Constructions of APN Permutations

by

Benjamin Chase

B.Sc., University of New Brunswick, 2019

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Fall 2021

Declaration of Committee

Name:	**Benjamin Chase**
Degree:	**Master of Science**
Thesis title:	**Constructions of APN Permutations**
Committee:	**Chair:** Imin Chen Professor, Department of Mathematics **Petr Lisoněk** Supervisor Professor, Department of Mathematics **Jonathan Jedwab** Committee Member Professor, Department of Mathematics **Nadish de Silva** Examiner Assistant Professor, Department of Mathematics

Abstract

APN functions defined on finite fields of characteristic two provide the best protection against differential cryptanalysis. They are used extensively in modern symmetric block ciphers. It is beneficial when APN functions are permutations. EA-equivalence and more generally CCZ-equivalence preserves the APN property. Only one example of APN permutations is known in even dimensions and its generalizations are called Kim-type functions. Our first result proves that all Kim-type APN functions in even dimensions greater than six are EA-equivalent to Gold functions. Combined with a previous result this shows that Kim-type APN functions are never CCZ-equivalent to permutations, except for dimension six. Our second result provides several theoretical constructions of Walsh zero spaces for Gold APN functions in odd dimensions. This allows one to construct new APN permutations that are CCZ-equivalent to Gold functions, but they are not EA-equivalent to them or their inverses.

Keywords: finite field; Boolean function; cryptography; APN function; Walsh zero

Acknowledgements

I would like to thank my supervisor Dr. Petr Lisoněk for the many helpful in-depth discussions and for his hospitality towards me during my time at SFU. I thank the examiners Dr. Jedwab and Dr. de Silva for careful reading of my thesis and helpful comments. I am thankful to many other people and organizations for various forms of support. In particular, I would like to thank Jenika Merriam for all her love and unending support throughout the thesis and for traveling across the country with me. I thank my parents for their love and all of the opportunities they have provided for me over the years. I thank the Centre for Experimental and Constructive Mathematics (CECM) for computational support and Magma license, and Léo Perrin for releasing an updated version of the software sboxU which has been extremely useful to the thesis. I am grateful for the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) as well as the British Columbia Graduate Scholarship.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

The main objects of study in this thesis, *almost perfect nonlinear functions* (typically referred to as *APN functions*), are critical components in the S-boxes of many modern symmetric block ciphers, wherein they perform nonlinear substitutions on bitstrings. Examples of block cipher designs that use S-boxes are Substitution-Permutation-Networks such as the internationally adopted Advanced Encryption Standard (AES). Within these ciphers, multiple rounds of permutations and substitutions are applied to a plaintext with a goal to attain the cryptographic properties of confusion and diffusion. Functions with low differential uniformity provide the provably best resistance to differential cryptanalysis, and those that achieve the lowest possible differential uniformity are called APN functions. In many cipher designs, it is required that the S-boxes be invertible in order to facilitate decryption. Therefore, there is immense interest in finding APN functions that are also permutations. For implementation purposes, it is necessary to work with functions defined on an n-dimensional binary vector space. There exist APN permutations in odd dimensions, although few have been classified into infinite families. The situation is more challenging in even dimensions, where only one example of an APN permutation, which occurs in dimension six was discovered in 2009 by Browning et al. [7]. To date, no other APN permutations in even dimensions have been found. On account of hardware considerations, it is often desirable that S-boxes operate in even-dimensional space. Especially common is dimension eight due to the standard of a byte being eight bits. AES uses the field inverse function in dimension eight which has the lowest known differential uniformity in that dimension. We will only consider functions mapping n input bits to n output bits but ciphers like CAST do use S-boxes that map n input bits to m output bits.

1.1 Thesis outline

In Chapter 2 we give some necessary background on finite fields. We also give more details on APN functions and describe some equivalences between functions that preserve important cryptographic properties. The last two sections of Chapter 2 provide background for Chapter 3 and Chapter 4 respectively.

In Chapter 3 we study an infinite family of functions, called Kim-type functions, that generalize the Kim function used by Browning et al. [7]. Finding more APN functions from this family was originally posed as an open problem by Carlet in [12]. In July 2020, Li, Li, Helleseth, and Qu [24] solved this by finding the exact conditions on the coefficients of Kim-type functions that result in APN functions. Using this result, we prove that Kim-type functions are affine equivalent to one of two Gold functions. A recent result of Göloğlu and Langevin [20] showed that, for even n, Gold APN functions are never CCZ-equivalent to permutations. Combined with our result, this shows that Kim-type functions in even dimensions greater than six are never CCZ-equivalent to permutations.

In Chapter 4 we find new methods to construct APN permutations. We explore the zeros of the Walsh transform of Gold APN permutations in odd dimensions. Specifically, we provide several theoretical and computer-free descriptions of Walsh zero spaces. Recently, there has been increased interest in Walsh zero spaces [10, 1]. Other than two trivial spaces, our constructions are, as far as we know, the first explicit descriptions of Walsh zero spaces. We also provide some theoretical constructions of trivially intersecting Walsh zero spaces for Gold APN permutations. Browning et al. [7] gave an implicit proof that, if two Walsh zero spaces of a function f intersect trivially, then f must be CCZ-equivalent to a permutation. We modify this proof to allow us to explicitly construct permutations CCZ-equivalent to f. Our hope is that the method of explicitly constructing trivially intersecting pairs of Walsh zero spaces of various APN functions may eventually lead to finding APN permutations in even dimension. We start Chapter 4 with description of how computations in low dimensions aided us, providing examples along the way.

1.2 Brief history

In the early 1970s, joint work done by IBM and the NSA culminated in the internationally adopted Data Encryption Standard (DES). The public release of DES in 1975 was met with much criticism from cryptographers. Many had suspicions of a backdoor, since the explanation for the structure of the S-boxes was not made available to the public, see page 107 of [34]. Hellman and Diffie argued that DES could be broken by brute force [17], which it eventually was in 1997. In 1991, Biham and Shamir [3] discovered a new type of attack on block ciphers called differential cryptanalysis. Indeed, later declassified documents showed that the ideas of differential cryptanalysis were known to IBM and the NSA during the process of designing DES.

Shortly after the techniques of differential cryptanalysis were made public, Nyberg [31] introduced precise mathematical descriptions of functions that optimally protect against this type of attack, called APN functions. A couple years later, in 1995, Nyberg and Knudsen

[32] proved that ciphers that are secure from differential cryptanalysis do exist, and they gave a prototype of such a cipher. Most importantly, this lead to the concept of open source cryptography where the *complete* mathematical structure of the ciphers is made public and can be rigorously analyzed and peer reviewed.

In 1997 the National Institute of Standards and Technology (NIST) initiated a transparent international competition to choose a replacement for DES, with the intention that the winner would become the Advanced Encryption Standard (AES) [29]. There were twenty-one submissions. After three years of peer review and elimination of many candidates that were proven to be insecure, Rijndael was chosen to be the algorithm for AES. Among the candidates was CAST, a cipher developed by Carlisle Adams and Stafford Tavares which has been approved for Government of Canada use by the Communications Security Establishment. Both Rijndael and CAST use S-boxes.

Many modern block ciphers rely on S-boxes. Recently, NIST has opened a competition to chose a standard cipher, or a set of standard ciphers, for use in lightweight cryptography [30]. With the recent growth of The Internet of Things, distributed control systems, smart cards and similar devices, there is increased demand for cryptographic algorithms that can efficiently fit into constrained devices. Out of the ten finalists, seven use S-boxes in their designs.

Chapter 2

Background

In this chapter we present some necessary background information on finite fields, almost perfect nonlinear functions, and equivalences between functions that preserve cryptographic properties. We also present background information regarding Kim-type functions and Walsh zeros which is needed in Chapter 3 and Chapter 4 respectively. This chapter does not contain any original material; instead it aims to make the thesis self-contained to a large extent. We note that the large amount of background material that was available to us at the start of our research brought many results within reach. In particular our work rests heavily on the work of Gold [18], Göloğlu, Krasnayová and Lisoněk [19], Li, Li, Helleseth and Qu [24], and Perrin and Joly [33].

Many computations in this thesis were done with the support of the computer algebra system Magma [5]. Computations illustrating or proving various parts of the thesis are collected in Appendices A, B and C. They would have been possible with other computer algebra systems such as Sage or GAP as well. We chose to use Magma as it appears to be the most commonly used system in the area of APN functions, and we also have had previous experience with it.

2.1 Finite fields

The contents of this section, unless otherwise specified, are taken from the first three chapters of the monograph by Lidl and Niederreiter [25]. We use $\mathbb{F}_{2^n}$ to denote the finite field of order 2^n. We will assume some basic knowledge of field theory. In particular we will often use the following without reference. The field $\mathbb{F}_{2^n}$ contains a subfield of order 2^m if and only if m divides n, and such a subfield is unique. The subfield $\mathbb{F}_{2^m} \subseteq \mathbb{F}_{2^n}$ consists precisely of elements $a \in \mathbb{F}_{2^n}$ such that $a = a^{2^m}$. We let $\mathbb{F}_{2^n}^*$ denote the multiplicative cyclic group of nonzero elements of $\mathbb{F}_{2^n}$. A generator of $\mathbb{F}_{2^n}^*$ is called a primitive element of $\mathbb{F}_{2^n}$. Since $\mathbb{F}_{2^n}$ is a field of characteristic two, we have that $a+a = 0$ for all $a \in \mathbb{F}_{2^n}$ and $(a+b)^{2^k} = a^{2^k}+b^{2^k}$ for all $a, b \in \mathbb{F}_{2^n}$ and any integer k. It follows that the map $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, given by $F(x) = x^2$ is a field automorphism called the *Frobenius automorphism*. If $x \mapsto x^k$ is a permutation of

$\mathbb{F}_{2^n}$ then $z^{1/k}$ will denote the unique $u \in \mathbb{F}_{2^n}$ such that $u^k = z$. As always, we will denote the ring of univariate polynomials over $\mathbb{F}_{2^n}$ by $\mathbb{F}_{2^n}[x]$ and the ring of multivariate polynomials in variables $x_1, \ldots, x_n$ over $\mathbb{F}_{2^n}$ by $\mathbb{F}_{2^n}[x_1, \ldots, x_n]$.

The additive group of $\mathbb{F}_{2^n}$ naturally forms an n-dimensional *vector space* over $\mathbb{F}_2$, which as usual will be denoted by $\mathbb{F}_2^n$.

Throughout this thesis, we will call a map $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *linear* if $L(a+b) = L(a) + L(b)$ for all $a, b \in \mathbb{F}_2^n$.

Definition 2.1.1 (Trace function). *For positive integers m and n such that m divides n, the* trace function *from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ is defined as*

$$\mathrm{Tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}.$$

The trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is called the absolute trace *and we will denote it by* $\mathrm{Tr}(x)$*.*

Lemma 2.1.2. *Suppose m and n are positive integers such that m divides n. Then the trace function $\mathrm{Tr}_m^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ satisfies the following properties.*

(i) $\mathrm{Tr}_m^n(a+b) = \mathrm{Tr}_m^n(a) + \mathrm{Tr}_m^n(b)$ *for all $a, b \in \mathbb{F}_{2^n}$,*

(ii) $\mathrm{Tr}_m^n(ca) = c\mathrm{Tr}_m^n(a)$ *for all $c \in \mathbb{F}_{2^m}$, $a \in \mathbb{F}_{2^n}$,*

(iii) $\mathrm{Tr}_m^n(a^{2^m}) = \mathrm{Tr}_m^n(a)$ *for all $a \in \mathbb{F}_{2^n}$,*

(iv) $\mathrm{Tr}_m^n(a) = \frac{n}{m} \cdot a$ *for all $a \in \mathbb{F}_{2^m}$,*

(v) if d is a positive integer that divides m, then $\mathrm{Tr}_d^n(a) = \mathrm{Tr}_d^m(\mathrm{Tr}_m^n(a))$ *for all $a \in \mathbb{F}_{2^n}$.*

Lemma 2.1.3. *For any $a \in \mathbb{F}_{2^n}$, $\mathrm{Tr}(a) = 0$ if and only if $a = t^2 + t$ for some $t \in \mathbb{F}_{2^n}$.*

Corollary 2.1.4. *For a fixed $a \in \mathbb{F}_{2^n}^*$, the set $\{x \in \mathbb{F}_{2^n} : \mathrm{Tr}(ax) = 0\}$, equal to $\{a^{-1}(t^2+t) : t \in \mathbb{F}_{2^n}\}$, forms an $(n-1)$-dimensional subspace (hyperplane) of $\mathbb{F}_{2^n}$.*

Proof. The map $t \to t^2 + t$ is linear and the dimension of its kernel is 1. □

We will often consider functions $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. It is well known that any such function can be written uniquely as a univariate polynomial of degree less than 2^n over $\mathbb{F}_{2^n}$ as

$$f(x) = \sum_{i=0}^{2^n-1} c_i x^i$$

with $c_i \in \mathbb{F}_{2^n}$. It is clear that f is linear if and only if the exponent of each term of f is a power of 2.

Lemma 2.1.5. *Let $A, B \in \mathbb{F}_{2^n}^*$ and $C \in \mathbb{F}_{2^n}$. Then the equation $Ax^2 + Bx + C = 0$ has exactly two roots in $\mathbb{F}_{2^n}$ if $\mathrm{Tr}\left(\frac{AC}{B^2}\right) = 0$ and no roots in $\mathbb{F}_{2^n}$ if $\mathrm{Tr}\left(\frac{AC}{B^2}\right) = 1$.*

Proof. After substituting $x \mapsto \frac{B}{A}y$ into $Ax^2 + Bx + C = 0$ and simplifying, we get

$$y^2 + y + \frac{AC}{B^2} = 0$$

and the conclusion follows from applying Lemma 2.1.3. □

Proposition 2.1.6. *(Theorem 7.8 (ii) of [25]) Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be given by $f(x) = x^d$. Then $f(x)$ is a permutation of $\mathbb{F}_{2^n}$ if and only if $\gcd(d, 2^n - 1) = 1$.*

Lemma 2.1.7. *If $\gcd(n, m) = 1$ then $\gcd(2^n - 1, 2^m - 1) = 1$.*

Proof. Let $d = \gcd(2^n - 1, 2^m - 1)$. Then $2^n \equiv 1 \pmod{d}$ and $2^m \equiv 1 \pmod{d}$ which implies $2^{rm+sn} \equiv 1 \pmod{d}$ for any $r, s \in \mathbb{Z}$. Specifically, since $\gcd(m, n) = 1$, we can choose r and s so that $rm + sn = 1$. Then $2^1 \equiv 1 \pmod{d}$ and $d = 1$. □

If $n = 2m$ then throughout the thesis we will write $q = 2^m$ so that $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{2^n}$. The set

$$U = \{z \in \mathbb{F}_{q^2} \mid z^{q+1} = 1\},$$

sometimes called the "unit circle" in $\mathbb{F}_{q^2}$, will play an important role. Note that U forms a cyclic subgroup of $\mathbb{F}_{q^2}^*$ of order $q + 1$. We will often use the fact that $z = 1$ is the only element of U that is also an element of $\mathbb{F}_q$. The following lemma is well known.

Lemma 2.1.8. *Every $y \in \mathbb{F}_{q^2}^*$ can be written uniquely as $y = xz$ where $x \in \mathbb{F}_q^*$ and $z \in U$.*

Proof. There are $(q - 1)(q + 1) = |\mathbb{F}_{q^2}^*|$ products of the form xz. Suppose $x_1 z_1 = x_2 z_2$ for $x_1, x_2 \in \mathbb{F}_q^*$ and $z_1, z_2 \in U$. Then $x_1/x_2 = z_2/z_1 \in \mathbb{F}_q^* \cap U = \{1\}$ and it follows that each product xz is unique. □

We say $\omega \in \mathbb{F}_{2^n}$ is a primitive cube root of unity of $\mathbb{F}_{2^n}$ if $\omega \neq 1$ and $\omega^3 = 1$. We will use ω to denote a primitive cube root of unity of $\mathbb{F}_{2^n}$ throughout the thesis without further reminders.

Lemma 2.1.9. *The finite field $\mathbb{F}_{2^n}$ contains a primitive cube root of unity if and only if n is even.*

Proof. A primitive cube root of unity, say ω, is a solution in $\mathbb{F}_{2^n}$ to the equation $x^3 + 1 = 0$. This equation factors as $(x + 1)(x^2 + x + 1) = 0$. Since $\omega \neq 1$, we are looking for solutions in $\mathbb{F}_{2^n}$ to $x^2 + x + 1 = 0$ which exist if and only if n is even by Lemma 2.1.5. □

We will need a condition for certain quadratic equations with arguments belonging to $U \backslash \{1\}$.

Lemma 2.1.10. *Assume that $A, B, C \in \mathbb{F}_q$ and the equation $Az^2 + Bz + C = 0$ has a solution $z \in U \setminus \{1\}$. Then $A = C$.*

Proof. Suppose $Az^2 + Bz + C = 0$ and $z \in U \setminus \{1\}$. Raising the equation to the q-th power and multiplying by z^2 gives

$$\begin{aligned} z^2(Az^2 + Bz + C)^q &= z^2(A^q z^{2q} + B^q z^q + C^q) \\ &= z^2(Az^{-2} + Bz^{-1} + C) \\ &= A + Bz + Cz^2 = 0. \end{aligned}$$

Adding the equations yields

$$\begin{aligned} (Az^2 + Bz + C) + (A + Bz + Cz^2) &= A(z^2 + 1) + C(z^2 + 1) \\ &= (A + C)(z^2 + 1) = 0. \end{aligned}$$

Since $z \neq 1$, the conclusion follows. □

In Chapter 3 we will use the *resultant* to eliminate one variable from two multivariate polynomials. Since including the full definition of the resultant would add unnecessary complexity to the thesis, we treat the resultant as a "black box". We use the most common definition of resultant which is the determinant of the Sylvester matrix, see Chapter 3, Definition 2 of [16]. This resultant is also implemented in Magma [5]. We denote by $\mathrm{res}_y(A, B)$ the resultant of polynomials A and B with respect to the eliminated variable y.

The following proposition follows from Chapter 4, Corollary 4 of [16].

Proposition 2.1.11. *Let K be a ring. Let $A, B \in K[x_1, \ldots, x_n, y]$ and let $R(x_1, \ldots, x_n) = \mathrm{res}_y(A, B)$. Let $(x_1^*, \ldots, x_n^*, y^*) \in K^{n+1}$ be such that $A(x_1^*, \ldots, x_n^*, y^*) = B(x_1^*, \ldots, x_n^*, y^*) = 0$. Then $R(x_1^*, x_2^*, \ldots, x_n^*) = 0$.*

Example 2.1.12. *Let $\mathbb{F}_{101}$ denote the finite field of order 101. Suppose $A, B \in \mathbb{F}_{101}[x, y]$ are given by $A(x, y) = 4x^4 + 3x^3y^2 + xy + y + 5$ and $B(x, y) = x^4y^3 + 2x^2y + xy^4$. The solutions to the system of equations $A(x, y) = B(x, y) = 0$ are*

$$(0, 96), (49, 0), (15, 0), (11, 77), (52, 0) \text{ and } (86, 0).$$

The roots of $\mathrm{res}_y(A, B)$ are $0, 11, 15, 49, 52$ and 86 and the roots of $\mathrm{res}_x(A, B)$ are $0, 77$ and 96. One can see that if (x^*, y^*) is a solution to the original system then x^* is also a solution to $\mathrm{res}_y(A, B) = 0$ and y^* is also a solution to $\mathrm{res}_x(A, B) = 0$.

2.2 Almost perfect nonlinear functions

Recall that we denote by $\mathbb{F}_2^n$ the n-dimensional vector space over $\mathbb{F}_2$. Denote by $(\mathbb{F}_2^n)^*$ the set of nonzero vectors in $\mathbb{F}_2^n$. Functions mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ are called Boolean functions. Functions of this type have found many applications in computer science and in digital communications (cryptography, coding theory). More generally, one can view vectorial Boolean functions, $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$, as mapping to vectors of length m with Boolean functions as components. Vectorial Boolean functions are used extensively in block ciphers. Balanced functions are favored in cryptography as they remove biases that could be used by attackers.

Definition 2.2.1. *A function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is balanced if $|\{x \in \mathbb{F}_2^n \ : \ f(x) = a\}| = 2^{n-m}$ for each $a \in \mathbb{F}_2^m$.*

Lemma 2.2.2. *The trace function $\mathrm{Tr}_m^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is balanced.*

We recall from Chapter 1 that almost perfect nonlinear (APN) functions were introduced in the mid-1990s, when the mathematical methods started to play a significant role in the design of symmetric cryptography. APN functions are highly sought after since they optimally protect against differential cryptanalysis. For an in-depth overview of differential cryptanalysis, see Section 4.4 of [34]. Differential cryptanalysis of a cipher F assumes that an attacker knows a large number of pairs of plaintexts $x, x+a \in \mathbb{F}_2^n$ that have a fixed difference a, as well as their corresponding ciphertext pairs $F(x)$ and $F(x+a)$ which are encrypted using an unknown but fixed key. If a poor design of S-boxes used in F causes a certain output difference $b = F(x) - F(x+a)$ to occur much more or less given a certain input difference a, then this statistical dependency can be exploited by an attacker to recover (parts of) the secret key. It is therefore desired that these output differences are as uniformly distributed as possible for a given input difference, which motivates the following definitions.

Definition 2.2.3. *The* differential uniformity *of a function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is given by*

$$\Delta_f = \max_{a \in (\mathbb{F}_2^n)^*, b \in \mathbb{F}_2^n} \delta_f(a, b),$$

where

$$\delta_f(a, b) = |\{x \in \mathbb{F}_2^n : f(x+a) + f(x) = b\}|.$$

In this thesis we only consider differential uniformity in characteristic 2 but it can also be defined for functions on vector spaces of odd characteristic.

Proposition 2.2.4. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Then Δ_f is even and $\Delta_f \geq 2$.*

Proof. Suppose $a \in (\mathbb{F}_2^n)^*$ and $b \in \mathbb{F}_2^n$ are fixed. If $r \in \mathbb{F}_2^n$ is a solution to $f(x+a)+f(x) = b$ then $r + a$ must also be a solution. For a fixed $a \in (\mathbb{F}_2^n)^*$ we have $\sum_{b \in \mathbb{F}_2^n} \delta_f(a, b) = 2^n$ and by applying the pigeonhole principle we have $\Delta_f \geq 2^{n-n} = 1$. But since Δ_f is even we have $\Delta_f \geq 2$. □

Definition 2.2.5. *We call a function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$* almost perfect nonlinear (APN) *if $\Delta_f = 2$.*

2.2.1 APN functions on finite fields

It is important to note that the definition of APN function given above only uses the vector space structure of $\mathbb{F}_2^n$ but it does not require the domain to be the field $\mathbb{F}_{2^n}$. We only work with APN functions defined on fields $\mathbb{F}_{2^n}$ throughout this thesis, in order to exploit their rich algebraic structure. Most of the literature follows this approach.

There exist six known families of APN monomial functions over $\mathbb{F}_{2^n}$, see Table 1 of [9]. Moreover, for odd dimension n all of these families are permutations.

Name	Exponent d	Conditions
Gold	2^i+1	$\gcd(i,n)=1$
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$
Welch	2^i+3	$n=2i+1$
Inverse	$2^{2i}-1$	$n=2i+1$
Niho	$2^i+2^{\frac{i}{2}}-1$, i even $2^i+2^{\frac{3i+1}{2}}-1$, i odd	$n=2i+1$ $n=2i+1$

Table 2.1: Known infinite families of APN power functions $f(x)=x^d$.

The formal definition of an APN function was introduced by Nyberg in 1993 and some of the material in this section is taken from her paper "Differentially uniform mappings for cryptography" [31].

Proposition 2.2.6 ([31])**.** *For integers n, i with $\gcd(i,n)=1$, the Gold function $f(x)=x^{2^i+1}$ is APN.*

Proof. Suppose $a\in\mathbb{F}_{2^n}^*$ and $b\in\mathbb{F}_{2^n}$ are fixed. By Definition 2.2.3, we must show that the number of solutions in $\mathbb{F}_{2^n}$ of the equation

$$(x+a)^{2^i+1}+x^{2^i+1}=b$$

is at most 2. Expanding and simplifying gives

$$ax^{2^i}+a^{2^i}x+a^{2^i+1}=b. \tag{2.1}$$

If (2.1) has no solutions then we are done. Suppose (2.1) has distinct solutions $r,s\in\mathbb{F}_{2^n}$ so that

$$\begin{aligned} ar^{2^i}+a^{2^i}r+a^{2^i+1}&=b,\\ as^{2^i}+a^{2^i}s+a^{2^i+1}&=b. \end{aligned}$$

Adding these two equations and rearranging gives

$$\left(\frac{r+s}{a}\right)^{2^i} = \frac{r+s}{a}$$

which implies $\frac{r+s}{a} \in \mathbb{F}_{2^i}$. But since $\gcd(i,n) = 1$, it must be that $\mathbb{F}_{2^i} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$. Since $r+s \neq 0$, it follows that $r = s+a$. Since r, s are freely chosen from the set of all possible solutions to (2.1), the equality $r = s+a$ means that there are exactly two solutions. □

Proposition 2.2.7. *For n odd and $\gcd(i,n) = 1$, the Gold function $f(x) = x^{2^i+1}$ is a permutation of $\mathbb{F}_{2^n}$.*

Proof. Let $d = \gcd(2^n-1, 2^i+1)$. Then d divides $\gcd(2^n-1, (2^i+1)(2^i-1)) = \gcd(2^n - 1, 2^{2i}-1)$. Since n is odd, $\gcd(2i,n) = 1$ and by Lemma 2.1.7, $\gcd(2^n-1, 2^{2i}-1) = 1$. By Proposition 2.1.6, $f(x) = x^{2^i+1}$ is a permutation of $\mathbb{F}_{2^n}$. □

The binary weight of a nonnegative integer z is the number of ones in its binary expansion and it will be denoted by $w_2(z)$.

Definition 2.2.8 (Algebraic degree, page 45 of [11])**.** *The* algebraic degree *of a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is the maximum binary weight of an exponent of any nonzero term of f.*

Example 2.2.9. *For $n = 9$, the algebraic degree of $f(x) = x^3$ is 2, and the algebraic degree of its compositional inverse $g(x) = x^{1/3} = x^{341}$, which is also an APN permutation, is 5 since* $341 = 2^0 + 2^2 + 2^4 + 2^6 + 2^8$.

Example 2.2.10. *A linear polynomial over $\mathbb{F}_{2^n}$ has the form $f(x) = \sum_{i=0}^{n-1} c_i x^{2^i}$ for some $c_i \in \mathbb{F}_{2^n}$. Each exponent of every term is $2^i$and has binary weight $w_2(2^i) = 1$. Hence, a polynomial $f(x)$ over $\mathbb{F}_{2^n}$ is linear if and only if its algebraic degree is* 1 *and $f(x)$ has no constant term.*

Example 2.2.11. *For distinct integers i and j, the binary weight of $2^i + 2^j$ is $w_2(2^i + 2^j) = 2$. Polynomials of algebraic degree* 2 *are called quadratic polynomials. In particular Gold functions $x \mapsto x^{2^i+1}$ are quadratic.*

Example 2.2.12. *Let $f(x) = \frac{1}{x}$, with $f(0) = 0$, be the field inverse function on $\mathbb{F}_{2^n}$. Equivalently, $f(x) = x^{2^n-2}$. We have*

$$w_2(2^n-2) = w_2\left(\sum_{i=1}^{n-1} 2^i\right) = n-1.$$

So the field inverse function has algebraic degree $n-1$.

There are properties other than differential uniformity to consider when looking for optimal cryptographic functions. For example, functions with low algebraic degree (like the Gold function with algebraic degree 2) are prone to higher order differential attacks. Thus finding APN functions with high algebraic degree is desirable. One particular way of possibly increasing the algebraic degree is by taking the compositional inverse of the given function if it exists. In particular for the Gold functions, taking the compositional inverse already provides APN permutations of higher algebraic degree, see Example 2.2.9.

Proposition 2.2.13 ([31]). *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be given by $f(x) = 1/x$ and define $f(0) = 0$. Equivalently, $f(x) = x^{2^n-2}$. Then $\Delta_f = 2$ when n is odd and $\Delta_f = 4$ when n is even.*

Proof. Suppose $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$ are fixed. Following Definition 2.2.3, we consider the number of solutions in $\mathbb{F}_{2^n}$ of the equation

$$(x+a)^{2^n-2} + x^{2^n-2} = b. \tag{2.2}$$

By Proposition 2.1.6, $f(x)$ is a permutation of $\mathbb{F}_{2^n}$ and so we can assume that $b \neq 0$. It is clear that $x = 0$ and $x = a$ are solutions if and only if $a^{2^n-2} = b$, in which case, $ab = 1$. If $x \neq 0$ and $x \neq a$ then (2.2) becomes

$$(x+a)^{-1} + x^{-1} = b$$

and rearranging gives

$$bx^2 + abx + a = 0 \tag{2.3}$$

which has at most two solutions in $\mathbb{F}_{2^n}$. Therefore Δ_f is at least 2, regardless of the parity of n. Furthermore, the only way that Δ_f is greater than 2 is when $ab = 1$. In which case (2.3) becomes

$$x^2 + ax + a^2 = 0$$

and the result follows by applying Lemma 2.1.5. □

The field inverse function of Proposition 2.2.13 has high algebraic degree $(n-1)$ and it is always a permutation. It is close to being APN for even n since $\Delta_f = 4$. For these reasons, among others such as simplicity of description, in dimension 8 this function is used in the S-box of the Advanced Encryption Standard, which we discussed in Chapter 1.

One of the most important open problems concerning APN permutations is their existence in even dimensions. In 2006, Hou proved that for dimensions $n = 2$ and $n = 4$ no APN permutations exist [21] and it was conjectured that no APN permutations exist in even dimensions. Surprisingly, in 2009 Browning et al. [7] constructed an example of an APN permutation of $\mathbb{F}_{2^6}$, but it is not known if other APN permutations in dimension 6 exist. Since then, no new APN permutations in even dimensions have been found. The question of the existence of APN permutations in even dimensions greater than six is known as the Big APN Problem.

2.3 Equivalences which preserve cryptographic properties

In this section we introduce some notions of equivalence that we will use throughout the next two chapters. We follow Section 2.1 of [11].

Definition 2.3.1 (Linear and Affine function)**.** *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Recall that f is called* linear *if $f(x+y) = f(x)+f(y)$ for all $x, y \in \mathbb{F}_2^n$. Further, f is called* affine *if $f(x) = g(x)+c$ where g is linear and $c \in \mathbb{F}_2^n$.*

Definition 2.3.2. *Two functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are called* affine equivalent *if there exist affine permutations L_1, L_2 of $\mathbb{F}_2^n$ such that*

$$F(x) = L_1(G(L_2(x))).$$

Furthermore, if there exists an affine function $L_3 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that

$$F(x) = L_1(G(L_2(x))) + L_3(x),$$

then we say that F and G are extended affine or EA-equivalent*.*

It is well known that EA-equivalence preserves the algebraic degree of a function when the algebraic degree is greater than one. EA-equivalence also preserves the differential uniformity of a function. In particular, applying EA-equivalence to an APN function produces another APN function.

The following lemmas will be useful when constructing affine equivalences from linear permutations.

Lemma 2.3.3. *A linear map $L : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ is a bijection if and only if $L(z)$ has no nonzero roots in $\mathbb{F}_{q^2}$.*

Proof. Suppose $L(z)$ is a bijection. Since $L(0) = 0$ it follows that 0 is the only root of $L(z)$. Conversely, suppose $L(z)$ has no nonzero roots in $\mathbb{F}_{q^2}$. If $L(\alpha) = L(\beta)$ for $\alpha, \beta \in \mathbb{F}_{q^2}$ then $L(\alpha + \beta) = 0$. Since 0 is the only root of $L(z)$, it must be that $\alpha = \beta$. So $L(z)$ is injective on $\mathbb{F}_{q^2}$. Thus $L(z)$ is a bijection. □

We will use the following lemma extensively in Chapter 3.

Lemma 2.3.4. *Suppose $L(z)$ is a linear map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_{q^2}$ given by $L(z) = z^q + tz$. Then $L(z)$ is a bijection if and only if $t \notin U$.*

Proof. In light of Lemma 2.3.3, we will show that $L(z)$ has a nonzero root in $\mathbb{F}_{q^2}$ if and only if $t \in U$. Suppose $\alpha \in \mathbb{F}_{q^2}^*$ such that $0 = L(\alpha) = \alpha^q + t\alpha$. Then $\alpha^{q-1} = t$ and

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

Therefore $t \in U$. Conversely, suppose $t \in U$. If $t = 1$ then $L(z) = z^q + z$ for which every element of $\mathbb{F}_q$ is a root. If $t \in U \backslash \{1\}$ then $L(t^q + 1) = (t^q + 1)^q + t(t^q + 1) = t^{q+1} + 1 = 0$ and $t^q + 1$ is a nonzero root of $L(z)$. □

In 1998 an important equivalence relation more general than EA equivalence was introduced by Carlet, Charpin, and Zinoviev [13]. Later it has become known as *CCZ-equivalence.*

Definition 2.3.5. *Two functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are* CCZ-equivalent *if there exists an affine automorphism L of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that*

$$\{(x, F(x)) : x \in \mathbb{F}_2^n\} = L(\{(x, G(x)) : x \in \mathbb{F}_2^n\}).$$

CCZ-equivalence is strictly more general than EA-equivalence together with taking inverses of permutations, see Section 2.1.1 of [11]. CCZ-equivalence preserves the differential spectrum of functions, in particular their differential uniformity. That is, it preserves the multiset of values $\delta_f(a, b) = |\{x \in \mathbb{F}_2^n \ : \ f(x + a) + f(x) = b\}|$, see page 136, paragraph 2, of [11].

Example 2.3.6. *Suppose $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a bijection. The transformation $L(x, y) = (y, x)$ is an affine automorphism of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ and*

$$L(\{(x, F(x)) : x \in \mathbb{F}_2^n\}) = \{(F(x), x) : x \in \mathbb{F}_2^n\}.$$

Therefore $F(x)$ is CCZ-equivalent to $F^{-1}(x)$. It follows that if $F(x)$ is an APN permutation, then its compositional inverse $F^{-1}(x)$ is also APN.

There is much active research [10] into how to partition a class of CCZ-equivalent functions into EA equivalence classes. Data that remain invariant under certain equivalences are often used to examine the possible equivalence between functions. Unlike EA-equivalence, the algebraic degree of a function is not preserved under CCZ-equivalence, see page 36 of [11]. Since CCZ-equivalence does not preserve the permutation property of a function, applying CCZ transformations may be used as a tool for finding new APN permutations. See page 403 of [11] for a list of some other CCZ invariant parameters.

We will need some background from coding theory (see Chapter 3 of [28]) in order to give the code-based criterion of CCZ-equivalence.

Definition 2.3.7. *The* Hamming weight $w(x)$ of a vector $x \in \mathbb{F}_2^n$ is the number of nonzero coordinates in x.

Definition 2.3.8. *A* binary code C with parameters $[n, k, d]$ is an $\mathbb{F}_2$-linear subspace of $\mathbb{F}_2^n$ where $\dim_{\mathbb{F}_2} C = k$ and $d = \min\{w(x) \ : \ x \in C \backslash \{0\}\}$. We say d is the distance of C. It is usual to refer to elements of C as codewords.

Definition 2.3.9. *A generator matrix for a binary code C is a $k \times n$ matrix whose rows form a basis for C.*

We say that binary codes C and C' are *equivalent* if they are equal up to some permutation of their coordinates. Thus permuting the columns of a generator matrix for a code C will produce the generator matrix of an equivalent code C'.

Definition 2.3.10. *A parity check matrix for a binary code C is a generator matrix for the* dual code $C^{\perp} = \{x \in \mathbb{F}_2^n \ : \ \forall y \in C, \ x \cdot y = 0\}$

Definition 2.3.11. *For a positive integer r, the* binary simplex code $\mathcal{S}_r$ is a binary code with parameters $[2^r - 1, r, 2^{r-1}]$.

It is well known that for every nonzero $x \in S_r$ the Hamming weight of x is 2^{r-1}. The generator matrix for the code S_r is a $r \times (2^r - 1)$ matrix whose columns consist of all distinct nonzero vectors of $\mathbb{F}_2^r$. Therefore each such code is unique up to equivalence and a generator matrix for S_r naturally corresponds to a permutation of $\mathbb{F}_2^n$ that fixes zero.

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Assume that $F(0) = 0$, which can be achieved by an affine transformation which is a special kind of CCZ-equivalence. Let α be a primitive element of $\mathbb{F}_{2^n}$ and fix a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. In the matrix below we express elements of $\mathbb{F}_{2^n}$ as n-dimensional column vectors over $\mathbb{F}_2$ with respect to that fixed basis. Let

$$H_F = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^n-2} \\ F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{2^n-2}) \end{bmatrix}.$$

We will denote by C_F the binary code with parity check matrix H_F. The following was observed by Browning et al. [6] and is given as Remark 4 of Proposition 160 of [11].

Proposition 2.3.12 ([6])**.** *Let $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ satisfy $F(0) = G(0) = 0$. If C_F and C_G are equivalent then F and G are CCZ-equivalent.*

In this thesis we will show CCZ-equivalence by using Proposition 2.3.12, instead of Definition 2.3.5.

2.4 Kim-type functions

The only known APN permutation in even dimensions was discovered by Browning et al. in [7]. It was obtained by applying a certain CCZ-equivalence transformation (which we formalize in Proposition 2.5.7) to the function

$$\kappa : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}, \qquad \kappa(x) = x^3 + x^{10} + ux^{24},$$

where u is a primitive element of $\mathbb{F}_{2^6}$ whose minimal polynomial over $\mathbb{F}_2$ is $X^6 + X^4 + X^3 + X + 1$. The function κ is known as the *Kim function*, named after the first author of [7]. An interesting property of this function, known as the *subspace property*, is that $\kappa(cx) = c^3\kappa(x)$ for all $c \in \mathbb{F}_{2^3} \subset \mathbb{F}_{2^6}$.

Naturally, there has been much interest in generalizing the Kim function in hopes of solving the Big APN Problem. In 2014, Carlet posed the following open problem regarding generalized Kim functions:

Problem 2.4.1. *[12, Section 3.7] Find more APN functions or, better, infinite classes of APN functions of the form* $X^3 + aX^{2+q} + bX^{2q+1} + cX^{3q}$ *where* $q = 2^{n/2}$ *with* n *even, or more generally of the form* $X^{2^k+1} + aX^{2^k+q} + bX^{2^kq+1} + cX^{2^kq+q}$*, where* $\gcd(k, n) = 1$.

It has been customary to call functions of this form *Kim-type functions*, to recognize that they generalize the Kim function.

The motivation for solving Problem 2.4.1 is given by possibly using the Kim-type APN function as an ingredient to a suitable CCZ transformation to obtain APN permutations, by analogy to the approach of [7]. We characterize such suitable transformations in Proposition 2.5.7. There have been several lines of attack to approach Problem 2.4.1; we refer to the Introduction section of [24] for a recent and detailed account of them. For the rest of this section we write $n = 2m$ and $q = 2^m$ so that $\mathbb{F}_q \subset \mathbb{F}_{q^2}$.

The first part of Problem 2.4.1 was resolved in the special case when the coefficients a, b, c belong to the subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^2}$. Specifically, in Theorem 3.2 of [22] Krasnayová proved that the function $F : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ given by $F(X) = X^3+bX^{3q}+cX^{2q+1}+dX^{2+q}$ is APN if and only if the conditions in Table 2.2 are satisfied. Please note that the notation used in Table 2.2 is different from that of Problem 2.4.1. We chose to not change the notation in order to stay consistent with the original references. We also note that our main reference [24] uses yet another different but equivalent form of the Kim-type function. Starting from Theorem 2.4.2 we will be using the notation of [24] for Kim-type functions.

m odd	m even
$\Delta = 1 + b + c + d \neq 0$	
$\mathrm{Tr}_1^m\left(\frac{1+b}{1+b+c+d}\right) = 1$	$\mathrm{Tr}_1^m\left(\frac{1+b}{1+b+c+d}\right) = 0$
$1 + c + b^2 + bd \neq 0$	-
$\mathrm{Tr}_1^m\left(\frac{\Delta^2}{1+b^2+c+bd}\right) = 1$	-
if $\mathrm{Tr}_1^m\left(\frac{bd+c}{\Delta^2}\right) = 1$, then $b^2c^2 + d^2 \neq \Delta^2(bd + c)$	
$\mathrm{Tr}_1^m\left(\frac{\Delta(T\Delta+c+d)(T^2\Delta^2+bd+c)}{(T\Delta^2+bc+d)^2}\right) = 1$, for every T such that $\mathrm{Tr}_1^m(T) = 1$, $\Delta T + 1 + b \neq 0$, $T\Delta^2 + bc + d \neq 0$ and $\Delta^2T^2 + bd + c \neq 0$	

Table 2.2: Krasnayová's APN conditions.

The conditions given in Table 2.2 are not computationally efficient since there are exponentially many conditions to check as the dimension increases. In an unpublished manuscript by Göloğlu, Krasnayová, and Lisoněk [19], it is shown that the last condition in Table 2.2

can be simplified. Specifically, it leads to the conditions $bd+c^2+c+d^2=0$ when m is even or odd and $b^2+bd+c+1=0$ when m is even (see Appendix A for these calculations), and one more case which is shown in [19] to never occur. This led to the following theorem regarding Kim-type functions with coefficients restricted to the subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^2}$.

Theorem 2.4.2. *[19] Suppose that $m \geq 4$ is an integer and let $q = 2^m$. Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1x^{2q+1} + a_2x^{q+2} + a_3x^3$ where $a_1, a_2, a_3 \in \mathbb{F}_q$. If f is APN, then f is affine equivalent to $G_1(x) = x^3$ or f is affine equivalent to $G_2(x) = x^{2^{m-1}+1}$.*

Therefore Kim-type functions with $a_1, a_2, a_3 \in \mathbb{F}_q$ produce no new APN functions. The results of [19] were presented in a talk at the 13^{th} International Conference on Finite Fields and their Applications Fq13 in 2017 [27].

In July 2020, a major advance on the subject was obtained by Li, Li, Helleseth and Qu [24] who resolved the first part of Problem 2.4.1 by completely characterizing APN functions on $\mathbb{F}_{q^2}$ of the form $f(x) = x^{3q} + a_1x^{2q+1} + a_2x^{q+2} + a_3x^3$, where $m \geq 4$ and $a_1, a_2, a_3 \in \mathbb{F}_{q^2}$. We state their result in this section as Theorem 2.4.4. In contrast to Table 2.2, the conditions given in [24] are much simpler and the number of conditions does not increase as the dimension of $\mathbb{F}_{2^n}$ increases. This result was crucial for enabling our research.

For the rest of this section we summarize the most important results of Li, Li, Helleseth and Qu [24], without which our work would not be possible. Then we use the results of [24] to present a much simpler proof of the main result from [19].

The following is an observation which is not stated as a numbered item in [24] but we want to give it a label for our future reference, and we also state it in a slightly different form.

Lemma 2.4.3. *[24] Any function $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ given by $f(x) = x^{3q} + a_1x^{2q+1} + a_2x^{q+2} + a_3x^3$ where $a_1, a_2, a_3 \in \mathbb{F}_{q^2}$ is affine equivalent to a function $f'(x) = x^{3q} + a_1'x^{2q+1} + a_2'x^{q+2} + a_3'x^3$ where $a_1' \in \mathbb{F}_q$ and $a_2', a_3' \in \mathbb{F}_{q^2}$. If $a_2 = 0$, then it is possible to choose f' such that $a_2' = 0$.*

Proof. If $a_1 = 0$ then we are done. For any fixed $a_1 \in \mathbb{F}_{q^2}^*$ let $b = a_1^{2^{m-1}}$. Then

$$\begin{aligned} f(bx) &= b^{3q}x^{3q} + a_1b^{2q+1}x^{2q+1} + a_2b^{q+2}x^{q+2} + a_3b^3x^3 \\ &= b^{3q}\left(x^{3q} + a_1\left(\frac{b}{b^q}\right)x^{2q+1} + a_2\left(\frac{b^2}{b^{2q}}\right)x^{q+2} + a_3\left(\frac{b^3}{b^{3q}}\right)x^3\right). \end{aligned}$$

Let

$$f'(x) = \left(\frac{1}{b^{3q}}\right) \cdot f(bx) = x^{3q} + a_1'x^{2q+1} + a_2'x^{q+2} + a_3'x^3$$

where $a_1' = a_1\left(\frac{b}{b^q}\right)$, $a_2' = a_2\left(\frac{b^2}{b^{2q}}\right)$, and $a_3' = a_3\left(\frac{b^3}{b^{3q}}\right)$. Note that $f(x)$ is affine equivalent to $f'(x)$ and since $a_1 = b^{2q}$, it follows that $a_1\left(\frac{b}{b^q}\right) = b^{q+1} \in \mathbb{F}_q$. □

For $z \in \mathbb{F}_{q^2}$ we denote $\bar{z} = z^q$. The following constants are introduced in [24] where they are used in Theorem 2.4.4; we will use them frequently in this section and throughout Chapter 3.

$$\begin{aligned} \theta_1 &= 1 + a_1^2 + a_2\bar{a}_2 + a_3\bar{a}_3, \\ \theta_2 &= a_1 + \bar{a}_2 a_3, \\ \theta_3 &= \bar{a}_2 + a_1\bar{a}_3, \\ \theta_4 &= a_1^2 + a_2\bar{a}_2. \end{aligned} \tag{2.4}$$

The following theorem is the main result of [24].

Theorem 2.4.4. *[24, Theorem 1] Let $n = 2m$ with $m \geq 4$ and $f(x) = \bar{x}^3 + a_1\bar{x}^2 x + a_2\bar{x}x^2 + a_3x^3$, where $a_1 \in \mathbb{F}_{2^m}, a_2, a_3 \in \mathbb{F}_{2^n}$. Let θ_i's be defined as in (2.4) and define*

$$\Gamma_1 = \left\{(a_1, a_2, a_3) \mid \theta_1 \neq 0,\ \mathrm{Tr}_1^m\left(\frac{\theta_2\bar{\theta}_2}{\theta_1^2}\right) = 0,\ \theta_1^2\theta_4 + \theta_1\theta_2\bar{\theta}_2 + \theta_2^2\theta_3 + \bar{\theta}_2^2\bar{\theta}_3 = 0\right\} \tag{2.5}$$

and

$$\Gamma_2 = \left\{(a_1, a_2, a_3) \mid \theta_1 \neq 0,\ \mathrm{Tr}_1^m\left(\frac{\theta_2\bar{\theta}_2}{\theta_1^2}\right) = 0,\ \theta_1^2\theta_3 + \theta_1\bar{\theta}_2^2 + \theta_2^2\theta_3 + \bar{\theta}_2^2\bar{\theta}_3 = 0\right\}. \tag{2.6}$$

Then f is APN over $\mathbb{F}_{2^n}$ if and only if

(1) m is even, $(a_1, a_2, a_3) \in \Gamma_1 \cup \Gamma_2$; or

(2) m is odd, $(a_1, a_2, a_3) \in \Gamma_1$.

Any time we try to show affine equivalence using a linear permutation(s) of the input and/or output of a function, we find the coefficients of those permutation(s) by expanding its/their sufficiently general form and comparing coefficients.

Lemma 2.4.5. *The Gold functions $G_2(x) = x^{2^{m-1}+1}$ and $G_2'(x) = x^{2^{m+1}+1}$ over $\mathbb{F}_{q^2}$ are affine equivalent.*

Proof. The result follows from observing that

$$G_2(x^{2q}) = \left(x^{2^{m+1}}\right)^{2^{m-1}+1} = x^{2^{2m}+2^{m+1}} = x^{2^{m+1}+1} = x^{2q+1} = G_2'(x).$$

□

Lemma 2.4.6. *Let $L_1(u) = u^q + tu$ and $L_2(u) = ru^q + su$ for some $r, s, t \in \mathbb{F}_{q^2}$. Let $G_1(x) = x^3$ and $G_2'(x) = x^{2^{m+1}+1}$. Then*

$$L_1(G_1(L_2(x))) = (r^3t + s^{3q})x^{3q} + (r^qs^{2q} + r^2st)x^{2q+1} + (r^{2q}s^q + rs^2t)x^{q+2} + (r^{3q} + s^3t)x^3$$

and

$$L_1(G_2'(L_2(x))) = (r^2s^q{+}rs^{2q}t)x^{3q}{+}(r^{q+2}{+}s^{2q+1}t)x^{2q+1}{+}(r^{2q+1}t{+}s^{q+2})x^{q+2}{+}(r^{2q}st{+}r^qs^2)x^3.$$

Proof. Expanding gives

$$\begin{aligned}
L_1(G_1(L_2(x))) &= L_1((rx^q + sx)^3) \\
&= L_1((r^2x^{2q} + s^2x^2)(rx^q + sx)) \\
&= L_1(r^3x^{3q} + r^2sx^{2q+1} + rs^2x^{q+2} + s^3x^3) \\
&= s^{3q}x^{3q} + r^qs^{2q}x^{2q+1} + r^{2q}s^qx^{q+2} + r^{3q}x^3 \\
&\quad + r^3tx^{3q} + r^2stx^{2q+1} + rs^2tx^{q+2} + s^3tx^3
\end{aligned}$$

and

$$\begin{aligned}
L_1(G_2'(L_2(x))) &= L_1((rx^q + sx)^{2q+1}) \\
&= L_1((r^{2q}x^2 + s^{2q}x^{2q})(rx^q + sx)) \\
&= L_1(rs^{2q}x^{3q} + s^{2q+1}x^{2q+1} + r^{2q+1}x^{q+2} + r^{2q}sx^3) \\
&= r^2s^qx^{3q} + r^{q+2}x^{2q+1} + s^{q+2}x^{q+2} + r^qs^2x^3 \\
&\quad + rs^{2q}tx^{3q} + s^{2q+1}tx^{2q+1} + r^{2q+1}tx^{q+2} + r^{2q}stx^3.
\end{aligned}$$

The proof is completed by rearranging the terms in the last expression of each expansion. □

In the remainder of this section we include the proof of Theorem 2.4.2 using Theorem 2.4.4. We mostly follow the original line of proof in [19] but we take significant advantage of [24] which allows major simplifications in comparison to the original proof in [19]. In the following proof we will often use linear maps $L : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ of the form $L(u) = u^q + tu$ given in Lemma 2.3.4. Note that for the case of $t \in \mathbb{F}_q$ we only need to check that $t \neq 1$ for L to be a bijection.

Proof of Theorem 2.4.2. Assume $a_1, a_2, a_3 \in \mathbb{F}_q$. Then the θ_i defined in (2.4) satisfy

$$\begin{aligned}
\theta_1 &= (1 + a_1 + a_2 + a_3)^2 \\
\theta_2 &= a_1 + a_2a_3 \\
\theta_3 &= a_2 + a_1a_3 \\
\theta_4 &= a_1^2 + a_2^2.
\end{aligned}$$

Assume $f(x) = x^{3q} + a_1x^{2q+1} + a_2x^{q+2} + a_3x^3$ is APN and therefore satisfies the conditions given in Theorem 2.4.4. The third condition of Γ_1 becomes $\theta_1(\theta_1\theta_4{+}\theta_2^2) = 0$ which simplifies to

$$\theta_1 S^2 = 0 \tag{2.7}$$

where

$$S = a_1^2 + a_1 a_3 + a_2^2 + a_2.$$

The third condition of Γ_2 becomes $\theta_1(\theta_1\theta_3 + \theta_2^2) = 0$ which factors as

$$\theta_1 ST = 0 \tag{2.8}$$

where

$$T = a_1 a_3 + a_2 + a_3^2 + 1.$$

If f is APN, then it follows from Theorem 2.4.4 that $\theta_1 \neq 0$. Thus we must have $S = 0$ for (2.7) to hold, and we must have $ST = 0$ for (2.8) to hold. Note that $S = 0$ and $ST = 0$ are exactly the conditions that result from simplifications of the conditions in Table 2.2 which we computed in Appendix A.

First we will show that f is affine equivalent to a function that has one of the following forms:

(i) $f_1(x) = x^{3q} + c_1 x^{2q+1} + c_2 x^{q+2}$,

(ii) $f_2(x) = x^{3q} + c_2 x^{q+2} + x^3$,

with $c_1, c_2 \in \mathbb{F}_q$.

If $a_3 = 0$ then f is of the form (i) and we are done. Assume $a_3 = 1$. If $a_1 = 0$ then f is of the form (ii) and we are done. If $a_1 = a_2$ then $f(x)^q = f(x)$. Thus, $f(x) \in \mathbb{F}_q$ for all $x \in \mathbb{F}_{q^2}$, which contradicts f being APN. If $a_1 \notin \{0, a_2\}$ then let $r = a_2/a_1$. Since $r \notin U$, it follows by Lemma 2.3.4 that $L(u) = u^q + ru$ is a permutation of $\mathbb{F}_{q^2}$. Also,

$$\begin{aligned} L(f(x)) &= L(x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + x^3) \\ &= x^{3q} + a_2 x^{2q+1} + a_1 x^{q+2} + x^3 + \left(\frac{a_2}{a_1}\right) x^{3q} + a_2 x^{2q+1} + \left(\frac{a_2^2}{a_1} x^{q+2}\right) + \left(\frac{a_2}{a_1} x^3\right) \\ &= \left(\frac{a_2}{a_1} + 1\right) x^{3q} + \left(a_1 + \frac{a_2^2}{a_1}\right) x^{q+2} + \left(\frac{a_2}{a_1} + 1\right) x^3. \end{aligned}$$

Dividing the above by $r + 1$ gives a function that is affine equivalent to f and of the form (ii).

Now assume $a_3 \notin \{0, 1\}$. It follows from Lemma 2.3.4 that $L(u) = a_3 u^q + u$ is a permutation of $\mathbb{F}_{q^2}$. Also,

$$\begin{aligned} L(f(x)) &= L(x^{3q} + a_1x^{2q+1} + a_2x^{q+2} + a_3x^3) \\ &= a_3^2x^{3q} + a_2a_3x^{2q+1} + a_1a_3x^{q+2} + a_3x^3 + x^{3q} + a_1x^{2q+1} + a_2x^{q+2} + a_3x^3 \\ &= (a_3^2 + 1)x^{3q} + (a_1 + a_2a_3)x^{2q+1} + (a_1a_3 + a_2)x^{q+2}. \end{aligned}$$

Dividing the above by $a_3^2 + 1$ gives a function that is affine equivalent to f and of the form (i). Therefore, if f is APN, it must be affine equivalent to a function of the form (i) or (ii).

Now we will show that APN functions of the form f_1 or f_2 are affine equivalent to $G_1(x) = x^3$ or $G_2(x) = x^{2^{m-1}+1}$.

First consider $f_1(x) = x^{3q} + c_1x^{2q+1} + c_2x^{q+2}$. Let S and T be defined relative to the coefficients c_1 and c_2 of f_1. That is,

$$S = c_1^2 + c_2^2 + c_2$$

and

$$T = c_2 + 1.$$

We consider the case of $S = 0$ and $S \neq 0$ separately. First suppose $S = 0$. If $c_2 = 0$ then $c_1 = 0$ and $f_1(x)^q = G_1(x)$. If $c_2 = 1$ then $S = c_1^2 = 0$, but by Theorem 2.4.4, we require that $\theta_1 = c_1^2 \neq 0$. So assume $c_2 \notin \{0, 1\}$. Let $b \in \mathbb{F}_q \setminus \mathbb{F}_2$ be such that $c_2 = (b+1)^2$. Then it follows from $S = 0$ that $c_1 = b^2 + b$. So f_1 is of the form

$$f_1(x) = x^{3q} + (b^2 + b)x^{2q+1} + (b+1)^2x^{q+2}. \tag{2.9}$$

Let $r \in \mathbb{F}_q$ be such that $r^3 \neq 1$. The linear maps $L_1(x) = x^q + r^3x$ and $L_2(x) = rx^q + x$ are permutations of $\mathbb{F}_{q^2}$. By Lemma 2.4.6 we have

$$L_1(G_1(L_2(x))) = (r^6 + 1)x^{3q} + (r^5 + r)x^{2q+1} + (r^4 + r^2)x^{q+2}.$$

Dividing by $r^6 + 1$, we see that G_1 is affine equivalent to

$$F_1(x) = x^{3q} + \frac{r^5 + r}{r^6 + 1}x^{2q+1} + \frac{r^4 + r^2}{r^6 + 1}x^{q+2}.$$

Letting

$$b' = \frac{(r+1)^3}{r^3 + 1} = \frac{(r+1)^2}{r^2 + r + 1}, \tag{2.10}$$

we have

$$F_1(x) = x^{3q} + (b'^2 + b')x^{2q+1} + (b' + 1)^2x^{q+2}.$$

From the trace condition of Theorem 2.4.4 applied to function f_1 in equation (2.9) we have

$$\mathrm{Tr}_1^m\left(\frac{\theta_2^{q+1}}{\theta_1^2}\right) = \mathrm{Tr}_1^m\left(\frac{\theta_2}{\theta_1}\right) = \mathrm{Tr}_1^m\left(\frac{b^2+b}{b^2}\right) = 0,$$

equivalently

$$\mathrm{Tr}_1^m\left(\frac{1}{b}\right) = \mathrm{Tr}_1^m(1).$$

To show that f_1 is affine equivalent to G_1, we must show that b' takes all values from $\mathbb{F}_q \setminus \mathbb{F}_2$ such that $\mathrm{Tr}_1^m(b'^{-1}) = \mathrm{Tr}_1^m(1)$ as r runs through $\mathbb{F}_q \setminus \mathbb{F}_4$. Let $r' = r+1$. Then

$$\begin{aligned}\mathrm{Tr}_1^m(b'^{-1}) = \mathrm{Tr}_1^m\left(\frac{r^3+1}{(r+1)^3}\right) &= \mathrm{Tr}_1^m\left(\frac{r'^3+r'^2+r'}{r'^3}\right)\\ &= \mathrm{Tr}_1^m(1) + \mathrm{Tr}_1^m\left(\frac{1}{r'}\right) + \mathrm{Tr}_1^m\left(\frac{1}{r'^2}\right) = \mathrm{Tr}_1^m(1).\end{aligned}$$

For any fixed value of b', equation (2.10) can be written as a quadratic equation in variable r, hence any b' has at most two preimages r. It then follows by a counting argument, which has to be performed separately for m odd and m even, that all values b' such that $\mathrm{Tr}_1^m(b'^{-1}) = \mathrm{Tr}_1^m(1)$ are produced from a suitable r. In both cases we have to note that $b' = 1$ has exactly one preimage $r = 0$. It follows that if $S = 0$, then f_1 is affine equivalent to G_1.

Now suppose $S \neq 0$, then from Theorem 2.4.4 it follows that m is even and $T = c_2 + 1 = 0$. Then $c_2 = 1$ and

$$f_1(x) = x^{3q} + c_1 x^{2q+1} + x^{q+2}.$$

By Theorem 2.4.4, we require $\theta_1 = c_1^2 \neq 0$, that is, $c_1 \neq 0$. We also require the trace condition

$$\mathrm{Tr}_1^m\left(\frac{\theta_2^{q+1}}{\theta_2^2}\right) = \mathrm{Tr}_1^m\left(\frac{1}{c_1}\right) = 0.$$

Let $r \in \mathbb{F}_q \setminus \mathbb{F}_2$ so that $L(x) = x^q + rx$ is a linear permutation of $\mathbb{F}_{q^2}$. By Lemma 2.4.5, $G_2(x)$ is affine equivalent to $G_2'(x) = x^{2q+1}$ and by Lemma 2.4.6 we have

$$L(G_2'(L(x))) = (r^3+r)x^{3q} + (r^4+1)x^{2q+1} + (r^3+r)x^{q+2}.$$

After dividing by $r^3 + r$, we see that G_2 is affine equivalent to

$$F_1(x) = x^{3q} + dx^{2q+1} + x^{q+2}$$

where

$$d = \frac{(r+1)^2}{r}.$$

Let $r' = r + 1$ so that r' is also in $\mathbb{F}_q \setminus \mathbb{F}_2$. We have

$$\mathrm{Tr}_1^m\left(\frac{1}{d}\right) = \mathrm{Tr}_1^m\left(\frac{r}{(r+1)^2}\right) = \mathrm{Tr}_1^m\left(\frac{r'+1}{r'^2}\right) = \mathrm{Tr}_1^m\left(\frac{1}{r'}\right) + \mathrm{Tr}_1^m\left(\frac{1}{r'^2}\right) = 0.$$

Since each d is produced by at most two values of r, it follows again by a counting argument that d takes all values in $\mathbb{F}_q^*$ such that $\mathrm{Tr}_1^m(d^{-1}) = 0$. Thus f_1 is affine equivalent to G_2 when $S \neq 0$.

Finally, we consider $f_2(x) = x^{3q} + c_2x^{q+2} + x^3$. Let S and T be defined relative to the coefficient c_2 of f_2. That is,

$$S = c_2^2 + c_2$$

and

$$T = c_2.$$

We note that $\theta_1 = c_2^2$ must be nonzero. Since $T = c_2 \neq 0$ we must also have $S = c_2^2 + c_2 = 0$. Therefore $c_2 = 1$ and it follows that $\theta_1 = \theta_2 = 1$. From the trace condition, we have

$$0 = \mathrm{Tr}_1^m\left(\frac{\theta_2^{q+1}}{\theta_1^2}\right) = \mathrm{Tr}_1^m\left(\frac{\theta_2}{\theta_1}\right) = \mathrm{Tr}_1^m(1).$$

Therefore m must be even, hence $\mathbb{F}_q$ contains a primitive cube root of unity ω. Let $L(x) = x^q + \omega x$ which is a permutation of $\mathbb{F}_{q^2}$ since $\omega \notin U$ when m is even. By Lemma 2.4.6 we have

$$L(G_1(L(x))) = (\omega+1)x^{3q} + (\omega+1)x^{q+2} + (\omega+1)x^3.$$

So f_2 is affine equivalent to G_1.

This completes the proof of Theorem 2.4.2. □

2.5 Walsh zeros

Browning et al. [7] introduced a method that, assuming certain conditions are satisfied, constructs a permutation that is CCZ-equivalent to a given function. In particular if the given function is APN then this allows the possibility of finding an APN permutation. In Proposition 2.5.7 we present this method in a different but equivalent form, using the concept of Walsh zero spaces. We also include a proof of the proposition, which is contained only implicitly in [7], because it allows one to *explicitly construct* a permutation CCZ-equivalent to the given function.

The Walsh transform is well known and is used often in the area of mathematics of digital communications. The Walsh transform is used to measures the correlation between a function $f(x)$ and an affine function $ax+c$. See Section 2.3.3 of [11] for a detailed introduction to the Walsh transform and Chapter 5 of [11] for an up-to-date overview of how the Walsh transform relates to the study of Boolean and APN functions.

Definition 2.5.1. *The* Walsh transform of a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is given by

$$\mathcal{W}_f(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax + bf(x))}.$$

The *Walsh spectrum* of f is the multiset of values of $\mathcal{W}_f(a, b)$ for all $a, b \in \mathbb{F}_{2^n}$.

Originally, the Walsh transform was used to study Boolean functions and the interest was in finding the absolute values that the Walsh transform can take, in particular in collectively minimizing the amplitudes of the Walsh spectrum. This was the motivation for the original Gold paper [18] in which the application was finding sequences with favourable correlation properties. As such, there is much infrastructure surrounding the Walsh transform that is already in place. For our research, we are only interested in the Walsh zeros.

Definition 2.5.2. *Given a function* $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$*, an element* $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ *is a* Walsh zero of f if $\mathcal{W}_f(a, b) = 0$.

Definition 2.5.3. *Let* f *be a function from* $\mathbb{F}_{2^n}$ *to* $\mathbb{F}_{2^n}$*. Suppose that* Z *is an* $\mathbb{F}_2$*-linear subspace of* $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ *such that* $\dim_{\mathbb{F}_2} Z = n$ *and each element of* Z *other than* $(0, 0)$ *is a Walsh zero of* f*. We say that* Z *is a* Walsh zero space of f (WZ space of f).

Definition 2.5.4. *For a given function* $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$*, we say that two WZ spaces* Y, Z *of* f *intersect trivially if* $Y \cap Z = \{(0, 0)\}$*. We call* $\{Y, Z\}$ *a* TI pair *(trivially intersecting pair).*

Suppose $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Since $\mathrm{Tr}(ax)$ is a balanced function of x, the space

$$Z_{[n,0]} = \{(a, 0) : a \in \mathbb{F}_{2^n}\}$$

is a WZ space of f. Furthermore,

$$Z_{[0,n]} = \{(0, b) : b \in \mathbb{F}_{2^n}\}$$

is a WZ space of f if and only if f is a permutation, since then $\mathrm{Tr}(bf(x))$ is a balanced function of x when $b \neq 0$. We call these two spaces *trivial* WZ spaces. Note also that $\{Z_{[n,0]}, Z_{[0,n]}\}$ is a TI pair.

We will also require the notion of dual bases for $\mathbb{F}_{2^n}$ (see page 58 of [25]).

Definition 2.5.5. *Two bases* $\{\alpha_1, \ldots, \alpha_n\}$ *and* $\{\beta_1, \ldots, \beta_n\}$ *of* $\mathbb{F}_{2^n}$ *over* $\mathbb{F}_2$ *are called* dual bases if $\mathrm{Tr}(\alpha_i \beta_j) = \delta_{i,j}$ for $1 \leq i, j \leq n$ where $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise.

Proposition 2.5.6. *For any basis* $\{\alpha_1, \ldots, \alpha_n\}$ *of* $\mathbb{F}_{2^n}$ *over* $\mathbb{F}_2$ *there exists a unique dual basis* $\{\beta_1, \ldots, \beta_n\}$*.*

We now present a method from Browning et al. [7] which we formalize in terms of Walsh zero spaces. The proof given below is taken from our joint paper with Dr. Lisoněk [14]. Because there is no originality other than reformulating the result of [7], we included the following proposition as well as some other ones in this background chapter of the thesis.

Proposition 2.5.7. *Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. If there exist two WZ spaces of f that intersect trivially, then f is CCZ-equivalent to an APN permutation of $\mathbb{F}_{2^n}$.*

Proof. Without loss of generality we can assume that $f(0) = 0$, since this can be achieved by an affine transformation which is a special kind of CCZ-equivalence.

Let $\{\alpha_1, \dots, \alpha_n\}$ and $\{\beta_1, \dots, \beta_n\}$ be two dual bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, that is, $\mathrm{Tr}(\alpha_i\beta_j) = \delta_{i,j}$ where for $1 \le i, j \le n$ we let $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ otherwise. Let the nonzero elements of $\mathbb{F}_{2^n}$ be labelled $x_1, \dots, x_{2^n-1}$.

Let $G = \begin{pmatrix} G_1 \\ G_2 \end{pmatrix}$ be a $(2n) \times (2^n - 1)$ matrix over $\mathbb{F}_2$ where G_1 and G_2 are $n \times (2^n - 1)$ matrices over $\mathbb{F}_2$ defined as follows. The entry in row i and column j of G_1 is $\mathrm{Tr}(\alpha_i x_j)$. With respect to the basis $\{\beta_1, \dots, \beta_n\}$ we have

$$x_j = \sum_{k=1}^{n} c_k \beta_k$$

where $c_1, \dots, c_n \in \mathbb{F}_2$. Then the entry in row i and column j of G_1 is

$$\mathrm{Tr}(\alpha_i x_j) = \mathrm{Tr}\left(\alpha_i \sum_{k=1}^{n} c_k \beta_k\right) = \sum_{k=1}^{n} c_k \mathrm{Tr}(\alpha_i \beta_k) = c_i$$

by the property of the dual bases. The entry in row i and column j of G_2 is $\mathrm{Tr}(\alpha_i f(x_j))$. Similarly as above, we write $f(x_j)$ with respect to the basis $\{\beta_1, \dots, \beta_n\}$. Therefore the j-th column of G is of the form $\begin{pmatrix} x_j \\ f(x_j) \end{pmatrix}$ where x_j and $f(x_j)$ are represented as n-dimensional column vectors with respect to the basis $\{\beta_1, \dots, \beta_n\}$. Let C be the binary linear code which is the row space of G. Each codeword of C is of the form $\mathrm{Tr}(rx_j + sf(x_j))_{j=1,\dots,2^n-1}$ where r, s are fixed elements of $\mathbb{F}_{2^n}$.

Let S and T be the two given trivially intersecting WZ spaces, and let $B_1 = \{(a_1, b_1), \dots, (a_n, b_n)\}$ and $B_2 = \{(a_{n+1}, b_{n+1}), \dots, (a_{2n}, b_{2n})\}$ be their bases. Note that $B_1 \cup B_2$ is a basis for $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.

Let $G' = \begin{pmatrix} G'_1 \\ G'_2 \end{pmatrix}$ be a $(2n) \times (2^n - 1)$ matrix over $\mathbb{F}_2$ where G'_1 and G'_2 are $n \times (2^n - 1)$ matrices over $\mathbb{F}_2$ defined as follows. The entry in row i and column j of G'_1 is $\mathrm{Tr}(a_i x_j + b_i f(x_j))$. The entry in row i and column j of G'_2 is $\mathrm{Tr}(a_{n+i} x_j + b_{n+i} f(x_j))$.

For $i = 1, 2$ let C'_i be the row space of G'_i. Since S and T are WZ spaces for f, each nonzero codeword of C'_i has weight 2^{n-1} for $i = 1, 2$. Thus C'_1, C'_2 are simplex codes S_n, and

G_1', G_2' are formed by pairwise distinct nonzero columns. Thus, with respect to the basis $\{\beta_1, \ldots, \beta_n\}$, the columns of G' can be viewed as $\begin{pmatrix} x \\ g(x) \end{pmatrix}$ where x runs through all nonzero elements of $\mathbb{F}_{2^n}$ and $g(x) \in \mathbb{F}_{2^n}$. After letting $g(0) = 0$ we see that g is a permutation of $\mathbb{F}_{2^n}$.

Let C' be the rowspace of G'. Since $B_1 \cup B_2$ is a basis for $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, each codeword of C' is of the form $\mathrm{Tr}(rx_j + sf(x_j))_{j=1,\ldots,2^n-1}$ where r, s are fixed elements of $\mathbb{F}_{2^n}$. Thus the codes C and C' are equal, and functions f and g are CCZ-equivalent by Proposition 2.3.12. □

Chapter 3

Kim-type APN permutations

It has been 12 years since the discovery of APN permutations of $\mathbb{F}_{2^6}$ by Browning et al. [7]. To date, no other APN permutations in even dimensions have been found despite immense interest in solving this aptly named "Big APN Problem". There was hope that by generalizing the Kim function used by Browning et al., one might find more APN permutations over $\mathbb{F}_{2^{2m}}$ for $m \geq 4$. Recall from Chapter 2 that one such generalization, called Kim-type functions, have the form

$$f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$$

with $q = 2^m$. Carlet's open problem (see Problem 2.4.1) asked to find more Kim-type functions that are also APN. The highly technical paper of Li, Li, Helleseth, and Qu [24] resolved this by finding exact conditions on $a_1, a_2, a_3 \in \mathbb{F}_{q^2}$, for $m \geq 4$ that determine if f is APN or not. The arXiv version of [24] appeared in July 2020 and triggered a question of immediate importance as to whether it enables a generalization of Theorem 2.4.2 to the case when $a_1, a_2, a_3 \in \mathbb{F}_{q^2}$. Indeed, by performing linear transformations on $f(x)$ we were able to restrict the attention from this general case to several special cases which we were able to resolve completely using the results of [24]. By case analysis we were able to either reduce to the case of $a_1, a_2, a_3 \in \mathbb{F}_q$ and apply Theorem 2.4.2, or apply suitable linear permutations to show that here too f is affine equivalent to a Gold function, or arrive at a contradiction by showing that f is not APN. In this way, in Chapter 3 we prove that Kim-type APN functions in their most general form are affine equivalent to one of two well known Gold functions $G_1(x) = x^3$ or $G_2(x) = x^{2^{m-1}+1}$. This research is described in the remainder of this chapter. A recent result of Göloğlu and Langevin [20] proves that, for even n, Gold APN functions are never CCZ-equivalent to permutations. Hence, Kim-type functions with $m \geq 4$ are never CCZ-equivalent to APN permutations, thereby ending one approach to the Big APN Problem. On the other hand, there is still a possibility for further research after enriching the Kim-type functions by adding more monomials to them [26].

The material in this chapter is joint work with Dr. Lisoněk and has been published in the Springer journal Cryptography and Communications (special issue for the conference Boolean Functions and their Applications 2020) [15]. Dr. Lisoněk suggested some of the formulations of the propositions and theorems and I contributed the remaining ones. We worked together on the proofs, which are quite technical and would be hard to construct just by a single author. I wrote Magma scripts to verify all nontrivial calculations for this chapter (see Appendix B). Additionally, in the thesis I add some lemmas which have been moved to Chapter 2, and I work out the proofs in much more detail. I also rearrange the order of presentation to make it easier to follow, and I add a numerical example to show that some very technical parts of the proof are unavoidable since the APN functions addressed in those places in fact do exist.

3.1 Preliminaries

For the rest of this chapter we assume $m \geq 4$ is an integer, $n = 2m$, and $q = 2^m$ so that $\mathbb{F}_q$ is subfield of $\mathbb{F}_{q^2}$. Recall from Chapter 2 that the unit circle $U = \{z \in \mathbb{F}_{q^2} : z^{q+1} = 1\}$ is a cyclic subgroup of $\mathbb{F}_{q^2}^*$ and that $\mathbb{F}_q \cap U = \{1\}$. For $z \in U$ we have $z^q = z^{-1}$. This computational rule is of critical importance in many proofs in this chapter. Note in particular that Kim-type functions have exponents containing q. Since q is a power of 2 (characteristic of the field), powers of q distribute over addition. To give an illustration of these computational rules, consider a rational function $f : \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ with coefficients in $\mathbb{F}_q$. If $a \in \mathbb{F}_q$ and $z \in U$ then $f(a, z)^q = f(a^q, z^q) = f(a, z^{-1})$. Manipulating rational functions in this way will be needed for many of the following propositions. They enable us to eliminate exponents containing q from the expressions in our proofs, which is needed since computer algebra systems cannot handle general exponents q. Expressions involving exponents containing q describe infinitely many functions but after eliminating q (if possible) they are reduced to a single expression. Lemma 2.1.8 is useful for this purpose. Although it introduces two variables in place of one, the new variables are restricted to $\mathbb{F}_q$ or U and simplifications are achieved. The terms involving exponent q must be simplified by hand and afterwards a computer algebra system, such as Magma, can handle the rest.

Example 3.1.1. *It follows from Lemma 2.1.9 that $\mathbb{F}_{q^2}$ contains a primitive cube root of unity, say ω. Suppose $f(a, u, z)$ is a rational function with variables ranging over $\mathbb{F}_{q^2}$ given by*

$$f(a, u, z) = \frac{\omega^2 a}{u + z} + \frac{a + z^2}{u + \omega}$$

and suppose that we would like to express the term $f(a, u, z)^q$ in a form that is free of q. Under the general assumptions $a, u, z \in \mathbb{F}_{q^2}$, we have

$$f(a, u, z)^q = \left(\frac{\omega^2 a}{u + z}\right)^q + \left(\frac{a + z^2}{u + \omega}\right)^q = \frac{\omega^{2q} a^q}{(u + z)^q} + \frac{(a + z^2)^q}{(u + \omega)^q} = \frac{\omega^2 a^q}{u^q + z^q} + \frac{a^q + z^{2q}}{u^q + \omega}$$

and no further simplification is possible. On the other hand, if we assume $a \in \mathbb{F}_q$ and $u, z \in U$ then

$$f(a,u,z)^q = \frac{\omega^2 a}{u^{-1}+z^{-1}} + \frac{a+z^{-2}}{u^{-1}+\omega}.$$

Note that once the assumptions on $a, u,$ and z are in place, a significant simplification was achieved. Specifically the exponents containing q were removed.

3.2 Main result

Recall from Theorem 2.4.2 that Kim-type functions with coefficients belonging to $\mathbb{F}_q$ are affine equivalent to Gold functions, that is, they do not produce any new APN functions. We state the main result of this chapter, which generalizes Theorem 2.4.2 by allowing coefficients of the Kim-type function to be in $\mathbb{F}_{q^2}$.

Theorem 3.2.1. *Suppose that $m \geq 4$ is an integer and let $q = 2^m$. Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$ where $a_1, a_2, a_3 \in \mathbb{F}_{q^2}$. If f is APN, then f is affine equivalent to $G_1(x) = x^3$ or f is affine equivalent to $G_2(x) = x^{2^{m-1}+1}$.*

The proof of Theorem 3.2.1 follows from applying the propositions presented in the rest of this chapter. We start by explaining the reasons for following our particular proof strategy, and then we give a high level brief outline of the proof of Theorem 3.2.1, which is visualized in Figure 3.1. The details of the proof then follow in the rest of the chapter.

3.2.1 Strategy of the proof

Of course, one of the main tools we will use in our proof is affine equivalence. Recall from Chapter 2 that constructing affine equivalent functions requires affine permutations of $\mathbb{F}_{q^2}$. In this chapter we will only use linear permutations of $\mathbb{F}_{q^2}$. The resulting equivalence is called linear equivalence but we will use the more general term affine equivalence since this is used more commonly in the area of APN functions, and it still preserves the invariants that we care about. It follows from Lemmas 2.3.3 and 2.3.4 that linear transformations of the form $L(x) = x^{2^{m+k}} + tx^{2^k}$ are permutations of $\mathbb{F}_{q^2}$ if and only if $t \notin U$. We will often use a chain of these transformations as well as the affine permutation $x \mapsto ax$ for $a \in \mathbb{F}_{q^2}^*$.

Recall from Lemma 2.4.6 that applying an outer transformation of the form $L_1(x) = x^q + tx$ and an inner transformation of the form $L_2(x) = rx^q + sx$ to either one of the Gold functions $G_1(x) = x^3$ or $G_2'(x) = x^{2q+1}$ and expanding, results in a polynomial with Kim-type exponents, for any $r, s, t \in \mathbb{F}_{q^2}$. Similarly, applying transformations of the form of L_1 and L_2 to Kim-type polynomials and expanding results only in polynomials that have Kim-type exponents. Therefore, to find a suitable choice of r, s and t we will expand expressions and compare coefficients. For example, to construct an affine equivalence between G_1 and a Kim-type APN function f, we fully expand $L_1(G_1(L_2(x)))$ and compare its coefficients to the coefficients a_1, a_2, a_3 of $f(x)$. If the expressions are simple enough, we will simply use trial and error along with pattern matching. Note that there are three degrees of freedom for r, s, t as well as three degrees of freedom for a_1, a_2, a_3. At least at the first glance, it looks hopeful that we may be able to construct suitable linear transformations. Indeed, by Lemma 2.3.4 the proportion of the transformations which are not permutations is $|U|/(q^2-1) \approx 1/q$, which tends to zero with growing q.

As the characterizations of APNness of f in Theorem 2.4.4 are fairly complex expressions, we first explore whether some simplifications are possible, keeping in mind that we are allowed to consider a function affinely equivalent to f instead. Such simplifications can be achieved by letting one of the coefficients vanish, as long as that can be done in full generality, that is, by using affine equivalence. The motivation for the particular strategy of the proof that we chose was the observation that letting $a_2 = 0$ in the Kim-type function $f(x) = x^{3q} + a_1x^{2q+1} + a_2x^{q+2} + a_3x^3$ achieves the most simplifications in the APN conditions of Theorem 2.4.4. Thus we analyzed this case first, and the rest of the proof was essentially forced by covering the remaining special cases.

Before going through with the effort of analyzing the case of $a_2 = 0$, it would be nice to know how much work will remain to be done after. Fortunately it turns out that we can transform a general Kim-type function to one with $a_2 = 0$, except in two special cases characterized below.

Proposition 3.2.2. *Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1x^{2q+1} + a_2x^{q+2} + a_3x^3$ where $a_1 \in \mathbb{F}_q$, $a_2 \in \mathbb{F}_{q^2}^*$ and $a_3 \in \mathbb{F}_{q^2}$. If $a_1/a_2 \notin U$ and $a_1/a_2 \neq a_3^q$, then f is affine equivalent to $h(x) = x^{3q} + a_1'x^{2q+1} + a_3'x^3$ where $a_1' \in \mathbb{F}_q$ and $a_3' \in \mathbb{F}_{q^2}$.*

Proof. Let $t = a_1/a_2$. Since $t \notin U$, $L(z) = z^q + tz$ is a bijection of $\mathbb{F}_{q^2}$ by Lemma 2.3.4. Let $h_0(x) = L(f(x))$ so that

$$h_0(x) = \left(\frac{a_1}{a_2} + a_3^q\right) x^{3q} + \left(\frac{a_1^2}{a_2} + a_2^q\right) x^{2q+1} + \left(\frac{a_1a_3}{a_2} + 1\right) x^3$$

where f and h_0 are affine equivalent. Now let

$$h_1(x) = \left(\frac{a_1}{a_2} + a_3^q\right)^{-1} h_0(x)$$

so that f and h_1 are also affine equivalent. The result follows from applying Lemma 2.4.3 to h_1. □

It turned out that one of the two remaining cases in Proposition 3.2.2 produced Kim-type APN functions with complex coefficients and resolving this case ended up being an extensive portion of the proof of Theorem 3.2.1. At the outset we could not have been sure that we would resolve this case completely but throughout the focus was on isolating the possible Kim-type APN functions as much as possible. Fortunately we were able to resolve all of these cases.

3.2.2 Outline of the proof

Assume that $m \geq 4$ is an integer and let $q = 2^m$. Let $f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$ be a Kim-type function where $a_1, a_2, a_3 \in \mathbb{F}_{q^2}$, and assume that f is APN. By Lemma 2.4.3, f is affine equivalent to $f'(x) = x^{3q} + a_1' x^{2q+1} + a_2' x^{q+2} + a_3' x^3$ where $a_1' \in \mathbb{F}_q$ and $a_2', a_3' \in \mathbb{F}_{q^2}$.

Apply Proposition 3.2.2 to f'. First suppose that the transformation succeeded in producing $a_2' = 0$. Then we will show in Propositions 3.2.4 and 3.2.5 that f' is affine equivalent to $G_1(x) = x^3$ or $G_2(x) = x^{2^{m-1}+1}$.

Now suppose that the transformation to $a_2' = 0$ was not possible. Then we know that there are two cases to be analyzed. First let $a_1'/a_2' \in U$. In Proposition 3.2.6 we will show that m is even, and furthermore either $a_1', a_2', a_3' \in \mathbb{F}_q$ (which reduces to Theorem 2.4.2) or there exist $u, z \in U$ such that a_1', a_2', a_3' have the form as given in the proposition. In the latter case, we will show that f' is affine equivalent to G_1 or to G_2 in Proposition 3.2.8. Suppose that $a_2' \neq 0$ and $a_1'/a_2' = (a_3')^q$, then in Proposition 3.2.9 we will show that the function f' is not APN, hence this case can not occur.

Since by now all possible cases have been exhausted, the outline of the proof of Theorem 3.2.1 is complete.

The visualization of the proof given in Figure 3.1 is another possible view of this chain of arguments, in fact the one given in the paper [15]. The diagram gives a more clear and succinct representation of this process while the version of the proof given in this thesis may be more intuitive.

3.2.3 Case $a_2 = 0$

In the next three propositions we show that a Kim-type APN functions with $a_2 = 0$ must be affine equivalent to a Gold function.

Proposition 3.2.3. *Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1 x^{2q+1} + a_3 x^3$ where $a_1, a_3 \in \mathbb{F}_{q^2}$ and $a_1 = 0$ or $a_3 = 0$. If f is APN, then f is affine equivalent to $G_1(x) = x^3$.*

Proof. Suppose $a_1 = a_2 = 0$. Then $\theta_1 = a_3^{q+1} + 1$ and if f is APN then by Theorem 2.4.4, $\theta_1 \neq 0$ which implies $a_3 \notin U$. Thus, $a_3^q \notin U$ and $L(x) = x^q + a_3^q x$ is a permutation of $\mathbb{F}_{q^2}$. Now

$$\begin{aligned} L(f(x)) &= (x^{3q} + a_3 x^3)^q + a_3^q (x^{3q} + a_3 x^3) \\ &= (a_3^{q+1} + 1) x^3 \end{aligned}$$

and it follows that $f(x)$ is affine equivalent to $G_1(x) = x^3$.

Suppose $a_2 = a_3 = 0$. By Lemma 2.4.3 we can assume $a_1 \in \mathbb{F}_q$. Then $\theta_1 = a_1^2 + 1$, $\theta_2 = a_1$, $\theta_3 = 0$, and $\theta_4 = a_1^2$. Since f is APN it must satisfy the conditions given in Theorem 2.4.4.

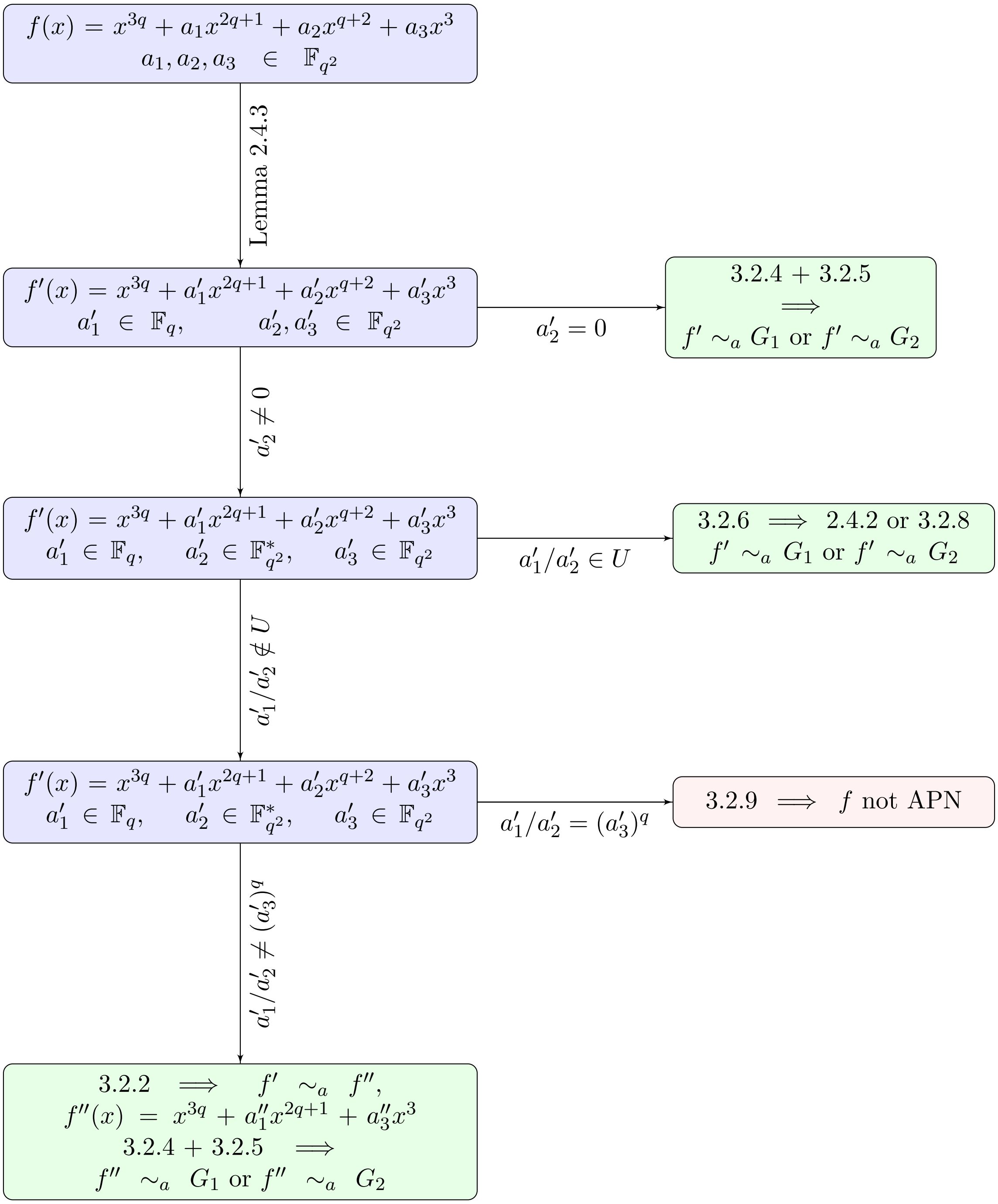
$f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$
$a_1, a_2, a_3 \in \mathbb{F}_{q^2}$
Lemma 2.4.3
$f'(x) = x^{3q} + a_1' x^{2q+1} + a_2' x^{q+2} + a_3' x^3$
$a_1' \in \mathbb{F}_q, \quad a_2', a_3' \in \mathbb{F}_{q^2}$
$a_2' = 0$
3.2.4 + 3.2.5 $\Longrightarrow$ $f' \sim_a G_1$ or $f' \sim_a G_2$
$a_2' \neq 0$
$f'(x) = x^{3q} + a_1' x^{2q+1} + a_2' x^{q+2} + a_3' x^3$
$a_1' \in \mathbb{F}_q, \quad a_2' \in \mathbb{F}_{q^2}^*, \quad a_3' \in \mathbb{F}_{q^2}$
$a_1'/a_2' \in U$
3.2.6 $\Longrightarrow$ 2.4.2 or 3.2.8
$f' \sim_a G_1$ or $f' \sim_a G_2$
$a_1'/a_2' \notin U$
$f'(x) = x^{3q} + a_1' x^{2q+1} + a_2' x^{q+2} + a_3' x^3$
$a_1' \in \mathbb{F}_q, \quad a_2' \in \mathbb{F}_{q^2}^*, \quad a_3' \in \mathbb{F}_{q^2}$
$a_1'/a_2' = (a_3')^q$
3.2.9 $\Longrightarrow$ f not APN
$a_1'/a_2' \neq (a_3')^q$
3.2.2 $\Longrightarrow$ $f' \sim_a f''$,
$f''(x) = x^{3q} + a_1'' x^{2q+1} + a_3'' x^3$
3.2.4 + 3.2.5 $\Longrightarrow$
$f'' \sim_a G_1$ or $f'' \sim_a G_2$

Figure 3.1: Diagram for proof of Theorem 3.2.1.

The third condition of Γ_1 (2.5) becomes $0 = \theta_1\theta_4+\theta_2^{q+1} = (a_1^2+1)a_1^2+a_1^{q+1} = (a_1^2+1)a_1^2+a_1^2 = a_1^4$. So $a_1 = 0$. The third condition of Γ_2 (2.6) becomes $0 = \theta_2^{2q} = a_1^2$, and again $a_1 = 0$. In both cases we have $f(x) = x^{3q}$ which is affine equivalent to $G_1(x) = x^3$. □

Proposition 3.2.4. *Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1x^{2q+1} + a_3x^3$ where $a_1 \in \mathbb{F}_q$ and $a_3 \in \mathbb{F}_{q^2}$. If $(a_1, 0, a_3) \in \Gamma_1$ as defined in equation (2.5) then f is affine equivalent to $G_1(x) = x^3$ or f is affine equivalent to $G_2(x) = x^{2^{m-1}+1}$.*

Proof. The cases of $a_1 = 0$ or $a_3 = 0$ are covered by Proposition 3.2.3, so assume $a_1 \neq 0$ and $a_3 \neq 0$. By Lemma 2.1.8 we can write a_3 uniquely as $a_3 = yz$ with $y \in \mathbb{F}_q^*$ and $z \in U$. We have

$$\begin{aligned}
\theta_1 &= a_1^2 + a_3^{q+1} + 1 = a_1^2 + y^2 + 1,\\
\theta_2 &= a_1,\\
\theta_3 &= a_1a_3^q = a_1yz^q,\\
\theta_4 &= a_1^2.
\end{aligned}$$

The second condition of Γ_1 becomes

$$\mathrm{Tr}_1^m\left(\frac{\theta_2^{q+1}}{\theta_1^2}\right) = \mathrm{Tr}_1^m\left(\frac{a_1^2}{(a_1^2+y^2+1)^2}\right) = \mathrm{Tr}_1^m\left(\frac{a_1}{a_1^2+y^2+1}\right) = 0.$$

By Lemma 2.1.3 there exists $t \in \mathbb{F}_q$ such that

$$(t^2 + t)(a_1^2 + y^2 + 1) + a_1 = 0. \tag{3.1}$$

The third condition of Γ_1 becomes

$$\begin{aligned}
0 &= \theta_1^2\theta_4 + \theta_1\theta_2^{q+1} + \theta_2^2\theta_3 + \theta_2^{2q}\theta_3^q\\
&= (a_1^2 + y^2 + 1)^2a_1^2 + (a_1^2 + y^2 + 1)a_1^{q+1} + a_1^2(a_1yz^q) + a_1^{2q}(a_1yz^q)^q\\
&= (a_1^4 + y^4 + 1)a_1^2 + (a_1^2 + y^2 + 1)a_1^2 + a_1^2(a_1yz^{-1}) + a_1^2(a_1yz).
\end{aligned}$$

Multiplying by za_1^{-2} and simplifying gives

$$a_1yz^2 + (a_1^4 + a_1^2 + y^4 + y^2)z + a_1y = 0. \tag{3.2}$$

The resultant of equations (3.1) and (3.2) with respect to y is

$$a_1^2(Az^2 + B)(Bz^2 + A)$$

where $A = (a_1t+t+1)t^3$ and $B = (a_1t+a_1+t)(t+1)^3$. See Appendix B for this computation.

If $z = 1$ then $a_3 \in \mathbb{F}_q$ and by Theorem 2.4.2 $f(x)$ is affine equivalent to $G_1(x)$ or $G_2(x)$. So assume $z \in U\backslash\{1\}$ which implies $z \notin \mathbb{F}_q$ and $z^2 \notin \mathbb{F}_q$. Since $A, B \in \mathbb{F}_q$, the resultant can vanish only if $A = B = 0$. Simplifying $A = B$ gives $a_1 = t^2 + t$ and substituting this into $A = 0$ gives $(t + 1)^3 t^3 = 0$. Thus $t = 0$ or $t = 1$ and in both cases $a_1 = 0$, a contradiction. As we have exhausted all cases, this completes the proof. □

Proposition 3.2.5. *Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1 x^{2q+1} + a_3 x^3$ where $a_1 \in \mathbb{F}_q$ and $a_3 \in \mathbb{F}_{q^2}$. If $(a_1, 0, a_3) \in \Gamma_2$ as defined in equation (2.6) then f is affine equivalent to $G_1(x) = x^3$ or f is affine equivalent to $G_2(x) = x^{2^{m-1}+1}$.*

Proof. Note that $\theta_1, \theta_2, \theta_3, \theta_4$ are the same as in the proof of Proposition 3.2.4. The third condition of Γ_2 becomes

$$\begin{aligned} 0 &= \theta_1^2\theta_3 + \theta_1\theta_2^{2q} + \theta_2^2\theta_3 + \theta_2^{2q}\theta_3^q \\ &= (a_1^2 + y^2 + 1)^2 a_1 y z^q + (a_1^2 + y^2 + 1)a_1^{2q} + a_1^2(a_1 y z^q) + a_1^{2q}(a_1 y z^q)^q \\ &= (a_1^2 + y^2 + 1)^2 a_1 y z^{-1} + (a_1^2 + y^2 + 1)a_1^2 + a_1^3 y z^{-1} + a_1^3 y z. \end{aligned}$$

Multiplying by $a_1^{-1} z$ gives

$$\begin{aligned} 0 &= (a_1^2 y)z^2 + (a_1^3 + a_1 y^2 + a_1)z + (a_1^4 y + a_1^2 y + y^5 + y) \\ &= Az^2 + Bz + C \end{aligned}$$

where $A = a_1^2 y$, $B = a_1^3 + a_1 y^2 + a_1$, and $C = a_1^4 y + a_1^2 y + y^5 + y$. If $z = 1$ then $a_3 \in \mathbb{F}_q$ and by Theorem 2.4.2 f is affine equivalent to G_1 or G_2. If $z \in U\backslash\{1\}$ then by Lemma 2.1.10 we have $A = C$. Hence,

$$A + C = y(a_1 + y + 1)^4 = 0.$$

If $y = 0$ then $a_3 \in \mathbb{F}_q$ and the result follows from Theorem 2.4.2. On the other hand, if $(a_1 + y + 1)^4 = 0$ then $\theta_1 = (a_1 + y + 1)^2 = 0$ and $(a_1, 0, a_3) \notin \Gamma_2$. □

3.2.4 Case $a_2 \neq 0$

Having covered the case $a_2 = 0$, we now turn our attention to the cases where it was impossible to drive the original function to the form $a_2 = 0$ by linear permutations. The next three propositions deal with the case of $a_2 \neq 0$.

Proposition 3.2.6. *Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$ where $a_1 \in \mathbb{F}_q$, $a_2 \in \mathbb{F}_{q^2}^*$ and $a_3 \in \mathbb{F}_{q^2}$, and assume that $a_1/a_2 \in U$. If f is APN, then m is even, and furthermore $a_1, a_2, a_3 \in \mathbb{F}_q$ or there exist $u, z \in U$ such that*

$$\begin{aligned} a_1 &= \frac{(u^3+z)^2}{u(u^2+z)^2}, \\ a_2 &= \frac{(u^3+z)^2}{(u^2+z)^2}, \\ a_3 &= \frac{uz^2(u+1)^2}{(u^2+z)^2}. \end{aligned}$$

Proof. Under the assumptions listed in the proposition, we first prove that $(a_1, a_2, a_3) \notin \Gamma_1$ which, by Theorem 2.4.4, implies m is even and $(a_1, a_2, a_3) \in \Gamma_2$. Next we prove that $(a_1, a_2, a_3) \in \Gamma_2$ implies the conclusions given in the statement.

If $a_1/a_2 \in U$ then $a_1 \neq 0$. Since U forms a group under multiplication, there exists $u \in U$ such that $a_2 = a_1 u$. By Lemma 2.1.8 we can write a_3 uniquely as $a_3 = yz$ with $y \in \mathbb{F}_q$ and $z \in U$. We have

$$\begin{aligned} \theta_1 &= a_1^2 + (a_1u)^{q+1} + (yz)^{q+1} + 1 = y^2 + 1, \\ \theta_2 &= a_1 + (a_1u)^q yz = a_1 + a_1 y u^q z, \\ \theta_3 &= (a_1u)^q + a_1(yz)^q = a_1u^q + a_1yz^q, \\ \theta_4 &= a_1^2 + (a_1u)^{q+1} = 0. \end{aligned}$$

If $y = 1$ then $\theta_1 = 0$ and $(a_1, a_2, a_3) \notin \Gamma_1 \cup \Gamma_2$ which, by Theorem 2.4.4 contradicts f being APN. So assume $y \neq 1$.

The third condition of Γ_1 becomes $\theta_1\theta_2^{q+1} + \theta_2^2\theta_3 + \theta_2^{2q}\theta_3^q = 0$. Looking at each term individually, we have

$$\begin{aligned} \theta_1\theta_2^{q+1} &= (y^2+1)(a_1 + a_1yu^qz)^{q+1} = (y^2+1)(a_1 + a_1yuz^q)(a_1 + a_1yu^qz), \\ \theta_2^2\theta_3 &= (a_1 + a_1yu^qz)^2(a_1u^q + a_1yz^q) = (a_1^2 + a_1^2y^2u^{2q}z^2)(a_1u^q + a_1yz^q), \\ \theta_2^{2q}\theta_3^q &= (a_1 + a_1yu^qz)^{2q}(a_1u^q + a_1yz^q)^q = (a_1^2 + a_1^2y^2u^2z^{2q})(a_1u + a_1yz). \end{aligned}$$

We can now factorize $\theta_1\theta_2^{q+1} + \theta_2^2\theta_3 + \theta_2^{2q}\theta_3^q$ with the help of Magma (see Appendix B) to get

$$a_1^2(a_1yu^4 + a_1yz^2 + a_1u^3z + a_1uz + y^2u^2z + u^2z)(yz+u)(yu+z) = 0. \tag{3.3}$$

Recall that the only element of U that also belongs to $\mathbb{F}_q$ is 1. Since $uz^{-1}, u^{-1}z \in U$ and $y \in \mathbb{F}_q \backslash \{1\}$, the last two factors of equation (3.3) cannot vanish. Since $a_1 \neq 0$, the second factor of equation (3.3) must vanish. That is,

$$a_1(yu^4 + yz^2 + u^3z + uz) = u^2z(y^2+1).$$

Since the right-hand side of the above is nonzero, we can write a_1 as

$$a_1 = \frac{u^2 z(y^2+1)}{D} \tag{3.4}$$

where $D = yu^4 + yz^2 + u^3 z + uz$. Substituting a_1 into θ_2^{q+1} (which we have already expanded above) we get

$$\theta_2^{q+1} = \frac{u^4 z^2 (y^2+1)^2 (1+yuz^q)(1+yu^q z)}{D^2}$$

and

$$\begin{aligned}\frac{\theta_2^{q+1}}{\theta_1^2} &= \frac{u^4 z^2 (1 + yu^q z + yuz^q + y^2)}{D^2}\\ &= \frac{u^3 z(yz+u)(yu+z)}{D^2}\\ &= \frac{z(yz+u)(D+z(yz+u))}{D^2}\\ &= \frac{z(yz+u)}{D} + \frac{z^2(yz+u)^2}{D^2}\\ &= w + w^2\end{aligned}$$

where $w = z(yz+u)/D$. Note that for a fixed value of $\theta_2^{q+1}/\theta_1^2$, the equation

$$w^2 + w + \theta_2^{q+1}/\theta_1^2 = 0$$

has exactly two solutions in $\mathbb{F}_q$, by Lemma 2.1.5. However, a computation (see Appendix B) gives $w^q + w = 1$ which implies $w \notin \mathbb{F}_q$. It follows from Lemma 2.1.3 that $\mathrm{Tr}_1^m(\frac{\theta_2^{q+1}}{\theta_1^2}) \neq 0$ and therefore $(a_1, a_2, a_3) \notin \Gamma_1$. Since f is APN, it must be that $(a_1, a_2, a_3) \in \Gamma_2$ and m is even.

Given that $(a_1, a_2, a_3) \in \Gamma_2$, we are left to show that $(a_1, a_2, a_3) = (a_1, a_1 u, yz)$ can be written in terms of u and z as in the conclusion of the proposition.

First suppose that $a_3 = 0$. Then

$$\begin{aligned}\theta_1 &= 1,\\ \theta_2 &= a_1,\\ \theta_3 &= a_1 u^q,\\ \theta_4 &= 0.\end{aligned}$$

The third condition of Γ_2 becomes

$$a_1 u^q + a_1^2 + a_1^3 u^q + a_1^3 u = 0. \tag{3.5}$$

Raising (3.5) to power q and adding the result back to (3.5) gives $a_1(u^q+u)=0$. Since $a_1 \neq 0$ it must be that $u^q+u=0$. So $u \in \mathbb{F}_q \cap U$ which implies $u=1$ and substituting back gives $a_1=a_2=1$. Therefore $a_1, a_2, a_3 \in \mathbb{F}_q$.

Now suppose $a_3 \neq 0$, hence $y \neq 0$. Again we have $\theta_1 = y^2+1$, $\theta_2 = a_1 + a_1 y u^q z$, and $\theta_3 = a_1 u^q + a_1 y z^q$. The third condition of Γ_2 is $\theta_1^2\theta_3 + \theta_1\theta_2^{2q} + \theta_2^2\theta_3 + \theta_2^{2q}\theta_3^q = 0$. Looking at each term individually, we have

$$\begin{aligned}
\theta_1^2\theta_3 &= (y^4+1)(a_1u^q + a_1yz^q),\\
\theta_1\theta_2^{2q} &= (y^2+1)(a_1^2 + a_1^2y^2u^2z^{2q}),\\
\theta_2^2\theta_3 &= (a_1^2 + a_1^2y^2u^{2q}z^2)(a_1u^q + a_1yz^q),\\
\theta_2^{2q}\theta_3^q &= (a_1^2 + a_1^2y^2u^2z^{2q})(a_1u + a_1yz).
\end{aligned}$$

We can now factorize $\theta_1^2\theta_3 + \theta_1\theta_2^{2q} + \theta_2^2\theta_3 + \theta_2^{2q}\theta_3^q$ (see Appendix B) to get

$$a_1(yu+z)(Aa_1^2 + Ba_1 + C) = 0$$

where $A = D(yz+u)$, $D = (u^2+z)^2y + uz(u^2+1)$, $B = (y+1)^2u^3(yu+z)$ and $C = (y+1)^4u^2z$. Since $\theta_1 \neq 0$, we have $y \neq 1$, and again it follows that $yu+z \neq 0$ and $yz+u \neq 0$. Since $a_1 \neq 0$ we are left with

$$Aa_1^2 + Ba_1 + C = 0$$

We will distinguish two cases: $A=0$ and $A \neq 0$, equivalently, $D=0$ and $D \neq 0$.

First let us assume that $D=0$. If $u^2=z$, then $D = u^3(u^2+1) = 0$ and it follows that $u=z=1$ and $a_1, a_2, a_3 \in \mathbb{F}_q$. Otherwise

$$y = \frac{uz(u^2+1)}{(u^2+z)^2}$$

and

$$a_1 = \frac{C}{B} = \frac{(y+1)^2z}{u(yu+z)} = \frac{(u^3+z)^2}{u(u^2+z)^2}.$$

Then

$$a_2 = a_1u = \frac{(u^3+z)^2}{(u^2+z)^2}$$

and

$$a_3 = yz = \frac{uz^2(u+1)^2}{(u^2+z)^2}.$$

Now

$$\theta_2^{q+1}/\theta_1^2 = \frac{(a_1 + a_1yu^qz)^{q+1}}{(y^2+1)^2} = \frac{(a_1+a_1yuz^q)(a_1+a_1yu^qz)}{(y^4+1)}$$

and after substituting our new values for a_1 and y given above, a computation (see Appendix B) gives $\theta_2^{q+1}/\theta_1^2 = 1$. Hence, $\mathrm{Tr}_1^m(\theta_2^{q+1}/\theta_1^2) = 0$ since m is even, and $(a_1, a_2, a_3) \in \Gamma_2$.

We complete the proof by analyzing the case $A \neq 0$. We note that a_1 is also a root of

$$Aa_1^2 + Ba_1 + C + \frac{A}{A^q}(A^q a_1^2 + B^q a_1 + C^q) = 0,$$

which after simplifications (see Appendix B) becomes

$$u(Ra_1 + S) = 0$$

where $R = (u+z)^4(y+1)^2y^2$ and $S = (y+1)^4(yuz^2 + u^2z + yu + z)uz$. Since $u \in U$, we have $u \neq 0$. Since $\theta_1 = y^2 + 1 \neq 0$, we have $y + 1 \neq 0$. We also know that $y \neq 0$ since $a_3 = yz \neq 0$. If $R = 0$ then it follows that $u = z$ and we get $S = u^3(y+1)^5(u^2+1) = 0$. Thus $u = z = 1$ and $a_1, a_2, a_3 \in \mathbb{F}_q$. Now suppose $R \neq 0$ so that $Ra_1 + S = 0$ and

$$a_1 = \frac{S}{R} = \frac{(y+1)^2(yuz^2 + u^2z + yu + z)uz}{(u+z)^4y^2}. \tag{3.6}$$

Plugging this value for a_1 into the third condition of Γ_2 and simplifying (see Appendix B) yields

$$\frac{u^2z^2(y+1)^4(u+1)^2(u+yz)(y(u+z^2)+z(u+1))^2D}{(y(u+z)^2)^4} = 0. \tag{3.7}$$

Note that $(u+1)^2$ and $(y(u+z^2)+z(u+1))^2$ are the only factors in the numerator of equation (3.7) that can vanish. If $u = 1$ then

$$a_1 = \frac{z(y+1)^2}{y(z+1)^2}$$

and

$$\frac{\theta_2^{q+1}}{\theta_1^2} = \frac{(yz+1)(y+z)z}{y^2(z+1)^4} = w^2 + w$$

where $w = \frac{y+z}{y(z^2+1)}$. A calculation (see Appendix B) shows that $w^q + w = 1$. So $w \notin \mathbb{F}_q$ and by Lemma 2.1.3 we have $\mathrm{Tr}_1^m\left(\frac{\theta_2^{q+1}}{\theta_1^2}\right) \neq 0$. Therefore the factor $(u+1)^2$ cannot vanish. We are left with the case of the other factor vanishing, that is,

$$y = \frac{z(u+1)}{u+z^2}.$$

Substituting this into (3.6) and simplifying (see Appendix B) gives

$$a_1 = \frac{u(z+1)^2}{(u+1)(u+z^2)}.$$

After plugging these values for y and a_1 into $\theta_2^{q+1}/\theta_1^2$ and simplifying (see Appendix B) we get

$$\frac{\theta_2^{q+1}}{\theta_1^2} = \frac{u}{(u+1)^2} = w^2 + w$$

where $w = \frac{1}{u+1}$. Since $u \notin \mathbb{F}_q$ it follows that $w \notin \mathbb{F}_q$ (also it is easy to see that $w^q + w = 1$). Again, by Lemma 2.1.3 we have $\mathrm{Tr}_1^m \left(\frac{\theta_2^{q+1}}{\theta_1^2} \right) \neq 0$. Therefore the case $A \neq 0$ does not produce any APN functions, and we have exhausted all cases. □

We notice that a significant effort was spent analyzing the case $a_1/a_2 \in U$ in the previous proposition, and one may wonder if that extensive effort is necessary, that is, do the APN functions obtained in that proposition in fact exist? Next we show a numerical example of such a function which demonstrates that Propositions 3.2.6 and 3.2.8 are unavoidable. The values for u and z used in the following example were found by a randomized computer search.

Example 3.2.7. *Let $q = 2^4$. Suppose $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ is given by*

$$f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$$

where

$$\begin{aligned} a_1 &= \frac{(u^3+z)^2}{u(u^2+z)^2} \\ a_2 &= \frac{(u^3+z)^2}{(u^2+z)^2} \\ a_3 &= \frac{uz^2(u+1)^2}{(u^2+z)^2}. \end{aligned}$$

Suppose α is a primitive element of $\mathbb{F}_{q^2}$, which is a root of $X^8 + X^4 + X^3 + X^2 + 1$. If $u = \alpha^{225}$ and $z = \alpha^{135}$ then $u, z \in U$ and f is APN. See Appendix B for this calculation.

Proposition 3.2.8. *Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$ where*

$$\begin{aligned} a_1 &= \frac{(u^3+z)^2}{u(u^2+z)^2} \\ a_2 &= \frac{(u^3+z)^2}{(u^2+z)^2} \\ a_3 &= \frac{uz^2(u+1)^2}{(u^2+z)^2} \end{aligned}$$

for some $u, z \in U$ such that $u^2 \neq z$, and m is even. If f is APN, then f is affine equivalent to $G_1(x) = x^3$ or f is affine equivalent to $G_2(x) = x^{2^{m-1}+1}$.

Proof. Since m is even, $\mathbb{F}_q$ contains a primitive cube root of unity, say ω, where $\omega^2+\omega+1=0$. Since $\omega \neq 1$, it follows that $\omega \notin U$. Let $G_2'(x) = x^{2^{m+1}+1}$ and let

$$L_1(x) = x^q + tx$$

and

$$L_2(x) = rx^q + sx$$

for some $r, s, t \in \mathbb{F}_{q^2}$. By Lemma 2.4.6 we have

$$L_1(G_2'(L_2(x))) = c_0 x^{3q} + c_1 x^{2q+1} + c_2 x^{q+2} + c_3 x^3$$

where

$$\begin{aligned} c_0 &= r^2 s^q + r s^{2q} t, \\ c_1 &= r^{q+2} + s^{2q+1} t, \\ c_2 &= r^{2q+1} t + s^{q+2}, \\ c_3 &= r^{2q} s t + r^q s^2. \end{aligned}$$

To show the affine equivalence, we are left to find suitable r, s, t such that $c_i/c_0 = a_i$ for $i = 1, 2, 3$, that is, to compare coefficients. Suppose $s = 1$ and $r = \omega^2 v$ where $v \in U$ (other choices for r, s are possible). Then

$$\begin{aligned} c_0 &= \omega v^2 + \omega^2 v t, \\ c_1 &= v + t, \\ c_2 &= v^q t + 1, \\ c_3 &= \omega v^{2q} t + \omega^2 v^q. \end{aligned}$$

Assume c_0 is nonzero, that is, $v \neq 0$ and $t \neq \omega^2 v$. Recall that $ua_1 + a_2 = 0$. A computation (see Appendix B) shows that

$$u\frac{c_1}{c_0} + \frac{c_2}{c_0} = \frac{\omega(t+v)(uv+1)}{v^2(t+\omega^2 v)}$$

which vanishes if $v = 1/u$. So let $v = 1/u$ for the rest of the proof. After substituting this into c_0 and c_1, another computation (see Appendix B) gives

$$a_1 + \frac{c_1}{c_0} = \frac{\omega^2(u^7 t + \omega u^6 + \omega^2 u^3 z^2 t + \omega^2 u^2 z^2 + \omega u z^2 t + z^2)}{u(ut+\omega^2)(u^2+z)^2}.$$

The above vanishes when

$$t = \frac{\omega u^6 + \omega^2 u^2 z^2 + z^2}{u^7 + \omega^2 u^3 z^2 + \omega u z^2}$$

which factors as (see Appendix B)

$$t = \frac{(\omega u^3 + (u+\omega^2)z)^2}{uD} \tag{3.8}$$

where $D = (\omega^2 u^3 + (u+\omega)z)^2$. So fix t as the value of the right-hand side of (3.8) for the rest of the proof. At this point we have determined the coefficients of L_1 and L_2.

We need to show that $D \neq 0$. Suppose towards a contradiction that $D = 0$. This happens for $z_1 \in U$ where

$$z_1 = \frac{\omega^2 u^3}{u+\omega}.$$

Recall that $z_1^q = \frac{1}{z_1}$ for $z_1 \in U$, which is an important computational rule throughout this chapter. A computation (see Appendix B) gives

$$z_1^q + \frac{1}{z_1} = \frac{\omega(u+1)^2}{u^3(\omega+u+1)},$$

so it must be that $u = 1$. But then $z_1 = 1$ and $u^2 = z_1$, a contradiction.

Next we show that $t \neq \omega^2/u$. Suppose towards a contradiction that $t = \omega^2/u$. Then (3.8) becomes

$$\omega^2 D = (\omega u^3 + (u+\omega^2)z)^2.$$

Thus,

$$\omega^2(\omega u^6 + u^2 z^2 + \omega^2 z^2) = \omega^2 u^6 + u^2 z^2 + \omega z^2$$

which simplifies to $\omega u^6 = \omega u^2 z^2$ which implies $u^2 = z$, a contradiction.

With these values for r,s and t, a computation (see Appendix B) shows that

$$\begin{aligned} c_0 &= \frac{(u^2+z)^2}{D}, \\ c_1 &= \frac{(u^3+z)^2}{uD}, \\ c_2 &= \frac{(u^3+z)^2}{D}, \\ c_3 &= \frac{uz^2(u+1)^2}{D}. \end{aligned}$$

Since $u^2 \neq z$, we have $c_0 \neq 0$ and

$$\begin{aligned} f(x) &= x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3 \\ &= x^{3q} + \frac{c_1}{c_0} x^{2q+1} + \frac{c_2}{c_0} x^{q+2} + \frac{c_3}{c_0} x^3. \end{aligned}$$

We are left to show that L_1 and L_2 are affine permutations of $\mathbb{F}_{q^2}$, or prove the conclusion in some other way. Since $r = \omega^2/u \notin U$, it follows from Lemma 2.3.4 that L_2 is a permutation of $\mathbb{F}_{q^2}$. We will show that if L_1 is not a permutation of $\mathbb{F}_{q^2}$ then f is affine equivalent to G_1 and if L_1 is a permutation of $\mathbb{F}_{q^2}$ then f is affine equivalent to G_2.

If $t = 0$ then L_1 is clearly a permutation. Suppose $t \neq 0$. Note that

$$t^q = \frac{(\omega u^{3q} + (u^q + \omega^2)z^q)^2}{u^q(\omega^2 u^{3q} + (u^q + \omega)z^q)^2}.$$

Then by a factorization (see Appendix B), we have

$$t^q + \frac{1}{t} = \frac{u^3(u^3+z)^2(u+z)^2}{\omega(u^3+\omega^2 uz + \omega z)^2(u^3 + \omega^2 u^2 + \omega z)^2}$$

which implies $t \notin U$ unless $u^3 = z$ or $u = z$. If $u^3 = z$ then $a_1 = a_2 = 0$ and f is affine equivalent to G_1 by Proposition 3.2.3. If $u = z$ then

$$\begin{aligned}
\theta_1 &= 1 + a_1^2 + a_2^{q+1} + a_3^{q+1} \\
&= 1 + \frac{(u^3+u)^4}{u^2(u^2+u)^4} + \frac{(u^{2q}+u^2)^2}{u^{2q}+u^2} + \frac{u^{2q}+u^2}{u^{2q}+u^2} \\
&= \frac{u^8+1}{u^6+u^2} + \frac{(u^{2q}+u^2)(u^6+u^2)}{u^6+u^2} \\
&= \frac{u^8+1+u^4+1+u^8+u^4}{u^6+u^2} \\
&= 0
\end{aligned}$$

which contradicts f being APN. Therefore, assuming $u^3 \neq z$, we have that L_1 is a permutation of $\mathbb{F}_{q^2}$ and $f(x)$ is affine equivalent to $G_2'(x)$ which is affine equivalent to $G_2(x)$ by Lemma 2.4.5. □

Proposition 3.2.9. *Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ be given by $f(x) = x^{3q} + a_1 x^{2q+1} + a_2 x^{q+2} + a_3 x^3$ where $a_1 \in \mathbb{F}_q$, $a_2 \in \mathbb{F}_{q^2}^*$ and $a_3 \in \mathbb{F}_{q^2}$, and assume that $a_1/a_2 = a_3^q$. Then f is not APN.*

Proof. We will show that, under the given conditions, $(a_1, a_2, a_3) \notin \Gamma_1 \cup \Gamma_2$. Hence the result follows by Theorem 2.4.4.

By Lemma 2.1.8 we can write a_2 uniquely as $a_2 = vz$ for $v \in \mathbb{F}_q^*$ and $z \in U$. Now choose $y \in \mathbb{F}_q$ so that $a_1 = vy$. Plugging these into $a_1 = a_2 a_3^q$ gives $y = z^q a_3$, so $a_3 = yz$. Substituting these into $\theta_1, \theta_2, \theta_3$, and θ_4 gives

$$\begin{aligned}
\theta_1 &= a_1^2 + a_2^{q+1} + a_3^{q+1} + 1 = (v+1)^2(y+1)^2, \\
\theta_2 &= a_1 + a_2^q a_3 = 0, \\
\theta_3 &= a_2^q + a_1 a_3^q = vz^q(y+1)^2, \\
\theta_4 &= a_1^2 + a_2^{q+1} = v^2(y+1)^2.
\end{aligned}$$

Suppose $(a_1, a_2, a_3) \in \Gamma_1$. Since $\theta_2 = 0$, the third condition of Γ_1 is simply $\theta_1^2\theta_4 = 0$ and substitution results in

$$v^2(v+1)^4(y+1)^6 = 0.$$

By definition of Γ_1, $\theta_1 \neq 0$, so the last two factors above cannot vanish. Then it must be that $v = 0$ which is a contradiction.

Suppose $(a_1, a_2, a_3) \in \Gamma_2$. Since $\theta_2 = 0$, the third condition of Γ_2 simplifies to $\theta_1^2\theta_3 = 0$. Substitution gives

$$\frac{v(v+1)^4(y+1)^6}{z} = 0$$

and we have a contradiction by the same reasoning as the previous case. □

As was explained in the proof outline in Section 3.2.2, we have exhausted all possible cases and the proof of Theorem 3.2.1 is now complete.

Chapter 4

Walsh zero spaces

Although finding APN permutations in even dimensions is of great interest, only one example in dimension six has been found. The situation is slightly better in odd dimensions, but still not many APN permutations are known in general. Currently, all known APN permutations in odd dimensions, up to CCZ-equivalence, belong either to a monomial family (see Table 2.2.1) or one of the following sets: an infinite family of quadratic APN permutations in odd dimension found in 2008 by Budaghyan, Carlet and Leander [8], and two quadratic APN permutations in dimension nine found in 2020 by Beierle and Leander [2]. As such, it is certainly still desirable to find more constructions of APN permutations in odd dimensions as well.

Our motivation for this chapter is the following. Given a pair of trivially intersecting Walsh zero spaces of a function f, one can apply the method of Browning et al. [7], which we formalized in terms of Walsh zero spaces in Proposition 2.5.7, to construct permutations CCZ-equivalent to f. Therefore, theoretical descriptions of Walsh zero spaces and their trivially intersecting pairs are of interest in regards to constructing more and possibly new APN permutations. But as far as we know, no such general descriptions are known except for the two trivial Walsh zero spaces described in Section 2.5. Recently the importance and applications of WZ spaces have been recognized more explicitly, see [10] and references therein.

In this chapter, we study the Walsh zero spaces of Gold APN functions in odd dimensions, because they have the simplest description of Walsh zeros among all known APN functions whose Walsh zeros have been studied. Much research has already been done with Gold functions due to their extensive applications in communication systems. In 1968, Robert Gold [18] implicitly characterized the Walsh zeros of Gold functions while researching their correlation properties. This simplicity is helpful when working on theoretical constructions of trivially intersecting pairs of Walsh zero spaces.

In order to construct WZ spaces, we started by numerically listing WZ spaces for Gold functions in small odd dimensions. Recall from Chapter 2 that this means we search for n-dimensional subspaces of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that every element except for $(0, 0)$ is a Walsh zero.

It is not straightforward what form these spaces should take. We were able to take advantage of computer algebra systems to analyze these spaces in low dimensions and because of this, our theoretical constructions have been heavily motivated by these computational results. Therefore we start by presenting our computational results in Section 4.2, followed by our theoretical constructions of Walsh zero spaces and trivially intersecting pairs in Sections 4.3 and 4.4 respectively.

The material in this chapter is joint work with Dr. Lisoněk and it has been submitted in October 2021 to Springer journal Cryptography and Communications (special issue for the conference Boolean Functions and their Applications 2021). It was also accepted based on a refereed five-page abstract by this conference as a talk. The full paper is also available on arXiv [14].

I started by computing the Walsh zero spaces for the Gold APN functions in odd dimensions up to and including dimension 9, see Appendix C. I analyzed numerically the structure of the trivially intersecting pairs of Walsh zero spaces and presented the results in the form of graphs in Section 4.2. I also automated the conversion of data format between Magma and sboxU. By analyzing this data, we jointly inferred some patterns for constructions of the Walsh zero spaces and their trivially intersecting pairs. I formalized these constructions into the propositions and I authored most of the proofs.

4.1 The Walsh zero test and compatible subspaces

Recall the following definitions from Chapter 2. The Walsh transform of a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is given by $\mathcal{W}_f(a,b) = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(ax+bf(x))}$. We say that (a,b) is a Walsh zero (WZ) of f if $\mathcal{W}_f(a,b) = 0$. We call a subspace S of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ a WZ space of f if every element of S expect for $(0,0)$ is a Walsh zero of f and S has dimension n. We say that two WZ spaces S, T of the same function intersect trivially if $S \cap T = \{(0,0)\}$, and we call them a TI pair.

In this section we characterize Walsh zeros of Gold APN permutations. That is, we work in odd dimension throughout. We also define and give some results on certain additive subspaces of $\mathbb{F}_{2^n}$ which we call *compatible subspaces* that we introduce for the purpose of constructing Walsh zero spaces of Gold APN permutations.

The following proposition is useful as it allows us to check if a pair $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ is a Walsh zero of $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ without having to compute the sum $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(ax+bf(x))}$ which grows with exponential time complexity in n. This simple characterization also allows the theoretical constructions of WZ spaces given in Section 4.3. The following proposition was proved implicitly by Robert Gold in [18].

Proposition 4.1.1 (The Walsh zero test for Gold APN functions)**.** *Suppose n is odd and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $f(x) = x^{2^i+1}$ such that $\gcd(i,n) = 1$ (so f is a Gold APN function). Then $(a,b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ is a Walsh zero of f if and only if $\mathrm{Tr}(ab^{-\frac{1}{2^i+1}}) = 0$ or $a \neq b = 0$.*

Proof. First we present a proof given in [23] which covers the case $b = 1$. We then extend it to $b \neq 1$. The notation $\chi(y) = (-1)^{\mathrm{Tr}(y)}$ is introduced only to improve readability. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be given by $f(y) = y^{2^i+1}$ with $\gcd(i, n) = 1$. Then for any $c \in \mathbb{F}_{2^n}$,

$$\begin{aligned}
\mathcal{W}_f(A, 1) &= \sum_{y \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(Ay + f(y))} \\
&= \sum_{z \in \mathbb{F}_{2^n}} \chi((z + c)^{2^i+1} + A(z + c)) \\
&= \sum_{z \in \mathbb{F}_{2^n}} \chi(z^{2^i+1} + cz^{2^i} + c^{2^i}z + c^{2^i+1} + Az + Ac) \\
&= \chi(Ac + c^{2^i+1}) \sum_{z \in \mathbb{F}_{2^n}} \chi(z^{2^i+1} + c^{2^{-i}}z + c^{2^i}z + Az) \\
&= \chi(Ac + c^{2^i+1}) \sum_{z \in \mathbb{F}_{2^n}} \chi(z^{2^i+1} + z(L(c) + A))
\end{aligned}$$

where $L(c) = c^{2^i} + c^{2^{-i}}$.

It is clear that L is linear and that $\mathrm{Tr}(L(c)) = 0$ for all c. Since the kernel of L is $\{0, 1\}$, the image of L contains all elements of $\mathbb{F}_{2^n}$ with trace 0. So if $\mathrm{Tr}(A) = 0$ we can choose c such that $A = L(c)$. With this choice of c, we have

$$W_f(A, 1) = \chi(Ac + c^{2^i+1}) \sum_{z \in \mathbb{F}_{2^n}} \chi(z^{2^i+1}) = 0$$

where $\sum_{z \in \mathbb{F}_{2^n}} \chi(z^{2^i+1}) = 0$ since z^{2^i+1} is a permutation of $\mathbb{F}_{2^n}$ when n is odd.

If $\mathrm{Tr}(A) = 1$, choose c so that $L(c) = A + 1$. Then

$$W_f(A, 1) = \chi(Ac + c^{2^i+1}) \sum_{z \in \mathbb{F}_{2^n}} \chi(z^{2^i+1} + z) = \chi(Ac + c^{2^i+1}) W_f(1, 1).$$

The following is proved as Theorem 5 of [23],

$$W_f(1, 1) = \begin{cases} +2^{(n+1)/2} & \text{if } n \equiv \pm 1 \pmod 8 \\ -2^{(n+1)/2} & \text{if } n \equiv \pm 3 \pmod 8). \end{cases}$$

So $W_f(A, 1)$ is nonzero when $\mathrm{Tr}(A) = 1$. Therefore $\mathcal{W}_f(A, 1) = 0$ if and only if $\mathrm{Tr}(A) = 0$.

This result is extended to $b \neq 0, 1$ with a change of variables. Let $z = b^{\frac{1}{2^i+1}}x$. Then

$$\begin{aligned}
\mathcal{W}_f(A, 1) &= \sum_{z \in \mathbb{F}_{2^n}} \chi(Az + f(z)) \\
&= \sum_{x \in \mathbb{F}_{2^n}} \chi(Ab^{\frac{1}{2^i+1}}x + bf(x)) \\
&= \mathcal{W}_f(a, b)
\end{aligned}$$

where A is chosen such that $a = Ab^{\frac{1}{2^i+1}}$. The condition $\mathrm{Tr}(A) = 0$ becomes $\mathrm{Tr}(ab^{-\frac{1}{2^i+1}}) = 0$. Finally, if $a \neq b = 0$ then $\mathcal{W}_f(a,b) = \sum_{x\in\mathbb{F}_{2^n}} \chi(ax) = 0$. $\square$

Throughout this chapter this is the only Walsh zero test we use and so will refer to Proposition 4.1.1 simply as *the Walsh zero test*. Now that we can easily determine Walsh zeros for Gold APN permutations, we are tasked with the problem of finding Walsh zero spaces.

WZ spaces have been recently appearing in literature. In Theorem 4 of [10], Canteaut and Perrin prove that the number of EA-classes inside the CCZ-class of $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is upper bounded by the number of WZ spaces of f. Beierle, Carlet, Leander, and Perrin in [1] have studied two new quadratic APN permutations in dimension 9 using numerical properties of their WZ spaces. Furthermore, in [1] the authors show an interesting similarity between their new APN permutations and Gold APN permutations in odd dimensions divisible by 3. We describe these new APN permutations in Section 4.6.3 and present our perspective on the similarities to Gold APN permutations.

From now on let us define $0^{-\frac{1}{2^i+1}} = 0$ as this will simplify some of the forthcoming constructions and arguments and this convention is common in the literature. Let us note that this works correctly for the Walsh zero test for Gold APN permutations, where for a pair $(a,0)$ we get $\mathrm{Tr}(a\cdot 0^{-\frac{1}{2^i+1}}) = \mathrm{Tr}(a\cdot 0) = 0$, as desired.

Definition 4.1.2. *Let n be odd and $\gcd(i,n) = 1$. Let S be an additive subspace of $\mathbb{F}_{2^n}$. We say that S is i-*compatible *if the set $S^{-\frac{1}{2^i+1}} = \{s^{-\frac{1}{2^i+1}} : s \in S\}$ is also an additive subspace of $\mathbb{F}_{2^n}$.*

Suppose X is an additive subspace of Y. Because the subspace relation is transitive, if S is an i-compatible subspace of X then S is also an i-compatible subspace of Y.

For $U \subseteq \mathbb{F}_{2^n}$ and $a \in \mathbb{F}_{2^n}$ denote $aU = \{au : u \in U\}$.

Example 4.1.3.
(i) If n is odd and $\gcd(i,n) = 1$ then the following subspaces of $\mathbb{F}_{2^n}$ are i-compatible: $\{0\}$, $\mathbb{F}_2$ and $\mathbb{F}_{2^n}$.
(ii) If S is an i-compatible subspace of $\mathbb{F}_{2^n}$, then μS is also i-compatible for each $\mu \in \mathbb{F}_{2^n}$.

We thank Claude Carlet for suggesting to us the current form of the following proposition which was previously stated only for $m = 3$.

Proposition 4.1.4. *Suppose m divides n and $\gcd(i,n) = 1$. Then $\mathbb{F}_{2^m}$ is an i-compatible subspace of $\mathbb{F}_{2^n}$.*

Proof. Let $\xi \in \mathbb{F}_{2^m}$. Then $(\xi^{-\frac{1}{2^i+1}})^{2^m} = (\xi^{2^m})^{-\frac{1}{2^i+1}} = \xi^{-\frac{1}{2^i+1}}$. So $\xi^{-\frac{1}{2^i+1}} \in \mathbb{F}_{2^m}$ and it follows that $\{\xi^{-\frac{1}{2^i+1}} : \xi \in \mathbb{F}_{2^m}\} = \mathbb{F}_{2^m}$ since $x \mapsto x^{-\frac{1}{2^i+1}}$ permutes $\mathbb{F}_{2^n}$. $\square$

Moreover, when n is a multiple of 3, then $\mathbb{F}_{2^n}$ contains the subfield $\mathbb{F}_{2^3}$ and the following lemma applies.

Lemma 4.1.5. *Suppose n is a multiple of 3 and $\gcd(i,n) = 1$. Let $\xi \in \mathbb{F}_{2^3} \subset \mathbb{F}_{2^n}$. Then $\xi^{-\frac{1}{2^i+1}} = \xi^{2^i}$.*

Proof. If $\xi = 0$ then the result follows from our definition $0^{-\frac{1}{2^i+1}} = 0$. Otherwise, note that raising both sides of $\xi^{-\frac{1}{2^i+1}} = \xi^{2^i}$ to $2^i + 1$ yields the equivalent equation

$$\xi^{-1} = \xi^{2^{2i}+2^i}.$$

Since $\xi \in \mathbb{F}_{2^3} \backslash \{0\}$ there are only two cases to consider: For $i \equiv 1 \pmod 3$, we have

$$\xi^{2^{2i}+2^i} = \xi^{2^2+2} = \xi^6 = \xi^{-1}.$$

For $i \equiv 2 \pmod 3$ we have

$$\xi^{2^{2i}+2^i} = \xi^{2^4+2^2} = \xi^{2+4} = \xi^6 = \xi^{-1}.$$

□

Lemma 4.1.6. *Assume that n is odd and divisible by 3. Let S be the subspace of $\mathbb{F}_{2^n}$ isomorphic to $\mathbb{F}_{2^3}$. Then each additive subspace of S is i-compatible whenever $\gcd(i,n) = 1$.*

Proof. This follows from Lemma 4.1.5. Indeed $\xi \mapsto \xi^{-\frac{1}{2^i+1}}$ is a linear mapping on $\mathbb{F}_{2^3}$. □

As any two 2-dimensional subspaces (hyperplanes) of $\mathbb{F}_{2^3}$ can be obtained from each other just by scaling by an element of $\mathbb{F}_{2^3}^*$, it follows that if 3 divides n, then Lemma 4.1.6 and Example 4.1.3(ii) provide $2^n - 1$ two-dimensional i-compatible subspaces of $\mathbb{F}_{2^n}$ and $(2^n - 1)/7$ three-dimensional i-compatible subspaces of $\mathbb{F}_{2^n}$. The latter ones are the cosets of $\mathbb{F}_{2^3}^*$ in $\mathbb{F}_{2^n}^*$.

For $i = 1$ it is easy to see that the proof of Lemma 4.1.6 does not extend to any higher dimension. Indeed suppose that $s \mapsto s^{-1/3}$ is linear on $\mathbb{F}_{2^n}$ where $n > 3$ is odd, then $-1/3 \equiv 2^k \pmod{2^n - 1}$ for some integer $0 \leq k < n$. It follows that

$$3 \cdot 2^k + 1 = M(2^n - 1)$$

for some integer positive integer M. If $n > 3$ and $k < n - 1$ then $3 \cdot 2^k + 1$ is too small for this to happen. The only remaining possibility is $3 \cdot 2^{n-1} + 1 = 2^n - 1$, which can not occur either.

In Proposition 4.3.1 below we will see that i-compatible spaces can be used to construct WZ spaces. Thus it is interesting to obtain as many i-compatible spaces as we can. We have checked by exhaustive search that there are no two-dimensional i-compatible subspaces of $\mathbb{F}_{2^n}$ other than those described above for odd n and relatively prime i in the range $n \leq 17$ (see Appendix C). This motivates us to present the following open problem:

Problem 4.1.7. *For odd n, do there exist i-compatible subspaces of $\mathbb{F}_{2^n}$ other than those described by Example 4.1.3(i,ii), Proposition 4.1.4 and Lemma 4.1.6?*

4.2 Computational investigations in low dimensions

In this section we describe our approach for obtaining the computational descriptions of WZ spaces and their TI pairs for Gold APN permutations. Subsequently, in Sections 4.3 and 4.4 we analyze them and develop theoretical constructions. At first we attempted the naive approach of a randomized vector subspace search with Magma for the Gold APN permutation $f(x) = x^3$. Along with the randomized vector space search being inefficient, there is inherent uncertainty of whether or not it had found all possible WZ spaces of a certain dimension. But these early results showed us that there do indeed exist nontrivial TI pairs of Walsh zero spaces for Gold APN permutations which provided motivation for further study.

Fortunately, a new algorithm for efficient searches of vector subspaces of specific dimensions is given in [4]. Given a general subset S of elements, this algorithm finds subspaces of a given dimension completely contained in S. This algorithm along with other tools for analyzing S-boxes are implemented in Léo Perrin's and Mathias Joly's software package sboxU [33]. The software uses C++ for multi-threading and Python for bindings. With the help of sboxU, we have exhaustively listed all WZ spaces for Gold APN permutations up to and including dimension 9.

We started our computational search with the Gold function $f(x) = x^3$ in odd dimensions. With sboxU, we were able to efficiently list every WZ space basis for $f(x)$ up to dimension 9. Of course the full vector space is needed for analysis, therefore we converted the sboxU data to Magma for further processing described below. We analyzed these WZ spaces with Magma since it has one of the best implementations of finite fields and linear codes. Magma is also used by many authors of publications in this area. Later we checked that our theoretical constructions do cover all the computed WZ spaces for all possible Gold functions in odd dimensions up to and including dimension 9.

4.2.1 Dimension 3

First we exhaustively computed every Walsh zero for $f(x) = x^3$ in Magma using the Walsh zero test. That is, $(a, b) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ is a Walsh zero of f if and only if $\mathrm{Tr}(ab^{-\frac{1}{3}}) = 0$. Then we converted each Walsh zero (a, b) to its corresponding integer representation when viewed as an element of $\mathbb{F}_2^{2n}$, which is the required input format for sboxU. For example, $(0, 0, 1, 1, 0, 1) \in \mathbb{F}_2^6$ corresponds to 13. Starting with $n = 3$, sboxU gives us 30 bases of WZ spaces for $f(x) = x^3$ which have no discernible patterns at first glance (see Appendix C). Next we formatted the bases from sboxU back into elements of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ from their integer representations and generated all Walsh zero spaces for $f(x)$. For example, one of these spaces is

$$Z = \{(0,0), (\alpha^4, \alpha^6), (\alpha^2, \alpha^3), (\alpha^6, \alpha^6), (\alpha, \alpha^4), (\alpha^3, 0), (\alpha^5, \alpha^3), (1, \alpha^4)\}$$

where α is a primitive element of $\mathbb{F}_{2^3}$. We needed some way of categorizing theses spaces. Since each element of Z belongs to $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, projecting onto either the first or second component gives us a subspace of Z. One idea is to find the dimensions of both of these component projections for all 30 WZ spaces, which is easy to do but we will need some notation to compactly present the data. Suppose a WZ space has d_a and d_b as dimensions of the projections onto the first and second component respectively. Then we can represent that WZ space by the symbol $[d_a, d_b]$. For example, we represent the WZ space Z given above by $[3,2]$.

For the 30 WZ spaces of $f(x) = x^3$, there are 120 TI pairs. We can represent all of this data in a *WZ graph* as shown in Figure 4.1. Each node of the graph represents a set of WZ spaces with corresponding component dimensions and the superscript indicates the number of such spaces that exist. Each labelled edge indicates the number of TI pairs that exist for the corresponding spaces.

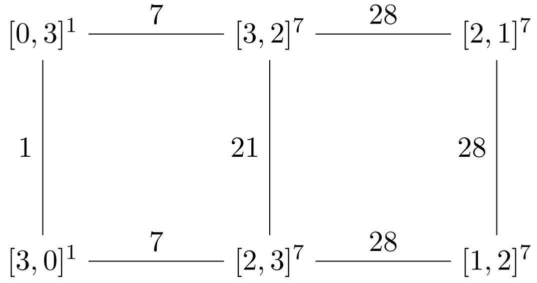

Figure 4.1: WZ graph of the Gold APN permutation $f(x) = x^3$ on $\mathbb{F}_{2^3}$.

Therefore, we have organized the $30 = 1+1+7+7+7+7$ WZ spaces into six categories based on their different component projections. As a result we have also categorized the $120 = 1 + 7 + 7 + 21 + 28 + 28 + 28$ TI pairs. Note that every WZ space belongs to a TI pair; this is not the case in higher dimensions. Also, note that there happens to be no edges connecting a node to itself. That is, no TI pair contains WZ spaces possessing identical component projection dimensions.

The data given above are covered by theoretical constructions as follows. Proposition 4.3.1 accounts for all spaces of the form $[3,0], [2,1], [1,2]$, and $[0,3]$. Spaces of the form $[3,2]$ are obtained from Proposition 4.3.2. Spaces of the form $[2,3]$ are obtained from Proposition 4.3.3 with $m = 3$.

However we did not try to obtain theoretical constructions from dimension 3 since the small size of the space could force conditions that do not hold in higher dimensions. Our first theoretical constructions were extracted by closely analyzing dimensions 5 and 7; since they are prime we expect simpler behavior. The remaining theoretical constructions were obtained by analyzing dimension 9 which has much more structure since $\mathbb{F}_{2^3}$ is a subfield of $\mathbb{F}_{2^9}$.

4.2.2 Dimension 5

There are 64 WZ spaces and 32 TI pairs in dimension 5. Spaces of the form $[4,1]$ do not belong to any TI pair. The WZ graph is shown in Figure 4.2. Recall from Chapter 2, that

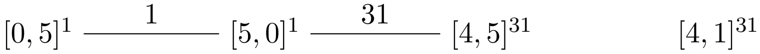

Figure 4.2: WZ graph of the Gold APN permutation $f(x) = x^3$ on $\mathbb{F}_{2^5}$.

$\{Z_{[5,0]}, Z_{[0,5]}\}$ is a TI pair. We see this trivial TI pair represented as an edge with label 1 in Figure 4.2. The remaining edge in Figure 4.2 indicating 31 TI pairs gave us initial data for the first theoretical construction of a nontrivial TI pair. Note that the multiplicity of the nontrivial WZ spaces is $31 = 2^5 - 1 = |\mathbb{F}_{2^5}^*|$ indicating that perhaps these are scaled versions of a single construction.

Before obtaining constructions for TI pairs we obtained constructions of WZ spaces. Since WZ spaces of the form $[4,5]$ are n-dimensional in the second component, these spaces must be of the form $\{(g(x), x) : x \in \mathbb{F}_{2^5}\}$ for some $g(x) \in \mathbb{F}_{2^5}[x]$. Thus, we can use interpolation to find the unique polynomial $g(x)$ for each WZ space of the form $[4,5]$. After doing this and analyzing the results, we find that each of these WZ spaces are of the form $\{(ax^{16} + a^4x, x) : x \in \mathbb{F}_{2^5}\}$ for $a \in \mathbb{F}_{2^5}^*$. We noticed that $x^{16} = x^{\frac{1}{2}}$ in $\mathbb{F}_{2^5}$ and eventually we generalized this construction into the current form of Proposition 4.3.3: $\{(\mu a, \mu^{2^i+1}b) : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m} \text{ and } \mathrm{Tr}_m^n(a) = b + b^{\frac{1}{2^i}}\}$ with μ fixed in $\mathbb{F}_{2^n}^*$ and $\gcd(i,n) = 1$.

Observe that WZ spaces of the form $[4,1]$ are $(n-1)$-dimensional in the first component. That is, the projections onto the first component are hyperplanes (see Corollary 2.1.4). It follows that for every $\alpha \in \mathbb{F}_{2^5}^*$, projections onto the first component are given by $\{(x,0) \in \mathbb{F}_{2^5} \times \mathbb{F}_{2^5} \ : \ \mathrm{Tr}(\alpha x) = 0\}$. In other words, each WZ space of the form $[4,1]$ is characterized uniquely by $\alpha \in \mathbb{F}_{2^5}^*$ and the nonzero second component, say b. Let $Z_{\alpha b}$ denote such a WZ space. Then,

$$Z_{\alpha b} = \{(x,c) \in \mathbb{F}_{2^5} \times \mathbb{F}_{2^5} \ : \ \mathrm{Tr}(\alpha x) = 0 \quad \text{and} \quad c \in \{0, b\}\}.$$

Ultimately, this construction was generalized to Proposition 4.3.1, which we can see by modifying notation: Let $S = b\mathbb{F}_2 := \{0, b\}$ and $S^{-\frac{1}{2^i+1}} = \{0, b^{-\frac{1}{2^i+1}}\}$. Let $X = \{x \in \mathbb{F}_{2^5} \ : \ \forall a \in S^{-\frac{1}{2^i+1}}, \ \mathrm{Tr}(ax) = 0\}$. Then $Z_{\alpha b} = X \times S$.

4.2.3 Dimension 7

There are 256 WZ spaces and 128 TI pairs in dimension 7. Spaces of the form $[6,1]$ do not belong to any TI pair. The WZ graph is shown in Figure 4.3. As one can see, the WZ graphs in dimensions 5 and 7 have a very similar structure. Note the simple structure for primes 5 and 7 in comparison to 9. This indicates that some forms of WZ spaces may be "lifted" up to higher dimension. At the time, this gave us hope that theoretical descriptions for WZ spaces were possible in general dimensions. Indeed we were able to achieve such general constructions, not only for WZ spaces but also for TI pairs, which we present in the next two sections. We found that Proposition 4.3.1 accounts for all spaces of the form $[7,0],[6,1]$, and $[0,7]$ and spaces of the form $[6,7]$ are obtained from Proposition 4.3.3 with $m=7$.

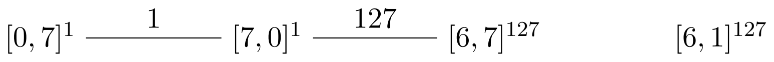

Figure 4.3: WZ graph of the Gold APN permutation $f(x)=x^3$ on $\mathbb{F}_{2^7}$.

4.2.4 Dimension 9

There are 2630 WZ spaces and 262144 TI pairs in dimension 9. The WZ spaces corresponding to $[6,3]^{73},[8,1]^{511},[8,3]^{511}$ do not participate in any TI pair. Note that the WZ graph looks similar to that of dimension 3, suggesting that dimensions which are multiples of 3 may have extra structure. In fact any nonprime dimension has a nontrivial subfield which gives extra structure that may contribute to extra WZ spaces.

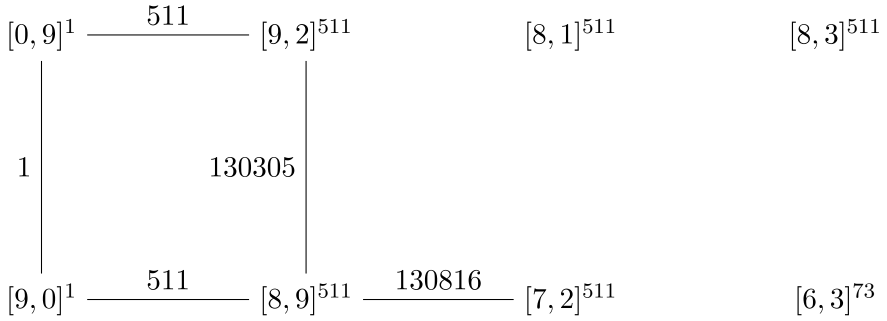

Figure 4.4: WZ graph of the Gold APN permutation $f(x)=x^3$ on $\mathbb{F}_{2^9}$.

Luckily, most of the WZ spaces in dimension 9 have at least one small or one large component dimension. If the component dimensions are small, then it is easier to organize and to provide general constructions. If one of the component dimensions is large, then we can use methods similar to the ones described for dimension 5.

Proposition 4.3.1 accounts for all spaces of the form $[9,0],[8,1],[7,2],[6,3]$, and $[0,9]$. Spaces of the form $[9,2]$ are obtained from Proposition 4.3.2. Spaces of the form $[8,9]$ and $[8,3]$ are obtained from Proposition 4.3.3 with $m=9$ and $m=3$ respectively.

Once we had generalized the constructions of WZ spaces as much as we could, which included merging many constructions, we started to characterize their trivial intersections. Doing so was mostly straightforward except for TI pairs of the form $\{[9,2],[8,9]\}$ and $\{[8,9],[7,2]\}$. To find exactly which conditions must hold for these WZ spaces to intersect trivially, there was a lot of back and forth between analyzing our generalized constructions and the data provided computationally.

4.2.5 Dimension 11

In dimension 11, we were not able to list any WZ spaces of $f(x)=x^3$ with sboxU in a reasonable time. This may be because we could not get sboxU to output spaces continuously. Therefore, we tried sampling subsets of Walsh zeros uniformly at random to use as input with sboxU. Even after sampling up to 97% of all possible Walsh zeros, sboxU did not return any WZ spaces.

4.3 Constructions of some WZ spaces for Gold APN permutations

In this section we provide constructions of nontrivial WZ spaces for Gold APN permutations in odd dimensions which are, as far as we know, the first such theoretical (computer-free) constructions. As indicated before, these constructions are informed by the numerical examples in the previous section.

Proposition 4.3.1. *Assume that n is odd and S is an i-compatible additive subspace of $\mathbb{F}_{2^n}$. Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$, $f(x)=x^{2^i+1}$, with $\gcd(i,n)=1$. Let*

$$X=\{x\in\mathbb{F}_{2^n}\ :\ (\forall a\in S^{-\frac{1}{2^i+1}})\ \mathrm{Tr}(ax)=0\}.$$

Then $X\times S$ is a WZ space for f.

Proof. Let $(0,0)\neq(x,s)\in X\times S$. Then $\mathrm{Tr}(xs^{-\frac{1}{2^i+1}})=0$ by construction, hence (x,s) is a Walsh zero of f. Since both X and S are linear spaces, $X\times S$ is also a linear space. Finally, since $s\mapsto s^{-\frac{1}{2^i+1}}$ is a bijection on $\mathbb{F}_{2^n}$, we get $\dim S^{-\frac{1}{2^i+1}}=\dim S$, and

$$\dim(X\times S)=\dim X+\dim S=(n-\dim S)+\dim S=n.$$

□

Proposition 4.3.2. *Assume that $n = 3k$ where k is odd. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1}$, with $\gcd(i, n) = 1$. Suppose ξ is a fixed element of $\mathbb{F}_{2^3} \subset \mathbb{F}_{2^n}$ and μ is a fixed element of $\mathbb{F}^*_{2^n}$. Then*

$$Z = \left\{ \left(x \, , \, \mu^{-(2^i+1)}(\xi \mathrm{Tr}(\mu x) + \mathrm{Tr}(\xi^{2^i} \mu x)) \right) \ : \ x \in \mathbb{F}_{2^n} \right\}$$

is a WZ space of f.

Proof. The additive closure of Z follows from the fact that

$$g(x) = \mu^{-(2^i+1)}(\xi \mathrm{Tr}(\mu x) + \mathrm{Tr}(\xi^{2^i} \mu x))$$

is an $\mathbb{F}_2$-linear function.

We now prove that each element $(x, g(x)) \in Z \backslash \{(0, 0)\}$ is a Walsh zero of f. We only need to address the cases when $g(x) \neq 0$. Note that $\mu^{2^i+1} g(x) \in \mathbb{F}_{2^3}$. Using Lemma 4.1.5 we get

$$\begin{aligned}
\mathrm{Tr}(x g(x)^{-\frac{1}{2^i+1}}) &= \mathrm{Tr}(x\mu(\mu^{2^i+1} g(x))^{-\frac{1}{2^i+1}}) \\
&= \mathrm{Tr}(x\mu(\xi \mathrm{Tr}(\mu x) + \mathrm{Tr}(\xi^{2^i}\mu x))^{2^i}) \\
&= \mathrm{Tr}(x\mu\xi^{2^i}\mathrm{Tr}(\mu x) + x\mu \mathrm{Tr}(\xi^{2^i}\mu x)) \\
&= \mathrm{Tr}(x\mu\xi^{2^i}\mathrm{Tr}(\mu x)) + \mathrm{Tr}(x\mu \mathrm{Tr}(\xi^{2^i}\mu x)) \\
&= 0
\end{aligned}$$

because $\mathrm{Tr}(x\mu\xi^{2^i}\mathrm{Tr}(\mu x)) = \mathrm{Tr}(x\mu\xi^{2^i})\mathrm{Tr}(\mu x) = \mathrm{Tr}(x\mu \mathrm{Tr}(\xi^{2^i}\mu x))$. By considering the first components of the elements of Z it is clear that $\dim Z = n$. □

While Proposition 4.3.2 holds for each $\xi \in \mathbb{F}_{2^3}$, one obtains interesting results only when ξ is a primitive element of $\mathbb{F}_{2^3}$. If $\xi = 0, 1$ then Z is the trivial WZ space $Z_{[n,0]}$.

Proposition 4.3.3. *Suppose n is odd and m divides n. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1}$, with $\gcd(i, n) = 1$. Suppose μ is a fixed element of $\mathbb{F}^*_{2^n}$. Then*

$$Z = \{(\mu a, \mu^{2^i+1} b) : a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^m} \text{ and } \mathrm{Tr}^n_m(a) = b + b^{\frac{1}{2^i}}\}$$

is a WZ space of f.

Proof. First we show that each element $(\mu a, \mu^{2^i+1} b)$ of Z except for $(0, 0)$ is a Walsh zero of f. Note that $b^{-\frac{1}{2^i+1}} \in \mathbb{F}_{2^m}$. We have

$$\begin{aligned}
\mathrm{Tr}_1^n(\mu a(\mu^{2^i+1}b)^{-\frac{1}{2^i+1}}) &= \mathrm{Tr}_1^n(ab^{-\frac{1}{2^i+1}}) \\
&= \mathrm{Tr}_1^m(\mathrm{Tr}_m^n(ab^{-\frac{1}{2^i+1}})) \\
&= \mathrm{Tr}_1^m(b^{-\frac{1}{2^i+1}}\mathrm{Tr}_m^n(a)) \\
&= \mathrm{Tr}_1^m(b^{-\frac{1}{2^i+1}}(b+b^{\frac{1}{2^i}})) \\
&= \mathrm{Tr}_1^m(b^{\frac{2^i}{2^i+1}}+b^{\frac{1}{2^i(2^i+1)}}) \\
&= \mathrm{Tr}_1^m(b^{\frac{2^i}{2^i+1}})+\mathrm{Tr}_1^m\left(b^{\frac{2^{2i}}{2^i(2^i+1)}}\right) \\
&= 0
\end{aligned}$$

hence each nonzero element of Z is a Walsh zero of f.

Let $(\mu a_1, \mu^{2^i+1}b_1), (\mu a_2, \mu^{2^i+1}b_2) \in Z$. Then

$$(\mu a_1, \mu^{2^i+1}b_1) + (\mu a_2, \mu^{2^i+1}b_2) = (\mu(a_1+a_2), \mu^{2^i+1}(b_1+b_2)) \in Z$$

since $b_1 + b_2 \in \mathbb{F}_{2^m}$ and

$$\begin{aligned}
\mathrm{Tr}_m^n(a_1+a_2) &= \mathrm{Tr}_m^n(a_1)+\mathrm{Tr}_m^n(a_2) \\
&= b_1 + b_1^{\frac{1}{2^i}} + b_2 + b_2^{\frac{1}{2^i}} \\
&= (b_1+b_2)+(b_1+b_2)^{\frac{1}{2^i}}.
\end{aligned}$$

Therefore Z is additively closed.

For each of the 2^m choices for the second component $\mu^{2^i+1}b$ of an element of Z, there are 2^{n-m} choices for the first component μa such that $\mathrm{Tr}_m^n(a) = b + b^{\frac{1}{2^i}}$. It follows that the dimension of Z is n. □

Remark 4.3.4. *The WZ spaces given in Propositions 4.3.1, 4.3.2, and 4.3.3 along with the trivial WZ spaces $Z_{[n,0]}$ and $Z_{[0,n]}$ cover all possible WZ spaces for Gold APN permutations in odd dimension up to and including dimension 9.*

4.4 TI pairs of WZ spaces for Gold APN permutations

In this section we describe several theoretical constructions of trivially intersecting pairs of WZ spaces for Gold APN permutations in odd dimensions. We checked using the sboxU software package that these constructions cover all such pairs in dimensions less than or equal to 9. Obviously, the two trivial WZ spaces $Z_{[n,0]}, Z_{[0,n]}$ intersect trivially.

Proposition 4.4.1. *Let $n = 3k$ where k is odd and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1}$, with* $\gcd(i, n) = 1$. *Let*

$$Z = \{(x, \mu^{-(2^i+1)}(\xi \mathrm{Tr}(\mu x) + \mathrm{Tr}(\xi^{2^i} \mu x))) : x \in \mathbb{F}_{2^n}\}$$

where ξ is a fixed element of $\mathbb{F}_{2^3} \subset \mathbb{F}_{2^n}$ and μ is a fixed element of $\mathbb{F}_{2^n}^*$. Then Z is a WZ space of f and the pair $\{Z_{[0,n]}, Z\}$ intersects trivially.

Proof. It follows from Proposition 4.3.2 that Z is a WZ space of f. If $(x, c) \in Z_{[0,n]} \cap Z$, then $x = 0$ which implies $c = 0$. Therefore the pair $\{Z_{[0,n]}, Z\}$ intersects trivially. □

Note that in the above proposition, if $\xi \in \{0, 1\}$ then Z becomes the trivial WZ space $Z_{[n,0]}$.

Proposition 4.4.2. *Let n be odd and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1}$, with* $\gcd(i, n) = 1$. *Let*

$$Z = \{(\mu(b + b^{\frac{1}{2^i}}), \mu^{2^i+1} b) : b \in \mathbb{F}_{2^n}\}$$

with μ a fixed element of $\mathbb{F}_{2^n}^*$. Then Z is a WZ space of f and the pair $\{Z_{[n,0]}, Z\}$ intersects trivially.

Proof. It follows from Proposition 4.3.3 with $m := n$ that Z is a WZ space of f.

Suppose $(\mu(\beta + \beta^{\frac{1}{2^i}}), \mu^{2^i+1}\beta) \in Z \cap Z_{[n,0]}$. Then $\mu^{2^i+1}\beta = 0$ and since $\mu \neq 0$, we have $\beta = 0$. Therefore $\mu(\beta + \beta^{\frac{1}{2^i}}) = 0$ and the only element in the intersection is $(0, 0)$. □

Proposition 4.4.3. *Let $n = 3k$ where k is odd and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1}$, with* $\gcd(i, n) = 1$. *Let*

$$Y = \{(x, \mu^{-(2^i+1)}(\xi \mathrm{Tr}(\mu x) + \mathrm{Tr}(\xi^{2^i} \mu x))) : x \in \mathbb{F}_{2^n}\}$$

where ξ is a fixed element of $\mathbb{F}_{2^3} \subset \mathbb{F}_{2^n}$ and μ is a fixed element of $\mathbb{F}_{2^n}^*$. Let

$$Z = \{(\nu(b + b^{\frac{1}{2^i}}), \nu^{2^i+1} b) : b \in \mathbb{F}_{2^n}\}$$

with ν a fixed element of $\mathbb{F}_{2^n}^*$. Suppose also that $\mathrm{Tr}((\xi + \xi^{2^i})(\mu\nu)^{-2^i}) = 0$. *Then Y and Z are WZ spaces of f and the pair $\{Y, Z\}$ intersects trivially.*

Proof. It follows from Proposition 4.3.2 that Y is a WZ space of f and from Proposition 4.3.3 with $m = n$ that Z is a WZ space of f.

Suppose towards a contradiction that there exists an element, different from $(0, 0)$, in $Y \cap Z$. Then for this element, we have $x = \nu(b + b^{\frac{1}{2^i}})$. It follows that $b \neq 0$ and

$$(\mu\nu)^{2^i+1} b = \xi \mathrm{Tr}(\mu\nu(b + b^{\frac{1}{2^i}})) + \mathrm{Tr}(\xi^{2^i} \mu\nu(b + b^{\frac{1}{2^i}})). \tag{4.1}$$

By looking at the right-hand side of (4.1) we can see that $(\mu\nu)^{2^i+1}b \in \{0, 1, \xi, \xi+1\}$. But since $\mu \neq 0$, $\nu \neq 0$, and $b \neq 0$, we have $(\mu\nu)^{2^i+1}b \in \{1, \xi, \xi+1\}$. We will look at these three cases below.

First assume that $(\mu\nu)^{2^i+1}b = 1$. Observe that

$$\begin{aligned}
\mathrm{Tr}(\xi^{2^i}\mu\nu(b + b^{\frac{1}{2^i}})) &= \mathrm{Tr}(\xi^{2^i}\mu\nu(\mu\nu)^{-(2^i+1)} + \xi^{2^i}\mu\nu(\mu\nu)^{-\frac{2^i+1}{2^i}}) \\
&= \mathrm{Tr}(\xi^{2^i}(\mu\nu)^{-2^i}) + \mathrm{Tr}(\xi^{2^i}(\mu\nu)^{-\frac{1}{2^i}}) \\
&= \mathrm{Tr}(\xi^{2^i}(\mu\nu)^{-2^i}) + \mathrm{Tr}\left(\xi^{2^{3i}}(\mu\nu)^{-\frac{2^{2i}}{2^i}}\right) \\
&= \mathrm{Tr}(\xi^{2^i}(\mu\nu)^{-2^i}) + \mathrm{Tr}(\xi^{2^{3i}}(\mu\nu)^{-2^i}) \\
&= \mathrm{Tr}((\xi^{2^i} + \xi)(\mu\nu)^{-2^i}) = 0
\end{aligned}$$

which contradicts (4.1).

Finally assume that $(\mu\nu)^{2^i+1}b = z$ and $z \in \{\xi, \xi+1\}$. Then

$$\begin{aligned}
\mathrm{Tr}(\mu\nu(b + b^{\frac{1}{2^i}})) &= \mathrm{Tr}(z\mu\nu(\mu\nu)^{-(2^i+1)} + z^{\frac{1}{2^i}}\mu\nu(\mu\nu)^{-\frac{2^i+1}{2^i}}) \\
&= \mathrm{Tr}(z(\mu\nu)^{-2^i}) + \mathrm{Tr}(z^{\frac{1}{2^i}}(\mu\nu)^{-\frac{1}{2^i}}) \\
&= \mathrm{Tr}(z(\mu\nu)^{-2^i}) + \mathrm{Tr}\left(z^{\frac{2^{2i}}{2^i}}(\mu\nu)^{-\frac{2^{2i}}{2^i}}\right) \\
&= \mathrm{Tr}(z(\mu\nu)^{-2^i}) + \mathrm{Tr}(z^{2^i}(\mu\nu)^{-2^i}) \\
&= \mathrm{Tr}((\xi + \xi^{2^i})(\mu\nu)^{-2^i}) = 0
\end{aligned}$$

which again contradicts (4.1).

Since all cases are exhausted, the only element in the intersection is $(0, 0)$ and the proof is complete. □

Proposition 4.4.4. *Let $n = 3k$ where k is odd and $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^{2^i+1}$, with $\gcd(i, n) = 1$. Let*

$$Y = \{(\nu(b + b^{\frac{1}{2^i}}), \nu^{2^i+1}b) : b \in \mathbb{F}_{2^n}\}$$

with ν a fixed element of $\mathbb{F}_{2^n}^*$. Suppose ξ is a fixed primitive element of $\mathbb{F}_{2^3} \subset \mathbb{F}_{2^n}$. Let

$$Z = X \times S$$

with $S = \mathrm{span}_{\mathbb{F}_2}\{\mu, \xi\mu\}$ for some fixed $\mu \in \mathbb{F}_{2^n}^*$ and Z is constructed by applying Proposition 4.3.1. Suppose also that $\mathrm{Tr}((\xi + \xi^{2^i})\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) = 1$. Then Y and Z are WZ spaces of f and the pair $\{Y, Z\}$ intersects trivially.

Proof. It follows from Proposition 4.3.3 with $m = n$ that Y is a WZ space of f.

Note that S is i-compatible by Lemma 4.1.6 and Example 4.1.3(ii): If $T = \operatorname{span}_{\mathbb{F}_2}\{1, \xi\}$ then $S = \mu T$. From Proposition 4.3.1 we have

$$X = \{x \in \mathbb{F}_{2^n} : (\forall \alpha \in S^{-\frac{1}{2^i+1}})\mathrm{Tr}(\alpha x) = 0\}$$

where

$$S^{-\frac{1}{2^i+1}} = \{0, \mu^{-\frac{1}{2^i+1}}, (\xi\mu)^{-\frac{1}{2^i+1}}, ((1+\xi)\mu)^{-\frac{1}{2^i+1}}\}.$$

Suppose towards a contradiction that $(\nu(b + b^{\frac{1}{2^i}}), \nu^{2^i+1}b)$ is a nonzero element belonging to $Y \cap Z$. Then $\nu^{2^i+1}b \in S \setminus \{0\} = \{\mu, \xi\mu, (1+\xi)\mu\}$. We will look at these three cases below.

First assume $\nu^{2^i+1}b = \mu$. Take $\alpha = (\xi\mu)^{-\frac{1}{2^i+1}} \in S^{-\frac{1}{2^i+1}}$. By Lemma 4.1.5 we have $\alpha = \xi^{2^i}\mu^{-\frac{1}{2^i+1}}$. Then by the condition defining X, we should have $\mathrm{Tr}(\alpha\nu(b + b^{\frac{1}{2^i}})) = 0$. But

$$\begin{aligned}
\mathrm{Tr}(\alpha\nu(b + b^{\frac{1}{2^i}})) &= \mathrm{Tr}(\xi^{2^i}\mu^{-\frac{1}{2^i+1}}\nu(\mu\nu^{-2^i-1} + \mu^{\frac{1}{2^i}}\nu^{-\frac{1}{2^i}-1})) \\
&= \mathrm{Tr}(\xi^{2^i}(\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i} + \mu^{\frac{1}{(2^i+1)2^i}}\nu^{-\frac{1}{2^i}})) \\
&= \mathrm{Tr}(\xi^{2^i}\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) + \mathrm{Tr}(\xi^{2^{3i}}\mu^{\frac{2^{2i}}{(2^i+1)2^i}}\nu^{-\frac{2^{2i}}{2^i}}) \\
&= \mathrm{Tr}(\xi^{2^i}\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) + \mathrm{Tr}(\xi\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) \\
&= \mathrm{Tr}((\xi + \xi^{2^i})\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) = 1.
\end{aligned}$$

Finally assume that $\nu^{2^i+1}b = z\mu$ and $z \in \{\xi, \xi+1\}$. Take $\alpha = \mu^{-\frac{1}{2^i+1}} \in S^{-\frac{1}{2^i+1}}$. By the condition defining X, we should have $\mathrm{Tr}(\alpha\nu(b + b^{\frac{1}{2^i}})) = 0$. But

$$\begin{aligned}
\mathrm{Tr}(\alpha\nu(b + b^{\frac{1}{2^i}})) &= \mathrm{Tr}(\mu^{-\frac{1}{2^i+1}}\nu(z\mu\nu^{-2^i-1} + z^{\frac{1}{2^i}}\mu^{\frac{1}{2^i}}\nu^{-\frac{1}{2^i}-1})) \\
&= \mathrm{Tr}(z\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i} + z^{\frac{1}{2^i}}\mu^{\frac{1}{(2^i+1)2^i}}\nu^{-\frac{1}{2^i}}) \\
&= \mathrm{Tr}(z\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) + \mathrm{Tr}(z^{\frac{2^{2i}}{2^i}}\mu^{\frac{2^{2i}}{(2^i+1)2^i}}\nu^{-\frac{2^{2i}}{2^i}}) \\
&= \mathrm{Tr}(z\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) + \mathrm{Tr}(z^{2^i}\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) \\
&= \mathrm{Tr}((\xi + \xi^{2^i})\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) = 1.
\end{aligned}$$

Since all cases are exhausted, the only element in the intersection is $(0, 0)$ and we are done. □

There are some similarities between both TI pair constructions above. Proposition 4.4.3 requires the condition

$$\mathrm{Tr}((\xi + \xi^{2^i})(\mu\nu)^{-2^i}) = 0 \tag{4.2}$$

while Proposition 4.4.4 requires the condition

$$\mathrm{Tr}((\xi + \xi^{2^i})\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) = 1. \tag{4.3}$$

If $\xi = 0, 1$ then (4.2) is always satisfied, while (4.3) is never satisfied.

A natural question to ask is how often the pairs of WZ spaces above intersect trivially. Since there are too many pairs to list exhaustively, we could randomly generate possible TI pairs by sampling ξ, μ, and ν uniformly from their domains. If $\xi \in \{0, 1\}$ then in Proposition 4.4.3 the trace condition is always satisfied and we get a trivial WZ space for Y. In the following we analyze the cases when $\xi \notin \{0, 1\}$. We compute the probability of the trace condition being satisfied in Propositions 4.4.3 and 4.4.4.

Denote $a = \xi + \xi^{2^i}$ which is nonzero when ξ is chosen uniformly at random from $\mathbb{F}_{2^3}\backslash\{0, 1\}$. Let $\in \mathbb{F}_{2^3}^*$ be fixed and let $i \in \mathbb{N}$. Then $\mathrm{Tr}(a(\mu\nu)^{-2^i}) = 0$ is satisfied with probability close to 1/2 assuming that μ, ν are sampled uniformly at random from $\mathbb{F}_{2^n}^*$, for the following reasons. It is clear that $\mu\nu$ is uniform and hence so is $(\mu\nu)^{-1}$. Since $x \mapsto x^{2^i}$ is a bijection, it also preserves the uniform distribution and so $(\mu\nu)^{-2^i}$ is uniform. Therefore, for $\mu\nu \in \mathbb{F}_{2^n}^*$ chosen uniformly at random, $\mathrm{Tr}(a(\mu\nu)^{-2^i}) = 0$ is satisfied with probability close to 1/2 because the trace function is balanced, see Proposition 2.2.2. (It will not be satisfied with probability exactly 1/2 since 0 is the only element of $\mathbb{F}_{2^n}$ that cannot be expressed as $(\mu\nu)^{-2^i}$.)

Similarly, let $a \in \mathbb{F}_{2^3}^*$ be fixed and let $i \in \mathbb{N}$. Then $\mathrm{Tr}(a(\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}) = 1$ is satisfied with probability close to 1/2 assuming that μ, ν are sampled uniformly at random from $\mathbb{F}_{2^n}^*$, for the following reasons. From Proposition 2.2.7 $x \mapsto x^{2^i+1}$ is a permutation of $\mathbb{F}_{2^n}$, hence the inverse function $x^{\frac{1}{2^i+1}}$ is also a permutation of $\mathbb{F}_{2^n}$. Thus $\mu^{\frac{1}{2^i+1}}$ has a uniform distribution. By the same reasoning as above, it follows that $\mu^{\frac{2^i}{2^i+1}}$ is uniform and so is $\mu^{\frac{2^i}{2^i+1}}\nu^{-2^i}$.

4.5 Applications

4.5.1 Classifying EA classes of functions

Recall that functions f and g mapping $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ are extended affine equivalent (EA-equivalent) if there exist affine permutations L_1, L_2 of $\mathbb{F}_{2^n}$ and an affine function L_3 such that $L_1(f(L_2(x))) + L_3(x) = g(x)$ for all $x \in \mathbb{F}_{2^n}$. In Chapter 2 we observed that EA-equivalent functions are also CCZ-equivalent, but partitioning CCZ classes into EA classes is in general a hard problem. This problem was addressed by Canteaut and Perrin [10] by studying the structure of the Walsh zeros of functions. WZ spaces play an important role in their investigations.

To bring up a more specific example, in [10, Lemma 12] it is stated that the CCZ class of $f(x) = x^3$ on $\mathbb{F}_{2^5}$ contains three EA classes, and this is based on the classification of 64 WZ spaces that according to [10] were found experimentally. Here we can give a computer-free description of these spaces: 32 of them are obtained from Proposition 4.3.3 with $m = n = 5$, and the remaining 32 of them are obtained from Proposition 4.3.1 with $S = \mu\mathbb{F}_2$ where $\mu \in \mathbb{F}_{2^5}$.

4.5.2 Construction of new APN permutations

If we know two trivially intersecting WZ spaces for an APN function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, then Proposition 2.5.7 allows us to construct an APN permutation f' of $\mathbb{F}_{2^n}$. Then f' is CCZ-equivalent to f, but in general it need not be EA-equivalent to it.

Recall from Example 2.2.9 that for $n = 9$, $f(x) = x^3$ has algebraic degree 2 while its compositional inverse $g(x) = x^{\frac{1}{3}}$ has algebraic degree 5. By applying Proposition 2.5.7 along with constructions of trivially intersecting WZ spaces provided in Section 4.4 above, we found APN permutations of $\mathbb{F}_{2^9}$ of algebraic degrees 2, 4 and 5. Since the algebraic degree is preserved by EA equivalence, the APN permutations of degree 4 are not EA-equivalent to f or g.

But in general, it is hard to determine if a given APN function is “new”. One could check if their new APN permutation is EA-equivalent to an already known one. However, many APN functions are being constructed numerically. For example, in [35] over 8000 CCZ-inequivalent APN functions in dimension 8 were found that do not belong to any known families. Recently, 12921 more APN functions have been added to this list [2]. While checking EA-equivalence is a relatively straightforward process, this would add large volumes of computations to this thesis.

The constructions in Section 4.4 work in arbitrary odd dimensions and for all Gold APN functions. It will be interesting to investigate how many EA-inequivalent APN permutations they provide.

4.6 Other functions

Having constructed families of TI pairs for the Gold functions naturally we ask if similar research is possible for other known APN functions. Given an APN function f, this would amount to characterizing the Walsh zeros of f, listing the WZ spaces of f (although one might be able to infer WZ spaces of f just from its Walsh zeros), and finally constructing TI pairs of f.

We give details on several APN functions and their WZ graphs which may be of interest due to their similarities to Gold functions.

4.6.1 Monomial APN functions

We have computed the WZ graphs of monomial APN functions of the form $x \mapsto x^d$ given in Table 2.2.1 up to and including dimension 9.

In dimension $n = 3$ we have found that all monomial APN functions have the same WZ graph as the Gold WZ graph given in Figure 4.1.

In dimension $n = 5$ we have found that the Kasami APN monomial with $d = 24$ has the same WZ graph as the Gold WZ graph given in Figure 4.2. The Kasami APN monomials with $d = 13, 26$ and the Welch APN monomial with $d = 7$ all have the WZ graph given in Figure 4.5.

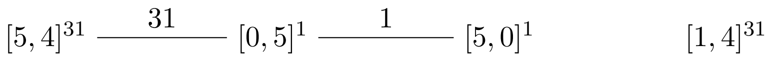

Figure 4.5: WZ graph of Kasami and Welch APN monomials on $\mathbb{F}_{2^5}$.

The Dobbertin APN monomial with $d = 29$ and the Inverse APN monomial with $d = 15$ both have the two trivial Walsh zero spaces as their only Walsh zero spaces.

In dimension $n = 7$ we have found that the Kasami APN monomial with $d = 96$ has the same WZ graph as the Gold WZ graph given in Figure 4.3. The Kasami APN monomials with $d = 13, 57, 104, 114$ and the Welch APN monomial with $d = 11$ and the Niho APN monomial with $d = 39$ and the Inverse APN monomial with $d = 63$ all have the two trivial Walsh zero spaces as their only Walsh zero spaces.

In dimension $n = 9$ we have found that the Kasami APN monomial with $d = 384$ has the same WZ graph as the Gold WZ graph given in Figure 4.4. The Kasami APN monomials with $d = 13, 241, 416, 482$ and the Welch and Niho APN monomials, both with $d = 19$, and the Inverse APN monomial with $d = 255$ all have the two trivial Walsh zero spaces as their only Walsh zero spaces.

4.6.2 The Budaghyan-Carlet-Leander function

In 2008, Budaghyan, Carlet and Leander [8] discovered an infinite class of APN functions which we describe below. Suppose $\gcd(k, 3) = 1$, $\gcd(s, 3k) = 1$, $i = sk \mod 3$, $t = 3 - i$, $n = 3k$, and the order of $\omega \in \mathbb{F}_{2^n}$ is $2^{2k} + 2^k + 1$. It is proved in [8] that the function

$$f(x) = x^{2^s+1} + \omega x^{2^{ik}+2^{tk+s}}$$

is APN. We call this function a BCL function and we will examine the case when $s = 1$.

Computationally we find that there are 190 WZ spaces of $f(x)$ in $\mathbb{F}_{2^6}$. The multiset containing dimensions of projections onto each component is

$$\{[6,0], [6,1]^{63}, [6,2]^{126}\}$$

which is the same as that for the Gold function x^3. But it is not clear how the constructions of the WZ spaces for Gold and BCL are related.

The only other dimension for the BCL function that we can compute is dimension 12, which takes too long to compute completely. But we can look at cases where either component is restricted to a subfield.

Restriction on WZ components	Multiset of dimensions of WZ spaces
$a \in \mathbb{F}_{2^{12}}, b \in \mathbb{F}_{2^2}$	$\{[12,0],[12,1]^3\}$
$a \in \mathbb{F}_{2^{12}}, b \in \mathbb{F}_{2^3}$	$\{[12,0],[12,1]^{21},[12,2]^{42}\}$
$a \in \mathbb{F}_{2^{12}}, b \in \mathbb{F}_{2^6}$	$\{[12,0],[12,1]^{64},[12,4]^{126}\}$
$a \in \mathbb{F}_{2^2}, b \in \mathbb{F}_{2^{12}}$	$\emptyset$
$a \in \mathbb{F}_{2^3}, b \in \mathbb{F}_{2^{12}}$	$\emptyset$
$a \in \mathbb{F}_{2^6}, b \in \mathbb{F}_{2^{12}}$	$\emptyset$

Table 4.1: Component dimensions for the BCL function in dimension 12.

Restriction on WZ components	Multiset of dimensions of WZ spaces
$a \in \mathbb{F}_{2^{12}}, b \in \mathbb{F}_{2^2}$	$\{[12,0],[12,1]^9\}$
$a \in \mathbb{F}_{2^{12}}, b \in \mathbb{F}_{2^3}$	$\{[12,0],[12,1]^{21},[12,2]^{42}\}$
$a \in \mathbb{F}_{2^{12}}, b \in \mathbb{F}_{2^6}$	$\{[12,0],[12,1]^{64},[12,4]^{126}\}$
$a \in \mathbb{F}_{2^2}, b \in \mathbb{F}_{2^{12}}$	$\emptyset$
$a \in \mathbb{F}_{2^3}, b \in \mathbb{F}_{2^{12}}$	$\emptyset$
$a \in \mathbb{F}_{2^6}, b \in \mathbb{F}_{2^{12}}$	$\emptyset$

Table 4.2: Component dimensions for $f(x) = x^3$ in dimension 12.

As we can see, Tables 4.1 and 4.2 are very similar but the Gold function has six extra WZ spaces of the form $[12, 1]$.

4.6.3 The Beierle-Carlet-Leander-Perrin function

In 2020, Beierle and Leander [2] proved that the functions $F_0, F_1 : \mathbb{F}_{2^9} \to \mathbb{F}_{2^9}$ given by

$$F_0(x) = x^3 + u^2x^{10} + ux^{24} + u^4x^{80} + u^6x^{136},$$
$$F_1(x) = x^3 + ux^{10} + u^2x^{17} + u^4x^{80} + u^5x^{192}$$

are APN permutations.

There are 4758 WZ spaces and 663552 TI pairs for F_0 and the WZ spaces corresponding to $[6,3]^{143}, [8,1]^{511}, [8,3]^{1001}$ do not participate in any TI pair. There are 5150 WZ spaces and 663552 TI pairs for F_1 and the WZ spaces corresponding to $[6,3]^{192}, [8,1]^{511}, [8,3]^{1344}$ do not participate in any TI pair. Note that the WZ graphs given in Figures 4.6 and 4.7 have a similar structure to the WZ graph of the Gold function in dimension 9.

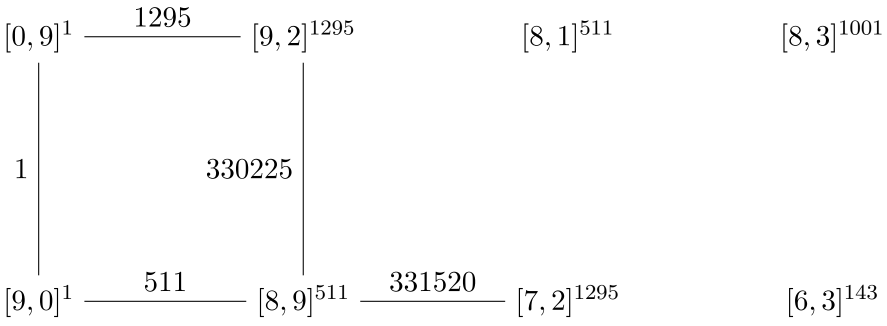

Figure 4.6: WZ graph of F_0.

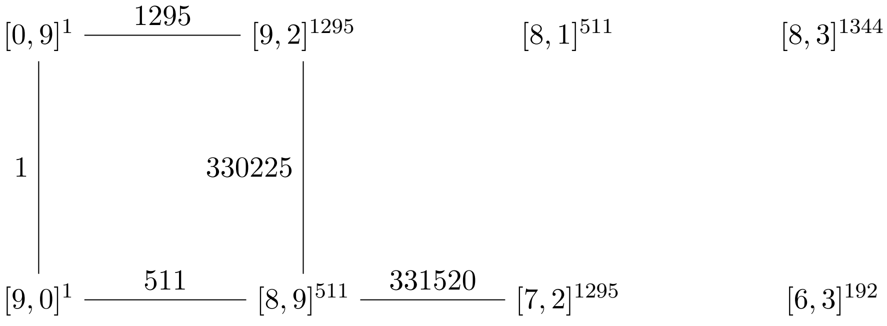

Figure 4.7: WZ graph of F_1.

4.6.4 Outlook

As far as our results show, WZ graphs of distinct Gold functions are the same for the dimensions for which we computed them. This could lead to a new and hopefully useful equivalence relation more general than CCZ-equivalence.

So far we have worked with WZ graphs which contract all WZ spaces with the same component dimensions into a single vertex. We can also consider more detailed WZ graphs in which each vertex represents a distinct WZ space. While we do not draw these graphs in larger dimensions due to their higher complexity, we can investigate them by using Magma. Computationally, we have found that up to and including dimension $n = 9$, any two of these detailed WZ graphs for Gold APN functions of $\mathbb{F}_{2^n}$ are isomorphic. Furthermore, certain Kasami APN functions, which are described in Section 4.6.1, also have detailed WZ graphs which are isomorphic to those of the Gold APN functions. It could be that there exist simple transformations between such functions that explain these structural similarities.

Overall, given all the results in Section 4.6, the prospect of future research seems very promising. It looks like our research can be continued with these APN functions or with any of the sporadic APN functions that have not been generalized into an infinite family.

Bibliography

[1] C. Beierle, C. Carlet, G. Leander, L. Perrin. A further study of quadratic APN permutations in dimension nine. arXiv:2104.08008, 2021.

[2] C. Beierle, G. Leander. New instances of quadratic APN functions. *IEEE Transactions on Information Theory*, 2021.

[3] E. Biham, A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

[4] X. Bonnetain, L. Perrin, T. Shizhu. Anomalies and vector space search: Tools for S-Box analysis. *Proceedings of ASIACRYPT 2019, pages 196–223.*

[5] W. Bosma, J. Cannon, C. Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

[6] K.A. Browning, J.F. Dillon, R.E. Kibler, M.T. McQuistan. APN polynomials and related codes. *Journal of Combinatorics, Information and System Science, Special Issue in honor of Prof. DK Ray-Chaudhuri on the occasion of his 75th birthday*, 34:135–159, 2009.

[7] K.A. Browning, J.F. Dillon, M.T. McQuistan, A.J. Wolfe. An APN permutation in dimension six. *Finite Fields: Theory and Applications*, 518:33–42, 2010.

[8] L. Budaghyan, C. Carlet, G. Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Transactions on Information Theory*, 54(9):4218–4229, 2008.

[9] M. Calderini, L. Budaghyan, C. Carlet. On known constructions of APN and AB functions and their relation to each other. *Cryptology ePrint Archive, Report 2020/1444*, 2020.

[10] A. Canteaut, L. Perrin. On CCZ-equivalence, extended-affine equivalence, and function twisting. *Finite Fields and Their Applications*, 56:209–246, 2019.

[11] C. Carlet. *Boolean functions for cryptography and coding theory.* Cambridge University Press, 2021.

[12] C. Carlet. Open questions on nonlinearity and on APN functions. In *International Workshop on the Arithmetic of Finite Fields*, pages 83–107. Springer, 2014.

[13] C. Carlet, P. Charpin, V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[14] B. Chase, P. Lisoněk. Construction of APN permutations via Walsh zero spaces. arXiv:2110.15582, 2021.

[15] B. Chase, P. Lisoněk. Kim-type APN functions are affine equivalent to Gold functions. *Cryptography and Communications*, 13:981-983, 2021.

[16] D. Cox, J. Little, D. O'Shea. *Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra.* Springer Science & Business Media, 2013.

[17] W. Diffie, M.E. Hellman. Cryptanalysis of the NBS data encryption standard, 1976.

[18] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE Transactions on Information Theory*, 14(1):154–156, 1968.

[19] F. Göloğlu, D. Krasnayová, P. Lisoněk. Generalized Kim APN functions are not equivalent to permutations. Preprint, 2020.

[20] F. Göloğlu, P. Langevin. Almost perfect nonlinear families which are not equivalent to permutations. *Finite Fields and Their Applications*, 67:101707, 2020.

[21] X. Hou. Affinity of permutations of $\mathbb{F}_2^n$. *Discrete Applied Mathematics*, 154(2):313–325, 2006.

[22] D. Krasnayová. *Constructions of APN permutations.* Master's thesis, Charles University, 2016. `https://dspace.cuni.cz/handle/20.500.11956/83075`.

[23] J. Lahtonen, G. McGuire, H.N. Ward. Gold and Kasami-Welch functions, quadratic forms, and bent functions. *Advances in Mathematics of Communications*, 1(2):243, 2007.

[24] K. Li, C. Li, T. Helleseth, L. Qu. A complete characterization of the APN property of a class of quadrinomials. *IEEE Transactions on Information Theory*, 67(11):7535–7549, 2021.

[25] R. Lidl, H. Niederreiter. *Introduction to Finite Fields and their Applications.* Cambridge University Press, 1994.

[26] P. Lisoněk. APN permutations and double simplex codes. `https://www.birs.ca/workshops/2015/15w5139/files/Lisonek.pdf`, accessed on 2021-11-23.

[27] P. Lisoněk, F. Göloğlu, D. Krasnayová. On a family of APN quadrinomials. The 13th International Conference on Finite Fields and Their Applications. `http://www.dma.unina.it/Fq13/Files/Booklet/Abstracts-Fq13.pdf`, accessed on 2021-11-20.

[28] J.H. van Lint. *Introduction to coding theory*, volume 86. Springer Science & Business Media, 2012.

[29] National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory. AES development - cryptographic standards and guidelines: CSRC. `https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development`, accessed on 2021-11-10.

[30] National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory. Finalists - lightweight cryptography: CSRC. `https://csrc.nist.gov/Projects/lightweight-cryptography/finalists`, accessed on 2021-11-10.

[31] K. Nyberg. Differentially uniform mappings for cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 55–64. Springer, 1993.

[32] K. Nyberg, L.R. Knudsen. Provable security against a differential attack. *Journal of Cryptology*, 8(1):27–37, 1995.

[33] L. Perrin, M. Joly. sboxU, 2021. `https://github.com/lpp-crypto/sboxU`, accessed on 2021-10-25.

[34] D.R. Stinson, M.B. Paterson. *Cryptography: Theory and Practice.* Fourth Edition. Taylor & Francis/CRC Press, 2019.

[35] Y. Yu, M. Wang, Y. Li. A matrix approach for constructing quadratic APN functions. *Designs, Codes and Cryptography*, 73(2):587–600, 2014.

Appendix A

Magma code for Chapter 2

The following is Magma code for Example 2.1.12.

```
> F := GF(101);
> K<x,y> := PolynomialRing(F,2);
>
> A := 4*x^4 + 3*x^3*y^2 + x*y + y + 5;
> B := x^4*y^3 + 2*x^2*y + x*y^4;
>
> Ry := UnivariatePolynomial(Resultant(A,B,x));
> "Roots of R(y)", Roots(Ry);
Roots of R(y) [ <0, 4>, <77, 1>, <96, 1> ]
>
> Rx := UnivariatePolynomial(Resultant(A,B,y));
> "Roots of R(x) ", Roots(Rx);
Roots of R(x)  [ <0, 2>, <11, 1>, <15, 1>, <49, 1>, <52, 1>, <86, 1> ]
>
> { [X,Y] : X,Y in F | Evaluate(A,[X,Y]) eq 0 and Evaluate(B,[X,Y]) eq 0 };
{
    [ 0, 96 ],
    [ 49, 0 ],
    [ 15, 0 ],
    [ 11, 77 ],
    [ 52, 0 ],
    [ 86, 0 ]
}
```

The following is Magma code showing how Krasnayová's APN conditions can be simplified.

```
> R<b,c,d> := RationalFunctionField(GF(2),3);
> S<T> := PolynomialRing(R,1);
>
> frf := function(f) // Factor Rational Function
>       mult := f/Normalize(f); // scalar multiple (w or w^2)
>       if mult ne 1 then print mult; end if;
>       return Factorization(Numerator(f)), Factorization(Denominator(f));
> end function;
>
> Delta := 1 + b + c + d;
>
> f := Delta*(T*Delta + c + d)*(T^2*Delta^2 + b*d + c);
> g := (T*Delta^2 + b*c + d)^2;
>
> q,r := Quotrem(f,g);
> f/g eq q + r/g;
true
>
> q; // Tr_1^m(q) = 0
T + (c + d)/(b + c + d + 1)
>
> frf(r);
b^3*d + b^2*c^2 + b^2*c + b*c^2*d + b*d^3 + b*d + c^3 + c*d^2 + c + d^2
[
    <T + (c + d)/(b + c + d + 1), 1>
]
[]
>
> frf(b^3*d + b^2*c^2 + b^2*c + b*c^2*d
   + b*d^3 + b*d + c^3 + c*d^2 + c + d^2);
[
    <b*d + c^2 + c + d^2, 1>,
    <b^2 + b*d + c + 1, 1>
]
[]
```

Appendix B

Magma code for Chapter 3

```
> R1<aa1,yy,zz,tt> := PolynomialRing(GF(2),4);
> R2<a1,y,u,z> := RationalFunctionField(GF(2),4);
> F4<w> := GF(4); //w is a primitive cube root of unity
> R3<U,Z,T,V> := RationalFunctionField(F4,4);
>
> frf := function(f) // Factor Rational Function
>       mult := f/Normalize(f); // scalar multiple (w or w^2)
>       if mult ne 1 then print mult; end if;
>       return Factorization(Numerator(f)), Factorization(Denominator(f));
> end function;
>
> // Proposition 3.2.4
> A := (aa1*tt + tt + 1)*tt^3;
> B := (aa1*tt + aa1 + tt)*(tt + 1)^3;
> Resultant(
>  aa1*yy*zz^2 + (aa1^4 + aa1^2 + yy^4 + yy^2)*zz + aa1*yy,
>   (tt^2 + tt)*(aa1^2 + yy^2 + 1) + aa1, yy )
> eq aa1^2*(A*zz^2 + B)*(B*zz^2 + A);
true
>
> // Proposition 3.2.6
> frf(
>  (y^2 + 1)*(a1 + a1*y*u*1/z)*(a1 + a1*y*1/u*z)
>  + (a1^2 + a1^2*y^2*1/u^2*z^2)*(a1*1/u + a1*y*1/z)
>   + (a1^2 + a1^2*y^2*u^2*1/z^2)*(a1*u + a1*y*z)
>    );
[
    <y*z + u, 1>,
    <y*u + z, 1>,
    <a1, 2>,
    <a1*y*u^4 + a1*y*z^2 + a1*u^3*z + a1*u*z + y^2*u^2*z + u^2*z, 1>
]
```

```
[
    <z, 2>,
    <u, 3>
]
>
> D := y*u^4 + y*z^2 + u^3*z + u*z;
> W := z*(y*z + u)/D;
>
> (u^4*z^2*(1 + y*1/u*z + y*u*1/z + y^2)/D^2) eq W^2 + W;
true
>
> Wq := 1/z*(y*1/z + 1/u)/(y*1/u^4 + y*1/z^2 + 1/u^3*1/z + 1/u*1/z);
> W + Wq;
1
>
> frf(
>  (y^4 + 1)*(a1*1/u + a1*y*1/z)
>   + (y^2 + 1)*(a1^2 + a1^2*y^2*u^2*1/z^2)
>   + (a1^2 + a1^2*y^2*1/u^2*z^2)*(a1*1/u + a1*y*1/z)
>   + (a1^2 + a1^2*y^2*u^2*1/z^2)*(a1*u + a1*y*z)
>    );
[
    <y*u + z, 1>,
    <a1, 1>,
    <a1^2*y^2*u^4*z + a1^2*y^2*z^3 + a1^2*y*u^5 + a1^2*y*u^3*z^2
    + a1^2*u^4*z + a1^2*u^2*z + a1*y^3*u^4 + a1*y^2*u^3*z
    + a1*y*u^4 + a1*u^3*z + y^4*u^2*z + u^2*z, 1>
]
[
    <z, 2>,
    <u, 3>
]
>
> A := D*(y*z + u);
> A eq y^2*u^4*z + y^2*z^3 + y*u^5 + y*u^3*z^2 + u^4*z + u^2*z;
true
> B := (y + 1)^2*u^3*(y*u + z);
> B eq y^3*u^4 + y^2*u^3*z + y*u^4 + u^3*z;
true
> C := (y + 1)^4*u^2*z;
> C eq y^4*u^2*z + u^2*z;
true
>
> Y := u*z*(u^2 + 1)/(u^2 + z)^2;
> frf( (Y+1)^2*z/(u*(Y*u + z)) );
[
    <u^3 + z, 2>
]
[
    <u, 1>,
    <u^2 + z, 2>
]
> A1 := (u^3 + z)^2/(u*(u^2 + z)^2);
> (A1 + A1*Y*u*1/z)*(A1 + A1*Y*1/u*z)/(Y^4 + 1);
1
>
> Aq := ((1/u^2 + 1/z)^2*y + 1/u*1/z*(1/u^2 + 1))*(y*1/z + 1/u);
> Bq := (y + 1)^2*1/u^3*(y*1/u + 1/z);
> Cq := (y + 1)^4*1/u^2*1/z;
> frf(
>               B*a1 + C + (A*Bq/Aq)*a1 + A*Cq/Aq
>               );
[
    <u, 1>,
    <y + 1, 2>,
    <a1*y^2*u^4 + a1*y^2*z^4 + y^3*u^2*z^3 + y^3*u^2*z + y^2*u^3*z^2
    + y^2*u*z^2 + y*u^2*z^3 + y*u^2*z + u^3*z^2 + u*z^2, 1>
]
[
    <y*u + z, 1>
]
>
> A1 := (y+1)^2*(y*u*z^2 + u^2*z + y*u + z)*u*z/((u+z)^4*y^2);
> frf(A*A1^2 + B*A1 + C);
[
    <z, 2>,
    <u, 2>,
    <u + 1, 2>,
    <y + 1, 4>,
    <y*z + u, 1>,
    <y*u + y*z^2 + u*z + z, 2>,
    <y*u^4 + y*z^2 + u^3*z + u*z, 1>
]
[
    <u + z, 8>,
    <y, 4>
]
>
> (y + z)/(y*(z^2 + 1)) + (y + 1/z)/(y*(1/z^2 + 1));
1
>
> Y := z*(u+1)/(u+z^2);
> A1 := (Y+1)^2*(Y*u*z^2 + u^2*z + Y*u + z)*u*z/((u+z)^4*Y^2);
> frf(A1);
```

```
[
    <z + 1, 2>,
    <u, 1>
]
[
    <u + 1, 1>,
    <u + z^2, 1>
]
> (A1 + A1*Y*u*1/z)*(A1 + A1*Y*1/u*z)/(Y^4 + 1);
u/(u^2 + 1)
>
>
> // Proposition 3.2.8
> a1 := (U^3 + Z)^2/(U*(U^2 + Z)^2);
> a2 := a1*U;
> a3 := U*Z^2*(U + 1)^2/(U^2 + Z)^2;
>
> //r = w^2*V;
> c0 := w*V^2 + w^2*V*T;
> frf(c0);
w^2
[
    <V, 1>,
    <T + w^2*V, 1>
]
[]
> c1 := V + T;
> c2 := 1/V*T + 1;
> c3 := w*1/V^2*T + w^2*1/V;
>
> frf( U*c1/c0 + c2/c0 );
w
[
    <T + V, 1>,
    <U*V + 1, 1>
]
[
    <V, 2>,
    <T + w^2*V, 1>
]
>
> // V = 1/U
> c0 := w*1/U^2 + w^2*1/U*T;
> c1 := 1/U + T;
> c2 := U*T + 1;
> c3 := w*U^2*T + w^2*U;
>
```

```
> frf(a1 + c1/c0);
w^2
[
    <U^7*T + w*U^6 + w^2*U^3*Z^2*T + w^2*U^2*Z^2 + w*U*Z^2*T + Z^2, 1>
]
[
    <U, 1>,
    <U*T + w^2, 1>,
    <U^2 + Z, 2>
]
> frf( (w*U^6 + w^2*U^2*Z^2 + Z^2)/(U^7 + w^2*U^3*Z^2 + w*U*Z^2) );
w
[
    <U^3 + w^2*U*Z + w*Z, 2>
]
[
    <U, 1>,
    <U^3 + w*U*Z + w^2*Z, 2>
]
> D := (w^2*U^3 + (U + w)*Z)^2;
> t := (w*U^3 + (U + w^2)*Z)^2/(U*D);
> t eq (w*U^6 + w^2*U^2*Z^2 + Z^2)/(U^7 + w^2*U^3*Z^2 + w*U*Z^2);
true
>
> frf( w^2*1/U^3/(1/U + w) + (U + w)/(w^2*U^3) );
w
[
    <U + 1, 2>
]
[
    <U, 3>,
    <U + w^2, 1>
]
>
> frf( w*1/U^2 + w^2*1/U*t );
w^2
[
    <U^2 + Z, 2>
]
[
    <U^3 + w*U*Z + w^2*Z, 2>
]
> frf( 1/U + t );
w^2
[
    <U^3 + Z, 2>
]
```

```
[
    <U, 1>,
    <U^3 + w*U*Z + w^2*Z, 2>
]
> frf( 1 + U*t );
w^2
[
    <U^3 + Z, 2>
]
[
    <U^3 + w*U*Z + w^2*Z, 2>
]
> frf( w^2*U + w*U^2*t );
w^2
[
    <Z, 2>,
    <U, 1>,
    <U + 1, 2>
]
[
    <U^3 + w*U*Z + w^2*Z, 2>
]
>
> frf(
>  (w*1/U^3 + (1/U + w^2)*1/Z)^2/(1/U*(w^2*1/U^3 + (1/U + w)*1/Z)^2)
>   + U*(w^2*U^3 + (U + w)*Z)^2/(w*U^3 + (U + w^2)*Z)^2
>    );
w^2
[
    <U, 3>,
    <U + Z, 2>,
    <U^3 + Z, 2>
]
[
    <U^3 + w^2*U*Z + w*Z, 2>,
    <U^3 + w^2*U^2 + w*Z, 2>
]
```

The following is Magma code demonstrating an example of the complex APN function in Proposition 3.2.6.

```
> m := 4;
> q := 2^m;
> F<alpha> := GF(2,2*m);
> U := { u : u in F | u^(2^m + 1) eq 1 };
> R<x> := PolynomialRing(GF(2));
> R!MinimalPolynomial(alpha);
```

```
x^8 + x^4 + x^3 + x^2 + 1
> u := alpha^225;
> z := alpha^135;
> u in U; z in U;
true
true
> a1 := (u^3 + z)^2/(u*(u^2 + z)^2);
> a2 := a1*u;
> a3 := u*z^2*(u + 1)^2/(u^2 + z)^2;
> f := func<x | x^(3*q) + a1*x^(2*q + 1) + a2*x^(q + 2) + a3*x^3 >;
>
> {
> { Multiplicity({* f(x+a) + f(x) : x in F *},b)
>       : b in {* f(x+a) + f(x) : x in F *} }
> : a in F | a ne 0
> };
{
    { 2 }
}
```

Appendix C

Magma code for Chapter 4

Below is Magma code that counts the number of two-dimensional *i*-compatible subspaces of $\mathbb{F}_{2^n}$.

```
for n in [3..17 by 2] do
printf"n = %o\n", n;
F := GF(2,n);
Fs := Set(F) diff {F!0};
Zn := Integers(2^n - 1);

for i in [1..n-1] do
if Gcd(i,n) eq 1 then

E := { e : e in Zn | ((2^i + 1)*e + 1 eq 0) };
assert(#E eq 1);
e := Z!Random(E);

numspaces := #{ {a,b,a+b} : a,b in Fs
               | (a^e + b^e eq (a+b)^e) and (a ne b)};
printf"CPU time %o \n", Cputime();
printf"[%o, %o], ", i, numspaces;

end if;
end for;
printf"\n\n";
end for;
```

```
n = 3
CPU time 0.820
[1, 7], CPU time 0.820
[2, 7],

n = 5
```

```
CPU time 0.860
[1, 0], CPU time 0.900
[2, 0], CPU time 0.920
[3, 0], CPU time 0.940
[4, 0],

n = 7
CPU time 1.200
[1, 0], CPU time 1.460
[2, 0], CPU time 1.740
[3, 0], CPU time 1.950
[4, 0], CPU time 1.970
[5, 0], CPU time 1.980
[6, 0],

n = 9
CPU time 2.220
[1, 511], CPU time 2.460
[2, 511], CPU time 2.700
[4, 511], CPU time 2.940
[5, 511], CPU time 3.180
[7, 511], CPU time 3.420
[8, 511],

n = 11
CPU time 7.180
[1, 0], CPU time 10.930
[2, 0], CPU time 14.690
[3, 0], CPU time 18.460
[4, 0], CPU time 22.210
[5, 0], CPU time 25.970
[6, 0], CPU time 29.720
[7, 0], CPU time 33.480
[8, 0], CPU time 37.230
[9, 0], CPU time 40.990
[10, 0],

n = 13
CPU time 101.120
[1, 0], CPU time 161.260
[2, 0], CPU time 221.410
[3, 0], CPU time 281.520
[4, 0], CPU time 341.670
[5, 0], CPU time 401.800
[6, 0], CPU time 461.900
[7, 0], CPU time 521.990
[8, 0], CPU time 582.090
```

```
[9, 0], CPU time 642.170
[10, 0], CPU time 702.250
[11, 0], CPU time 762.340
[12, 0],

n = 15
CPU time 1798.220
[1, 32767], CPU time 2838.110
[2, 32767], CPU time 3878.040
[4, 32767], CPU time 4917.970
[7, 32767], CPU time 5957.760
[8, 32767], CPU time 6997.550
[11, 32767], CPU time 8038.430
[13, 32767], CPU time 9079.290
[14, 32767],
```

The Magma code below finds bases for Walsh zero spaces for the Gold function x^3 in dimension $n = 3$. During its execution, it prepares the input data for sboxU, then it calls sboxU to compute the Walsh zero spaces bases. Then it reformats the data for further processing in Magma. It can be adapted for any function.

```
path := GetCurrentDirectory() cat "/";
ChangeDirectory(path cat "sboxu");

n := 3;
F<u> := GF(2^n);
Z := Integers();
R<x> := PolynomialRing(F);

IntRep := function(a,b)
  S := Eltseq(a) cat Eltseq(b);
  return &+[Z!S[i]*2^(i-1) : i in [1..2*n]];
end function;

// gold f(x) = x^(2^i + 1), gcd(i,n) = 1
d := 3;
f := x^d;

name := "3";
name;
WZ := [IntRep(a,b) : a,b in F | b eq 0 or Trace(a/Root(b,d)) eq 0];

//=======================================================================
// sboxU

SetOutputFile(path cat "sboxu/" cat name cat ".py": Overwrite := true);
printf"#!/usr/bin/sage
```

```
from sage.all import *
from sboxU import *\n\n";
printf"wz = %o\n\n", WZ;

printf"n = %o
N_threads = 10
word_length = 2*n
out = extract_bases(wz, n, word_length, N_threads, \"fixed dimension\")
print \'wzs := [%%s];\\n\' %% \', \'.join(map(str,out)) ", n;

UnsetOutputFile();

System("~/sage/sage-8.9/sage " cat name cat ".py
     > " cat "I" cat name cat ".m");

// reformat for magma
SetOutputFile(path cat "sboxu/" cat "I" cat name cat ".m":
  Overwrite := false);

printf"n := %o;
F<u> := GF(2^n);
Z := Integers();
R<x> := PolynomialRing(F);\n", n;

printf"
F2 := GF(2);
FRep := function(I)
  // find the binary representation of I
  S := Intseq(I,2);
  S := S cat [0 : i in [1..2*n-#S]];
  // now split S into [a,b] in (F x F)
  return [Seqelt([F2!S[i] : i in [1..n]], F),
          Seqelt([F2!S[i] : i in [n+1..2*n]], F)];
end function;
WZS := [ [FRep(I) : I in S] : S in wzs ];
printf\"WZS := \"; WZS;
printf\";\";
exit;
";

UnsetOutputFile();

SetOutputFile(path cat name cat ".m": Overwrite := true);
printf"n := %o;
F<u> := GF(2^n);
Z := Integers();
R<x> := PolynomialRing(F);
```

```
f := %o;\n", n, f;

UnsetOutputFile();
System("magma -b " cat "I" cat name cat ".m
>> " cat path cat name cat ".m");
SetOutputFile(path cat name cat ".m": Overwrite := false);

printf"
// create sequence of all F2-linear WZ spaces
V := VectorSpace(GF(2),2*n);
WZS := [ VectorSpaceWithBasis( [V![Eltseq(S[1])
         cat Eltseq(S[2])] : S in V1] ) : V1 in WZS];

// dimensions of projections onto components
{* [#{Eltseq(v)[1..n] : v in W},
 #{Eltseq(v)[n+1..2*n] : v in W}] : W in WZS *};

/*
// [d1,d2]^d
sd := [ W : W in WZS | [#{Eltseq(v)[1..n] : v in W},
                        #{Eltseq(v)[n+1..2*n] : v in W}] eq [2^d1,2^d2] ];
sd := [{[Seqelt(Eltseq(v)[1..n],F),
         Seqelt(Eltseq(v)[n+1..2*n],F)] : v in s} : s in sd];
//{* [ #{ab[1] : ab in s}, #{ab[2] : ab in s} ] : s in sd *};
*/
";
UnsetOutputFile();
exit;

// output
> n := 3;
> F<u> := GF(2^n);
> Z := Integers();
> R<x> := PolynomialRing(F);
> f := x^3;
> WZS := [
>     [
>         [ 1, 0 ],
>         [ u, 0 ],
>         [ u^2, 0 ]
>     ],
>     [
>         [ 1, 0 ],
>         [ u, 0 ],
>         [ 0, u^4 ]
>     ],
>     [
>           [ 1, 0 ],
>           [ u^2, 0 ],
>           [ 0, u ]
>       ],
>       [
>           [ 1, 0 ],
>           [ u^4, 0 ],
>           [ 0, u^2 ]
>       ],
>       [
>           [ 1, 0 ],
>           [ 0, u ],
>           [ 0, u^2 ]
>       ],
>       [
>           [ 1, 0 ],
>           [ u^2, u ],
>           [ u^4, u^2 ]
>       ],
>       [
>           [ u^4, 1 ],
>           [ 1, u ],
>           [ 0, u^2 ]
>       ],
>       [
>           [ u^4, 1 ],
>           [ u^6, u ],
>           [ u^4, u^2 ]
>       ],
>       [
>           [ u, 0 ],
>           [ u^2, 0 ],
>           [ 0, 1 ]
>       ],
>       [
>           [ u, 0 ],
>           [ u^6, 0 ],
>           [ 0, u^5 ]
>       ],
>       [
>           [ u, 0 ],
>           [ 0, 1 ],
>           [ 0, u^4 ]
>       ],
>       [
>           [ u, 0 ],
>           [ u^2, 1 ],
>          [ 1, u^4 ]
>      ],
>      [
>          [ u^3, 0 ],
>          [ u^2, 0 ],
>          [ 0, u^3 ]
>      ],
>      [
>          [ u^3, 0 ],
>          [ u^6, 0 ],
>          [ 0, u^6 ]
>      ],
>      [
>          [ u^3, 0 ],
>          [ 0, u^3 ],
>          [ 0, u^6 ]
>      ],
>      [
>          [ u^3, 0 ],
>          [ u^2, u^3 ],
>          [ u^6, u^6 ]
>      ],
>      [
>          [ u^2, 0 ],
>          [ 0, 1 ],
>          [ 0, u ]
>      ],
>      [
>          [ u^2, 0 ],
>          [ u, 1 ],
>          [ 1, u ]
>      ],
>      [
>          [ u^6, 0 ],
>          [ 0, u ],
>          [ 0, u^6 ]
>      ],
>      [
>          [ u^6, 0 ],
>          [ 1, u ],
>          [ u^3, u^6 ]
>      ],
>      [
>          [ u^4, 0 ],
>          [ 0, 1 ],
>          [ 0, u^2 ]
>      ],
>     [
>         [ u^4, 0 ],
>         [ u, 1 ],
>         [ 1, u^2 ]
>     ],
>     [
>         [ u^5, 0 ],
>         [ 0, u^3 ],
>         [ 0, u^2 ]
>     ],
>     [
>         [ u^5, 0 ],
>         [ u^3, u^3 ],
>         [ 1, u^2 ]
>     ],
>     [
>         [ 0, 1 ],
>         [ 0, u ],
>         [ 0, u^2 ]
>     ],
>     [
>         [ 0, 1 ],
>         [ u^2, u ],
>         [ u^4, u^2 ]
>     ],
>     [
>         [ u, 1 ],
>         [ 1, u ],
>         [ 1, u^2 ]
>     ],
>     [
>         [ u, 1 ],
>         [ u^6, u ],
>         [ u^5, u^2 ]
>     ],
>     [
>         [ u^2, 1 ],
>         [ 0, u ],
>         [ 1, u^2 ]
>     ],
>     [
>         [ u^2, 1 ],
>         [ u^2, u ],
>         [ u^5, u^2 ]
>     ]
> ]
> ;
> // create sequence of all F2-linear WZ spaces
> V := VectorSpace(GF(2),2*n);
> WZS := [ VectorSpaceWithBasis( [V![Eltseq(S[1])
>          cat Eltseq(S[2])] : S in V1] ) : V1 in WZS];
>
> // dimensions of projections onto components
> {* [#{Eltseq(v)[1..n] : v in W},
>  #{Eltseq(v)[n+1..2*n] : v in W}] : W in WZS *};
{*
    [ 1, 8 ],
    [ 2, 4 ]^^7,
    [ 4, 2 ]^^7,
    [ 4, 8 ]^^7,
    [ 8, 1 ],
    [ 8, 4 ]^^7
*}
>
> /*
> // [d1,d2]^d
> sd := [ W : W in WZS | [#{Eltseq(v)[1..n] : v in W},
>         #{Eltseq(v)[n+1..2*n] : v in W}] eq [2^d1,2^d2] ];
> sd := [{[Seqelt(Eltseq(v)[1..n],F),
>          Seqelt(Eltseq(v)[n+1..2*n],F)] : v in s} : s in sd];
> //{* [ #{ab[1] : ab in s}, #{ab[2] : ab in s} ] : s in sd *};
> */
```