m - 1) \equiv uf \mod x^m - 1\), \(u \in \mathbb{F}_r[x]\), and let

\[
h_i = u \cdot \frac{(x^{\epsilon_i} - 1)g}{f, x^m - 1}, \quad 1 \leq i \leq k - 1.
\]

Set

\[
x_i = h_i(\epsilon), \quad 1 \leq i \leq k - 1.
\]

Remark.

(i) In Theorem 5.2.5, let \(q\) be odd, \(k = 2\), \(\sigma\) a generator of \(\text{Aut}(\mathbb{F}_q/\mathbb{F}_r)\), \(L(x) = \sigma(x) - x, \delta \in \mathbb{F}_q\) with \(\text{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(\delta) \neq 0\), \(\sigma_0 = \sigma, \delta_0 = \frac{\delta}{2}, \sigma_1 = \text{id}, \delta_1 = -\frac{\delta}{2}\). Then

\[
F(x) = \frac{1}{2}[(\sigma(x) - x + \delta)\frac{1}{2}(q+1) + \sigma(x) + x],
\]

which is the PP in [39, Theorem 1].

(ii) In Theorem 5.2.1 and Remark 5.2.2, let \(q = 3^u, r = 3^l, k = 2\), \(\sigma\) a generator of \(\text{Aut}(\mathbb{F}_q/\mathbb{F}_r)\), \(L = \sigma - \text{id}, \delta \in \mathbb{F}_r, g = \text{id}, \delta_\infty = 0\), \(\sigma_0 = \sigma, \beta_0(x) = 0, \delta_0 = \delta, \sigma_1 = \sigma^2, \beta_1(x) = -\text{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(x), \delta_1 = -\delta\). (Note that \(\sigma_1 + \beta_1 = \sigma^2 - \text{Tr}_{\mathbb{F}_q/\mathbb{F}_r}\) is a
PP of $\mathbb{F}_q$ and $L \circ \beta_1 = 0$ on $\mathbb{F}_q$.) Then $F(x) = (\sigma(x) - x + \delta)^\frac{1}{2}(q+1) + x$ is a PP of $\mathbb{F}_q$.

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

Let $g = \sigma^2$, $\delta_0 = 0$, $\sigma_0 = \text{id}$, $\beta_0(x) = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(x)$, $\sigma_1 = \sigma$, $\beta_1(x) = \text{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(x)$, $\delta_1 = -\delta$. Then $F(x) = (\sigma(x) - x + \delta)^\frac{1}{2}(q+1) + \sigma^2(x)$ 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 $k | q - 1$ and let $\omega \in \mathbb{F}_q^*$ be an element of order $k$. Let

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

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 $\gcd(a_i, \frac{1}{k}(q - 1)) = 1$ for all $0 \leq i \leq k - 1$ and $ia_i$, $0 \leq i \leq k - 1$, are all distinct in $\mathbb{Z}_k$.

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

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

$$\left(\frac{x_1}{x_2}\right)^\frac{1}{k}(q-1) = \frac{x_1^\frac{1}{k}(q-1)}{x_2^\frac{1}{k}(q-1)} = \frac{\omega^j}{\omega^j} = 1.$$

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

Now we show that $f_i(\theta^{-1}(\omega^j)) \cap f_j(\theta^{-1}(\omega^j)) = \emptyset$ for $0 \leq i < j < k - 1$. Assume to the contrary that there exists $b \in f_i(\theta^{-1}(\omega^j)) \cap f_j(\theta^{-1}(\omega^j))$. 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

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

$(\Rightarrow)$ First assume that $\gcd(a_i, \frac{1}{k}(q-1)) = l > 1$ for some $0 \leq i \leq k-1$. 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 $i\alpha_i = ja_j$ in $\mathbb{Z}_k$ for some $0 \leq i < j \leq k-1$. Let $\gamma$ 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 $\gcd(a_i, \frac{1}{k}(q-1)) = 1$ for all $0 \leq i \leq k-1$, and $i\alpha_i, 0 \leq i \leq k-1$, 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 $\tau_d$ of $\mathbb{Z}_{k/d}^*$. 
2. For each $0 \leq i \leq k-1$, let 

$$\alpha_i = \left(\frac{i}{(i,k)}\right)^{-1} \tau_{(i,k)} \left(\frac{i}{(i,k)}\right) \in \mathbb{Z}_{k/(i,k)}^*.$$ 

(Note that in $\mathbb{Z}_k$, $i\alpha_i = (i,k)\tau_{(i,k)} \left(\frac{i}{(i,k)}\right)$, $0 \leq i \leq k-1$, which are all distinct.)

3. For each $0 \leq i \leq k-1$, 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 $\prod_{d \mid k} \phi(\frac{k}{d})! = \prod_{d \mid k} \phi(d)!$. Counting the number of choices in Step 3 requires some effort.

For positive integers $m \mid n$ define

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

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

79
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 \( e_i > 0, \ 0 \leq f_i \leq e_i \). Without loss of generality, assume \( f_1 = \cdots = f_t = 0, \ f_{t+1}, \ldots, f_s > 0 \). Then
\[
h(m, n) = \frac{n}{m} \left( 1 - \frac{1}{p_1} \right) \cdots \left( 1 - \frac{1}{p_t} \right).
\]

Proof. For \( 1 \leq i_1 < \cdots < i_t \leq t \), we have
\[
\left| \{ x \in \mathbb{Z}_n^m : 1 + mx \equiv 0 \pmod{p_{i_1} \cdots p_{i_t}} \} \right| = \frac{n}{m} \cdot \frac{1}{p_{i_1} \cdots p_{i_t}}.
\]
By the inclusion-exclusion formula,
\[
h(m, n) = \frac{n}{m} \sum_{l=0}^{t} (-1)^l \sum_{1 \leq i_1 < \cdots < i_l \leq t} \frac{1}{p_{i_1} \cdots p_{i_l}} = \frac{n}{m} \left( 1 - \frac{1}{p_1} \right) \cdots \left( 1 - \frac{1}{p_t} \right).
\]

It is quite clear that for any two positive integers \( m \) and \( n \) and \( \alpha \in \mathbb{Z}_n^* \),
\[
\left| \{ x \in \mathbb{Z}^m_{n^m} : \gcd(\alpha + mx, n) = 1 \} \right| = h((m, n), n).
\]
Using this notation, we see that in the above Step 3, for each \( 0 \leq i \leq k - 1 \), the number of choices for \( a_i \) is
\[
\left| \{ x \in \mathbb{Z}^m_{k^{(q-1)(i,k)}} : \gcd(\alpha_i + \frac{k}{(i,k)}x, \frac{q-1}{k}) = 1 \} \right|
\]
\[
= \left| \{ x \in \mathbb{Z}^m_{k^{(q-1)/(i,k), k^{-1}}(i,k)} : \gcd(\alpha_i + \frac{k}{(i,k)}x, \frac{q-1}{k}) = 1 \} \right| \cdot (i,k) \left( \frac{k}{(i,k)} \cdot \frac{q-1}{k} \right)
\]
\[
= (k, \frac{q-1}{k}, (i,k)) h\left( \left( \frac{k}{(i,k)}, \frac{q-1}{k} \right), \frac{q-1}{k} \right).
\]
Therefore the total number of choices in Step 3 is
\[
\prod_{0 \leq i \leq k-1} \left( k, \frac{q-1}{k} (i, k) \right) h \left( \left( \frac{k}{i}, \frac{q-1}{k} \right), \frac{q-1}{k} \right)
\]
\[
= \prod_{d | k} \left( k, \frac{q-1}{k} d \right) h \left( \left( \frac{k}{d}, \frac{q-1}{k} \right), \frac{q-1}{k} \right) \phi(d)
\]
\[
= \prod_{d | k} \left( k, \frac{q-1}{d} \right) h \left( \left( d, \frac{q-1}{k} \right), \frac{q-1}{k} \right) \phi(d).
\]

Thus
\[
|A_{q,k}| = \prod_{d | k} \left( k, \frac{q-1}{d} \right) h \left( \left( d, \frac{q-1}{k} \right), \frac{q-1}{k} \right) \phi(d)!.\]

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 \( \mathcal{F} = \{ f : \mathbb{Z}_k \to \mathbb{Z}_{q-1} : (f(0), \ldots, f(k-1)) \in A_{q,k} \} \). Then \( G := \{ F_f : f \in \mathcal{F} \} \) is a subgroup of the symmetric group \( \text{Sym}(\mathbb{F}_q) \). The composition in \( G \) is given by
\[
F_g \circ F_f = F_h,
\]
where
\[
h(i) = f(i) g(i \overline{f(i)}), \quad i \in \mathbb{Z}_k,
\]
and \( \overline{f(i)} \) is the image of \( f(i) \) in \( \mathbb{Z}_k \).

Now we determine the order of \( G \). Note that \( \theta^{-1}(\omega^j) = \{ x \in \mathbb{F}_q : x^{\frac{1}{k}(q-1)} = \omega^j \} = \{ \alpha^{j+kl} : 0 \leq l < \frac{1}{k}(q-1) \} \), where \( \alpha \) 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
\[
x^a = x^{a'} \quad \text{for all } x \in \theta^{-1}(\omega^j)
\]
\[
\Leftrightarrow (a - a')(j + kl) \equiv 0 \pmod{q - 1} \quad \text{for all } 0 \leq l < \frac{1}{k}(q-1)
\]
\[
\Leftrightarrow (a - a') j \equiv (a - a' k) \equiv 0 \pmod{q - 1}
\]
\[
\Leftrightarrow (a - a')(j, k) \equiv 0 \pmod{q - 1}
\]
\[
\Leftrightarrow a - a' \equiv 0 \pmod{\frac{q-1}{(j, k)}}.
\]
It is clear that the mapping
\[ F \rightarrow G, \quad f \mapsto F_f \]
is \( \prod_{j=0}^{k-1} (j, k) \) to 1. Thus
\[ |G| = \frac{|F|}{\prod_{j=0}^{k-1} (j, k)} = \frac{|A_{q,k}|}{\prod_{d|k} (\frac{k}{d})^{\phi(d)}} = \prod_{d|k} \left[ \left( d, \frac{q-1}{k} \right) \right]^{\phi(d)} \phi(d)! \]

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 \( k \)th 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 \( 0 \leq i \leq k-1 \), let \( r_i \) be a power of \( p \) such that \( k \mid r_i - 1 \) and \( b_i \in \mathbb{F}_q^* \) such that \( (-b_i)^{2^{r_i-1}} \neq \omega^{ia_i} \).

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

is a PP of \( \mathbb{F}_q \).

**Proof.** Let \( \theta(x) = x^{\frac{1}{k}(q-1)} \), \( f_i(x) = x^{a_i} (x^{a_i} + b_i)^{r_i-1}, \) \( 0 \leq i \leq k-1 \). 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 \( 0 \leq i < j \leq k-1 \). It remains to show that \( f_i \) is 1-1 on \( \theta^{-1}(\omega^i) \). Assume to the contrary that there exist \( x, y \in \theta^{-1}(\omega^i), x \neq y \), 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
\[(u - v)(v + 1)[u(u - v)^{r-1} + (v + 1)^{r-1}].\]

Note that \(v + 1 \neq 0\) since otherwise, \(\frac{y^a}{b^n} = v = -1\), which implies that \((-b_i)^{\frac{q-1}{k}} = (y^{\frac{a}{k}})^{\frac{a_i}{a}} = \omega^{ia_i}\), 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.,
\[-u = \left(\frac{v + 1}{u - v}\right)^{r-1}.\]

It follows that
\[-\left(\frac{x^{a_i}}{b_i}\right)^{\frac{q-1}{k}} = (-u)^{\frac{q-1}{k}} = \left(\frac{v + 1}{u - v}\right)^{(r-1)\frac{q-1}{k}} = 1.\]

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

\[\blacksquare\]

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 \(\gcd(t + l, \frac{1}{2}(q - 1)) = 1\). 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 $\gcd(t, \frac{1}{2}(q-1)) = 1$, $r_0 = 1$, $a_1 = 1$, $r_1 = 3$, $b_1 = -\epsilon$, where $\epsilon$ 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., $g_{m,q} \equiv g_{n,q} \pmod{x^{q^e} - x}$.
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


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


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.

```mathematica
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.

```mathematica
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] =
   ]
]```
Appendix A (Continued)

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]];
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.

\[
\begin{align*}
e &= \text{; (* input e *)} \\
q &= 3^e; \\
f0 &= 0; \\
f1 &= 0; \\
f2 &= 2; \\
M &= \{0, 1, 2\}; \\
n0 &= 2; \text{ (* n0 = last n *)} \\
\text{For} &\ [n = 3, n < 3^{3e} - 1, n++,
\text{(* Checking if n is the smallest in the cyclotomic class *)}
\text{m} &= \text{Min}\left[\text{Mod}\left[3^M*n, 3^{(3 \ e)} - 1\right]\right];
\text{If} &\ [n \neq \text{m}, \text{Continue[]}];
\text{For} &\ [k = n0 + 1, k \leq n, k++,
\text{f} &= x*f0 + f1; \\
\text{f} &= \text{PolynomialMod}\left[\text{f}, x^q - x, \text{Modulus} \rightarrow 3\right];
\text{f0} &= \text{f1}; \\
\text{f1} &= \text{f2}; \\
\text{f2} &= \text{f}; \\
\text{]},
\text{n0} &= n;
\text{(* Hermite’s criterion *)}
\text{IsPP} &= \text{True};
\text{h} &= 1;
\text{For} &\ [i = 1, i < q - 1, i++,
\text{h} &= \text{PolynomialMod}\left[\text{h}*\text{f}, x^q - x, \text{Modulus} \rightarrow 3\right];
\text{If} &\ [\text{Exponent}[\text{h}, x] > q - 2, \text{IsPP} = \text{False}; \text{Goto}[\text{step3}]];
\end{align*}
\]
Appendix A (Continued)

\[ h = \text{PolynomialMod}[h \cdot f, x^q - x, \text{Modulus} \to 3]; \]
\[ \text{If}[\text{Exponent}[h, x] \neq q - 1, \text{IsPP} = \text{False}]; \]
\[ \text{Label}[\text{step3}]; \]
\[ \text{If}[\text{IsPP}, \text{Print}[n, " ", \text{IntegerDigits}[n, 3]]; \text{Print}[f]];]; \]

**Mathematica Code 3**

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

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];
]
Appendix A (Continued)

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\[g, x^q^e - x, Modulus \to p\];
h = 1;
For [i = 1, i < q^e - 1, i++,
  h = PolynomialMod[h*f, x^q^e - x, Modulus \to p];
  If[Exponent[h, x] > q^e - 2, IsPP = False; Goto[step3];
];
  h = PolynomialMod[h*f, x^q^e - x, Modulus \to 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(y)^{2q^2+2} \equiv \\
8y^{-1+q^3} + 2y^{-3+q^4} + y^{-3+4q^2+q^3} + 2y^{1-4q^2+q^3} + 4y^{2+q-4q^2+q^3} + y^{-3+2q-4q^2+q^3} + 6y^{-1+2q-4q^2+q^3} + 5y^{1+2q-4q^2+q^3} + 2y^{-4+3q-4q^2+q^3} + 4y^{-2+3q-4q^2+q^3} + 2y^{3q-4q^2+q^3} + 2y^{-3+q-3q^2+q^3} + 6y^{1+q-3q^2+q^3} + 4y^{2q-3q^2+q^3} + y^{-3-2q^2+q^3} + 2y^{-1-2q^2+q^3} + 2y^{3-2q^2+q^3} + 2y^{-4+q-2q^2+q^3} + 4y^{-2+q-2q^2+q^3} + 6y^{q-2q^2+q^3} + 6y^{-2+q^2+q^3} + 2y^{-3+2q-2q^2+q^3} + 8y^{-1+2q-2q^2+q^3} + 6y^{1+2q-2q^2+q^3} + 2y^{-4+3q-2q^2+q^3} + 4y^{-2+3q-2q^2+q^3} + 2y^{3q-2q^2+q^3} + 4y^{-q^2+q^3} + 6y^{2-2q^2+q^3} + 4y^{-3+q^2+q^3} + 16y^{-1+q^2+q^3} + 12y^{1+q^2+q^3} + 6y^{-4+2q^2+q^3} + 12y^{-2+2q^2+q^3} + 6y^{2q^2+q^3} + y^{2+2q-4q^2} + 2y^{-1+3q-4q^2} + 2y^{1+3q-4q^2} + y^{-4+4q-4q^2} + 2y^{-2+4q-4q^2} + y^{4q-4q^2} + 2y^{-1+2q-3q^2} + 2y^{1+2q-3q^2} + 2y^{-4+3q-3q^2} + 2y^{2+3q-3q^2} + 2y^{3+q-2q^2} + y^{-4+2q-2q^2} + 2y^{2-2q-2q^2} + 5y^{2q-2q^2} + 6y^{2q^2-2q^2} + 2y^{-3+3q-2q^2} + 8y^{-1+3q-2q^2} + 6y^{1+3q-2q^2} + 2y^{-4+4q-2q^2} + 4y^{2+4q-2q^2} + 2y^{4q-2q^2} + 4y^{-q^2} + 6y^{2+q^2} + 4y^{-3+2q^2} + 16y^{-1+2q-q^2} + 12y^{1+2q-q^2} + 6y^{-4+3q-q^2} + 12y^{-2+3q-q^2} + 6y^{3q^2} + 2y^{-3+q^2} + 4y^{-1+q^2} + 4y^{1+q^2} + 4y^{3+q^2} + 2y^{-4+q^2+q^3} + 6y^{-2+q^2+q^3} + 14y^q+q^2 + 12y^{2+q^2+q^3} + 6y^{-3+2q+q^2} + 18y^{-1+2q+q^2} + 12y^{1+2q+q^2} + 4y^{-4+3q+q^2} + 8y^{-2+3q+q^2} + 8y^{3q+q^2} + y^{-2+2q^2} + 6y^{2+q^2} + 6y^{-3+q+2q^2} + 18y^{-1+q+2q^2} + 12y^{1+q+2q^2} + 6y^{-4+2q+2q^2} + 12y^{-2+2q+2q^2} + 6y^{2+2q^2} + 2y^{-3+3q^2} + 6y^{-1+3q^2} + 4y^{1+3q^2} + 4y^{-4+q+3q^2} + 8y^{-2+q+3q^2} + 4y^{q+3q^2} + y^{-4+q^2} + 2y^{-2+4q^2} + 8y^{-3+q} + 20y^{-1+q} + 12y^{2q} + y^{4q} + 6y^{2q^2} + y^{3q^2} + 14y^{1+q} + 4y^{3+q} + 6y^{-4+2q} + 13y^{-2+2q} + 6y^{2+2q} + 2y^{-3+3q} + 6y^{-1+3q} + 4y^{1+3q} + y^{-4+4q} + 2y^{-2+4q} + 6y^2 + y^4.
When \( q > 3 \) is even, 
\[
g(y)^{2q^2 + q + 3} \equiv \\
y^{q^3 - 1} + y^{q^3 - 5} + y^{q^3 - q + 4} + y^{q^3 - q + 2} + y^{q^3 - 2q + 5} + y^{q^3 - 2q + 1} + y^{q^3 - 2q - 1} + y^{q^3 - 2q - 3} \\
+ y^{q^3 - 2q - 5} + y^{q^3 - q^2 + 4q - 2} + y^{q^3 - q^2 + 4q - 6} + y^{q^3 - q^2 + 3q - 1} + y^{q^3 - q^2 + 3q - 3} + y^{q^3 - q^2 + 3q - 5} \\
+ y^{q^3 - q^2 + 3q - 7} + y^{q^3 - q^2 + 2q} + y^{q^3 - q^2 + 2q - 2} + y^{q^3 - q^2 + 2q - 6} + y^{q^3 - q^2 + q + 1} + y^{q^3 - q^2 + q - 1} \\
+ y^{q^3 - q^2 - 4} + y^{q^3 - q^2 - q + 1} + y^{q^3 - q^2 - q - 1} + y^{q^3 - q^2 - q - 3} + y^{q^3 - q^2 - q - 5} + y^{q^3 - q^2 - 2q} \\
+ y^{q^3 - q^2 - 2q - 4} + y^{q^3 - 2q^2 + 6q - 1} + y^{q^3 - 2q^2 + 6q - 3} + y^{q^3 - 2q^2 + 6q - 5} + y^{q^3 - 2q^2 + 6q - 7} \\
+ y^{q^3 - 2q^2 + 5q - 2} + y^{q^3 - 2q^2 + 5q - 6} + y^{q^3 - 2q^2 + 4q - 1} + y^{q^3 - 2q^2 + 4q - 3} + y^{q^3 - 2q^2 + 3q - 2} \\
+ y^{q^3 - 2q^2 + 3q - 4} + y^{q^3 - 2q^2 + 3q - 6} + y^{q^3 - 2q^2 + 2q + 3} + y^{q^3 - 2q^2 + 2q + 1} + y^{q^3 - 2q^2 + 2q - 3} \\
+ y^{q^3 - 2q^2 + q + 2} + y^{q^3 - 2q^2 + q - 4} + y^{q^3 - 2q^2 - q - 4} + y^{q^3 - 2q^2 - q - 1} + y^{q^3 - 2q^2 - 2q - 1} + y^{q^3 - 3q^2 + 2q} \\
+ y^{q^3 - 3q^2 + 2q - 1} + y^{q^3 - 3q^2 + q + 1} + y^{q^3 - 3q^2 + q - 1} + y^{q^3 - 3q^2 + q - 3} + y^{q^3 - 3q^2 + q - 5} \\
+ y^{q^3 - 3q^2 + 2} + y^{q^3 - 3q^2 + q - 4} + y^{q^3 - 3q^2 - q + 3} + y^{q^3 - 3q^2 - q + 1} + y^{q^3 - 3q^2 - 2q + 2} \\
+ y^{q^3 - 3q^2 - 2q - 4} + y^{q^3 - 4q^2 + 2q + 1} + y^{q^3 - 4q^2 + 2q - 1} + y^{q^3 - 4q^2 + q} + y^{q^3 - 4q^2 + q - 2} \\
+ y^{q^3 - 4q^2 + q - 4} + y^{q^3 - 4q^2 + 5} + y^{q^3 - 4q^2 + 3} + y^{q^3 - 4q^2 - 1} + y^{q^3 - 4q^2 - q + 4} + y^{q^3 - 4q^2 - q + 2} \\
+ y^{q^3 - 4q^2 - 2q + 3} + y^{6q^2} + y^{6q^2 - 2} + y^{6q^2 - 4} + y^{6q^2 - 6} + y^{6q^2 - 2q - 2} + y^{6q^2 - 2q - 4} \\
+ y^{6q^2 - 2q - 6} + y^{5q^2 - 1} + y^{5q^2 - 5} + y^{5q^2 - q - 2} + y^{5q^2 - q - 4} + y^{5q^2 - q - 6} \\
+ y^{5q^2 - 2q - 1} + y^{5q^2 - 2q - 5} + y^{4q^2 + 2q} + y^{4q^2 + 2q - 2} + y^{4q^2 + 2q - 4} + y^{4q^2 + 2q - 6} + y^{4q^2 + q - 1} \\
+ y^{4q^2 + q - 5} + y^{4q^2 + 2} + y^{4q^2 - 4} + y^{4q^2 - q + 1} + y^{4q^2 - q - 1} + y^{4q^2 - q - 3} + y^{4q^2 - q - 5} \\
+ y^{4q^2 - 2q + 2} + y^{4q^2 - 2q - 4} + y^{3q^2 - 3} + y^{3q^2 - q - 2} + y^{3q^2 - q - 4} + y^{3q^2 - 2q - 3} + y^{2q^2 + 4q} \\
+ y^{2q^2 + 4q - 2} + y^{2q^2 + 4q - 4} + y^{2q^2 + 4q - 6} + y^{2q^2 + q - 3} + y^{2q^2 + 1} + y^{2q^2 + 2} + y^{2q - 6} \\
+ y^{2q^2 - q - 1} + y^{2q^2 - q - 3} + y^{2q^2 - 2q + 1} + y^{2q^2 - 2q + 2} + y^{2q^2 - 2q} + y^{2q^2 + 4q - 1} + y^{2q^2 + 4q - 5} \\
+ y^{2q^2 + 3q} + y^{2q^2 + 3q - 2} + y^{2q^2 + 3q - 4} + y^{2q^2 + 3q - 6} + y^{2q^2 + 2q - 3} + y^{2q^2 + q + 2} + y^{2q^2 + q - 6} + y^{2q^2 + 3} \\
+ y^{2q^2 - 1} + y^{2q^2 - 1} + y^{2q^2 - 5} + y^{2q^2 - q + 4} + y^{2q^2 - q + 2} + y^{2q^2 - q - 3} + y^{6q} + y^{6q - 2} + y^{6q - 4} \\
+ y^{6q - 6} + y^{5q - 1} + y^{5q - 5} + y^{4q + 2} + y^{4q - 4} + y^{3q + 1} + y^{2q + 1} + y^{2q} + y^{2q - 2} + y^{2q - 4} \\
+ y^{2q - 6} + y^{q + 3} + y^{q + 1} + y^{q^2 - 5} + y^{6} + y^{2}.
\]
Appendix C - Copyright and Permissions

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.

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

<table>
<thead>
<tr>
<th>Rights</th>
<th>FAQ</th>
<th>Responsibilities</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use for classroom teaching by author or author’s institution and presentation at a meeting or conference and distributing copies to attendees</td>
<td>Yes</td>
<td>Yes with full acknowledgement of final article</td>
<td>Yes with full acknowledgement of final article</td>
</tr>
<tr>
<td>Use for internal training by author’s company</td>
<td>Yes</td>
<td>Yes with full acknowledgement of final article</td>
<td>Yes with full acknowledgement of final article</td>
</tr>
<tr>
<td>Distribution to colleagues for their research use</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Use in a subsequent compilation of the author’s works</td>
<td>Yes</td>
<td>Yes with full acknowledgement of final article</td>
<td>Yes with full acknowledgement of final article</td>
</tr>
<tr>
<td>Inclusion in a thesis or dissertation</td>
<td>Yes</td>
<td>Yes with full acknowledgement of final article</td>
<td>Yes with full acknowledgement of final article</td>
</tr>
<tr>
<td>Reuse of portions or extracts from the article in other works</td>
<td>Yes</td>
<td>Yes with full acknowledgement of final article</td>
<td>Yes with full acknowledgement of final article</td>
</tr>
<tr>
<td>Preparation of derivative works (other than for commercial purposes)</td>
<td>Yes</td>
<td>Yes with full acknowledgement of final article</td>
<td>Yes with full acknowledgement of final article</td>
</tr>
<tr>
<td>Preprint servers</td>
<td>Yes</td>
<td>Yes with the specific written permission of Elsevier</td>
<td>No</td>
</tr>
<tr>
<td>Voluntary posting on open web sites operated by author or author’s institution for scholarly</td>
<td>Yes (author may later add an appropriate bibliographic citation, indicating subsequent)</td>
<td>Yes, with appropriate bibliographic citation and a link to the article once</td>
<td>Only with the specific written permission of Elsevier</td>
</tr>
</tbody>
</table>
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.