Symmetry and Structures of APN Functions and Sidon Sets

A Senior Project submitted to
The Division of Science, Mathematics, and Computing
of
Bard College

by
Darrion Thornburgh

Annandale-on-Hudson, New York
May 2024

Abstract

Let F_p^n be the n-dimensional vector space over F_p. The graph $G_F = \{(x; F(x)) : x \in \mathrm{F}_p^n\}$ of a vectorial function $F : \mathrm{F}_p^n \to \mathrm{F}_p^m$ can have interesting combinatorial properties depending on varying cryptographic conditions on F. A vectorial Boolean function $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ is almost perfect nonlinear (APN) if there are at most 2 solutions to the equation $F(x + a) + F(x) = b$ for all $a, b \in \mathrm{F}_2^n$ where $a \neq 0$. Equivalently, F is APN if and only if G_F is a Sidon set, that is, a set in F_2^n where no four distinct points sum to zero. In this paper, we classify APN functions and important subclasses of APN functions in graph theoretical terms using the Kneser graph of all translations of G_F. We also study the properties of G_F as a Sidon set. In particular, we introduce the notion of uniform exclude distributions, and we study APN functions whose graphs have uniform exclude distributions.

Contents

Dedication

Dedicated to my late grandfather, Rex Thornburgh (May 1951 - January 2024).

Acknowledgments

I would like to give many thanks to my advisors Professor Bob McGrail and Professor Steven Simon for their time and suggestions throughout this work. I am very appreciative for Professor Lauren Rose for first introducing me to the study of Sidon sets during the summer of 2022 and always offering me strong encouragement and advice. I also extend much gratitude to Professor John Cullinan and Professor Caitlin Leverson for always being available, answering a plethora of questions, and supporting me throughout my time at Bard.

This work would have not been possible without the love and support of my family and friends. I thank Mom, Jordan, Kayla, Alex, Hannah, Vivian, Felicia, for always inspiring me and motivating throughout these four years and this year of research.

x

List of Symbols and Notation

p	a positive prime number	5
F_{p^n}	finite field of order p^n	5
F_p^n	n-dimensional vector space over F_p	5
F	a vectorial function $\mathrm{F}_p^n \to \mathrm{F}_p^m$	5
G_F	graph of a vectorial function	5
S	the set $S \setminus \{0\}$	5
$D_a F$	derivative of F in the direction of a	5
$_F(a;b)$	number of solutions to $F(x+a) - F(x) = b$	5
$_F$	differential spectrum of F	5
$_F(a;b)$	the Boolean function taking value 1 if and only if $a \neq 0$ and $_F(a;b) \neq 0$	7
f	a Boolean function $\mathrm{F}_p^n \to \mathrm{F}_2$	8
$NL(f)$	nonlinearity of a Boolean function	8
$d(g;h)$	Hamming distance	8
$b \quad F$	a component function of F	8
$NL(F)$	nonlinearity of a vectorial Boolean function	9
tr_n^m	the trace function from F_{2^n} into F_{2^m}	9
tr_n	the trace function from F_{2^n} into F_2	9
$x \quad y$	the standard dot product over F_2^n	9
W_F	Walsh transform of F	9
$\mathrm{wt}(f)$	weight of a Boolean function f	10
$_{a;b}$	the translation given by $(a;b)$	14
$[n]$	the set $\{1;2;\ldots;n\}$	16
$\#X$	size of a set X	16
$A \ t \ B$	the union of disjoint sets A and B	16
$\mathbf{X}_a(F)$	all translations of G_F of the form $_{a;b}(G_F)$ where a fixed	14

$\mathbf{Y}_b(F)$	all translations of G_F of the form $_{a;b}(G_F)$ where b xed	15
$\mathbf{G}(F)$	all translations of G_F of the form $_{x;F(x)}(G_F)$	19
$\mathbf{D}(F)$	all translations of G_F of the form $_{t;t}(G_F)$	20
$_F(x;y)$	diagonal translation multiplicity of $(x;y)$	20
K_F^n	the set of all points of diagonal translation multiplicity n	22
F	a family of sets	25
	a graph consisting of vertices and edges	25
$\overline{\ }$	complement graph of	26
K_n	complete graph with n vertices	26
$N\ (v)$	neighborhood of a vertex v	28
deg(v)	degree of a vertex v	28
Cay(f)	Cayley graph of a Boolean function f	30
KG(F)	Kneser graph of a family F	31
T_F	all translations of G_F	31
$!(\ )$	clique number of	36
$\mathbf{X}(S)$	exclude set of a Sidon set S	49
mult$_S(x)$	exclude point multiplicity	49
$e_{\min}(S)$	minimum exclude multiplicity of S	53
$e_{\max}(S)$	maximum exclude multiplicity of S	53
d_S	exclude distribution of a Sidon set S	54

1
Introduction

The study of Sidon sets goes back to Simon Sidon, who originally started studying this concept in the early 20th century. Sidon sets are well-known in number theory and have many interesting properties. In this thesis, we will study Sidon sets in F_2^n (which can also be thought of as Z_2^n). A Sidon set in F_2^n is a set such that no four distinct elements have a trivial sum. A very well-known open problem is to find the largest Sidon set in F_2^n for fixed n, and the exact answer to this problem is only known for $n \leq 10$.

Closely related to Sidon sets are almost perfect nonlinear (APN) functions. APN functions are those vectorial Boolean functions $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ such that the equation $F(x + a) + F(x) = b$ has either 0 or 2 solutions for all $a, b \in \mathrm{F}_2^n$ where $a \neq 0$. APN functions are an important notion in cryptography as they form the class of functions that are optimally resistant to differential cryptanalysis when used as an S-box in block ciphers (an important notion in symmetric cryptography). A key fact that we will reference throughout this work is that the graph $G_F = \{(x, F(x)) : x \in \mathrm{F}_2^n\}$ of a vectorial Boolean function $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ is a Sidon set if and only if F is APN. This fact draws a direct connection between symmetric cryptography and additive combinatorics.

Sidon sets can be used to model the card game EvenQuads [47], which is a SET-like card game. Similarly, so-called cap-sets can be used to model the card game SET. Cap-sets are those

sets in F_3^n where no three distinct points sum to zero, highlighting the analogy between cap sets and Sidon sets. The standard SET card deck is modeled by F_3^4, and it turns out that the largest size of a cap set in F_3^4 is 20.

One fact that motivated some of this work is that there exist four distinct cap sets in F_3^4 of size 20 (the largest size possible), which form a partition of F_3^4 minus a single point. Given that cap sets and Sidon sets are analogous, it would be interesting to similar partitions in F_2^n. While cap sets and Sidon sets are similar in their de nition, the mathematics of both vary signi cantly. Nonetheless, in Chapter 3, we provide constructions of partitions of $\mathrm{F}_2^n \quad \mathrm{F}_2^n$ consisting of 2^n maximal Sidon sets that are the graphs of APN functions. In Chapter 3, we use APN functions and their graphs in order to construct partitions of $(\mathrm{F}_2^n)^2$ into Sidon sets. In particular, we can use certain types of APN functions to construct partitions of $(\mathrm{F}_2^n)^2$ into 2^n distinct, pairwise disjoint, maximal Sidon sets for all n, see Theorem 3.1.2. In order to construct these partitions, we translate G_F.

By studying the collection of all translations of the graph of a vectorial function $F : \mathrm{F}_p^n \; ! \; \mathrm{F}_p^m$, where p is some positive prime, we are naturally led to studying exactly when two translations of G_F are disjoint. In fact, the intersections of two such translations are closely related to the di erential uniformity of F. In Chapter 4, we study the Kneser graph of all translations of the graph of a vectorial function, and we provide graph theoretical classi cations of APN and AB functions in Theorem 4.4.1 and Theorem 4.4.7, respectively. We classify AB functions by using strongly regular graphs, and we do this in Theorem 4.2.3 by providing a new direct proof that the Cayley graph of any bent Boolean function $f : \mathrm{F}_2^n \; ! \; \mathrm{F}_2$ is strongly regular with $= \quad = \mathrm{wt}(f) \quad 2^{n \;\; 2}$, and we also prove the converse of this statement.

In Chapter 5, we discuss the exclude distribution of a Sidon set in F_2^n. The exclude points of a Sidon set S are those points such that if any of them were to be included in S, the resulting set would not be Sidon. Each exclude point naturally has an exclude multiplicity, and the exclude distribution of S is the function that takes any point in $\mathrm{F}_2^n \; n \, S$ to its exclude multiplicity. We study in particular the exclude distributions of the graphs of APN functions. It is conjectured

that the graph of any APN function $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ is maximal [17] [12], that is, its exclude distribution always takes non-zero value. Little progress has been made on this conjecture, and it remains to be a very interesting open problem that has led to many fruitful discoveries.

We will discuss how a bound on the difference between the minimal and maximal values that the exclude distribution of G_F takes, where $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ is APN, can imply that G_F is maximal. In particular, a corollary to Theorem 5.3.10 is that if the difference between the minimal and maximal values that the exclude distribution of G_F takes is bounded by $\frac{2^n - 2}{6}$, then G_F must be a maximal Sidon set. Interestingly, almost bent (AB) functions (an important subclass of APN functions) are those functions $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ whose graph has an exclude distribution constant at $\frac{2^n - 2}{6}$.

Also in Chapter 5, we the notion of uniform exclude distributions. In short, an exclude distribution of a Sidon set $S \subset \mathrm{F}_2^n$ is uniform on an equally-sized partition of some subset of $\mathrm{F}_2^n \setminus S$ if it locally takes the same values at any element of the partition. We are interested in the case of when $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ is an APN function such that G_F has an exclude distribution that is uniform on an equally-sized partition of $(\mathrm{F}_2^n)^2 \setminus G_F$. We can partition $(\mathrm{F}_2^n)^2 \setminus G_F$ into the collection $Q(\mathrm{F}_2^n; F) = \{\{x\} \times (\mathrm{F}_2^n \setminus \{F(x)\}) : x \in \mathrm{F}_2^n\}$ which consists of sets that are n-dimensional affine subspaces (or flats) with a unique point, belonging to G_F, removed. That is, $Q(\mathrm{F}_2^n; F)$ is the collection of sets where given any set $Q \in Q(\mathrm{F}_2^n; F)$, all of the points in Q have their first coordinate as some fixed value x, and their second coordinate ranges across all values except $F(x)$. The significance of finding APN functions F whose graphs admit exclude distributions that are uniform on $Q(\mathrm{F}_2^n; F)$ is that we capture all of the information of the 3-sums of G_F by only considering the exclude distribution at a small collection of points. ,AB functions satisfy this by the van Dam, Fon-Der-Flaass characterization of AB functions [45]. We conclude Chapter 5 by using a of Carlet from Theorem 5.3.23 to prove if $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ is an APN plateaued function whose component functions are all unbalanced, then the exclude distribution of G_F is uniform on $Q(\mathrm{F}_2^n; F)$ of $(\mathrm{F}_2^n)^2$.

2
Background and survey

2.1 Vectorial functions and differential uniformity

For p prime, let F_{p^n} be the nite eld containing p^n elements. Denote by F_p^n the n-dimensional vector space over F_p. A **vectorial function** is a function $F : \mathrm{F}_p^n \to \mathrm{F}_p^m$. If $p = 2$, then we say that F is a **vectorial Boolean function**. The **graph** G_F of a vectorial function F is the set $(x; F(x)) : x \in \mathrm{F}_p^n$. Since both F_p^n and F_{p^n} can be considered as n-dimensional vector spaces, we will sometimes identify F_p^n with F_{p^n} in order to use its multiplicative structure. We also denote $S \setminus \{0\}$ as S^* for any set S.

Example 2.1.1. Consider the vectorial Boolean function $F : \mathrm{F}_2 \to \mathrm{F}_2$ de ned by $F(x) = x$ for all $x \in \mathrm{F}_2$. Then the graph of F is $G_F = \{(0;0); (1;1)\}$.

For any $a \neq 0$ in F_p^n, the function $D_a F : \mathrm{F}_p^n \to \mathrm{F}_p^m$ de ned by $D_a F(x) = F(x + a) - F(x)$ is the **derivative of F in the direction of a**. For any $a \in (\mathrm{F}_p^n)^*$ and $b \in \mathrm{F}_p^m$, we denote the number of solutions to $D_a F(x) = b$ as $_F(a;b)$. The set of all possible distinct values of $_F(a;b)$ is called the **differential spectrum** of F, denoted as $_F$. Hence,

$$_F = \{ _F(a;b) : a \in (\mathrm{F}_p^n)^* ; b \in \mathrm{F}_p^m \} :$$

Let be the maximal value in $_F$. Then, we call the **differential uniformity** of F, and we say F is **differentially -uniform**. Hence, if F is di erentially -uniform, then $D_aF(x) = b$ has at most solutions for all $a \in (\mathrm{F}_p^n)$ and all $b \in \mathrm{F}_p^m$.

Example 2.1.2. We will show that the function $F : \mathrm{F}_{2^n} \to \mathrm{F}_{2^n}$ de ned by $F(x) = x^3$ for all $x \in \mathrm{F}_{2^n}$ is di erentially 2-uniform. Let $a; b \in \mathrm{F}_{2^n}$ such that $a \neq 0$. Observe that since F_{2^n} is of characteristic 2, we have

$$\begin{aligned} D_aF(x) &= (x+a)^3 \quad x^3 \\ &= (x+a)^3 + x^3 \\ &= a^3 + 3a^2x + 3ax^2 + 2x^3 \\ &= a^3 + a^2x + ax^2. \end{aligned}$$

Therefore, $_F(a; b)$ is equal to the number of solutions to $a^3 + a^2x + ax^2 = b$, or equivalently, $x^2 + ax + a^2 = \frac{b}{a}$. Hence, $_F(a; b)$ 2, as these equations are quadratic in x. Also, it is clear that $_F \neq 0$, and since a solution x_0 to $D_aF(x) = b$ implies $x_0 + a$ is a solution, we know that F cannot be di erentially 1-uniform. Therefore, F is di erentially 2-uniform.

In general, the inequality $p^m \ n$ always holds for any vectorial function $F : \mathrm{F}_p^n \to \mathrm{F}_p^m$ [6], and in the case that the equality $= p^m \ n$ holds, we call F **perfect nonlinear** (PN). PN functions are those that are optimally resistant to a so-called di erential attack (see [5], [42]).

Cryptographers are particularly interested in the Boolean case, $p = 2$. However, as mentioned in [6], if $p = 2$, then PN functions only exist when $2m \ n$ and n is even. We easily verify the case $n = m$ and $p = 2$ because if x_0 is a solution to $F(x + a) + F(x) = b$, then $x_0 + a$ is also a solution.

Definition 2.1.3. Let $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ be a vectorial Boolean function. We call F **almost perfect nonlinear** (APN) if it is di erentially 2-uniform.

Since we already proved in Example 2.1.2 that the function $x \mapsto x^3$ over F_{2^n} is di erentially 2-uniform, we have our rst example of an APN function. APN functions are interesting, not

just due to their cryptographic characteristics but also because of their connections to additive combinatorics. In particular, APN functions are also those functions from $\mathbb{F}_2^n$ to itself whose graph is a Sidon set, which we de ne now.

Definition 2.1.4. Let $S \subseteq \mathbb{F}_2^n$ be a set. If no four distinct points in S sum to zero, we call S a **Sidon set**.

This connection between APN functions and Sidon sets holds because a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN if and only if the system of equations

$$\begin{cases} x + y + z + w = 0 \\ F(x) + F(y) + F(z) + F(w) = 0 \end{cases}$$

only has a solution $(x; y; z; w)$ if $x; y; z; w$ are not pairwise distinct [17]. Sidon sets are an important notion in combinatorics, and the connections between APN functions and Sidon sets are plentiful with many open problems (c.f. [17], [39], [43], [44], [19]).

Additionally, a function that we will use throughout this paper is the Boolean function $_F : \mathbb{F}_p^n \times \mathbb{F}_p^m \to \mathbb{F}_2$ de ned by

$$_F(a; b) = \begin{cases} 1 & \text{if } a \neq 0 \text{ and } _F(a; b) \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

We make the following observation.

Remark 2.1.5. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function. Then F is APN if and only if $2 \cdot _F(a; b) = _F(a; b)$ for all $a; b \in \mathbb{F}_2^n$ such that $a \neq 0$.

2.1.1 Notions of equivalence of vectorial functions

There are a few important equivalence relations of vectorial functions that have been introduced over the last few decades; and in this project, we may refer to the following three.

Definition 2.1.6. [9] Let F and F' be functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$. We say that F and F' are

1. **affine equivalent** if there exists a ne permutations $A_1 : \mathbb{F}_p^m \to \mathbb{F}_p^m$ and $A_2 : \mathbb{F}_p^n \to \mathbb{F}_p^n$ such that $F' = A_1 \circ F \circ A_2$;

2. **extended affine equivalent** (EA-equivalent) if there exist a ne maps $A; A_1; A_2$ from F_p^n to itself such that $F' = A_1 \quad F \quad A_2 + A$ and where A_1 and A_2 are permutations;

3. **Carlet-Charpin-Zinoviev equivalent** (CCZ-equivalent) if there exists an a ne permutation L of $(\mathrm{F}_p^n)^2$ such that $L(G_F) = G_{F'}$.

For each of the above equivalence relations, di erential uniformity is an invariant. As nomenclature would suggest, a ne equivalence is a particular case of EA-equivalence. Furthermore, it was shown in [18] that EA-equivalence is a particular case of CCZ-equivalence.

2.2 APN, AB, and crooked functions

In this section, we only consider the Boolean case, i.e. $p = 2$. As mentioned in Section 2.1, a function with the lowest possible di erential uniformity is optimally resistant to a so-called di erential attack. However, there is another type of attack, namely a linear attack (rst introduced in [36]), which is least e ective if the *nonlinearity* of $F : \mathrm{F}_2^n \ ! \ \mathrm{F}_2^m$ is high.

The **nonlinearity** $NL(f)$ of a Boolean function $f : \mathrm{F}_2^n \ ! \ \mathrm{F}_2$ is the minimum Hamming distance between f and all a ne Boolean functions. Recall that **Hamming distance** $d(g; h)$ of two functions $g; h : X \ ! \ Y$ is the cardinality of $fx \ 2 \ X : g(x) \ 6= \ h(x)g$ where X and Y are nite sets. we call $b \quad F$ a **component function** of $F : \mathrm{F}_2^n \ ! \ \mathrm{F}_2^m$. We then de ne the **nonlinearity** of $F : \mathrm{F}_2^n \ ! \ \mathrm{F}_2^m$ to be

$$NL(F) = \min_{\substack{b \in \mathrm{F}_2^m \\ b \neq 0}} NL(b \quad F):$$

Nonlinearity is invariant under CCZ-equivalence, meaning any two CCZ-equivalent vectorial Boolean functions have equal nonlinearity. One may correctly assume that the nonlinearity of a linear vectorial Boolean function is 0.

Remark 2.2.1. Consider some linear function $L : \mathrm{F}_2^n \ ! \ \mathrm{F}_2^m$, and let $b \ 2 \ \mathrm{F}_2^m$ such that all entries of b are equal to 1. Let $! : \mathrm{F}_2^m \ ! \ \mathrm{F}_2$ be the function de ned by

$$!(x) = \begin{cases} 0 & \text{if } x \text{ has an even number of non-zero entries} \\ 1 & \text{otherwise:} \end{cases}$$

It is straightforward that $b \circ F = \ell \circ F$. Furthermore, it is also easily observed that ℓ is linear, so $\ell \circ F = b \circ F$ is linear. Therefore, $NL(b \circ F) = 0$, implying $NL(F) = 0$.

The function $\mathrm{tr}_n^m : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ defined by $\mathrm{tr}_n^m(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{mi}}$ is called the **trace function**. If $m = 1$, then we denote tr_n^1 as tr_n. Note that tr_n is an inner product over $\mathbb{F}_{2^n}$.

For a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, the **Walsh transform** of f is the function $W_f : \mathbb{F}_2^n \to \mathbb{Z}$ defined by

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a \cdot x},$$

where $x \cdot y$ is the standard inner product over $\mathbb{F}_2^n$. In the case where we are considering $\mathbb{F}_2^n$ as $\mathbb{F}_{2^n}$, we use the trace inner product tr_n instead, that is, $x \cdot y = \mathrm{tr}_n(xy)$.

On the other hand, for a vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we define the **Walsh transform** of F to be the function $W_F : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{Z}$ defined by

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

Note that the formulae for the Walsh transform of a Boolean function and the formula for the Walsh transform of a vectorial Boolean function agree when $m = 1$. The Walsh transform is useful as it describes many important properties of F. In particular, the nonlinearity of F can be described by the Walsh transform since

$$NL(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n, b \in (\mathbb{F}_2^m)^*} |W_F(a, b)|,$$

see [10] for a proof of this. The maximal nonlinearity of a vectorial Boolean function is the universal bound $2^{n-1} - 2^{\frac{n}{2}-1}$ [10], we call functions achieving this bound **bent**. Equivalently, bent functions are those that are PN (see [37]). Note that $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is PN if and only if all derivatives $D_a f$ of f are **balanced**, taking the values of 0 and 1 equally often.

When $n = m$ and n odd, the nonlinearity of F is bounded by $2^{n-1} - 2^{\frac{n-1}{2}}$ [10]. Functions achieving this bound form an important class of functions, namely **almost bent** functions.

Definition 2.2.2. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function. We call F **almost bent** (AB) or **maximally nonlinear** if $NL(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$.

Clearly, the Walsh transform only takes integer values, so AB functions only exist for n odd. There are two other characterizations of AB functions that we will mention.

1. AB functions are those with $W_F(a,b) \in \left\{0, \pm 2^{\frac{n+1}{2}}\right\}$ for all $a,b \in \mathbb{F}_2^n$ such that $(a,b) \neq (0,0)$ (see [20]).

2. AB functions are those whose graph is a Sidon set $G_F \subset (\mathbb{F}_2^n)^2$ such that for any point $p \in (\mathbb{F}_2^n)^2 \cap G_F$, there are exactly $\frac{2^n-2}{6}$ subsets $\{a,b,c\} \subset G_F$ such that $a+b+c=p$ (see [45]). Using the terminology introduced in [43], all points in $(\mathbb{F}_2^n)^2 \cap G_F$ are "covered" $(\frac{2^n-2}{6})$ times if and only if F is AB.

We provide tables of the known infinite families of APN and AB power functions in Table 2.2.1 and Table 2.2.2, respectively. It has been conjectured since 1999 that Table 2.2.1 is complete, up to cyclotomic equivalence; recall that x^d and $x^{d'}$ are cyclotomic equivalent if there exists $0 \leq i < n$ such that $d \equiv 2^i d' \bmod 2^n - 1$ or, $d \equiv 2^i d^{-1} \bmod 2^n - 1$ when $\gcd(d, 2^n-1) = 1$. Note that in 2018, Dempwolff proved in [24] that cyclotomic equivalence and CCZ-equivalence coincide for power functions. Since cyclotomic equivalence is much easier to compute than CCZ-equivalence, this result was a breakthrough. Additionally, Yves Edel has computed that Table 2.2.1 is complete for $n \leq 34$ and $n = 36, 48, 40, 42$ (see [19] for further detail on Edel's computations).

Name	d	Condition	Reference
Gold	2^k+1	$\gcd(k,n)=1$	[30] [42]
Kasami	$2^{2k}-2^k+1$	$\gcd(k,n)=1$	[32] [33]
Welch	2^t+3	$n=2t+1$	[25]
Niho	$2^t+2^{\frac{t}{2}}-1$ if t even $2^t+2^{\frac{3t+1}{2}}-1$ if t odd	$n=2t+1$	[27]
Inverse	$2^{2t}-1$	$n=2t+1$	[42] [4]
Dobbertin	$2^{4t}+2^{3t}+2^{2t}+2^t-1$	$n=5t$	[26]

Table 2.2.1: Known infinite families of APN power functions $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ of the form $x \mapsto x^d$.

Now, we will introduce an important theorem which we will use in Chapter 4. First recall that the **weight** $\mathrm{wt}(f)$ of a Boolean function f over a finite set X is the sum $\sum_{x \in X} f(x)$. The

Name	d	Condition	Reference
Gold	$2^k + 1$	$\gcd(k,n) = 1$	[30] [42]
Kasami	$2^{2k} - 2^k + 1$	$\gcd(k,n) = 1$	[33]
Welch	$2^t + 3$	$n = 2t + 1$	[16] [15]
Niho	$\begin{cases} 2^t + 2^{\frac{t}{2}} - 1 & \text{if } t \text{ even} \\ 2^t + 2^{\frac{3t+1}{2}} - 1 & \text{if } t \text{ odd} \end{cases}$	$n = 2t + 1$	[31]

Table 2.2.2: Known infinite families of AB power functions $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ of the form $x \mapsto x^d$, n odd.

following theorem classifies APN (respectively AB) functions $\mathbb{F}_2^n \to \mathbb{F}_2^n$ in terms of the weight (respectively bentness) of $_F$, and it also provides additional useful properties of $_F$.

Theorem 2.2.3. [18] *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function. Then the following holds:*

1. *F is APN if and only if* $\mathrm{wt}(_F) = 2^{2n-1} - 2^{n-1}$.
2. *F is AB if and only if $_F$ is bent.*
3. *If F is APN, then the function $b \mapsto _F(a,b)$ is balanced for any nonzero $a \in \mathbb{F}_2^n$.*
4. *If F is an APN permutation, then the function $a \mapsto _F(a,b)$ is balanced for any nonzero $b \in \mathbb{F}_2^n$.*

2.2.1 Crooked functions

There is another important class of vectorial Boolean functions which are of interest: crooked functions.

Definition 2.2.4. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function. We call F **crooked** if the image set of the derivative D_aF is an affine hyperplane for all $a \in (\mathbb{F}_2^n)^*$.

This definition of crooked functions first appeared in [34], and it is a generalization of the definition first introduced in [1], which defines a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ to be crooked if F satisfies the following three properties:

1. $F(0) = 0$;
2. $F(x) + F(y) + F(x) + F(x + y + z) \neq 0$ for any distinct $x, y, z \in \mathbb{F}_2^n$;

3. $F(x) + F(y) + F(x) + F(x + a) + F(y + a) + F(z + a) \neq 0$ if $a \neq 0$ and $x; y; z \in \mathrm{F}_2^n$.

Unlike the original definition of crooked functions, the newer notion by Kyureghyan allows for crooked functions to also exist for n even. However, no crooked permutation exists for n even. Furthermore, Kyureghyan proved in [34] that the only crooked power maps are the quadratic maps $x \mapsto x^{2^i+2^j}$ where $\gcd(n; i - j) = 1$. Additionally, all crooked functions in odd dimensions are also AB, implying that they are also APN since all AB functions are APN (see [45]).

3
Translating graphs of vectorial functions

Before we begin this chapter, we will provide some motivating background. In nite geometry and combinatorics, a *cap set* is de ned to be a subset of $\mathbb{F}_3^n$ such that no three distinct elements sum to zero. The well-known cap set problem goes as follows: for a xed n, what is the largest size of a cap set in $\mathbb{F}_3^n$? Such a cap set is called *maximal*. Analogous to cap sets are Sidon sets in $\mathbb{F}_2^n$, which we recall to be the sets such that no four distinct points sum to zero. It is known that the graph of an APN power function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a *maximal* Sidon set, that is, $x \in \mathbb{F}_{2^n}^2 \setminus G_F$ implies $G_F \cup \{x\}$ is not Sidon (see [12], [17]). Note that although \maximal" has di erent meanings in the context of cap sets and Sidon sets, we will be considering maximal Sidon sets rather than Sidon sets with the largest possible size for a given n.

In [29], partitions of $\mathbb{F}_3^4$ into four distinct maximal cap sets, each of size 20, along with a single remaining point, were introduced. The question that motivates much of the research throughout this chapter is the following: can we do something similar for Sidon sets in $\mathbb{F}_{2^n}^2$ by partitioning $\mathbb{F}_{2^n}^2$ into 2^n distinct maximal Sidon sets? We show in this chapter that we indeed can construct such partitions.

3.1 Two different collections of translations of G_F

Recall that for a vectorial function $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$, the graph G_F of F is the set

$$G_F = \{(x; F(x)) : x \in \mathbb{F}_p^n\}:$$

In this section, we study translations of G_F and different collections of these translations.

For any $(a; b) \in \mathbb{F}_p^n \times \mathbb{F}_p^m$, let $\tau_{a;b} : \mathbb{F}_p^n \times \mathbb{F}_p^m \to \mathbb{F}_p^n \times \mathbb{F}_p^m$ be the translation given by $\tau_{a;b}(x; y) = (x + a; y + b)$ for all $(x; y) \in \mathbb{F}_p^n \times \mathbb{F}_p^m$. Hence

$$\begin{aligned}\tau_{a;b}(G_F) &= (a; b) + \{(x; F(x)) : x \in \mathbb{F}_p^m\} \\ &= \{(a + x; b + F(x)) : x \in \mathbb{F}_p^m\}:\end{aligned}$$

The following lemma demonstrates a direct connection between the differential spectrum of a vectorial function and the size of the intersection between any two translations of its graph.

Lemma 3.1.1. *Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ be a vectorial function. If $(a; b)$ and $(c; d)$ are in $\mathbb{F}_p^n \times \mathbb{F}_p^m$, then the size of the intersection $\tau_{a;b}(G_F) \cap \tau_{c;d}(G_F)$ is given by $\Delta_F(a - c; b - d)$.*

Proof. The size of $\tau_{a;b}(G_F) \cap \tau_{c;d}(G_F)$ is the number of solutions $(x; y)$ to the system of equations

$$x + a = y + c$$

$$F(x) + b = F(y) + d:$$

Thus, it is sufficient to count the number of solutions to $F(x + a - c) - F(x) = b - d$, which is given by $\Delta_F(a - c; b - d)$. □

Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ be a vectorial function. If $p = 2$ and $n = m$, Lemma 3.1.1 tells us that any two distinct translations of G_F must either be disjoint or intersect at exactly two points if F is APN. Now, we consider a collection of translations of G_F that form a partition of $\mathbb{F}_p^n \times \mathbb{F}_p^m$. For any $a \in \mathbb{F}_p^n$, let

$$\mathbf{X}_a(F) = \{\tau_{a;b}(G_F) : b \in \mathbb{F}_p^m\}: \tag{3.1.1}$$

We can think of $\mathbf{X}_a$ as the translations along the second coordinate with the first coordinate at a.

Let $a \in \mathbb{F}_p^n$. We now observe that $\mathbf{X}_a(F)$ partitions $\mathbb{F}_p^n \times \mathbb{F}_p^m$. Consider some point $(x_0; y_0) \in \mathbb{F}_p^n \times \mathbb{F}_p^m$, and let $x = x_0 - a$ and let $b = y_0 - F(x)$. Then $(x_0; y_0) = (a + x; b + F(x)) \in {}_{a;b}(G_F)$. Hence, $(x_0; y_0)$ is an element of a set in $\mathbf{X}_a(F)$. Said differently, any two translations ${}_{a;b_1}(G_F)$ and ${}_{a;b_2}(G_F)$ are disjoint if $b_1 \neq b_2$. Theorem 3.1.2 immediately follows.

Theorem 3.1.2. *Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ be a function, and let $a \in \mathbb{F}_p^n$. Then the sets in $\mathbf{X}_a(F)$ are pairwise disjoint. Equivalently, $\mathbf{X}_a(F)$ is a partition of $\mathbb{F}_p^n \times \mathbb{F}_p^m$.*

Corollary 3.1.3. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function, and let $a \in \mathbb{F}_2^n$. If F is APN, then $\mathbf{X}_a$ partitions $\mathbb{F}_2^n \times \mathbb{F}_2^n$ into 2^n distinct Sidon sets.*

Proof. Suppose F is APN. Then G_F is a Sidon set. Also for all $a; b \in (\mathbb{F}_2^n)^2$, the translation ${}_{a;b}(G_F)$ is a Sidon set because $(x; F(x)) + (y; F(y)) + (z; F(z)) + (w; F(w)) = 0$ if and only if $(a + x; b + F(x)) + (a + y; b + F(y)) + (a + z; b + F(z)) + (a + w; b + F(w)) = 0$ for all $x; y; z; w \in \mathbb{F}_2^n$.

Since the Sidon property is invariant under translation, ${}_{a;b}(G_F)$ is also a Sidon set for all $(a; b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$. Since all elements in $\mathbf{X}_a$ are disjoint, they must be distinct, so $\mathbf{X}_a$ is a partition of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ into 2^n distinct Sidon sets by Theorem 3.1.2. □

Now that we know that translating along the second coordinate where the first coordinate is fixed induces a partition of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ into 2^n distinct Sidon sets, we now study the opposite case: translating along the first coordinate where the second is fixed. For $b \in \mathbb{F}_p^m$, let

$$\mathbf{Y}_b(F) = \{ {}_{a;b}(G_F) : a \in \mathbb{F}_p^n \}. \tag{3.1.2}$$

Theorem 3.1.2 tells us that the size of the set $\bigcup_{X \in \mathbf{X}_a(F)} X$ is p^{n+m} for any $a \in \mathbb{F}_p^n$, or equivalently, partitions the entire space. However, as we will see in Theorem 3.1.5, it is possible that $\bigcup_{Y \in \mathbf{Y}_b(F)} Y$ does not cover all of $\mathbb{F}_p^n \times \mathbb{F}_p^m$.

Before we state Theorem 3.1.5, we introduce a definition and some notation.

Definition 3.1.4. Let A and B be sets, and let $f : A \to B$ be a function. We say f is N-to-1 over A if the size of the preimage set $f^{-1}(\{b\})$ is N for all $b \in \operatorname{im} f$. Furthermore, if $A' \subseteq A$, we say f is N-to-1 on A' if the restriction map $f|_{A'}$ is N-to-1.

Regarding notation, let denote by $[N]$ be the set $\{1, 2, \ldots, N\}$ for any $N \in \mathbb{N}$. Also, we use both $\#X$ and $|X|$ to denote the size of a finite set X, depending on which is most convenient. Finally, in the case where sets A and B are known to be disjoint, we can represent their union as $A \sqcup B$.

Theorem 3.1.5. *Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ be a function, and let $b \in \mathbb{F}_p^m$. If*

1. *$F(x) = 0$ if and only if $x = 0$, and*

2. *there exists $N \in \mathbb{N}$ dividing $p^n - 1$ such that F is N-to-1 on $(\mathbb{F}_p^n)^*$,*

then $\#\bigcup_{Y \in \mathbf{Y}_b(F)} Y = p^n + \frac{p^{2n} - p^n}{N}$. In particular, if F is a permutation, then $\mathbf{Y}_b(F)$ is a partition of $\mathbb{F}_p^n \times \mathbb{F}_p^n$.

Proof. Suppose (1) and (2) hold. Then, for any $a, a' \in \mathbb{F}_p^n$ and any $x \in (\mathbb{F}_p^n)^*$, we have

$$(a, b + F(0)) = (a, b) \neq (a' + x, b + F(x)).$$

Hence

$$\bigcup_{Y \in \mathbf{Y}_b(F)} Y = \bigcup_{a \in \mathbb{F}_p^n} G_{a,b}(F)$$
$$= \{(a, b + F(0)) : a \in \mathbb{F}_p^n\} \cup \{(a + x, b + F(x)) : a, x \in \mathbb{F}_p^n, x \neq 0\}.$$

Notice that the size of $\{(a, b + F(0)) : a \in \mathbb{F}_p^n\}$ is p^n.

It remains to compute the size of $\{(a + x, b + F(x)) : a, x \in \mathbb{F}_p^n, x \neq 0\}$. Let $a_0, x_0 \in \mathbb{F}_p^n$ such that $x_0 \neq 0$. First, we will show that

$$\{a \in \mathbb{F}_p^n : (a_0 + x_0, b + F(x_0)) \in G_{a,b}(F)\} = \{x_0 - x + a_0 : F(x) = F(x_0), x \in (\mathbb{F}_p^n)^*\}. \quad (3.1.3)$$

Indeed, the elements of the set on the left-hand side of eq. (3.1.3) are the elements $a \in \mathbb{F}_p^n$ where there exists $x \in \mathbb{F}_p^n$ such that $(a + x_0, b + F(x_0)) = (a + x, b + F(x))$, and since $F(x_0)$ must be equal to $F(x)$, we can rearrange to deduce that eq. (3.1.3) holds. Notice $x_0 - x + a_0 = x_0 - x' + a_0$ if and only if $x = x'$, so

$$\#\{a \in \mathbb{F}_p^n : (a_0 + x_0, b + F(x_0)) \in G_{a,b}(F)\} = N$$

since F is N-to-1 on $(\mathbb{F}_p^n)^*$. This means every point of the form $(a + x; b + F(x))$ where $x \neq 0$ is in exactly N distinct translations of G_F. Therefore

$$\#\left[_{Y \in \mathbf{Y}_b(F)} Y\right] = \#\{(a; b + F(0)) : a \in \mathbb{F}_p^n\} + \#\{(a + x; b + F(x)) : a; x \in \mathbb{F}_p^n; x \neq 0\}$$
$$= p^n + \frac{p^n(p^n - 1)}{N}.$$

Thus $\#\bigcup_{Y \in \mathbf{Y}_b(F)} Y = p^n + \frac{p^{2n} - p^n}{N}$, as desired. □

Corollary 3.1.6. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function, and let $b \in \mathbb{F}_2^n$. If F is an APN permutation, then $\mathbf{Y}_b$ partitions $\mathbb{F}_2^n \setminus \mathbb{F}_2^n$ into 2^n distinct Sidon sets.*

Proof. Suppose F is an APN permutation. Then F is 1-to-1 on all of $\mathbb{F}_2^n$. So, by Theorem 3.1.5, the size of the union of the translations in $\mathbf{Y}_a$ is $2^n + \frac{2^{2n} - 2^n}{1} = 2^{2n}$. Thus, $\mathbf{Y}_a$ is a partition of $\mathbb{F}_2^n \setminus \mathbb{F}_2^n$, and for similar reasoning as mentioned in Corollary 3.1.3, all elements of $\mathbf{Y}_b$ are Sidon sets. □

A special case of Corollary 3.1.6 is when F is a power function x^d over $\mathbb{F}_{2^n}$ for n odd. This is because an APN power function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $F(x) = x^d$ is bijective if n is odd and 3-to-1 on $\mathbb{F}_{2^n}$ (c.f. [28]). We can verify that any APN power function over $\mathbb{F}_{2^n}$ for n odd must be bijective by the following lemma. We thank John Cullinan for making key observations involved in the following proof.

Lemma 3.1.7. *Let $\psi : \mathbb{F}_{p^n}^* \to \mathbb{F}_{p^n}^*$ be a function given by $x \mapsto x^m$ for some integer m. Then*

1. *ψ is a homomorphism,*

2. *ψ is a permutation if and only if $p^n - 1$ is coprime to m.*

Proof. (1). Let $x; y \in \mathbb{F}_{p^n}$. Then $\psi(xy) = (xy)^m = x^m y^m = \psi(x)\psi(y)$. Hence ψ is a homomorphism.

(2). Since ψ is a homomorphism, we know that ψ is injective if and only if the kernel of ψ is trivial. Note that $\ker \psi = \{x \in \mathbb{F}_{p^n}^* \mid x^m = 1\}$. Since $\mathbb{F}_{p^n}^*$ is a cyclic group and the kernel of ψ is

a subgroup of $\mathbb{F}_{p^n}^?$, we deduce that $\ker\ '$ must be cyclic. Also, the order of $\ker\ '$ divides m. By Lagrange's Theorem, the order of $\ker\ '$ divides the order of $\mathbb{F}_{p^n}^?$ which is $p^n - 1$.

Suppose that $'$ is injective, and by way of contradiction suppose that $p^n - 1$ and m are not coprime. Then, there exists a positive integer $d > 1$ and integers $r; s$ such that $m = dr$ and $p^n - 1 = ds$. Also, recall that $x^{p^n - 1} = 1$ for all $x \in \mathbb{F}_{p^n}$. Therefore, for any $x \in \mathbb{F}_{p^n}$, we have

$$\begin{aligned}(x^s)^m &= (x^m)^s \\ &= (x^{dr})^s \\ &= (x^{ds})^r \\ &= (x^{p^n - 1})^r \\ &= 1^r \\ &= 1:\end{aligned}$$

Since $'$ is injective, this implies $x^s = 1$ for all $x \in \mathbb{F}_{p^n}$. However, this implies s is a multiple of $p^n - 1$, a contradiction since $p^n - 1 = ds$. Therefore, $p^n - 1$ must be coprime to m.

Conversely, suppose that $p^n - 1$ is coprime to m. Since $|\ker\ '|$ divides m, we know that $|\ker\ '|$ is also coprime to $p^n - 1$. However, since $|\ker\ '|$ divides $p^n - 1$, it follows that $|\ker\ '| = 1$. So the kernel of $'$ is trivial and $'$ is injective. □

Finding APN permutations $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, where n is even, is a large open problem in cryptography. Therefore, the only known instance for when the construction used in Theorem 3.1.5 can give a partition of $\mathbb{F}_2^n - \mathbb{F}_2^n$ into 2^n distinct Sidon sets is when $n = 6$. Namely, the APN permutation over $\mathbb{F}_{2^6}$ is given by

$$\begin{aligned}F(x) = {} & {}^{25}x^{57} + {}^{30}x^{56} + {}^{32}x^{50} + {}^{37}x^{49} + {}^{23}x^{48} + {}^{39}x^{43} + {}^{44}x^{42} + {}^{4}x^{41} + {}^{18}x^{40} + \\ & {}^{46}x^{36} + {}^{51}x^{35} + {}^{52}x^{34} + {}^{18}x^{33} + {}^{56}x^{32} + {}^{53}x^{29} + {}^{30}x^{28} + {}^{1}x^{25} + {}^{58}x^{24} + \\ & {}^{60}x^{22} + {}^{37}x^{21} + {}^{51}x^{20} + {}^{1}x^{18} + {}^{2}x^{17} + {}^{4}x^{15} + {}^{44}x^{14} + {}^{32}x^{13} + {}^{18}x^{12} + \\ & {}^{1}x^{11} + {}^{9}x^{10} + {}^{17}x^{8} + {}^{51}x^{7} + {}^{17}x^{6} + {}^{18}x^{5} + {}^{0}x^{4} + {}^{16}x^{3} + {}^{13}x^{1}\end{aligned}$$

where is a primitive element of F_{2^6} [8]. On the other hand, the construction used in Theorem 3.1.2 gives a partition of F_2^n F_2^n into 2^n distinct Sidon sets for all $n \in \mathbb{N}$ since there exists an APN function for all $n \in \mathbb{N}$.

3.2 Translations along the graph

Now, we will consider a third method of translating the graph of a vectorial function. For a function $F : F_p^n \to F_p^m$, let $\mathbf{G}(F)$ denote the set of translations

$$\mathbf{G}(F) = \{ {}_{a;F(a)}(G_F) : a \in F_p^n \}. \tag{3.2.1}$$

The set $\mathbf{G}(F)$ can be thought of as the translations along the graph of F.

Recall that if $X, Y \subseteq F_p^n$, then $X + Y$ denotes the set $\{x + y : x \in X, y \in Y\}$. We will now prove that the union of all translations in $\mathbf{G}(F)$ is equal to $G_F + G_F$ for any vectorial function $F : F_p^n \to F_p^m$.

Lemma 3.2.1. *Let $F : F_p^n \to F_p^m$ be a vectorial function. Then $\bigcup_{T \in \mathbf{G}(F)} T = G_F + G_F$.*

Proof. Let $(\ ,\ ) \in \bigcup_{T \in \mathbf{G}(F)} T$. Then there exists $a \in F_2^n$ such that $(\ ,\ ) \in {}_{a;F(a)}(G_F)$ $G_F + G_F$. Hence, $\bigcup_{T \in \mathbf{G}(F)} T \subseteq G_F + G_F$.

Now, suppose $(a + x, F(a) + F(x)) \in G_F + G_F$. Then

$$(a + x, F(a) + F(x)) \in {}_{a;F(a))}(G_F) \subseteq \bigcup_{T \in \mathbf{G}(F)} T.$$

Thus, $\bigcup_{T \in \mathbf{G}(F)} T \subseteq G_F + G_F$, and we conclude our proof. □

Proposition 3.2.2. *Let $F : F_2^n \to F_2^n$ be a function. If F is APN, then*

$$\# \bigcup_{T \in \mathbf{G}(F)} T = 2^{2n-1} - 2^{n-1} + 1$$

Proof. Suppose F is APN. By Lemma 3.2.1 $\bigcup_{T \in \mathbf{G}(F)} T = G_F + G_F$, so

$$\begin{aligned}\bigcup_{T \in \mathbf{G}(F)} T &= G_F + G_F \\ &= \{(a+b, F(a)+F(b)) : a, b \in \mathbb{F}_2^n\} \\ &= \{(0,0)\} \cup \{(a+b, F(a)+F(b)) : a, b \in \mathbb{F}_2^n, a \neq b\}.\end{aligned}$$

By the definition of a Sidon set, all pairwise sums of G_F are distinct, that is, $(a, F(a)) + (b, F(b)) = (c, F(c)) + (d, F(d))$ implies $\{a, b\} = \{c, d\}$ when $a, b, c, d \in \mathbb{F}_2^n$ are distinct. Therefore, $(a_1 + b_1, F(a_1) + F(b_1)) = (a_2 + b_2, F(a_2) + F(b_2))$ if and only if $\{a_1, b_1\} = \{a_2, b_2\}$ when F is APN. So,

$$|\{(a+b, F(a)+F(b)) : a, b \in \mathbb{F}_2^n, a \neq b\}| = \frac{1}{2}(2^{2n} - 2^n).$$

Thus, $\#\bigcup_{T \in \mathbf{G}(F)} T = 2^{2n-1} - 2^{n-1} + 1$. □

3.3 Translations along the diagonal

Similar to the previous section, we study collections of translations of the graph of a vectorial function. However, we now study the **diagonal translations** $\tau_{t,t}$ over $\mathbb{F}_p^n \times \mathbb{F}_p^n$. In particular, we are interested in computing the size of the collection of all diagonal translations of G_F where $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is a vectorial function. That is, given a vectorial function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$, we want to compute the size of $\mathbf{D}(F)$ where $\mathbf{D}(F)$ is the set

$$\mathbf{D}(F) = \bigcup_{t \in \mathbb{F}_p^n} \tau_{t,t}(G_F). \tag{3.3.1}$$

It is entirely possible that a point in $\mathbb{F}_p^n \times \mathbb{F}_p^n$ is contained in more than one diagonal translation of G_F. So, denote by $\delta_F(a, b)$ the number of diagonal translations of G_F that contain (a, b), that is,

$$\delta_F(a, b) = |\{t \in \mathbb{F}_p^n : (a, b) \in \tau_{t,t}(G_F)\}|.$$

We can easily show $\delta_F(a, b)$ is equal to the number of solutions to $F(x) + x = b - a$.

Lemma 3.3.1. *Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ be a function. Let $(a, b) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$. Then $\delta_F(a, b)$ is equal to the number of solutions to $F(x) - x = b - a$.*

Proof. Let $(a;b) \in \mathbf{D}(F)$. Then, $_F(a;b)$ is the number of $t \in \mathbb{F}_p^n$ where there exists $x \in \mathbb{F}_p^n$ such that

$$a = t + x$$

$$b = t + F(x);$$

which is equivalent to counting the number of solutions to $F(x) \quad x = b \quad a$. □

Clearly, for any function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$, we have the equality

$$\#\mathbf{D}(F) = \sum_{(a;b)\in\mathbf{D}(F)} \frac{1}{_F(a;b)}:$$

However, we can make this equality even simpler by realizing that the diagonal translation multiplicity of $(a;b) \in \mathbb{F}_p^n \quad \mathbb{F}_p^n$ is invariant under translation by $(t;t) \in \mathbb{F}_p^n \quad \mathbb{F}_p^n$. More explicitly, if $(a;b) \in \mathbf{D}(F)$, then we see that $_F(a;b) = _F(a + t;b + t)$ for any $t \in \mathbb{F}_p^n$ by Lemma 3.3.1. This gives the following.

Proposition 3.3.2. *The size of $\mathbf{D}(F)$ for a function F from $\mathbb{F}_p^n$ to itself is given by*

$$\#\mathbf{D}(F) = p^n \sum_{(a;b)\in G_F} \frac{1}{_F(a;b)}: \tag{3.3.2}$$

This tells us that we only need to compute the diagonal translation multiplicities of points in the graph of a vectorial function $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ to determine the size of $\mathbf{D}(F)$. Equivalently, to compute the size of $\mathbf{D}(F)$, it su ces to compute the number of solutions to $F(x) \quad x = F(a) \quad a$ for all $a \in \mathbb{F}_p^n$.

3.3.1 The Gold function

We now x $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ to be the vectorial Boolean function de ned by $F(x) = x^{2^k+1}$ where $\gcd(k;n) = 1$. As in Table 2.2.1, F is called the *Gold function*. The Gold function tends to be the \simplest" case of an APN power function to study. We will conjecture the size of $\mathbf{D}(F)$ where F is the Gold function motivated by computer calculations.

However, let us rst consider the case $F(x) = x^3$, or equivalently $x \mapsto x^{2^k+1}$ when $k = 1$. By Lemma 3.3.1, $_F(a;b)$ is the number of roots of $x^3 + x = a + b$ for any $(a;b) \in \mathbb{F}_{2^n}^2$. Therefore,

for this Gold function, $_F(a;b)$ is bounded above by 3, and we conjecture this holds for all other Gold functions as well.

Conjecture 3.3.3. *Let $k;n \in \mathbb{N}$, and suppose $\gcd(k;n) = 1$. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the Gold function given by $F(x) = x^{2^k+1}$. Then $_F(a;b) \leq 3$ for all $(a;b) \in \mathbb{F}_{2^n}^2$.*

Now, denote by K_F^n the set

$$K_F^n = \{(a;b) \in \mathbb{F}_{2^n}^2 : {}_F(a;b) = n\}:$$

Then $|\mathbf{D}(F)| = \sum_{i=1}^{M} i|K_F^i|$ where $M = \max_{(a;b)\in\mathbb{F}_{2^n}^2} {}_F(a;b)$. For the Gold function, we are able to compute K_F^2 by applying Lemma 3.3.1.

Theorem 3.3.4. *Let $k;n \in \mathbb{N}$, and suppose $\gcd(k;n) = 1$. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the Gold function given by $F(x) = x^{2^k+1}$. If $(a;b) \in \mathbf{D}(F)$ such that $a \neq b$, then $_F(a;b) = 2$.*

Proof. Let $(a;b) \in \mathbb{F}_{2^n}^2$. Suppose $(a;b) \in \mathbf{D}(F)$ such that $a + b = 0$. It suffices to count the number of solutions to $x(x+1)^{2^k} = 0$. We see that the only solutions must satisfy $x = 0$ or $x^{2^k} = 1$, and so therefore, the only solutions to $x(x+1)^{2^k} = 0$ are 0 and 1. Thus, $_F(a;b) = 2$. □

We conjecture that the converse of Theorem 3.3.4 holds as well. If true, this would mean all points $(a;b) \in \mathbf{D}(F)$ where $_F(a;b) = 2$ must satisfy $a = b$. However, notice that $x = x^{2^k+1}$ if and only if x is either 0 or 1. Therefore, our conjecture is equivalent to the following.

Conjecture 3.3.5. *Let $k;n \in \mathbb{N}$, and suppose $\gcd(k;n) = 1$. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the Gold function given by $F(x) = x^{2^k+1}$. Then $K_F^2 = \{(t;t) : t \in \mathbb{F}_{2^n}\}$.*

We also conjecture the following, which describes the size of K_F^1, K_F^2, and K_F^3. This conjecture is motivated by computer calculations and is verified for $x^{7} + x^3$ where $2 \leq n \leq 13$.

Conjecture 3.3.6. *Let $k;n \in \mathbb{N}$, and suppose $\gcd(k;n) = 1$. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the Gold function given by $F(x) = x^{2^k+1}$. Then the following holds:*

1. $|K_F^1| = \begin{cases} 2^{2n} - 1 & \text{if } n \text{ is even} \\ 2^{2n} - 1 - 2^n & \text{if } n \text{ is odd} \end{cases}$

2. $jK_F^2 j = 2^n$

3. $jK_F^3 j = \begin{cases} \frac{1}{3}(2^{2n} - 1 - 2^{n+1}) & \text{if } n \text{ is even} \\ \frac{1}{3}(2^{2n} - 1 - 2^n) & \text{if } n \text{ is odd} \end{cases}$

If both Conjecture 3.3.3 and Conjecture 3.3.6 hold true, then for any Gold function F, the size of $\mathbf{D}(F)$ is given by

$$j\mathbf{D}(F)j = \begin{cases} 2^{2n} - \frac{2^{2n} - 2^n}{3} & \text{if } n \text{ is even} \\ 2^{2n} - \frac{2^{2n} + 2^n}{3} & \text{if } n \text{ is odd:} \end{cases}$$

4
Graph theoretical connections to vectorial functions

The Kneser graph of a family of sets F is the graph that represents the disjointedness relations between elements of F. In this chapter, we study the Kneser graph of all translations of the graph of a vectorial function. We will show that these Kneser graphs can hold properties depending on the cryptographic properties of a function. In particular, we show that APN functions are those that correspond to a particular class of regular graphs and AB functions are those that give rise to strongly regular graphs.

4.1 Graph theory background

It is an unfortunate coincidence that the word \graph" is used for the mathematical structure consisting of vertices and edges and the set $(x; F(x)) : x \in \mathrm{F}_p^n$ for a function $F : \mathrm{F}_p^n \to \mathrm{F}_p^m$. For this reason, we will reserve the notation for a graph in the sense of vertices and edges, and G_F for the graph of a vectorial function F (see Chapter 2).

A (simple) **graph** is an ordered pair $(V; E)$ where V is a set and E is a set with elements of the form $\{u; v\}$ V V where $u \neq v$. Elements of V are called **vertices** and elements of E are called **edges**. If $(u; v) \in E$ is an edge, we say that u and v are **adjacent**. We will only be considering graphs with a nite number of vertices. Recall that two graphs are **isomorphic**

if they have the exact same structure. More formally, two graphs $= (V; E)$ and $^{0} = (V^{0}; E^{0})$ are isomorphic if there exists a bijection $' : V \; ! \; V^{0}$ such that v and u are adjacent in if and only if $'(v)$ and $'(u)$ are adjacent in ^{0}. If and ^{0} are isomorphic, we write $= \; ^{0}$.

Example 4.1.1. We call the graph with n vertices where any two vertices are adjacent the *complete graph* on n vertices, denoted as K_n. See Figure 4.1.1.

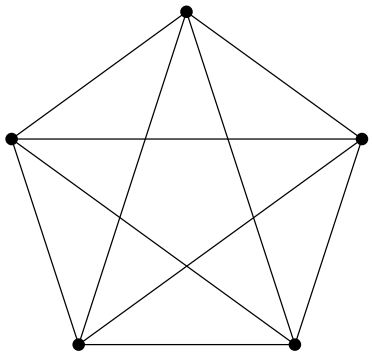


Figure 4.1.1: The complete graph on 5 vertices, K_5.

Definition 4.1.2. Let $= (V; E)$ be a graph. The **complement** graph $^{-}$ of is the graph $(V; E^{0})$ where any two vertices of $^{-}$ are adjacent if and only if they are non-adjacent with respect to .

Example 4.1.3. Consider the complete graph on 5 vertices, K_5. The complement of K_5 is the graph with 5 vertices and no edges. Graphs with no edges are often called *null graphs*. See Figure 4.1.2.

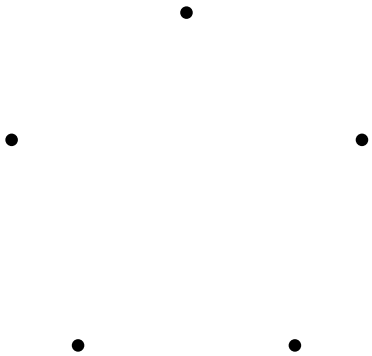


Figure 4.1.2: The complement graph of K_5.

If we think of the graph as a collection of points and line segments lying in a plane, one may ask if we can trace between any two points along the segments { this property is called connectedness.

Definition 4.1.4. Let = (*V; E*) be a graph. We call **connected** if for any two distinct vertices *u; v 2 V* , there exists a path of edges from *u* to *v*.

Clearly, the complete graph K_n is connected as any two vertices are adjacent. On the other hand, the complement of K_n is not connected because it has no edges. Moreover, if *any* vertex in a graph is not adjacent to any other vertex, the graph cannot be connected.

Since any nite, connected graph has a path of nite length between any two vertices, there is *always* well-de ned notion of (nite) diameter for nite connected graphs.

Definition 4.1.5. Let = (*V; E*) be a graph. Suppose is connected. For any two distinct vertices *u; v 2 V* , the **distance** of *u* and *v* is the length of the shortest path between *u* and *v*. The maximal distance of any two distinct vertices in *V* is called the **diameter** of .

Once again, the complete graph K_n is a trivial example as it has diameter 1. However, consider the following example.

Example 4.1.6. Consider the graph in Figure 4.1.3. This graph is connected as for any two distinct vertices, there exists a path between them. Furthermore, this graph is of diameter 3 since the vertices labeled 1 and 5 are of distance 3 and there is no other pair of vertices with greater distance. Indeed, there exist other paths of equal distance as the shortest path between the vertices labeled as 1 and 5, but none of these paths have length greater than 3.

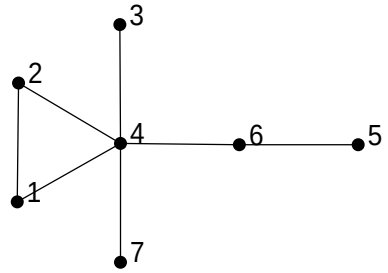


Figure 4.1.3: A connected graph with diameter 3.

An important class of graphs are those that we call *regular*.

Definition 4.1.7. Let $= (V; E)$ be a graph, and let $v \in V$. Then we say that

1. the set of vertices in $V \setminus \{v\}$ that are adjacent to v is the **neighborhood** of v, denoted as $N(v)$;
2. the **degree** of v is the size of $N(v)$, denoted as $\deg(v)$;
3. is **k-regular** if all vertices have degree k.

A well-known relation between the number of edges in a graph $= (V; E)$ and the degrees of vertices is the degree sum formula

$$2|E| = \sum_{v \in V} \deg(v). \tag{4.1.1}$$

In the case that is k-regular, the degree sum formula implies $2|E| = k|V|$. We now introduce an important subclass of regular graphs that not only exhibit symmetry with respect to the degrees of vertices but also in the neighborhoods of vertices.

Definition 4.1.8. Let be a graph, and let v be the number of vertices of . Then is **strongly regular** with parameters $(v; k; ;)$ if is a k-regular graph and there exist $; \in \mathbb{Z}_0$ such that every two adjacent vertices in have common neighbors and every two non-adjacent vertices in have common neighbors.

Hence, if $= (V; E)$ is a strongly regular graph with parameters $(v; k; ;)$, then for any $u; v \in V$ the size of $N(u) \setminus N(v)$ is if u and v are adjacent and otherwise.

Example 4.1.9. Suppose p is prime such that $p \equiv 1 \pmod 4$. Let $V = \mathbb{F}_{p^n}$ and $E = \{(x; y) : x; y \in \mathbb{F}_{p^n} \text{ s.t. } 9a \in \mathbb{F}_{p^n}; a^2 = x - y\}$. The graph $= (V; E)$ is called the *Paley graph* of order p^n. Consider the Paley graph of order 5. Recall that $\mathbb{F}_5$ is the same as the field $\mathbb{Z}_5$, so it suffices to consider the integers modulo 5, that is, $V = \mathbb{Z}_5$. Also, the squares of $\mathbb{Z}_5$ is exactly the set $\{1; 4\}$, so

$$E = \{(0; 1); (1; 2); (2; 3); (3; 4); (4; 0)\}:$$

It is straightforward to see that is a strongly regular graph with parameters $(5; 2; 0; 1)$ as it is also the 5-cycle graph (see Figure 4.1.4). More generally, all Paley graphs are strongly regular, and in particular, the Paley graph of order q has parameters $(q; \frac{q-1}{2}; \frac{q-5}{2}; \frac{q-1}{4})$ (see, for instance, [41]). We also picture the Paley graph of order 9 in Figure 4.1.5.

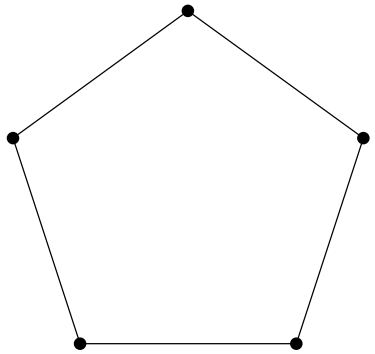


Figure 4.1.4: The Paley graph of order 5.

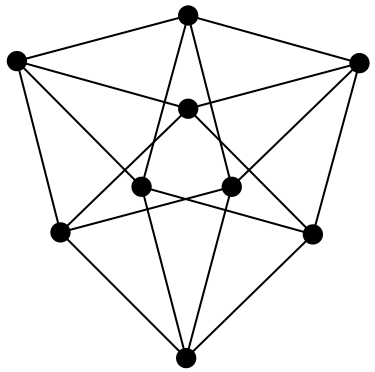


Figure 4.1.5: The Paley graph of order 9.

4.2 Cayley graphs of Boolean functions

Strongly regular graphs have appeared in the study of cryptographic functions before. In particular, [2] and [3] both explored the connections between perfect nonlinear Boolean functions (or equivalently, bent Boolean functions) and strongly regular graphs. In order to discuss these prior results, we must first define the Cayley graph of a Boolean function.

Definition 4.2.1. Let $f : \mathbb{F}_p^n \to \mathbb{F}_2$ be a function. We define the **Cayley graph** $\mathrm{Cay}(f)$ of f as the graph with vertex set $\mathbb{F}_p^n$ and edge set

$$E_f = \{\{u, v\} \subseteq \mathbb{F}_p^n \times \mathbb{F}_p^n : f(u + v) = 1\}.$$

Consider the Cayley graph of a function $f : \mathbb{F}_p^n \to \mathbb{F}_2$, and let $u \in \mathbb{F}_p^n$. Since the map $v \mapsto u + v$ is a bijection, it follows that the function $x \mapsto f(x + u)$ has the same weight as f. This implies that the degree of v with respect to $\mathrm{Cay}(f)$ is $\mathrm{wt}(f)$.

Proposition 4.2.2. *The Cayley graph of any Boolean function $f : \mathbb{F}_p^n \to \mathbb{F}_2$ is a regular graph such that all vertices have degree* $\mathrm{wt}(f)$.

Furthermore, in case that f is a bent function over $\mathbb{F}_2^n$, the Cayley graph of f is strongly regular as well { we will discuss in detail strongly regular graphs in Section 4.4.In [2], Bernasconi and Codenotti showed that the Cayley graph of any bent Boolean function over $\mathbb{F}_2^n$ is a strongly regular graph with $=$. Afterward Bernasconi, Codenotti, and VanderKam proved the converse in [3].

Theorem 4.2.3. [3] *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then* $\mathrm{Cay}(f)$ *is a strongly regular graph with the property that $=$ if and only if f is bent.*

Now, consider a vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Recall that by Theorem 2.2.3, F is AB if and only if $_F$ is bent. Therefore, by applying Theorem 4.2.3, F is AB if and only if $\mathrm{Cay}(_F)$ is a strongly regular graph with $=$. In the remainder of this chapter, we will focus on the properties of $\overline{\mathrm{Cay}(_F)}$, and therefore, we also apply our results to $\mathrm{Cay}(_F)$.

4.3 The Kneser graph of translations of G_F

In the previous section, we introduced the Cayley graph of a Boolean function. For a vectorial function, $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, it turns out that the Cayley graph of $_F$ is the Kneser graph of all the translations of G_F. To see why this is, we must first introduce the definition of the Kneser graph of a family of sets.

Definition 4.3.1. Let F be a family of sets. The **Kneser graph** $\mathrm{KG}(F)$ of F is the graph where vertices are elements of F, and two vertices are adjacent if and only if they are disjoint.

Example 4.3.2. Let F be the family of subsets of $[5] = \{1,2,3,4,5\}$ of size 2. We picture $\mathrm{KG}(F)$ in Figure 4.3.1. When considering the subsets of $[n]$ of size k, the Kneser graph of this family is often denoted as $\mathrm{KG}(n,k)$. We refer the reader to [38] for more on the Kneser graph $\mathrm{KG}(n,k)$ in the context of extremal combinatorics.

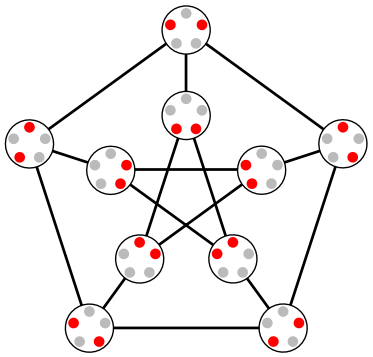


Figure 4.3.1: The Kneser graph of subsets of [5] of size 2. Image from Wikipedia.

For a vectorial function $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$, let T_F be the family of all translations of the graph of F, that is

$$T_F = \{\tau_{a,b}(G_F) = (a,b) + G_F : a \in \mathbb{F}_p^n, b \in \mathbb{F}_p^m\}.$$

While it is not immediately apparent, the number of distinct translations of G_F depends on the differential uniformity of F. Consequently, the size of T_F is dependent on the differential uniformity.

Lemma 4.3.3. *Suppose $n > 1$. Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ be a vectorial function. If F has a differential uniformity less than p^n, then $\tau_{a,b}(G_F) = \tau_{c,d}(G_F)$ if and only if $(a,b) = (c,d)$. Equivalently, there are p^{n+m} distinct translations of G_F if and only if the differential uniformity of F is less than p^n.*

Proof. Suppose the differential uniformity of F is less than p^n. By Lemma 3.1.1, the size of the intersection of any two translations $\tau_{a,b}(G_F)$ and $\tau_{c,d}(G_F)$ is equal to $\tau_F(a - c, b - d)$. If $a = c$,

then $_F(a \quad c; b \quad d)$ takes value p^n if $b = d$ and otherwise it takes value 0. If $a \neq c$, then $_F(a \quad c; b \quad d)$ 2 $_F$, implying $_F(a \quad c; b \quad d) < p^n$. Therefore, for any two distinct pairs $(a; b)$ and $(c; d)$, the translations $_{a;b}(G_F)$ and $_{c;d}(G_F)$ are distinct. □

Remark 4.3.4. Suppose $L : \mathbb{F}_p^n \to \mathbb{F}_p^m$ is linear, and let a 2 $(\mathbb{F}_p^n)$. Then $D_a L = L(x+a) \quad L(x) = L(a)$, so L has di erential uniformity p^n since $_L(a; L(a)) = 2^n$. Therefore the graph of any linear function from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$ has less than p^{n+m} distinct translations by Lemma 4.3.3.

Since the function $_F$ is closely related to $_F$, we are naturally led to realize that the adjacency relations in $\mathrm{KG}(T_F)$ are fully determined by $_F$. Recall from Lemma 3.1.1, that for any two distinct translations of G_F, say $_{a;b}(G_F)$ and $_{c;d}(G_F)$, the size of $_{a;b}(G_F) \setminus _{c;d}(G_F)$ is equal to $_F(a \quad c; b \quad d)$. Therefore, $_{a;b}(G_F)$ and $_{c;d}$ are disjoint if and only if $_F(a \quad c; b \quad d) = 0$. However, for $(a; b) \neq (c; d)$, observe that $_F(a \quad c; b \quad d) = 0$ if and only if $_F(a \quad c; b \quad d) = 0$. Therefore, $_{a;b}(G_F)$ and $_{c;d}(G_F)$ are disjoint if and only if $_F(a \quad c; b \quad d) = 0$.

Proposition 4.3.5. *Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ be a vectorial function. Then any two distinct vertices $_{a;b}(G_F)$ and $_{c;d}(G_F)$ of $\mathrm{KG}(T_F)$ are adjacent if and only if $_F(a \quad c; b \quad d) = 0$.*

It immediately follows that the Cayley graph of $_F$ is (up to graph isomorphism) the complement of the Kneser graph of T_F.

Proposition 4.3.6. *Let $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ be a vectorial function. If F has di erential uniformity less than p^n, then the complement graph of $\mathrm{Cay}(\ _F)$ is isomorphic to $\mathrm{KG}(T_F)$.*

Proof. Suppose the di erential uniformity of F is less than p^n. By the de nition of the Cayley graph of a Boolean function, the vertex set of $\mathrm{Cay}(\ _F)$ is $\mathbb{F}_p^n \quad \mathbb{F}_p^m$, and the edge set of $\mathrm{Cay}(\ _F)$ is

$$((a; b); (c; d)) \ 2 \ (\mathbb{F}_p^n \quad \mathbb{F}_p^m) \quad (\mathbb{F}_p^n \quad \mathbb{F}_p^m) : \ _F(a + c; b + d) = 1 \ :$$

By corresponding any pair of vertices $(a; b); (c; d)$ in $\mathrm{Cay}(\ _F)$ to vertices $_{a;b}(G_F); \ _{c;d}(G_F)$ in $\mathrm{KG}(T_F)$, it immediately follows by Proposition 4.3.5 that $(a; b)$ and $(c; d)$ are adjacent in $\mathrm{Cay}(\ _F)$ if and only if $_{a;b}(G_F)$ and $_{c;d}(G_F)$ are not adjacent in $\mathrm{KG}(T_F)$. Thus, $\overline{\mathrm{Cay}(\ _F)} = \mathrm{KG}(T_F)$. □

For an APN function $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$, the only possible case where $\mathrm{KG}(T_F)$ is not the complement graph of $\mathrm{Cay}(\ _F)$ is when $n = 1$. This is because for $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ to be APN, F must be is differentially 2-uniform, but $2^n = 2$ is satisfied only when $n = 1$. So, in general, any graph of any APN vectorial Boolean function from F_2^n to F_2^n has 2^{2n} distinct translations if $n > 1$.

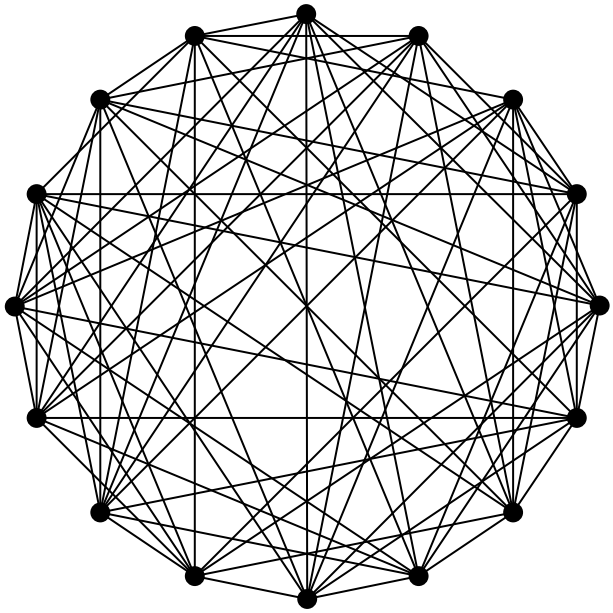


Figure 4.3.2: $\mathrm{KG}(T_F)$ where $F : \mathrm{F}_{2^2} \to \mathrm{F}_{2^2}$ is given by $x \mapsto x^3$.

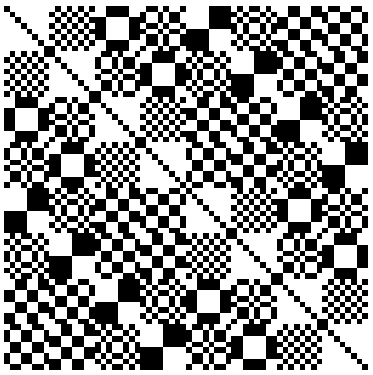


Figure 4.3.3: Adjacency matrix of $\mathrm{KG}(T_F)$ where $F : \mathrm{F}_{2^3} \to \mathrm{F}_{2^3}$ is defined by $F(x) = x^3$.

Example 4.3.7. Consider the function $F : \mathrm{F}_2 \to \mathrm{F}_2$ defined by $F(x) = x^3$. Then

$$G_F = \{(0,0),(1,1)\} \quad \mathrm{F}_2 \quad \mathrm{F}_2.$$

We will now show that there are only two distinct translations of G_F. Clearly $(0,0) + G_F = G_F$. Now, observe that $(1,0) + G_F = \{(1,0),(0,1)\} = (0,1) + G_F$. Finally, we see that $(1,1) + G_F = G_F$.

Thus, since there are only two distinct translations of G_F which are also disjoint, the size of T_F is 2 and KG(T_F) is the complete graph on 2 vertices. This means, there cannot exist a bijection between T_F and $\mathbb{F}_2 \quad \mathbb{F}_2$ as they have di erent sizes. Since the vertex set of Cay($_F$) is $\mathbb{F}_2 \quad \mathbb{F}_2$, we conclude that $\overline{\text{Cay}(\ _F)} \not\cong$ KG(T_F).

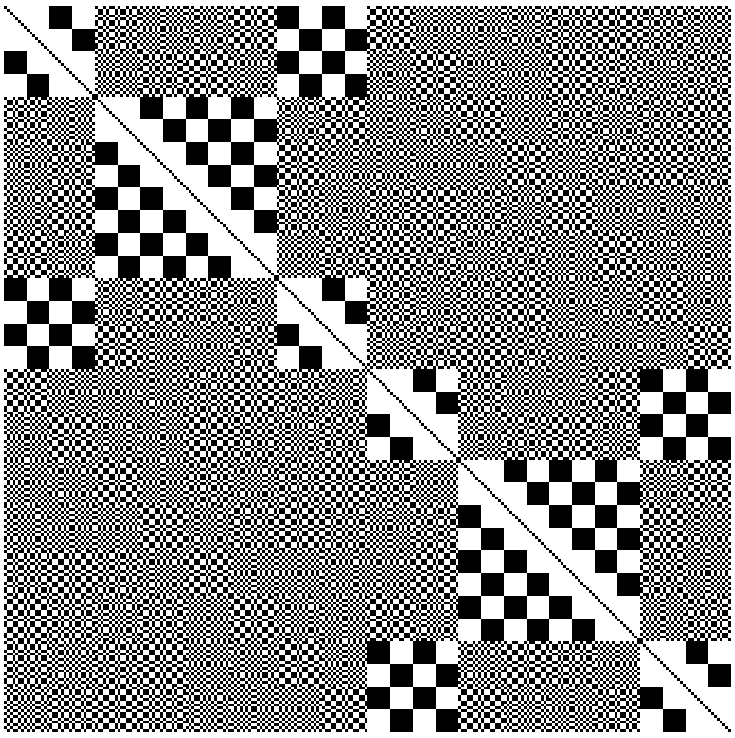


Figure 4.3.4: Adjacency matrix of KG(T_F) where $F : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ is de ned by $F(x) = x^3$.

As we will see, the Kneser graph of T_F can have interesting properties depending on $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$. Since the structure of KG(T_F) depends on the function $_F$, we will see that we can classify APN and AB functions by regularity conditions on KG(T_F). We reserve this for Section 4.4, and we will now discuss some basic elementary results on KG(T_F).

4.3.1 Preliminary observations and results

CCZ-equivalence naturally appears when discussing the graph of a vectorial Boolean function. Since CCZ-equivalence de nes two vectorial Boolean functions to be equivalent if their graphs are a nely equivalent, it is not unreasonable to expect that if $F; F' : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are CCZ-equivalent, then KG(T_F) and KG($T_{F'}$) are isomorphic. Indeed, this holds, and we prove this statement now.

Proposition 4.3.8. *Let F and F' be functions from $\mathbb{F}_2^n$ to itself. If F and F' are CCZ equivalent, then* KG(T_F) *and* KG($T_{F'}$) *are isomorphic.*

Proof. Suppose F and F' are CCZ equivalent. Then there exists an a ne permutation A of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $A(G_F) = G_{F'}$. Denote by $u_{a;b}$ (resp. $v_{a;b}$) the vertex $_{a;b}(G_F)$ in KG(T_F) (resp. $_{a;b}(G_{F'})$ in KG($T_{F'}$)). Let $u_{a;b}$ and $u_{c;d}$ be two distinct vertices in KG(T_F). Then $A(u_{a;b}) = A(a;b) + G_{F'}$ and $A(u_{c;d}) = A(c;d) + G_{F'}$, so the image of a vertex in KG(T_F) is a vertex in KG($T_{F'}$) under A. Clearly $u_{a;b}$ and $u_{c;d}$ are adjacent if and only if $A(u_{a;b})$ and $A(u_{c;d})$ are adjacent since A is a permutation. □

Another topic of interest is nding the number of pairs of translations that are disjoint. This is the same problem as counting the number of edges in KG(T_F). For a vectorial function $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ with di erential uniformity less than p^n, it su ces to count the number of edges in Cay($_F$) since Cay($_F$) is the complement graph of KG(T_F). Recall from Section 4.2 that Cay($_F$) is a k-regular graph where k = wt($_F$). By using the degree sum formula eq. (4.1.1), we know that the number of edges in Cay($_F$), say E, is equal to

$$\begin{aligned} E &= \frac{1}{2} \sum_{(a;b) \in \mathbb{F}_p^n \times \mathbb{F}_p^m} \deg(a;b) \\ &= \frac{1}{2} \sum_{a;b \in \mathbb{F}_p^n \times \mathbb{F}_p^m} \mathrm{wt}(\ _F) \\ &= \frac{p^{n+m}}{2} \mathrm{wt}(\ _F). \end{aligned}$$

Hence, for a vectorial function $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ with di erential uniformity less than p^n, the number of edges in KG(T_F) is

$$\binom{p^{n+m}}{2} - \frac{p^{n+m}}{2} \mathrm{wt}(\ _F). \tag{4.3.1}$$

Now, we consider some interesting substructures of KG(T_F). Recall the collection $\mathbf{X}_a(F) = \{ _{a;b}(G_F) : b \in \mathbb{F}_p^m \}$ where $a \in \mathbb{F}_p^n$ as de ned in eq. (3.1.1). As shown in Theorem 3.1.2, $\mathbf{X}_a(F)$ is a partition of $\mathbb{F}_p^n \times \mathbb{F}_p^m$ for any $a \in \mathbb{F}_p^n$. By de nition, any k distinct translations that are pairwise disjoint induce a copy of the complete graph on k vertices as a subgraph of KG(T_F), called a *clique*.

Definition 4.3.9. Let $= (V; E)$ be a graph. A **clique** in is a subset V^0 V such that the subgraph induced by V^0 is a complete graph. A **maximum clique** of is a clique in with the largest number of vertices possible, and the **clique number** of , denoted as $!( )$, is the number of vertices in a maximum clique.

Example 4.3.10. The complete graph K_m contains cliques of size $1; 2; : : : ; m$. Since K_m is a clique of size m, the maximum clique of K_m is itself, so $!(K_m) = m$.

Example 4.3.11. Let $F : F_2^n \to F_2^n$ be the identity function. Consider the Cayley graph of $_F$. By definition, $_F(a; b)$ is equal to 1 when $F(x + a) + F(x) = b$, and this equation is equivalent to $a = b$. Therefore the edge set $E_{_F}$ of Cay($_F$) is

$$\begin{aligned} E_{_F} &= f(a; b); (c; d)g \quad (F_2^n \quad F_2^n)^2 : {}_F(a + c; b + d) = 1 \\ &= f(a; b); (c; d)g \quad (F_2^n \quad F_2^n)^2 : a + c = b + d \\ &= f(a; b); (c; d)g \quad (F_2^n \quad F_2^n)^2 : a + b = c + d \ : \end{aligned}$$

It is then clear that Cay($_F$) is the disjoint union of 2^n copies of K_{2^n} since the map $(a; b) \mapsto a + b$ is 2^n-to-1.

The following proposition immediately follows from the fact that $\mathbf{X}_a(F)$ is a partition of $F_p^n \quad F_p^m$ for any $a \in F_p^n$.

Proposition 4.3.12. *Let $F : F_p^n \to F_p^m$ be a vectorial function. Then $\mathbf{X}_a(F)$ is a clique of size p^m in $\mathrm{KG}(T_F)$ for any $a \in F_p^n$.*

Hence, for a vectorial function $F : F_p^n \to F_p^m$ with non-maximal differential uniformity, there exist p^n distinct cliques of size p^m that partition the vertices of $\mathrm{KG}(T_F)$. We can quickly show that if $n < \log_p(p^m + 1)$, then all cliques of this size in $\mathrm{KG}(T_F)$ are maximal, implying $!(\mathrm{KG}(T_F)) = p^m$ if $n < \log_p(p^m + 1)$.

Theorem 4.3.13. *Let $F : F_p^n \to F_p^m$ be a vectorial function. If $n < \log_p(p^m + 1)$, then $!(\mathrm{KG}(T_F)) = p^m$. In particular, this inequality is satisfied if $m \quad n$, so $!(\mathrm{KG}(T_F)) = p^m$ if $m \quad n$.*

Proof. Suppose $n < \log_p(p^m + 1)$. Then $n + m = \log_p(p^{n+m}) < \log_p(p^m(p^m + 1))$. Hence $p^{n+m} < p^m(p^m + 1)$. By Proposition 4.3.12, the clique number of $\mathrm{KG}(T_F)$ is bounded below by p^m. If $!(\mathrm{KG}(T_F)) > p^m$, then there would exist $p^m + 1$ distinct sets in $\mathbb{F}_p^n \quad \mathbb{F}_p^m$ of size p^m that are pairwise disjoint, but this is impossible since $p^{m+n} < p^m(p^m + 1)$. Thus $!(\mathrm{KG}(T_F)) = p^m$. □

Corollary 4.3.14. *Let $F : \mathbb{F}_p^n \; ! \; \mathbb{F}_p^m$ be a vectorial function such that $n < \log_p(p^m + 1)$. Suppose $S \quad \mathbb{F}_p^n \quad \mathbb{F}_p^m$ such that $\quad_F(a + c; b + d) = 0$ for any distinct $(a; b); (c; d) \; 2 \; S$. Then $jSj \quad p^m$.*

It would also be interesting to answer the following: for a xed n, what is the minimal integer m such that any vectorial function $F : \mathbb{F}_p^n \; ! \; \mathbb{F}_p^m$, the clique number of $\mathrm{KG}(T_F)$ is no larger than p^m?

4.4 Graph-theoretically classifying APN and AB functions

APN functions, AB functions, and other important subclasses of APN functions have been classi ed in many di erent ways. In this section, we focus on the classi cations of APN and AB functions in graph-theoretical terms. Since the graphs in this section are very large (2^{2n} vertices, and often with many edges), we are not stating that such classi cation may be useful in computation. However, the symmetric behavior of APN functions can be seen when examining them with graph-theoretical tools.

4.4.1 APN functions

As seen in the previous section, for a vectorial function $F : \mathbb{F}_p^n \; ! \; \mathbb{F}_p^m$ with non-maximal di erential uniformity, we are able to compute the number of edges in $\mathrm{KG}(T_F)$ by simply knowing the weight of $\quad_F$. Since any APN function $F : \mathbb{F}_2^n \; ! \; \mathbb{F}_2^n$ has minimal di erential uniformity 2, it is guaranteed that the complement of $\mathrm{KG}(T_F)$ is $\mathrm{Cay}(\quad_F)$, which is $\mathrm{wt}(\quad_F)$-regular. Using this, we are able to demonstrate a connection between the number of edges and regularity of $\mathrm{KG}(T_F)$ with the APNness of a vectorial Boolean function F.

Theorem 4.4.1. *Let $F : \mathbb{F}_2^n \; ! \; \mathbb{F}_2^n$ such that the di erential uniformity of F is less than 2^n. The following are equivalent:*

1. *F is APN;*

2. $\mathrm{KG}(T_F)$ *has* $2^{2n-2}(2^n-1)(2^n+2)$ *edges;*

3. $\mathrm{KG}(T_F)$ *is a* $(2^{2n-1}+2^{n-1}-1)$*-regular graph.*

Proof. By Equation (4.3.1), the number of edges in $\mathrm{KG}(T_F)$ for a function $F:\mathrm{F}_2^n \to \mathrm{F}_2^n$ is $\binom{2^{2n}}{2} - \frac{2^{2n}}{2}\mathrm{wt}(\Delta_F)$. Since Theorem 2.2.3 states that F is APN if and only if $\mathrm{wt}(\Delta_F) = 2^{2n-1}-2^{n-1}$, we know that F is APN if and only if $\mathrm{KG}(T_F)$ has

$$\begin{aligned}\binom{2^{2n}}{2} - 2^{2n-1}(2^{2n-1}-2^{n-1}) &= 2^{2n-1}(2^{2n}-1) - 2^{2n-1}(2^{2n-1}-2^{n-1}) \\ &= 2^{2n-1}(2^{2n}-1-2^{2n-1}+2^{n-1}) \\ &= 2^{2n-2}(2^{2n+1}-2-2^{2n}+2^n) \\ &= 2^{2n-2}(2^n-1)(2^n+2)\end{aligned}$$

edges. Hence, (1) and (2) are equivalent. By Proposition 4.3.6, we know that $\mathrm{KG}(T_F)$ is the complement of $\mathrm{Cay}(\Delta_F)$ which is $\mathrm{wt}(\Delta_F)$-regular. Therefore, $\mathrm{KG}(T_F)$ is $(2^{2n}-\mathrm{wt}(\Delta_F)-1)$-regular. Thus, F is APN if and only if vertex in $\mathrm{KG}(T_F)$ has degree $2^{2n}-(2^{2n-1}-2^{n-1})-1 = 2^{2n-1}+2^{n-1}-1$, so (1) and (3) are equivalent. □

Therefore, from the Kneser graph of T_F for a vectorial Boolean function $F:\mathrm{F}_2^n \to \mathrm{F}_2^n$, we are able to retrieve information about the APNness of F. However, we are also able to classify APN functions with the Kneser graph in the following way.

Theorem 4.4.2. *Let $F:\mathrm{F}_2^n \to \mathrm{F}_2^n$ be function. For any $a \in \mathrm{F}_2^n$, let $\mathbf{X}_a(F)$ be as in eq.* (3.1.1)*. Then F is APN if and only if there are 2^{2n-1} edges between $\mathbf{X}_a(F)$ and $\mathbf{X}_{a'}(F)$ in $\mathrm{KG}(T_F)$ for any distinct $a, a' \in \mathrm{F}_2^n$. In particular, F is APN if and only if, for all distinct $a, a' \in \mathrm{F}_2^n$ any vertex in $\mathbf{X}_a(F)$ is adjacent to half of the vertices in $\mathbf{X}_{a'}(F)$*

Proof. As previously mentioned, $\mathbf{X}_a(F)$ is a clique of size 2^n for any $a \in \mathrm{F}_2^n$ by Theorem 3.1.2. Let $a, a' \in \mathrm{F}_2^n$ be distinct. Suppose F is APN, and let E be the number of edges between $\mathbf{X}_a(F)$ and $\mathbf{X}_{a'}(F)$. Recall from Lemma 3.1.1 that for any $b, b' \in \mathrm{F}_2^n$, the translations $\tau_{a,b}(G_F)$ and

$_{a',b'}(G_F)$ are disjoint if and only if $_F(a + a'; b + b') = 0$. Since $a \neq a'$, it is sufficient to count the number of pairs $(b; b')$ such that $_F(a + a'; b + b') = 0$. Hence,

$$E = 2^{2n} \sum_{b;b' \in \mathbb{F}_2^n} {}_F(a + a'; b + b'):$$

Since F is APN and $a + a' \neq 0$, the association $b \mapsto {}_F(a + a'; b)$ is balanced by Theorem 2.2.3. Therefore

$$\begin{aligned} E &= 2^{2n} \sum_{b;b' \in \mathbb{F}_2^n} {}_F(a + a'; b + b') \\ &= 2^{2n} \sum_{b \in \mathbb{F}_2^n} \sum_{b' \in \mathbb{F}_2^n} {}_F(a + a'; b + b') \\ &= 2^{2n} \quad 2^n \quad 2^{n-1} \\ &= 2^{2n-1}: \end{aligned}$$

Thus, there are 2^{2n-1} edges between $\mathbf{X}_a(F)$ and $\mathbf{X}_{a'}(F)$.

Conversely, if there are 2^{2n-1} edges between $\mathbf{X}_a(F)$ and $\mathbf{X}_{a'}(F)$ for all distinct $a; a' \in \mathbb{F}_2^n$, then there are

$$\begin{aligned} 2^n \binom{2^n}{2} + 2^{2n-1} \binom{2^n}{2} &= 2^n(2^{n-1})(2^n - 1) + 2^{2n-1}(2^{n-1})(2^n - 1) \\ &= 2^{2n-2}(2^n - 1)(2^n + 2) \end{aligned}$$

edges in $\mathrm{KG}(T_F)$, implying F is APN by Theorem 4.4.1. □

Remark 4.4.3. Suppose $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a vectorial Boolean function with differential uniformity less than 2^n. Consider the graph $_F$ whose vertices are the sets $\mathbf{X}_a(F)$ and such that $\mathbf{X}_a(F)$ and $\mathbf{X}_{a'}(F)$ are adjacent if and only if there is an edge between their respective cliques in $\mathrm{KG}(T_F)$. Additionally, assign each edge a weight for the number of edges between the associated cliques in $\mathrm{KG}(T_F)$. Then $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN if and only if $_F$ is the complete graph where all edges have weight 2^{2n-1}.

Informally, the graph discussed in Remark 4.4.3 is a \zoomed out" graph of $\mathrm{KG}(T_F)$. With this in mind, notice that Figure 4.4.1 directly shows that $\mathrm{KG}(T_F)$ is connected where $F : \mathbb{F}_2^2 \to \mathbb{F}_2^2$ is APN. This motivates us to generalize to all APN functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

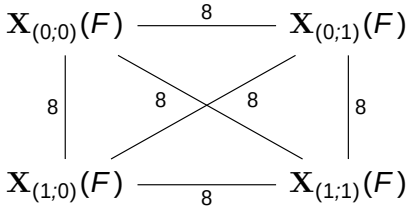


Figure 4.4.1: $_F$ where $F : \mathrm{F}_2^2 \to \mathrm{F}_2^2$ is APN.

Corollary 4.4.4. *Let $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ be a function. If F is APN, then* KG(T_F) *is a connected graph of diameter* 2.

Proof. Suppose F is APN. Let $(a;b);(c;d) \in \mathrm{F}_2^n \times \mathrm{F}_2^n$ be distinct. Then $_{a;b}(G_F) \in \mathbf{X}_a(F)$ and $_{c;d}(G_F) \in \mathbf{X}_c$. By Theorem 4.4.2 we know that $_{a;b}(G_F)$ is adjacent to half of the vertices in $\mathbf{X}_c$. Since $\mathbf{X}_c$ is a clique, all vertices in it are adjacent, and so, there exists a path between $_{a;b}(G_F)$ and $_{c;d}(G_F)$ of length at most 2. Therefore KG(T_F) is a connected graph of diameter 2.

□

4.4.2 AB Functions and strongly regular graphs

Recall that AB functions are those functions $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ whose Walsh transform takes values in the set $\left\{0;\ 2^{\frac{n+1}{2}}\right\}$ at any non-zero $(a;b) \in \mathrm{F}_2^n \times \mathrm{F}_2^n$. Additionally, AB functions can be classified by the indicator function $_F$, as stated in the result by Carlet, Charpin, and Zinoviev (see Theorem 2.2.3): $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ is AB if and only if $_F$ is bent. As briefly mentioned in Section 4.2, we are able to classify AB functions in terms of strongly regular graphs by applying the results of Bernasconi, Codenotti, and VanderKam (c.f. [2] [3]). We will now define strongly regular graphs.

Definition 4.4.5. Let be a graph, and let v be the number of vertices of . Then is **strongly regular** with parameters $(v;k;\ ;\ )$ if is a k-regular graph and there exist $;\ \in \mathbb{Z}_{\geq 0}$ such that every two adjacent vertices in have common neighbors and every two non-adjacent vertices in have common neighbors.

Although we can easily classify AB functions $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ as those whose $_F$ function has a strongly regular Cayley graph using results from Bernasconi, Codenotti, and VanderKam, we instead provide a new proof showing that the Cayley graph of a bent function $f : \mathrm{F}_2^n \to \mathrm{F}_2$ is strongly regular with $\quad = \quad = \mathrm{wt}(f) \quad 2^{n\ 2}$. We prove the converse as well. By Theorem 2.2.3, $_F$ is bent if and only if F is AB, and thus, provides a classi cation of AB functions in terms of strongly regular graphs. Note, however the converse of the above statement is not equivalent to proving that f is bent provided $\mathrm{Cay}(f)$ is strongly regular with $\quad = \quad$. Our proof of the following theorem involves simple counting and does not rely on an argument using eigenvalues of $\mathrm{Cay}(f)$.

Theorem 4.4.6. *Suppose n is even, and let $f : \mathrm{F}_2^n \to \mathrm{F}_2$. Suppose $f(0) = 0$. Then f is bent if and only if $\mathrm{Cay}(f)$ is a strongly regular graph with $\quad = \quad = \mathrm{wt}(f) \quad 2^{n\ 2}$.*

Proof. Throughout this proof, for any $a; b \in \mathrm{F}_2^n$ and any $i; j \in \mathrm{F}_2$, let $M_{i;j}(a; b)$ be the cardinality of the set $\{x \in \mathrm{F}_2^n : f(x + a) = i \text{ and } f(x + b) = j\}$. Note that for any $a; b \in \mathrm{F}_2^n$, the following holds by construction:

$$M_{0;0}(a; b) + M_{0;1}(a; b) = 2^n \quad \mathrm{wt}(f) \quad \text{and}$$

$$M_{1;0}(a; b) + M_{1;1}(a; b) = M_{0;1}(a; b) + M_{1;1}(a; b)$$

$$= \mathrm{wt}(f):$$

Suppose f is bent. Then, f is PN, so for all $a \neq 0$, the derivative $D_a f(x) = f(x + a) + f(x)$ is balanced. This means that, for all $a \in \mathrm{F}_2^n$ such that $a \neq 0$, the following equality holds

$$\sum_{x \in \mathrm{F}_2^n} (f(x + a) + f(x) \mod 2) = 2^{n\ 1}: \tag{4.4.1}$$

Let $a; b \in \mathrm{F}_2^n$ be distinct, and let $\quad$ be the number of common neighbors between a and b in $\mathrm{Cay}(f)$, that is, $\quad = |N_{\mathrm{Cay}(f)}(a) \setminus N_{\mathrm{Cay}(f)}(b)|$. Hence,

$$= |\{x \in \mathrm{F}_2^n \setminus \{a; b\} : f(x + a) = 1 = f(x + b)\}|$$

$$= |\{x \in \mathrm{F}_2^n : f(x + a) = 1 = f(x + b)\}|$$

$$= M_{1;1}(a; b):$$

Since $M_{0;0}(a;b) + M_{1;1}(a;b)$ is the number of $x \in \mathrm{F}_2^n$ such that $f(x+a) + f(x+b) \equiv 0 \pmod 2$, it follows that

$$\begin{aligned} M_{0;0}(a;b) + M_{1;1}(a;b) &= 2^n - \sum_{x \in \mathrm{F}_2^n} (f(x+a) + f(x+b) \pmod 2) \\ &= 2^n - \sum_{x \in \mathrm{F}_2^n} D_{a+b} f(x+b) \\ &= 2^n - \sum_{x \in \mathrm{F}_2^n} D_{a+b} f(x); \end{aligned}$$

and by Equation (4.4.1), we have $M_{0;0}(a;b) + M_{1;1}(a;b) = 2^{n-1}$. So far, we have shown $M_{0;0}(a;b) + M_{0;1}(a;b) = 2^n - \mathrm{wt}(f)$ and $M_{0;1}(a;b) + M_{1;1}(a;b) = \mathrm{wt}(f) = M_{1;0}(a;b) + M_{1;1}(a;b)$ and $M_{0;0}(a;b) + M_{1;1}(a;b) = 2^{n-1}$. By solving the system of equations, we have

$$\begin{aligned} M_{0;0}(a;b) &= 2^n - 2^{n-2} - \mathrm{wt}(f) \\ M_{0;1}(a;b) &= M_{1;0}(a;b) = 2^{n-2} \\ M_{1;1}(a;b) &= \mathrm{wt}(f) - 2^{n-2}. \end{aligned}$$

Therefore, the number of common neighbors of any two distinct vertices a and b in $\mathrm{Cay}(f)$ is $\mathrm{wt}(f) - 2^{n-2}$ regardless if a and b are adjacent. Thus, $\mathrm{Cay}(f)$ is a strongly regular graph with $= = \mathrm{wt}(f) - 2^{n-2}$.

Now, suppose that $\mathrm{Cay}(f)$ is a strongly regular graph with $= = \mathrm{wt}(f) - 2^{n-2}$. Then $M_{1;1}(a;b) =$ for all $a;b \in \mathrm{F}_2^n$ where $a \neq b$. For similar reasoning as the first part of this proof, we have the following for any $a;b \in \mathrm{F}_2^n$ where $a \neq b$:

$$\begin{aligned} M_{0;0}(a;b) + M_{0;1}(a;b) &= 2^n - \mathrm{wt}(f) \\ M_{1;0}(a;b) + M_{1;1}(a;b) &= \mathrm{wt}(f) \\ M_{0;1}(a;b) + M_{1;1}(a;b) &= \mathrm{wt}(f) \\ M_{0;0}(a;b) + M_{1;1}(a;b) &= 2^n - \sum_{x \in \mathrm{F}_2^n} D_{a+b} f(x). \end{aligned}$$

Therefore,

$$\begin{aligned}\sum_{x \in \mathbb{F}_2^n} D_{a+b}f(x) &= 2^n \quad M_{0;0}(a;b) \\ &= 2^n \quad (2^n \quad \mathrm{wt}(f) \quad M_{0;1}(a;b)) \\ &= M_{0;1}(a;b) \quad + \mathrm{wt}(f) \\ &= 2(\mathrm{wt}(f) \quad) \\ &= 2(\mathrm{wt}(f) \quad (\mathrm{wt}(f) \quad 2^{n\ 2})) \\ &= 2^{n\ 1};\end{aligned}$$

for any $a;b \in \mathbb{F}_2^n$ where $a \neq b$. Hence, all first-order derivatives of f are balanced, so f is PN. Thus, f is bent. □

Theorem 4.4.7. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial Boolean function. Then F is AB if and only if* $\mathrm{KG}(T_F)$ *is a strongly regular graph with parameters* $(2^{2n}; 2^{2n\ 1} + 2^{n\ 1} \quad 1; 2^{2n\ 2} + 2^{n\ 1} \quad 2; 2^{2n\ 2} + 2^{n\ 1})$.

Proof. It is well-known (c.f. [7]) that if is a strongly regular graph with parameters $(v;k; ;)$, then $\bar{}$ is strongly regular with parameters $(v;v \quad k \quad 1;v \quad 2 \quad 2k+ ;v \quad 2k+)$. By Theorem 4.2.3, $\mathrm{Cay}(_F)$ is a strongly regular graph with parameters $(2^{2n}; \mathrm{wt}(_F); \mathrm{wt}(_F) \quad 2^{n\ 2}; \mathrm{wt}(_F) \quad 2^{n\ 2})$ if and only if $_F$ is bent. Therefore, by taking the complement of $\mathrm{Cay}(_F)$ and applying Theorem 2.2.3, we conclude that $\mathrm{KG}(T_F)$ is a strongly regular graph with parameters $(2^{2n}; 2^{2n\ 1} + 2^{n\ 1} \quad 1; 2^{2n\ 2} + 2^{n\ 1} \quad 2; 2^{2n\ 2} + 2^{n\ 1})$ if and only if F is AB. □

As mentioned in [45], a characterization of AB functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ in terms of the sets $\mathrm{im}\, D_aF$ is an area of interest because both APN and crooked functions have been characterized in terms of the sets $\mathrm{im}\, D_aF$ (sometimes denoted as $H_a(F)$).

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial Boolean function. For any $(a;b);(c;d) \in \mathbb{F}_2^n \quad \mathbb{F}_2^n$, denote by $S_{a;b;c;d}$ the complement of $\{(a;b);(c;d)\}$. Then by Theorem 4.4.7, F is AB if and only if for any distinct $(a;b);(c;d) \in \mathbb{F}_2^n \quad \mathbb{F}_2^n$, the size of the set

$$\{(x;y) \in S_{a;b;c;d} : \ _F(a + x;b + y) = 0 = \ _F(c + x;d + y)\}$$

is $2^{2n-2} + 2^{n-1} - 2$ if $\Delta_F(a+c; b+d) = 0$ and $2^{2n-2} + 2^{n-1}$ otherwise. Notice that

$$f(x;y) \in S_{a;b;c;d} : \Delta_F(a+x; b+y) = 0 = \Delta_F(c+x; d+y)g$$

$$= f(x;y) \in S_{a;b;c;d} : x = a; y \neq b; \Delta_F(a+c; d+y) = 0g$$

$$\cup f(x;y) \in S_{a;b;c;d} : x = c; y \neq d; \Delta_F(a+c; b+y) = 0g$$

$$\cup f(x;y) \in S_{a;b;c;d} : a \neq x \neq c; \Delta_F(a+x; b+y) = 0 = \Delta_F(c+x; d+y)g$$

for any $(a;b);(c;d) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ distinct. Notice that

$$T_{a;b;c;d} := f(x;y) \in S_{a;b;c;d} : a \neq x \neq c; \Delta_F(a+x; b+y) = 0 = \Delta_F(c+x; d+y)g$$

$$= f(x;y) \in S_{a;b;c;d} : a \neq x \neq c; y \notin ((b + \operatorname{im} D_{a+x}F) \cup (d + \operatorname{im} D_{c+x}))g:$$

Let

$$U_{a;b;c;d} = f(x;y) \in S_{a;b;c;d} : x = a; y \neq b; \Delta_F(a+c; d+y) = 0g$$

$$V_{a;b;c;d} = f(x;y) \in S_{a;b;c;d} : x = a; y \neq b; \Delta_F(a+c; d+y) = 0g:$$

Then $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is AB if and only if $(a;b);(c;d) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n$ where $(a;b) \neq (c;d)$ implies

$$|T_{a;b;c;d}| + |U_{a;b;c;d}| + |V_{a;b;c;d}| = \begin{cases} 2^{2n-2} + 2^{n-1} - 2 & \text{if } \Delta_F(a+c; b+d) = 0 \\ 2^{2n-2} + 2^{n-1} & \text{otherwise:} \end{cases}$$

We can compute the size of $U_{a;b;c;d}$ and $V_{a;b;c;d}$ by noticing they both have size

$$2^n - 1 - \sum_{\in \mathbb{F}_2^n} \Delta_F(a+c; \ ) + \Delta_F(a+c; b+d):$$

Therefore, if $a + c = 0$, then $|U_{a;b;c;d}| = |V_{a;b;c;d}| = 2^n - 1$. If $a + c \neq 0$ and F is APN, we can apply Theorem 2.2.3 to determine that

$$|U_{a;b;c;d}| = |V_{a;b;c;d}| = 2^n - 1 - 2^{n-1} + \Delta_F(a+c; b+d)$$

$$= 2^{n-1} - 1 + \Delta_F(a+c; b+d)$$

for all $(a;b);(c;d) \in S_{a;b;c;d}$. Conversely, if $|U_{a;b;c;d}| = |V_{a;b;c;d}| = 2^{n-1} - 1 + \Delta_F(a+c; b+d)$ for all $(a;b);(c;d) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ where $(a;b) \neq (c;d)$, then F is APN. So for any distinct $(a;b);(c;d) \in$

$F_2^n \quad F_2^n$

$$jU_{a;b;c;d}j + jV_{a;b;c;d}j = \begin{cases} 2^{n+1} \quad 2 & \text{if } a = c \\ 2^n \quad 2 & \text{if } a \neq c \text{ and } {}_F(a + c; b + d) = 0 \\ 2^n & \text{if } a \neq c \text{ and } {}_F(a + c; b + d) = 1: \end{cases}$$

if and only if F is APN. From this, we are able to derive the following theorem.

Theorem 4.4.8. *Let $F : F_2^n \to F_2^n$ be a vectorial Boolean function. Then F is AB if and only if F is APN such that the size of*

$$T_{a;b;c;d} = f(x; y) \in S_{a;b;c;d} : a \neq x \neq c; y \in ((b + \operatorname{im} D_{a+x}F) \cup (d + \operatorname{im} D_{c+x}))g$$

is given by

$$jT_{a;b;c;d}j = \begin{cases} 2^{2n-2} \quad 2^{n+1} + 2^{n-1} & \text{if } a = c \\ 2^{2n-2} \quad 2^n + 2^{n-1} & \text{if } a \neq c \text{ and } {}_F(a + c; b + d) = 0 \\ 2^{2n-2} + 2^{n-1} \quad 2^n & \text{if } a \neq c \text{ and } {}_F(a + c; b + d) = 1 \end{cases}$$

for all distinct $(a; b); (c; d) \in F_2^n \quad F_2^n$.

Proof. Suppose F is AB, and let $(a; b); (c; d) \in F_2^n \quad F_2^n$ be distinct. Then

$$jT_{a;b;c;d}j + jU_{a;b;c;d}j + jV_{a;b;c;d}j = \begin{cases} 2^{2n-2} + 2^{n-1} \quad 2 & \text{if } {}_F(a + c; b + d) = 0 \\ 2^{2n-2} + 2^{n-1} & \text{otherwise:} \end{cases}$$

So,

$$\begin{aligned} jT_{a;b;c;d}j &= (U_{a;b;c;d} + V_{a;b;c;d}) + \begin{cases} 2^{2n-2} + 2^{n-1} \quad 2 & \text{if } {}_F(a + c; b + d) = 0 \\ 2^{2n-2} + 2^{n-1} & \text{otherwise} \end{cases} \\ &= \begin{cases} 2^{2n-2} \quad 2^{n+1} + 2^{n-1} & a = c \\ 2^{2n-2} \quad 2^n + 2^{n-1} & \text{if } a \neq c \text{ and } {}_F(a + c; b + d) = 0 : \\ 2^{2n-2} + 2^{n-1} \quad 2^n & \text{if } a \neq c \text{ and } {}_F(a + c; b + d) = 1 \end{cases} \end{aligned}$$

Now, assume the converse. Since F is APN, we have

$$jU_{a;b;c;d}j + jV_{a;b;c;d}j = \begin{cases} 2^{n+1} \quad 2 & \text{if } a = c \\ 2^n \quad 2 & \text{if } a \neq c \text{ and } {}_F(a + c; b + d) = 0 \\ 2^n & \text{if } a \neq c \text{ and } {}_F(a + c; b + d) = 1: \end{cases}$$

Therefore

$$
\begin{aligned}
|T_{a;b;c;d}| + |U_{a;b;c;d}| + |V_{a;b;c;d}| &= \begin{cases} 2^{2n-2} - 2^{n+1} + 2^{n-1} & a = c \\ 2^{2n-2} - 2^{n} + 2^{n-1} & \text{if } a \neq c \text{ and } \chi_F(a+c;b+d) = 0 \\ 2^{2n-2} + 2^{n-1} - 2^{n} & \text{if } a \neq c \text{ and } \chi_F(a+c;b+d) = 1 \end{cases} \\
&+ \begin{cases} 2^{n+1} - 2 & \text{if } a = c \\ 2^{n} - 2 & \text{if } a \neq c \text{ and } \chi_F(a+c;b+d) = 0 \\ 2^{n} & \text{if } a \neq c \text{ and } \chi_F(a+c;b+d) = 1 \end{cases} \\
&= \begin{cases} 2^{2n-2} + 2^{n-1} - 2 & \text{if } a = c \\ 2^{2n-2} + 2^{n-1} - 2 & \text{if } a \neq c \text{ and } \chi_F(a+c;b+d) = 0 \\ 2^{2n-2} + 2^{n-1} & \text{if } a \neq c \text{ and } \chi_F(a+c;b+d) = 1 \end{cases} \\
&= \begin{cases} 2^{2n-2} + 2^{n-1} - 2 & \text{if } \chi_F(a+c;b+d) = 0 \\ 2^{2n-2} + 2^{n-1} & \text{otherwise.} \end{cases}
\end{aligned}
$$

Thus, F is AB. □

Therefore, we have classified AB functions in terms of their APNness and a condition on their first-order derivatives. It is natural to ask whether the condition on the APNness of $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ in Theorem 4.4.8 necessary. This is a question that still needs further work, and we hope that in the near future there will be a classification of AB functions in terms of the images of their first-order derivatives.

4.4.3 Crooked functions

We now discuss crooked functions and why some graph-theoretical classification is reasonable. Recall that a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called crooked if $\operatorname{im} D_a F$ is an affine hyperplane for all non-zero $a \in \mathbb{F}_2^n$. Both APN and AB functions could be classified by properties of their χ_F functions, and it turns out that crooked functions can be as well. This classification was proved in [11], but first, we must introduce the following definition.

Definition 4.4.9. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Suppose n is even and f is bent. We say f is in the **Maiorana-McFarland class** (MM class) if there exists a permutation $\pi : \mathbb{F}_2^{n/2} \to \mathbb{F}_2^{n/2}$ and a Boolean function $g : \mathbb{F}_2^{n/2} \to \mathbb{F}_2$ such that $f(x;y) = x \cdot \pi(y) + g(y)$. Also, the **completed MM class** is the set of all functions that are EA-equivalent to MM functions.

We now are ready to introduce the classi cation of crooked functions proven in [11].

Proposition 4.4.10. [11] *A function* $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *is generalized crooked if and only if* $_F$ *is a ne with respect to* b*. If* n *is odd, then* F *is CCZ-equivalent to a generalized crooked function if and only if* $_F$ *is in the completed MM class.*

This proposition is evidence that we may be able to classify crooked functions in terms of the Cayley graph of $_F$, and therefore, the Kneser graph of T_F.

5
Uniform exclude distributions

As we have previously discussed, APN functions are an important notion in cryptography as they are those $(n;n)$-functions that are optimally resistant to a differential attack when used as a substitution box in a block cipher. However, APN functions are also those $(n;n)$-functions F whose graph $G_F = f(x;F(x)) : x \in \mathbb{F}_2^n g$ is a Sidon set in $(\mathbb{F}_2^n)^2$. In this chapter, we study the case when G_F is a Sidon set, and in particular, we study the exclude distribution of G_F for APN functions F.

Recall that a Sidon set $S \subseteq \mathbb{F}_2^n$ is a set such that the sum of any four distinct elements is non-trivial. Observe that if $a;b;c \in S$ are distinct and S is Sidon, then $a + b + c \notin S$. We call the set consisting of all the sums of three points in S the exclude set.

Definition 5.0.1. Let $S \subseteq \mathbb{F}_2^n$.

1. The **exclude set** $\mathbf{X}(S)$ of S is the set

$$\mathbf{X}(S) = fa + b + c : a;b;c \in S \text{ and } j fa;b;cg j = 3g :$$

2. We say $x \in \mathbf{X}(S)$ is an **exclude point** of S.

3. Furthermore, the **exclude multiplicity** (or simply the **multiplicity**) $\text{mult}_S(x)$ of $x \in \mathbb{F}_2^n \setminus S$ is the number of distinct subsets $fa;b;cg \subseteq S$ of size 3 such that $a + b + c = x$.

Hence, a set $S \subseteq \mathbb{F}_2^n$ is Sidon if and only if $S \setminus \mathbf{X}(S) = \emptyset$. A Sidon set $S \subseteq \mathbb{F}_2^n$ is called **maximal** if no point in $\mathbb{F}_2^n \setminus S$ has multiplicity 0. Determining the largest size of a maximal Sidon set is a well-known problem and is only known precisely for $n \leq 10$ (see [22], [39], [23]). However there are known bounds on the size of the largest maximal Sidon set (see also [44]).

In [12], it was conjectured that any $(n;n)$-function with so-called algebraic degree n must be not be APN for $n \geq 3$. If true, this conjecture would imply that any function F' obtained by changing the value of APN $(n;n)$-function F at a single point is not APN. As shown in [17], any such functions F' are not APN if and only if the graph of all APN functions are maximal Sidon sets. This seems reasonable as Redman, Rose, and Walker showed in [43] that the smallest maximal Sidon set in $\mathbb{F}_2^n$ is of size $O((n \cdot 2^n)^{\frac{1}{3}})$ by generalizing a result of Ruzsa. However, as mentioned in [17], "there seems to be room for the existence of APN functions whose graphs are non-maximal Sidon sets" since $|G_F| = 2^n$ is approximately $\sqrt{2}$ times smaller than the best known upper bounds on the largest maximal Sidon set (see [44], [23]).

The exclude distribution of a Sidon set $S \subseteq \mathbb{F}_2^n$ is the function that takes a point in $\mathbb{F}_2^n \setminus S$ to its multiplicity. To provide an overview of this chapter, we first give some preliminary results on the exclude distribution. Then, we explore the APN function-maximal Sidon set conjecture and introduce the notion of uniform exclude distributions. We then prove in Section 5.3 that the graph any Gold function (a power APN function $F(x) = x^{2^k+1}$ where $\gcd(k;n) = 1$) has an exclude distribution that is uniform on an equally-sized partition of $(\mathbb{F}_2^n)^2 \setminus G_F$. We conclude this chapter by extending this result to all APN plateaued functions whose component functions are all unbalanced in Section 5.3.3.

5.1 Visualizing Sidon sets in $\mathbb{F}_2^n$

A common way to think about $\mathbb{F}_2^n$ is as the vertices of the n-dimensional hypercube in $\mathbb{R}^n$, but clearly, this becomes difficult to do as soon as $n = 4$. In this section, we discuss visualizing $\mathbb{F}_2^n$ in a planar fashion. One tool created to visualize Sidon sets in $\mathbb{F}_2^n$ is the Qap Visualizer [46]. The Qap Visualizer is an online web-based tool used to visualize Sidon sets in $\mathbb{F}_2^n$ where $1 \leq n \leq 14$.

For any n, we will provide two algorithms for constructing the same planar grid of F_2^n. In particular, if n is even, then our grid will have $\frac{n}{2}$ rows and $\frac{n}{2}$ columns, and in the case of n odd, it will have $\frac{n+1}{2}$ rows and $\frac{n-1}{2}$ columns. Equivalently, the grid will have $b\frac{n}{2}c$ rows and $d\frac{n}{2}e$ columns for any $n > 1$, and in case $n = 1$, our grid will simply have 1 row and 2 columns.

Suppose $n > 1$, and consider a vector $a \in F_2^n$ as a bitstring, that is, a is a sequence of values in $\{0, 1\}$. We use standard indexing for bitstrings, that is, we index the right-most bit of a as 0 and the left-most as $n-1$. Let a_i denote the ith bit of a. We can then construct two vectors x_a and y_a consisting of the bits from the even and odd indices of a, respectively. Let $n_x = d\frac{n}{2}e$, let $n_y = b\frac{n}{2}c$. Now, let

$$x_a = (a_{2n_x-2}, a_{2n_x-4}, \ldots, a_2, a_0) \in F_2^{n_x} \text{ and}$$
$$y_a = (a_{2n_y-1}, a_{2n_y-3}, \ldots, a_3, a_1) \in F_2^{n_y},$$

said differently, x_a is the vector of all "even bits" in a and y_a is all of the "odd bits" in a. One can easily show that this process gives us an isomorphism from F_2^n to $F_2^{n_x} \times F_2^{n_y}$.

Example 5.1.1. Suppose $n = 4$ and $a = (0, 1, 0, 1) \in F_2^4$. Then $a_x = (1, 1)$ and $a_y = (0, 0)$.

Example 5.1.2. Suppose $n = 5$ and $a = (1, 0, 1, 1, 0) \in F_2^5$. Then $a_x = (1, 1, 0)$ and $a_y = (0, 1)$.

Consider the standard integer representation of $s \in F_2^n$, that is, we identify s with the integer $\sum_{i=0}^{n-1} 2^i s_i$. Therefore the bijection $a \mapsto (x_a, y_a)$ gives us a way of mapping a vector $a \in F_2^n$ to a pair of (x, y) coordinates by identifying x_a and y_a with their integer representations, giving us a way to map vectors in F_2^n to (x, y) coordinates in $Z \times Z$.

Now, for any $a \in F_2^n$, identify a with (x, y) where x and y are the integer representations of x_a and y_a, respectively. Doing this for all vectors in F_2^n, we have uniquely identified each vector with a (x, y) coordinate. Now, we consider a grid where we enumerate rows from top to bottom and columns from left to right – with all indices starting at 0. Then, we have a planar representation of F_2^n as a finite grid[1]. See Table 5.1.1 and Table 5.1.2.

[1] One can easily generalize this to provide a planar representation of Z_m^n for any $m, n \in N$.

0	1	4	6
2	3	5	7

Table 5.1.1: Planar representation of F_2^3 with integer coordinates.

0	1	4	6
2	3	5	7
8	9	12	13
10	11	14	15

Table 5.1.2: Planar representation of F_2^4 with integer coordinates.

Example 5.1.3. Let $a = (1;0;0;0)$ 2 F_2^4. Then $a_x = (0;0)$ and $a_y = (1;0)$. The integer representation of a is 8, and the integer representations of a_x and a_y are 0 and 2, respectively. Therefore, 8 has coordinates $(0;2)$ in our planar representation of F_2^4, that is, 8 appears in the 0th column and the 2nd row (with indices starting at 0), see Table 5.1.2.

Using this same planar representation of F_2^n, we can visualize Sidon sets in F_2^n. The Qap Visualizer represents F_2^n in the same way and pictures Sidon sets. For a Sidon set S F_2^n, we represent a point in S as a green diamond, and exclude points in $\mathbf{X}(S)$ are labeled with their multiplicity.

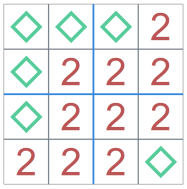


Figure 5.1.1: A Sidon set in F_2^4 of size 6, the largest possible.

Figure 5.1.2: A Sidon set in F_2^6 of size 9, the largest possible.

5.2 The exclude distribution

The exclude set of a Sidon set $S \subseteq \mathbb{F}_2^n$ is exactly the set of points such that any superset of S including a point from $\mathbf{X}(S)$ is not a Sidon set. For this reason, the exclude set of S plays a critical role in the structure of S.

Now, notice that $\mathbb{F}_2^n$ is the disjoint union of $\mathbf{X}(S)$ and the set of all points of exclude multiplicity 0 (with respect to S). For this reason, we have the following lemma.

Lemma 5.2.1. *Let $S \subseteq \mathbb{F}_2^n$ be a Sidon set. Then $\sum_{x \in \mathbf{X}(S)} \mathrm{mult}_S(x) = \sum_{x \in \mathbb{F}_2^n \setminus S} \mathrm{mult}_S(x)$.*

Proof. Notice that if $x \in \mathbb{F}_2^n \setminus S$, then $x \notin \mathbf{X}(S)$ if and only if $\mathrm{mult}_S(x) = 0$. Therefore, the sums of the multiplicities of points in $\mathbf{X}(S)$ and $\mathbb{F}_2^n \setminus S$ are equal. □

Now, recall the following proposition.

Proposition 5.2.2. [22] *Let $S \subseteq \mathbb{F}_2^n$ be a Sidon set. Then $\sum_{x \in \mathbf{X}(S)} \mathrm{mult}_S(x) = \binom{|S|}{3}$.*

Therefore, by combining Lemma 5.2.1 and Proposition 5.2.2, we have

$$\binom{|S|}{3} = \sum_{x \in \mathbf{X}(S)} \mathrm{mult}_S(x) = \sum_{x \in \mathbb{F}_2^n \setminus S} \mathrm{mult}_S(x). \tag{5.2.1}$$

We now introduce notation for the minimal and maximal exclude multiplicities for a given Sidon set S. Denote by $e_{\min}(S)$ and $e_{\max}(S)$ the minimal and maximal exclude point multiplicities, respectively. That is,

$$e_{\min}(S) = \min_{x \in \mathbb{F}_2^n \setminus S} \mathrm{mult}_S(x); \text{ and}$$
$$e_{\max}(S) = \max_{x \in \mathbb{F}_2^n \setminus S} \mathrm{mult}_S(x).$$

Proposition 5.2.3. *Let $S \subseteq \mathbb{F}_2^n$ be a Sidon set. Let z be the number of points in $\mathbb{F}_2^n \setminus S$ with multiplicity 0. Then*

$$(2^n - |S|)e_{\min}(S) \leq \binom{|S|}{3} \leq (2^n - |S| - z)e_{\max}(S). \tag{5.2.2}$$

Proof. By eq. (5.2.1), we have

$$\begin{aligned}\binom{|S|}{3} &= \sum_{x \in \mathbb{F}_2^n \setminus S} \mathrm{mult}_S(x) \\ &\quad |\mathbb{F}_2^n \setminus S| \; e_{\min}(S) \\ &= (2^n - |S|)e_{\min}(S).\end{aligned}$$

Similarly,

$$\begin{aligned}\binom{|S|}{3} &= \sum_{x \in \mathbf{X}(S)} \mathrm{mult}_S(x) \\ &\quad |\mathbf{X}(S)| \; e_{\max}(S) \\ &= (|\mathbb{F}_2^n \setminus S| - z)e_{\max}(S) \\ &= (2^n - |S| - z)e_{\max}(S).\end{aligned}$$

Thus, eq. (5.2.2) holds. □

In the case where $e_{\min}(S)$ and $e_{\min}(S)$ are equal, we call S a **k-cover** where $k = e_{\min}(S) = e_{\max}(S)$.[2] Notice that all k-covers are maximal Sidon sets if and only if $k \neq 0$. Hence, if S is a k-cover and $|S| \geq 3$, then S is maximal.

In general, very little is known about k-covers as it seems that they are difficult to find. However, we recall from Chapter 2 that AB functions are those whose graph is a maximal Sidon set with all exclude points having the same multiplicity [45]. Therefore AB functions are those APN functions such that G_F is a $(\frac{2^n - 2}{6})$-cover. We will now describe the exclude multiplicities of a Sidon set in terms of the exclude distribution.

Definition 5.2.4. Let S be a Sidon set in $\mathbb{F}_2^n$. We define the **exclude distribution** of S to be the function $d_S : \mathbb{F}_2^n \setminus S \to \mathbb{Z}_{\geq 0}$ defined by $d_S(x) = \mathrm{mult}_S(x)$ for all $x \in \mathbb{F}_2^n \setminus S$.

The exclude distribution captures information about the exclude points of a Sidon set and their multiplicities. Since we are working with finite sets, the image of d_S is bounded for any

[2] Note that k-covers do not exist in all dimensions (c.f. [22]).

Sidon set $S \subseteq \mathbb{F}_2^n$. In particular, the maximum value that d_S takes is $e_{\max}(S)$. Similarly, the minimum value that d_S takes is $e_{\min}(S)$.

The exclude distribution is useful in determining properties of a Sidon set, and studying the exclude distributions of two different Sidon sets $S, S' \subseteq \mathbb{F}_2^n$ can be quite useful in determining shared or differing properties of S and S'. To compare two different exclude distributions, we need a notion of equivalence. Exclude distribution equivalence (ED-equivalence) considers the exclude distributions of S and S' to be equivalent if and only if the number of k-points in $\mathbf{X}(S)$ is equal to the number of k-points in $\mathbf{X}(S')$.

Definition 5.2.5. Let S be a Sidon set in $\mathbb{F}_2^n$. If $S' \subseteq \mathbb{F}_2^n$ is a Sidon set, we say that S and S' are **exclude distribution equivalent** (ED-equivalent) if there exists a permutation $\pi : \mathbb{F}_2^n \setminus S \to \mathbb{F}_2^n \setminus S'$ such that $d_S = d_{S'\pi}$.

Now, we explore ED-equivalence and its relation to general affine equivalence. In particular, we will show that ED-equivalence is implied by affine equivalence while the converse is not true in general.

Theorem 5.2.6. *Let $S, S' \subseteq \mathbb{F}_2^n$ be Sidon sets. If there exists an affine permutation $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that $A(S) = S'$, then S and S' are ED-equivalent.*

Proof. Suppose there exists an affine permutation $A : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that $A(S) = S'$. Clearly, if $|S| = |S'| < 3$, then exclude points in both $\mathbb{F}_2^n \setminus S$ and $\mathbb{F}_2^n \setminus S'$ all have multiplicity 0, implying that $d_S = d_{S'\pi}$ where $\pi : \mathbb{F}_2^n \setminus S \to \mathbb{F}_2^n \setminus S'$ is any permutation. Hence S and S' are ED-equivalent if $|S| = |S'| < 3$. Suppose $|S| \geq 3$. Let $x \in \mathbb{F}_2^n \setminus S$, and let $k = \text{mult}_S(x)$.

Case 1: Suppose $k = 0$. Then $a_1 + a_2 + a_3 \neq x$ for all $a_1, a_2, a_3 \in S$, where a_1, a_2, a_3 are distinct. Then $A(a_1) + A(a_2) + A(a_3) = A(a_1 + a_2 + a_3) \neq x$ for all $a_1, a_2, a_3 \in S$, where a_1, a_2, a_3 are distinct. Hence $0 = \text{mult}_S(x) = \text{mult}_{S'}(A(x))$. Therefore $d_S = d_{S'\pi}$ A.

Case 2: Suppose $k > 0$. Then, there exists distinct points $a_1, \ldots, a_{3k} \in S$ such that $x = a_i + a_{2i} + a_{3i}$ for all $i \in [k]$. This implies

$$A(x) = A(a_i + a_{2i} + a_{3i}) = A(a_i) + A(a_{2i}) + A(a_{3i})$$

for all $i \in [k]$, so $\text{mult}_S(x) \leq \text{mult}_{S'}(A(x))$. However, we have that $\text{mult}_{S'}(A(x)) \leq \text{mult}_S(x)$ by applying the same argument and using A^{-1}. Therefore, $\text{mult}_S(x) = \text{mult}_{S'}(A(x))$, and we deduce $d_S = d_{S'} \circ A$.

Thus, S and S' are ED-equivalent. □

So, if any two Sidon sets are affinely equivalent, then they are ED-equivalent. However, the converse is not true in general, which we show by the following example.

Example 5.2.7. Let $F : \mathbb{F}_{2^5} \to \mathbb{F}_{2^5}$ be defined by $F(x) = x^3$ for all $x \in \mathbb{F}_{2^5}$, and let $F' : \mathbb{F}_{2^5} \to \mathbb{F}_{2^5}$ be defined by $F'(x) = x^7$ for all $x \in \mathbb{F}_{2^5}$. Notice that F is a Gold function and F' is a Welch function (see Table 2.2.1). Since F and F' are both AB, they are are ED-equivalent. Notice that, by definition, G_F and $G_{F'}$ are affinely equivalent if and only if F and F' are CCZ-equivalent. By a result of Dempwolff in [24], since F and F' are power functions, they are CCZ-equivalent if and only if they are cyclotomic equivalent (see Chapter 2). So, it remains to show that $3 \cdot 2^i \not\equiv 7^{-1} \bmod 31$ for all $0 \leq i < 5$. First, notice that $7 \cdot 9 = 63 \equiv 1 \bmod 31$, so $7^{-1} = 9$ over $\mathbb{Z}_{31}$. Now, we compute $2^i \cdot 7^{-1} \equiv 2^i \cdot 9 \bmod 31$ for all $0 \leq i < 5$:

$$2^0 \cdot 9 \equiv 9 \bmod 31$$

$$2^1 \cdot 9 \equiv 18 \bmod 31$$

$$2^2 \cdot 9 \equiv 5 \bmod 31$$

$$2^3 \cdot 9 \equiv 10 \bmod 31$$

$$2^4 \cdot 9 \equiv 20 \bmod 31.$$

Thus, $3 \cdot 2^i \not\equiv 7^{-1} \bmod 31$ for all $0 \leq i < 5$, and so F and F' are not CCZ-equivalent, implying that G_F and $G_{F'}$ are not affinely equivalent.

Definition 5.2.8. Let S be a Sidon set in $\mathbb{F}_2^n$. Let X and Y be disjoint subsets of $\mathbb{F}_2^n \setminus S$ of the same size. If there exists a permutation $\pi : X \to Y$ such that $d_S|_X = d_S|_Y \circ \pi$, we say that d_S is **locally equivalent** at X and Y.

Since AB functions are those whose graph is a $(\frac{2^n}{6}, 2)$-cover, the graphs of any two AB functions (with the same dimension) are ED-equivalent. More generally, it is a consequence of the following proposition that all k-covers in the same dimension are ED-equivalent. The following proposition is known.

Proposition 5.2.9. *Let S be a Sidon set in $\mathbb{F}_2^n$. The following are equivalent:*

1. *S is a k-cover,*
2. *$e_{\min}(S) = e_{\max}(S)$,*
3. *d_S is constant,*
4. *d_S is locally equivalent at X and Y for all subsets $X, Y \subseteq \mathbb{F}_2^n \setminus S$ where $|X| = |Y|$.*

Proof. We have that (1) is equivalent to (2) by definition. Also, (3) follows from (2) because $e_{\min}(S) = e_{\max}(S)$, then the minimal and maximal values that d_S takes coincide, so d_S is constant.

Now, suppose d_S is constant and let $X, Y \subseteq \mathbb{F}_2^n \setminus S$ such that $|X| = |Y|$. Then for any permutation $\sigma : X \to Y$, we have $d_S|_X = d_S \circ \sigma|_Y$ because d_S is constant, so (3) implies (4).

Now, suppose (4) holds. Let X be a subset of $\mathbb{F}_2^n \setminus S$ consisting of a single point. By our assumption, d_S is locally equivalent at X and any other subset of $\mathbb{F}_2^n \setminus S$ consisting of a single point. This implies that all points in $\mathbb{F}_2^n \setminus S$ have the same exclude multiplicity, so S is a k-cover for some $k \geq 2$ $\mathbb{N}$, and we conclude that (4) implies (1). □

By Proposition 5.2.9, k-covers naturally impose constraints on the exclude distribution. However, we will no longer focus on the k-cover case, and we begin to instead study *uniformity* of an exclude distribution. Before defining uniform exclude distributions, we first recall that an **equally-sized partition** P of a set S is a partition of S such that any two elements in P have the same size.

Definition 5.2.10. Let S be a Sidon set in $\mathbb{F}_2^n$. If P is an equally-sized partition of some set $Z \subseteq \mathbb{F}_2^n \setminus S$, then we call d_S **uniform** on P if d_S is locally equivalent at any two distinct elements of P.

We now provide examples of exclude distributions that are uniform on some partition of a subset of $\mathbb{F}_2^n$.

Example 5.2.11. Suppose $S \subseteq \mathbb{F}_2^n$ is a k-cover. Let $Z \subseteq \mathbb{F}_2^n \setminus S$, and let P be an equally-sized partition of Z. Then by Proposition 5.2.9, d_S is locally equivalent at any two elements of P, implying d_S is uniform on P.

Example 5.2.12. Consider the Sidon set pictured in Figure 5.2.1 and call it S. Let Z be the highlighted region pictured in Figure 5.2.1. Notice that Z is the union of 6 distinct 4- ats (or 4-dimensional a ne subspaces), and let $P_1, \ldots, P_6$ be these 4- ats. It is then immediately clear that d_S is locally equivalent at any two of these 4- ats. Therefore, d_S is uniform on $\{P_1, \ldots, P_6\}$.

◇	◇	◇	3	2	3	2	◇	2	3	2	◇	2	3	2	◇
◇	3	2	2	2	2	2	1	2	2	2	1	2	2	2	1
◇	2	5	2	3	2	3	2	3	2	3	2	3	2	3	2
3	2	2	◇	2	2	1	2	2	2	1	2	2	2	1	2
2	2	3	2	3	2	2	2	1	1	1	2	1	1	1	2
3	2	2	2	2	◇	1	2	1	2	2	2	1	2	2	2
2	2	3	1	2	1	3	2	1	2	1	2	1	2	1	2
◇	1	2	2	2	2	2	3	2	2	2	1	2	2	2	1
2	2	3	2	1	1	1	2	3	2	2	2	1	1	1	2
3	2	2	2	1	2	2	2	2	◇	1	2	1	2	2	2
2	2	3	1	1	2	1	2	2	1	3	2	1	2	1	2
◇	1	2	2	2	2	2	1	2	2	2	3	2	2	2	1
2	2	3	2	1	1	1	2	1	1	1	2	3	2	2	2
3	2	2	2	1	2	2	2	1	2	2	2	2	◇	1	2
2	2	3	1	1	2	1	2	1	2	1	2	2	1	3	2
◇	1	2	2	2	2	2	1	2	2	2	1	2	2	2	3

Figure 5.2.1: A Sidon set in $\mathbb{F}_2^8$ whose exclude distribution is uniform on 6 distinct 4- ats (or 4-dimensional a ne subspaces).

5.3 The exclude distribution of G_F

In this section, we focus on the exclude distributions of G_F where $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN function. In particular, we will study the excludes of G_F and the open problem on APN functions and maximal Sidon sets. Furthermore, we prove that the exclude distribution of the graph of any Gold function is uniform on a particular partition comprised of n- ats.

5.3.1 The maximal Sidon set conjecture for APN functions

Recall that a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN if and only if its graph G_F is a Sidon set. A Sidon set S is maximal if $S' \supseteq S$ for $S' \subseteq \mathbb{F}_2^n$ Sidon implies $S' = S$. It is conjectured that the graphs of all APN functions are maximal Sidon sets.

Conjecture 5.3.1. [12] [17] *The graphs of all APN functions are maximal Sidon sets.*

So far, it has been shown that the graphs of all APN power functions and APN plateaued functions (see Section 5.3.3) have graphs that are maximal Sidon sets [12] [17]. Clearly, the graph of an APN function F is maximal if and only if d_{G_F} only takes non-zero values, and so the exclude distribution is also a tool that we can use to study problems such as Conjecture 5.3.1.

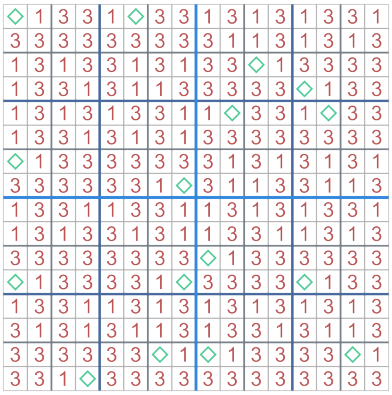


Figure 5.3.1: The graph of the Gold function $x \mapsto x^3$ over $\mathbb{F}_{2^4}$.

It has been known since [45], and perhaps earlier, that sums of subsets of size 3 of G_F (i.e. exclude points) are related to the Fourier-Hadamard transform of W_F^3. The following was shown in [17], but we will consider it a lemma and provide a proof for the sake of completeness.

Lemma 5.3.2. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN function. For any $(a, b) \in (\mathbb{F}_2^n)^2$, the sum $\sum_{u,v \in \mathbb{F}_2^n} (-1)^{v \cdot b + u \cdot a} W_F^3(u, v)$ equals*

$$2^{2n} \left| \{(x_1, x_2, x_3) \in (\mathbb{F}_2^n)^3 : (x_1 + x_2 + x_3, F(x_1) + F(x_2) + F(x_3)) = (a, b)\} \right|.$$

Proof. Let $(a, b) \in (\mathbb{F}_2^n)^2$. Then, we have

$$\begin{aligned} \sum_{u,v \in \mathbb{F}_2^n} (-1)^{v \cdot b + u \cdot a} W_F^3(u, v) &= \sum_{u,v \in \mathbb{F}_2^n} (-1)^{v \cdot b + u \cdot a} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot F(x)} \right) \\ &= \sum_{x_1, x_2, x_3 \in \mathbb{F}_2^n} \sum_{u,v \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x_1) + F(x_2) + F(x_3) + b) + u \cdot (x_1 + x_2 + x_3 + a)}, \end{aligned}$$

as mentioned by Carlet in [17]. Notice that if $x_1 + x_2 + x_3 + a = 0$ and $F(x_1) + F(x_2) + F(x_3) + b \neq 0$ for some fixed $x_1, x_2, x_3, a, b \in \mathbb{F}_2^n$, then

$$\begin{aligned} \sum_{u,v \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x_1) + F(x_2) + F(x_3) + b) + u \cdot (x_1 + x_2 + x_3 + a)} &= \sum_{u,v \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x_1) + F(x_2) + F(x_3) + b)} \\ &= 2^n \sum_{v \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x_1) + F(x_2) + F(x_3) + b)} \\ &= 0 \end{aligned}$$

because for any $x \in (\mathbb{F}_2^n)$, the function $v \mapsto v \cdot x$ is balanced. Similarly, if $x_1 + x_2 + x_3 + a \neq 0$ and $F(x_1) + F(x_2) + F(x_3) + b = 0$ for some fixed $x_1, x_2, x_3, a, b \in \mathbb{F}_2^n$, then

$$\sum_{u,v \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x_1) + F(x_2) + F(x_3) + b) + u \cdot (x_1 + x_2 + x_3 + a)} = 0.$$

Now, consider the case where $x_1 + x_2 + x_3 + a \neq 0$ and $F(x_1) + F(x_2) + F(x_3) + a \neq 0$ for some fixed $x_1, x_2, x_3, a, b \in \mathbb{F}_2^n$:

$$\begin{aligned} &\sum_{u,v \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x_1) + F(x_2) + F(x_3) + b) + u \cdot (x_1 + x_2 + x_3 + a)} \\ &= \sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot (x_1 + x_2 + x_3 + a)} \sum_{v \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x_1) + F(x_2) + F(x_3) + b)} \\ &= \sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot (x_1 + x_2 + x_3 + a)} \cdot 0 \\ &= 0. \end{aligned}$$

Therefore, when considering the entire sum, we have the following:

$$\begin{aligned}
&\sum_{x_1,x_2,x_3 \in \mathbb{F}_2^n} \sum_{u,v \in \mathbb{F}_2^n} (-1)^{v \cdot (F(x_1)+F(x_2)+F(x_3)+b)+u \cdot (x_1+x_2+x_3+a)} \\
&= \sum_{\substack{x_1,x_2,x_3 \in \mathbb{F}_2^n \\ x_1+x_2+x_3=a \\ F(x_1)+F(x_2)+F(x_3)=b}} \sum_{u,v \in \mathbb{F}_2^n} 1 \\
&= 2^{2n} \cdot |\{(x_1,x_2,x_3) \in (\mathbb{F}_2^n)^3 : (x_1+x_2+x_3, F(x_1)+F(x_2)+F(x_3)) = (a,b)\}|.
\end{aligned}$$

□

Corollary 5.3.3. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN function. If $(a,b) \in (\mathbb{F}_2^n)^2 \setminus G_F$, then*

$$d_{G_F}(a,b) = \frac{1}{3 \cdot 2^{2n+1}} \sum_{(u,v) \in (\mathbb{F}_2^n)^2} (-1)^{v \cdot b + u \cdot a} W_F^3(u,v).$$

Proof. Let $(a,b) \in (\mathbb{F}_2^n)^2 \setminus G_F$. Since $b \neq F(a)$, we know that

$$|\{(x,y,z) \in (\mathbb{F}_2^n)^3 : |\{x,y,z\}| < 3, (x+y+z, F(x)+F(y)+F(z)) = (a,b)\}| = 0.$$

Hence

$$\begin{aligned}
d_{G_F}(a,b) &= \frac{1}{6} |\{(x,y,z) \in (\mathbb{F}_2^n)^3 : |\{x,y,z\}| = 3, (x+y+z, F(x)+F(y)+F(z)) = (a,b)\}| \\
&= \frac{1}{6} |\{(x,y,z) \in (\mathbb{F}_2^n)^3 : (x+y+z, F(x)+F(y)+F(z)) = (a,b)\}|,
\end{aligned}$$

and by applying Lemma 5.3.2, we have

$$d_{G_F}(a,b) = \frac{1}{3 \cdot 2^{2n+1}} \sum_{u,v \in \mathbb{F}_2^n} (-1)^{v \cdot b + u \cdot a} W_F^3(u,v).$$

□

Carlet used this to show that the graph of APN function F is maximal if and only if for all $(a,b) \in (\mathbb{F}_2^n)^2$, the inequality $\sum_{u,v \in \mathbb{F}_2^n} (-1)^{v \cdot b + u \cdot a} W_F^3(u,v) \neq 0$ holds.

Remark 5.3.4. If F is APN and the exclude distribution of G_F is uniform on some equally-sized partition P of $(\mathbb{F}_2^n)^2$, then the inequality holding on an element of the equally-sized partition implies that it holds on all of $(\mathbb{F}_2^n)^2$. Hence, if d_{G_F} is uniform on P, then G_F is a maximal Sidon set if and only if there exists $P \in P$ such that for all $(a,b) \in P$ the inequality $\sum_{u,v \in \mathbb{F}_2^n} (-1)^{v \cdot b + u \cdot a} W_F^3(u,v) \neq 0$ holds.

As Carlet showed in [17], Conjecture 5.3.1 is equivalent to the following conjecture:

Conjecture 5.3.5. [12] *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN function. If $F' : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is equal to F except at a single point, then F' is not APN.*

We will demonstrate a new direct proof to show why these two conjectures are equivalent, but first, we introduce notation and provide some preliminary results.

Let P_x denote the set $\{x\} \times \mathbb{F}_2^n = \{(x,y) : y \in \mathbb{F}_2^n\} \subset (\mathbb{F}_2^n)^2$. Consider some vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Clearly, each P_x contains a unique point in G_F, so we also let $Q_x(F) = P_x \cap \{(x,F(x))\}$. Also, denote by $Q(\mathbb{F}_2^n, F)$ and $Q(\mathbb{F}_2^n, F)$ the following partitions of $(\mathbb{F}_2^n)^2$ and $(\mathbb{F}_2^n) \times \mathbb{F}_2^n$, respectively:

$$Q(\mathbb{F}_2^n, F) = \{Q_x(F) : x \in \mathbb{F}_2^n\} \tag{5.3.1}$$

$$Q(\mathbb{F}_2^n, F) = Q(\mathbb{F}_2^n, F) \cap Q_0(F). \tag{5.3.2}$$

When considering the exclude distribution of G_F (for $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ APN), we notice that any exclude point of G_F that lies in $Q_x(F)$ is not equal to a sum of three elements of G_F that contains $(x,F(x))$. That is, any exclude point in $Q_x(F)$ is completely determined by the points in $G_F \cap \{(x,F(x))\}$.

Lemma 5.3.6. *Suppose $n > 1$. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN function. Let $x \in \mathbb{F}_2^n$, and let $(a,b) \in Q_x(F)$. Then $(a,b) \neq (x,F(x)) + (y,F(y)) + (z,F(z))$ for all $y,z \in \mathbb{F}_2^n$ where $y \neq z$.*

Proof. Let $y,z \in \mathbb{F}_2^n$ such that $y \neq z$. Since $(a,b) \in Q_x(F)$, we have $a = x$ by construction of $Q_x(F)$. Therefore $a+x+y+z = y+z \neq 0$, implying $(a,b) \neq (x,F(x)) + (y,F(y)) + (z,F(z))$. □

This leads to the following proposition, which informally speaking states that local exclude multiplicity is preserved when the respective point in G_F is removed.

Proposition 5.3.7. *Suppose $n > 1$. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN function, and let $x \in \mathbb{F}_2^n$. Then the multiplicities of all points in $Q_x(F)$ remain unchanged when $(x,F(x))$ is removed from G_F. Equivalently, $d_{G_F}|_{Q_x(F)} = d_{G_F \cap \{(x,F(x))\}}|_{Q_x(F)}$.*

Proof. Let $(a;b) \in Q_x(F)$, and let $k = \text{mult}_{G_F}(a;b)$. If $k = 0$, then clearly $\text{mult}_{G_F \cap \{(x;F(x))\}}(a;b) = 0 = k$. So, suppose $k \geq 1$. Then, there exist $x_1;\ldots;x_{3k} \in \mathbb{F}_2^n$ such that

$$(a;b) = (x_i;F(x_i)) + (x_{2i};F(x_{2i})) + (x_{3i};F(x_{3i})):$$

for all $i \in [k]$. By Lemma 5.3.6, $x_i \neq a = x$ for all $i \in [3k]$. Hence $(x_i;F(x_i))$ is in $G_F \cap \{(x;F(x))\}$ for all $i \in [3k]$. Thus, $\text{mult}_{G_F \cap \{(x;F(x))\}}(a;b) = k$. Therefore, the restriction maps $d_{G_F} j_{Q_x(F)}$ and $d_{G_F \cap \{(x;F(x))\}} j_{Q_x(F)}$ are the same map. □

From this, we can quickly show that Conjecture 5.3.1 and Conjecture 5.3.5 are equivalent conjectures.

Corollary 5.3.8. *Let $F: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN function. Then G_F is maximal if and only if every function $F': \mathbb{F}_2^n \to \mathbb{F}_2^n$ by changing the value of F at a single point is not APN (i.e. Conjecture 5.3.1 and Conjecture 5.3.5 are equivalent).*

Proof. Suppose G_F is maximal. Let $a \in \mathbb{F}_2^n$, and let $F': \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function equal to F at all points except at a, i.e. $F(x) = F'(x)$ if and only if $x \neq a$. Let k be the exclude multiplicity of $(a;F'(a))$. Since G_F is maximal, we know k is non-zero. Therefore, by applying Proposition 5.3.7, we have $d_{G_F \cap \{(a;F(a))\}}(a;F'(a)) = k$. However, since $G_F \cap \{(a;F(a))\} = G_{F'} \cap \{(a;F'(a))\}$, we deduce $d_{G_{F'} \cap \{(a;F'(a))\}}(a;F'(a)) = k$. Hence $(a;F'(a))$ is an exclude point of $G_{F'}$, so $G_{F'}$ is not a Sidon set. Therefore F' is not APN.

Conversely, suppose every function obtained by changing the value of F at a single point is not APN. Let $(a;b) \in (\mathbb{F}_2^n)^2$ such that $b \neq F(a)$, so $(a;b) \in Q_a(F)$. Let $F': \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function de ned by

$$F'(x) = \begin{cases} b & x = a \\ F(x) & x \neq a: \end{cases}$$

for all $x \in \mathbb{F}_2^n$. By hypothesis, F' is not APN. Hence, $G_{F'}$ is not Sidon, but notice that $G_{F'} \cap \{(a;b)\}$ is Sidon since $G_{F'} \cap \{(a;b)\} = G_F \cap \{(a;F(a))\}$. Therefore $(a;b)$ must be an exclude point of $G_F \cap \{(a;F(a))\}$ because

$$\{(a;b)\} \cup (G_F \cap \{(a;F(a))\}) = G_{F'}$$

is not Sidon. This directly implies that $(a;b)$ is an exclude point of G_F, so we conclude G_F is maximal. □

Remark 5.3.9. A consequence of Proposition 5.3.7 is that if F is an APN function such that $\text{mult}_{G_F}(a;b) = 0$, then $(a;b) \neq (x;F(x)) + (y;F(y)) + (z;F(z))$ for all $x;y;z \in \mathbb{F}_2^n \setminus \{a\}$ where $x;y;z$ are distinct.

Another approach to proving that a Sidon set is maximal is to consider the difference between its minimal and maximal exclude multiplicities. This is because Proposition 5.2.3 provides a relation that involves the size of the Sidon set S, $e_{\min}(S)$ and $e_{\max}(S)$, and also the number of 0-points in $\mathbb{F}_2^n \setminus S$. Informally speaking, if the difference between the minimal and maximal exclude multiplicities is small enough, then the Sidon set is \dense" which implies that it is maximal.

Theorem 5.3.10. *Suppose $n > 1$ and $S \subseteq \mathbb{F}_2^n$ is a Sidon set of size 2^n. If*

$$e_{\max}(S) - e_{\min}(S) \leq \frac{2^n - 2}{6};$$

then S is maximal.

Proof. By way of contradiction, suppose S is not maximal. Then implies S has an exclude point of multiplicity 0, so $e_{\min}(S) = 0$. Hence, $e_{\max}(S) \leq \frac{2^n-2}{6}$. By Proposition 5.2.3, we have the inequality $\binom{2^n}{3} \leq (2^{2n} - 2^n - 1)e_{\max}(S)$, and since $e_{\max}(S) \leq \frac{2^n-2}{6}$, we have

$$\binom{2^n}{3} \leq (2^{2n} - 2^n - 1)\frac{2^n - 2}{6}.$$

Observe that this equation is equivalent to

$$\frac{2^n(2^n - 1)(2^n - 2)}{6} \leq (2^{2n} - 2^n - 1)\frac{2^n - 2}{6}.$$

Hence, $2^{2n} - 2^n = 2^n(2^n - 1) \leq 2^{2n} - 2^n - 1$, a contradiction. Thus, S is maximal. □

For a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, its graph G_F has size 2^n. So if F is APN and $e_{\max}(G_F) - e_{\min}(G_F) \leq \frac{2^n-2}{6}$, then G_F is a maximal Sidon set. However, we can describe this in terms of the Walsh

transform. By Corollary 5.3.3, we know that $e_{\max}(G_F) - e_{\min}(G_F)$ is equal to

$$\max_{(a;b)\,2\,(\mathrm{F}_2^n)^2 n G_F} \frac{1}{3\ 2^{2n+1}} \sum_{u;v2\mathrm{F}_2^n} (-1)^{v\,b+u\,a} W_F^3(u;v) \quad \min_{(c;d)\,2\,(\mathrm{F}_2^n)^2 n G_F} \frac{1}{3\ 2^{2n+1}} \sum_{u;v2\mathrm{F}_2^n} (-1)^{v\,d+u\,c} W_F^3(u;v):$$

By applying Theorem 5.3.10, we have the following.

Corollary 5.3.11. *Suppose $n > 1$, and suppose $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ is an APN function. If*

$$\sum_{\substack{u;v2\mathrm{F}_2^n \\ u\,(a+c)\neq v\,(b+d)}} (-1)^{v\,b+u\,a} W_F^3(u;v) \quad 2^{3n-1} \quad 2^{2n}; \tag{5.3.3}$$

holds for all $(a;b);(c;d)\ 2\ (\mathrm{F}_2^n)^2\ n\ G_F$, then G_F is maximal.

Proof. Suppose eq. (5.3.3) holds. Notice that for any $(a;b);(c;d)\ 2\ (\mathrm{F}_2^n)^2$ such that $b \neq F(a)$ and $d \neq F(c)$, we have

$$d_{G_F}(a;b) \quad d_{G_F}(c;d) = \frac{1}{3\ 2^{2n+1}} \left(\sum_{u;v2\mathrm{F}_2^n} (-1)^{v\,b+u\,a} W_F^3(u;v) \quad \sum_{u;v2\mathrm{F}_2^n} (-1)^{v\,d+u\,c} W_F^3(u;v) \right)$$

by Corollary 5.3.3. By simplifying the right-hand side of the equation above, we have

$$\begin{aligned} d_{G_F}(a;b) \quad d_{G_F}(c;d) &= \frac{1}{3\ 2^{2n+1}} \sum_{u;v2\mathrm{F}_2^n} (-1)^{v\,b+u\,a} \quad (-1)^{v\,d+u\,c} \quad W_F^3(u;v) \\ &= \frac{1}{3\ 2^{2n+1}} \sum_{\substack{u;v2\mathrm{F}_2^n \\ u\,(a+c)\neq v\,(b+d)}} (-1)^{v\,b+u\,a} \quad (-1)^{v\,d+u\,c} \quad W_F^3(u;v) \\ &= \frac{1}{3\ 2^{2n}} \sum_{\substack{u;v2\mathrm{F}_2^n \\ u\,(a+c)\neq v\,(b+d)}} (-1)^{v\,b+u\,a} W_F^3(u;v) \end{aligned}$$

for any $(a;b);(c;d)\ 2\ (\mathrm{F}_2^n)^2$ where $b \neq F(a)$ and $d \neq F(c)$. Therefore,

$$\begin{aligned} \max_{\substack{a;b;c;d2\mathrm{F}_2^n \\ b\neq F(a);d\neq F(c)}} j d_{G_F}(a;b) \quad d_{G_F}(c;d) j &= \frac{1}{3\ 2^{2n}} \max_{\substack{a;b;c;d2\mathrm{F}_2^n \\ b\neq F(a);d\neq F(c)}} \sum_{\substack{u;v2\mathrm{F}_2^n \\ u\,(a+c)\neq v\,(b+d)}} (-1)^{v\,b+u\,a} W_F^3(u;v) \\ &\quad \frac{2^{3n-1} \quad 2^{2n}}{3\ 2^{2n}} \\ &= \frac{2^n \quad 2}{6}: \end{aligned}$$

This implies that $e_{\max}(G_F) \quad e_{\min}(G_F) \quad \frac{2^n \quad 2}{6}$, so G_F is maximal by Theorem 5.3.10. □

Therefore, those APN functions satisfying the condition in Corollary 5.3.11 have graphs that are maximal. Note, however, that Corollary 5.3.11 does not state that all APN functions whose graph is a maximal Sidon set also satisfy inequality (5.3.3). Both of these results imply that an APN function whose graph is non-maximal must have an exclude point of multiplicity greater than $\frac{2^n-2}{6}$. While there are many APN functions whose graphs have exclude points with multiplicity greater than $\frac{2^n-2}{6}$ (e.g. the Dobbertin function when $n = 5$), all of our computed examples (mostly low-dimensional examples of power functions and some quadratics) have satisfied the inequalities from Theorem 5.3.10 and Corollary 5.3.11. It would be interesting to find a subclass of APN functions that always satisfy this bound on the difference between the maximal and minimal exclude multiplicities of their graphs, and therefore, a subclass of APN functions whose graphs are maximal.

We conjecture that if $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is an APN power function $F(x) = x^d$, then the exclude distribution of G_F is constant on $Q_0(F)$ with value $\frac{2^n-2}{6}$. Clearly, all AB functions satisfy this conjecture, since if F is AB, then d_{G_F} is constant on $Q_0(F)$ with constant value $\frac{2^n-2}{6}$. However, all of our computed examples of APN power functions (including those that are not AB) have aligned with this conjecture.

Conjecture 5.3.12. *Suppose n is odd. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a power function $F(x) = x^d$. If F is APN, then d_{G_F} is constant on $Q_0(F)$ with value $\frac{2^n-2}{6}$.*

We also make a very similar conjecture about APN power functions.

Conjecture 5.3.13. *Suppose n is odd. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a power function $F(x) = x^d$. If F is APN, then $d_{G_F}(a; 0) = \frac{2^n-2}{6}$ for all $a \in (\mathbb{F}_2^n)^*$.*

In the case that n is even, $2^n - 2$ is not divisible by 6, so the conjectures above can only hold for n odd. Since APN power functions over $\mathbb{F}_{2^n}$ are bijective when n is odd, one may be led to believe that d_{G_F} being constant on $Q_0(F)$ is related to being an APN permutation. However, this is untrue due to the following example.

Example 5.3.14. Recall Browning, Dillion, McQuistan, and Wolfe's APN permutation over $\mathbb{F}_2^6$, call it F (see page 18). We picture the graph of F in Figure 5.3.2. By direct observation, we see that d_{G_F} does not take a constant value on $Q_0(F)$. On another note, we also can directly observe that d_{G_F} is uniform on $Q(\mathbb{F}_2^6; F)$.

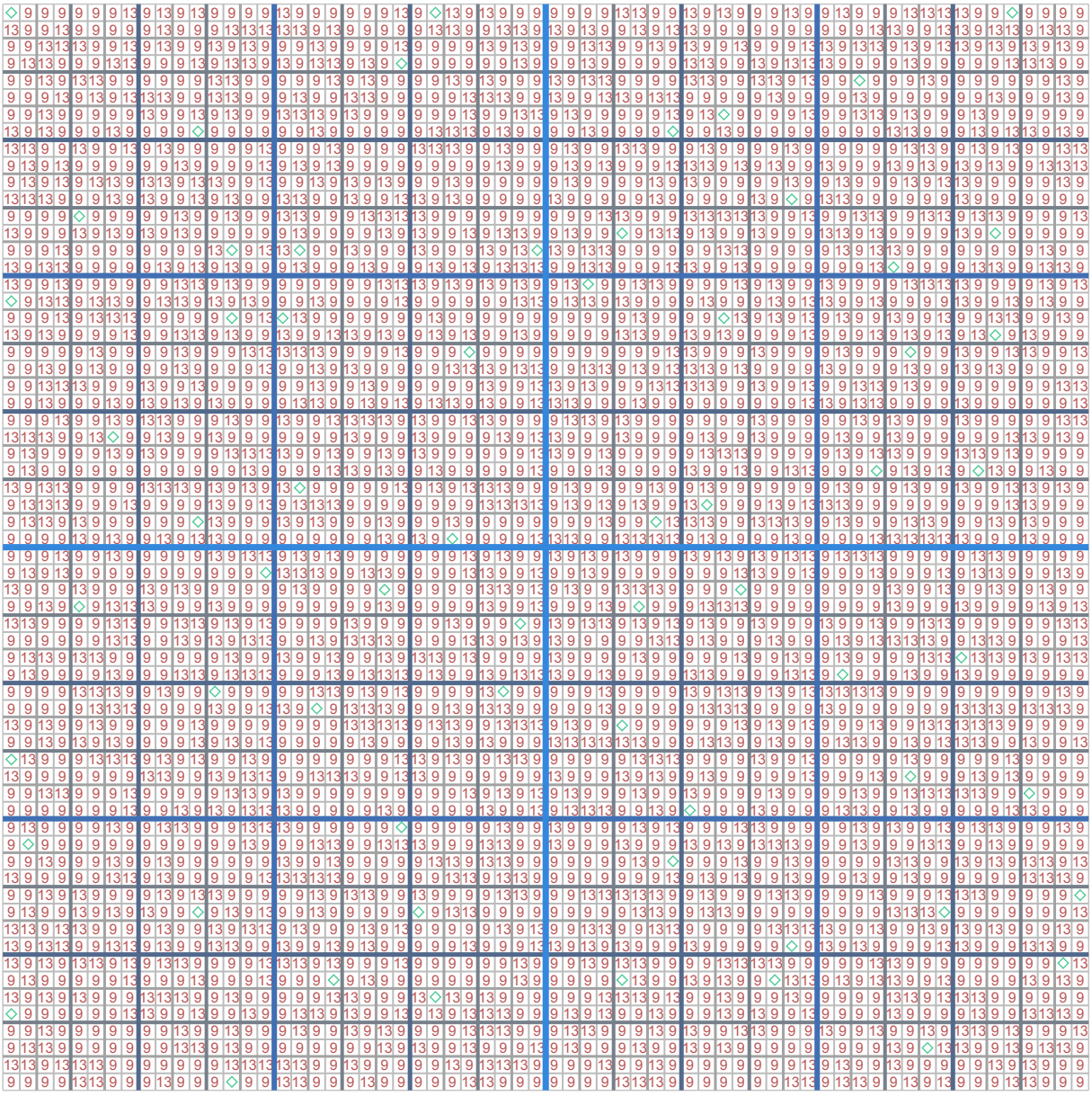


Figure 5.3.2: The graph of the only known example of an APN permutation over an even dimension.

Next, we provide many examples of APN functions that are not AB in which the exclude distributions of their graphs are uniform on $Q(\mathbb{F}_2^n; F)$ or $Q(\mathbb{F}_2^n; F)$, see Table 5.3.1. In other

words, all functions listed in Table 5.3.1 are not AB and they also have graphs whose exclude distribution is uniform on $Q(\mathbb{F}_2^n; F)$ or $Q^-(\mathbb{F}_2^n; F)$.

n	Function	d_{G_F} uniform on $Q(\mathbb{F}_2^n; F)$	d_{G_F} uniform on $Q^-(\mathbb{F}_2^n; F)$
4	Gold	True	True
4	$x^3 + a^{-1}\mathrm{tr}_n(a^3x^9)$	True	True
5	Inverse	False	True
5	Dobbertin	False	True
6	Gold	True	True
6	$x^3 + a^{-1}\mathrm{tr}_n(a^3x^9)$	True	True
6	$x^3 + a^{-1}\mathrm{tr}_n^3(a^3x^9 + a^6x^{18})$	True	True
6	From example 5.3.14	True	True
7	Inverse	False	True
8	Gold	True	True
8	$x^3 + a^{-1}\mathrm{tr}_n(a^3x^9)$	True	True
9	Inverse	False	True
10	Gold	True	True
10	Dobbertin	False	True
10	$x^3 + a^{-1}\mathrm{tr}_n(a^3x^9)$	True	True

Table 5.3.1: APN functions whose graph has a uniform exclude distribution on $Q(\mathbb{F}_2^n; F)$ or $Q^-(\mathbb{F}_2^n; F)$, excluding AB functions.

One interesting fact is that the Dobbertin (pictured in Figure 5.3.3) and Inverse functions computed in Table 5.3.1 have graphs G_F where d_{G_F} is not uniform on $Q(\mathbb{F}_2^n; F)$ but d_{G_F} is uniform on $Q^-(\mathbb{F}_2^n; F)$. We are unsure as to why this is, but it is clear that being uniform on $Q^-(\mathbb{F}_2^n; F)$ is very common, and this leads us to the following conjecture.

Conjecture 5.3.15. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function. If F is APN, then d_{G_F} is uniform on $Q^-(\mathbb{F}_2^n; F)$.*

These conjectures may be very hard to prove due to the very unpredictable nature and history of false conjectures on APN functions. However, we believe that the majority of APN functions (if not all) have graphs whose exclude distributions are uniform on $Q^-(\mathbb{F}_2^n; F)$. This possibly has consequences on the maximality of G_F since uniformity implies a periodicity in d_{G_F}.

Remark 5.3.16. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be APN such that d_{G_F} is uniform on $Q^-(\mathbb{F}_2^n; F)$. Suppose that $(a; b) \in Q_x(F)$ has exclude multiplicity 0 where $x \neq 0$. Then there are at least $2^n - 1$ points of exclude multiplicity 0 in $(\mathbb{F}_2^n)^2 \setminus G_F$.

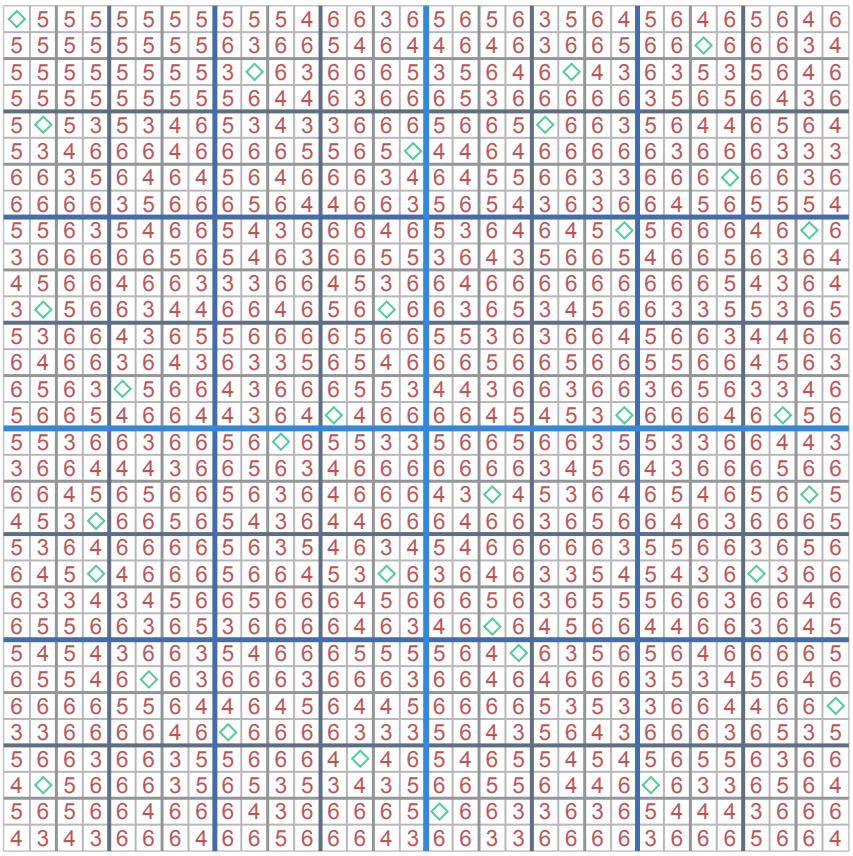


Figure 5.3.3: The graph of the Dobbertin function and its exclude distribution where $n = 5$.

5.3.2 The Gold function

While it may be di cult to prove Conjecture 5.3.15 in general, we are able to prove something even stronger in the case of the Gold function. We will prove that all Gold functions $F : \mathrm{F}_{2^n} \to \mathrm{F}_{2^n}$ have graphs whose exclude distributions are uniform on $Q(\mathrm{F}_{2^n}; F)$. See Figure 5.3.1 for an example.

Recall that when n is odd, any Gold function $F : \mathrm{F}_{2^n} \to \mathrm{F}_{2^n}$ is AB, and so d_{G_F} is uniform on $Q(\mathrm{F}_{2^n}; F)$. What makes the Gold function particularly interesting is that this still holds when n is even. To prove that the exclude distribution of the graph of any Gold function is uniform on $Q(\mathrm{F}_{2^n}; F)$, we need to prove that d_{G_F} is locally equivalent at any two elements of $Q(\mathrm{F}_{2^n}; F)$. This involves providing permutations that satisfy our condition of local equivalence on d_{G_F}.

Lemma 5.3.17. *Let $k; n \in \mathbb{N}$, and suppose* $\gcd(k; n) = 1$. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the Gold function given by $F(x) = x^{2^k+1}$. For any $a; \in \mathbb{F}_{2^n}$, let $_{a;} : Q_a(F) \to Q(F)$ be de ned by $(a; b) = (; b + F(a) + F( ))$. Then $d_{G_F} j_{Q_a(F)} = d_{G_F} j_{Q(F)}$ $_{a;}$ for all $a; \in \mathbb{F}_{2^n}$.*

Proof. Let $a; \in \mathbb{F}_{2^n}$, and let $(a; b) \in Q_a(F)$. Observe that $b \neq a$ by construction, so $b + F(a) + F(c) \neq F(c)$. We will show that $(x_1; x_2; x_3) \in \mathbb{F}_{2^n}^3$ is a solution to the system of equations

$$\begin{cases} x_1 + x_2 + x_3 = a \\ F(x_1) + F(x_2) + F(x_3) = b \end{cases} \tag{5.3.4}$$

if and only if $(w_1; w_2; w_3)$ is a solution to the system of equations

$$\begin{cases} w_1 + w_2 + w_3 = \\ F(w_1) + F(w_2) + F(w_3) = \ : \end{cases} \tag{5.3.5}$$

where $w_i = x_i + a +$ for $i \in [3]$ and $= b + F(a) + F( )$. Observe that if $(x_1; x_2; x_3) \in \mathbb{F}_{2^n}^3$ satis es the system of equations in eq. (5.3.4), then

$$\begin{aligned} w_1 + w_2 + w_3 &= \sum_{i=1}^{3} (x_i + a +) \\ &= \sum_{i=1}^{3} (x_i + x_1 + x_2 + x_3 +) \\ &= 4(x_1 + x_2 + x_3) + 3 \\ &= \end{aligned}$$

and

$$\begin{aligned}
F(w_1) + F(w_2) + F(w_3) &= \sum_{i=1}^{3} (x_i + a + \quad)^{2^k+1} \\
&= \sum_{i=1}^{3} (x_i^{2^k} + a^{2^k} + \quad^{2^k})(x_i + a + \quad) \\
&= \sum_{i=1}^{3} (x_i^{2^k+1} + a x_i^{2^k} + \quad x_i^{2^k} + a^{2^k} x_i + a^{2^k+1} + a^{2^k} \quad + \quad^{2^k} x_i + a \quad^{2^k} + \quad^{2^k+1}) \\
&= x_1^{2^k+1} + x_2^{2^k+1} + x_3^{2^k+1} + a^{2^k+1} + \quad^{2^k+1} \\
&+ \sum_{i=1}^{3} (a x_i^{2^k} + \quad x_i^{2^k} + a^{2^k} x_i + a^{2^k} \quad + \quad^{2^k} x_i + a \quad^{2^k}) \\
&= b + a^{2^k+1} + \quad^{2^k+1} + \sum_{i=1}^{3} (a x_i^{2^k} + \quad x_i^{2^k} + a^{2^k} x_i + a^{2^k} \quad + \quad^{2^k} x_i + a \quad^{2^k}) \\
&= b + a^{2^k+1} + \quad^{2^k+1} + a(x_1 + x_2 + x_3)^{2^k} + \quad (x_1 + x_2 + x_3)^{2^k} \\
&+ a^{2^k}(x_1 + x_2 + x_3) + \quad^{2^k}(x_1 + x_2 + x_3) + a^{2^k} \quad + a \quad^{2^k} \\
&= b + a^{2^k+1} + \quad^{2^k+1} + a^{2^k+1} + a^{2^k} \quad + a^{2^k+1} + a \quad^{2^k} + a^{2^k} \quad + a \quad^{2^k} \\
&= b + a^{2^k+1} + \quad^{2^k+1} \\
&= \quad :
\end{aligned}$$

Conversely, if $(w_1 = x_1 + a + \quad ; w_2 = x_2 + a + \quad ; w_3 = x_3 + a + \quad)$ is a solution to eq. (5.3.5), then $(x_1; x_2; x_3)$ is a solution to eq. (5.3.4). Thus, $d_{G_F}(a; b) = d_{G_F}(\quad ; b + F(a) + F(\quad))$, as desired. □

Our main theorem then follows as a corollary to Lemma 5.3.17.

Theorem 5.3.18. *Let $k; n \geq 2$ $\mathbb{N}$, and suppose $\gcd(k; n) = 1$. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the Gold function given by $F(x) = x^{2^k+1}$. Then d_{G_F} is uniform on $Q(\mathbb{F}_{2^n}; F)$.*

Proof. By Lemma 5.3.17, d_{G_F} is locally equivalent at Q_a and Q for any $Q_a; Q \in Q(\mathbb{F}_{2^n}; F)$. Thus, d_{G_F} is uniform on $Q(\mathbb{F}_{2^n}; F)$. □

Therefore, the Gold function always exhibits symmetry in its excludes. The following is another corollary to Lemma 5.3.17.

Corollary 5.3.19. *Let $k; n \in \mathbb{N}$, and suppose $\gcd(k; n) = 1$. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the Gold function given by $F(x) = x^{2^k+1}$. Then, for any $a, \ldots, b \in \mathbb{F}_{2^n}$ such that $b \neq F(a)$, the equality*

$$\sum_{(u;v)\in\mathbb{F}_{2^n}^2} (-1)^{\mathrm{tr}_n(ua+vb)} W_F^3(u; v) = \sum_{(u;v)\in\mathbb{F}_{2^n}^2} (-1)^{\mathrm{tr}_n(u\ldots+v(b+a^{2^k+1}+\ldots^{2^k+1}))} W_F^3(u; v)$$

holds. Equivalently,

$$\sum_{\substack{(u;v)\in\mathbb{F}_{2^n}^2 \\ \mathrm{tr}_n(u(a+\ldots)+v(a^{2^k+1}+\ldots^{2^k+1}))\neq 0}} (-1)^{\mathrm{tr}_n(vb)+\mathrm{tr}_n(ua)} W_F^3(u; v) = 0.$$

for any $a, \ldots, b \in \mathbb{F}_{2^n}$ such that $b \neq F(a)$.

Proof. Recall from Corollary 5.3.3 that $d_{G_F}(a; b) = \frac{1}{3\,2^{2n+1}} \sum_{(u;v)\in\mathbb{F}_{2^n}^2} (-1)^{\mathrm{tr}_n(vb)+\mathrm{tr}_n(ua)} W_F^3(u; v)$ for all $(a; b) \in \mathbb{F}_{2^n}^2 \setminus G_F$. Therefore, for any $(a; b), (c; d) \in \mathbb{F}_{2^n}^2 \setminus G_F$, we know that $d_{G_F}(a; b) = d_{G_F}(c; d)$ if and only if $\sum_{u;v\in\mathbb{F}_2^n} (-1)^{\mathrm{tr}_n(vb)+\mathrm{tr}_n(ua)} W_F^3(u; v) = \sum_{u;v\in\mathbb{F}_2^n} (-1)^{v\,d+u\,c} W_F^3(u; v)$.

By Lemma 5.3.17, we know that $d_{G_F}(a; b) = d_{G_F}(\ldots, b + F(a) + F(\ldots))$ for all $a, \ldots, b \in \mathbb{F}_{2^n}$ such that $b \neq F(a)$. Therefore,

$$\sum_{(u;v)\in\mathbb{F}_{2^n}^2} (-1)^{\mathrm{tr}_n(ua+vb)} W_F^3(u; v) = \sum_{(u;v)\in\mathbb{F}_{2^n}^2} (-1)^{\mathrm{tr}_n(u\ldots+v(b+a^{2^k+1}+\ldots^{2^k+1}))} W_F^3(u; v) \tag{5.3.6}$$

for any $a, \ldots, b \in \mathbb{F}_{2^n}$ such that $b \neq F(a)$. By rearrangement, eq. (5.3.6) becomes

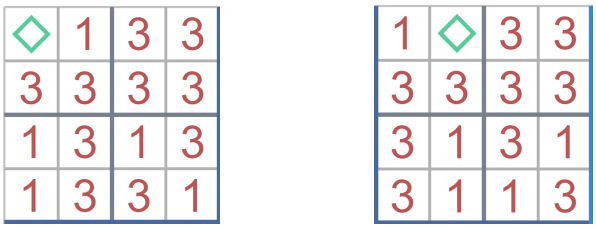
$$\sum_{(u;v)\in\mathbb{F}_{2^n}^2} (-1)^{\mathrm{tr}_n(ua+vb)} W_F^3(u; v) - \sum_{(u;v)\in\mathbb{F}_{2^n}^2} (-1)^{\mathrm{tr}_n(u\ldots+v(b+a^{2^k+1}+\ldots^{2^k+1}))} W_F^3(u; v) = 0. \tag{5.3.7}$$

By the same reasoning used in the proof of Corollary 5.3.11, we know that eq. (5.3.7) is equivalent to

$$\sum_{\substack{(u;v)\in\mathbb{F}_{2^n}^2 \\ \mathrm{tr}_n(u(a+\ldots)+v(a^{2^k+1}+\ldots^{2^k+1}))\neq 0}} (-1)^{\mathrm{tr}_n(vb)+\mathrm{tr}_n(ua)} W_F^3(u; v) = 0,$$

as desired. □

We will now explore the properties of the local permutations $(a; b) \mapsto (\ldots, b + F(a) + F(c))$ for any two $Q_a, Q \in Q(\mathbb{F}_{2^n}; F)$ where F is a Gold function. We start with the following example. Consider the graph of the Gold function $x \mapsto x^3$ which is in $\mathbb{F}_{2^4}^2$, pictured in Figure 5.3.1. In



(a) P_0 (b) P_1

Figure 5.3.4: The distinct a ne ats P_0 and P_1 from Figure 5.3.1.

particular, consider $P_0; P_1$ $F_{2^n}^2$, pictured in Figure 5.3.4 Observe that we can transform P_0 by switching the columns with indices 0 and 1 and those with 1 and 2, and this transformation results in P_1. Note that there are no row transpositions involved in this transformation since $F(0)$ and $F(1)$ are in rows with equal indices.

One can generalize and show that there exist transformations from P_a and P consisting of only row transpositions and column transpositions that preserve the multiplicity of exclude points of G_F where $F : F_{2^n} \to F_{2^n}$ is a Gold function. A transformation that does this is $b \mapsto b + F(a) + F( )$, which is one of the component functions of $_{a;}$ where $_{a;}$ is as in Lemma 5.3.17.

5.3.3 APN plateaued functions

Previously, we showed that all Gold functions F have graphs whose exclude distribution is uniform on $Q(F_{2^n}; F)$, and in this section, we generalize this result. In particular, we will prove that all APN plateaued functions whose component functions are all unbalanced have graphs whose exclude distributions are uniform on such partition.

As mentioned in the introduction to Section 5.3.1, it has been proven that all APN plateaued functions have maximal Sidon sets as their graphs. In fact, most of the known classes of APN functions are also plateaued functions [12]. We now recall the following de nitions.

Definition 5.3.20. Let $f : F_2^n \to F_2$ be a Boolean function. We call f **plateaued** if there exists a positive integer such that $W_f(a) \in \{0; g\}$ for all $a \in F_2^n$.

Definition 5.3.21. Let $F : \mathrm{F}_2^n \to \mathrm{F}_2^m$ be a vectorial Boolean function. We call F **plateaued** if all component functions $b \cdot F$ are plateaued.

In the case where $n = m$, a function $F : \mathrm{F}_2^n \to \mathrm{F}_2^m$ is plateaued if and only if, for every $v \in \mathrm{F}_2^n$, there exists $\lambda_v \neq 0$ such that $W_F(u,v) \in \{0, \pm\lambda_v\}$ for all $u \in \mathrm{F}_2^n$ [17]. All APN plateaued functions are also AB if n is odd.

We will now prove a lemma, which was first shown to be true in the proof of Corollary 3 from [17]. Originally, Carlet used this fact to show that any APN plateaued function $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ whose component functions are unbalanced satisfies $\operatorname{im} F + \operatorname{im} F = \mathrm{F}_2^n$. However, we use this fact to show that all APN plateaued functions F whose component functions are unbalanced have graphs whose exclude distributions are uniform on $Q(\mathrm{F}_2^n; F)$.

Lemma 5.3.22. [17] *Let $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ be a function. If F is an APN plateaued function whose component functions are all unbalanced, then the following equality holds for every $(a,b) \in (\mathrm{F}_2^n)^2$:*

$$\sum_{(u,v)\in(\mathrm{F}_2^n)^2} (-1)^{v\cdot b+u\cdot a} W_F^3(u,v) = 2^{2n}\left|\{(x,y) \in (\mathrm{F}_2^n)^2 : F(x) + F(y) + F(a) = b\}\right|.$$

The following is from the proof of Corollary 3 in [17].

Proof. Suppose F is APN and that the component functions $v \cdot F$ of F are unbalanced. Then $W_F(0,v) \neq 0$ for all $v \in \mathrm{F}_2^n$. Since $W_F(u,v) \in \{0, \pm\lambda_v\}$ for every $u \in \mathrm{F}_2^n$, we know that $W_F^3(u,v) = W_F^2(0,v)W_F(u,v)$, for all $(u,v) \in (\mathrm{F}_2^n)^2$. Therefore,

$$\begin{aligned}
\sum_{(u,v)\in(\mathrm{F}_2^n)^2} (-1)^{v\cdot b+u\cdot a} W_F^3(u,v) &= \sum_{(u,v)\in(\mathrm{F}_2^n)^2} (-1)^{v\cdot b+u\cdot a} W_F(u,v)W_F^2(0,v) \\
&= \sum_{v\in\mathrm{F}_2^n} (-1)^{v\cdot b} W_F^2(0,v) \left(\sum_{u\in\mathrm{F}_2^n} (-1)^{u\cdot a} W_F(u,v)\right) \\
&= 2^n \sum_{v\in\mathrm{F}_2^n} (-1)^{v\cdot b} W_F^2(0,v)(-1)^{v\cdot F(a)} \\
&= 2^n \sum_{v,x,y\in\mathrm{F}_2^n} (-1)^{v\cdot(b+F(x)+F(y)+F(a))} \\
&= 2^{2n}\left|\{(x,y) \in (\mathrm{F}_2^n)^2 : F(x) + F(y) + F(a) = b\}\right|.
\end{aligned}$$

□

By what we have already seen, the above Lemma provides a relation between the exclude multiplicity of a point $(a;b) \in (\mathbb{F}_2^n)^2 \times G_F$ to the size of the set

$$(x;y) \in (\mathbb{F}_2^n)^2 : F(x) + F(y) + F(a) = b \ :$$

We will see that this implies all APN plateaued functions F whose component functions are all unbalanced have graphs whose exclude distributions are uniform on $Q(\mathbb{F}_2^n; F)$, a highly symmetric property.

Theorem 5.3.23. *If $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN plateaued function whose component functions are all unbalanced, then d_{G_F} is uniform on $Q(\mathbb{F}_2^n; F)$.*

Proof. Suppose that F is an APN plateaued function whose component functions are all unbalanced. Then by Corollary 5.3.3 and Lemma 5.3.22, for any $(a;b) \in (\mathbb{F}_2^n)^2 \times G_F$ we have

$$\begin{aligned} d_{G_F}(a;b) &= \frac{1}{3 \cdot 2^{2n+1}} \sum_{(u;v) \in \mathbb{F}_2^n} (-1)^{v \cdot b + u \cdot a} W_F^3(u;v) \\ &= \frac{1}{6} \left| (x;y) \in (\mathbb{F}_2^n)^2 : F(x) + F(y) + F(a) = b \right|. \end{aligned}$$

Let $a, \ , b \in \mathbb{F}_2^n$ such that $b \neq F(a)$, and set $\ = b + F(a) + F(\ )$. Then $\neq F(\ )$, so $(\ , \ ) \notin G_F$. Therefore

$$\begin{aligned} d_{G_F}(a;b) &= \frac{1}{6} \left| (x;y) \in (\mathbb{F}_2^n)^2 : F(x) + F(y) + F(a) = b \right| \\ &= \frac{1}{6} \left| (x;y) \in (\mathbb{F}_2^n)^2 : F(x) + F(y) + F(\ ) = b + F(a) + F(\ ) \right| \\ &= \frac{1}{6} \left| (x;y) \in (\mathbb{F}_2^n)^2 : F(x) + F(y) + F(\ ) = \ \right| \\ &= d_{G_F}(\ , \ ). \end{aligned}$$

We then know that the permutation $\ _{a,\ } : Q_a(F) \to Q\ (F)$ given by $(a;b) \mapsto (\ , b + F(a) + F(\ ))$ satisfies $d_{G_F}|_{Q_a(F)} = d_{G_F}|_{Q\ (F)} \circ \ _{a,\ }$, implying d_{G_F} is uniform on $Q(\mathbb{F}_2^n; F)$, as desired. □

Finding more families of APN functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ whose graphs admit an exclude distribution that is uniform on the partition $Q(\mathbb{F}_2^n; F)$ may prove to be difficult. In summary, we have shown that AB functions and APN plateaued functions whose component functions are

unbalanced both satisfy this property. It would be very interesting to classify all APN functions that admit such a graph. Additionally, it would be interesting to classify all APN functions that do the same for Q $(\mathrm{F}_2^n; F)$.

6
Computational representation

In this chapter, we discuss abstractly representing the mathematical objects we have seen in previous chapters, and we provide the code that was created and used in this research. More specifically, we provide multiple parts of our code that represent vectorial Boolean functions, power functions over $\mathbb{F}_{2^n}$, the Kneser graph of all translations of G_F for $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, and Sidon sets in $\mathbb{F}_2^n$. As we will see in this chapter, while many of the questions that we have asked in previous chapters can be computed in finite time (for a given dimension), we run into the issue of high computational complexity (typically exponential) in most cases.

6.1 Computationally representing vectorial Boolean functions

In this section, we discuss how we represent vectorial Boolean functions, the case of power functions over $\mathbb{F}_{2^n}$, and polynomials over $\mathbb{F}_{2^n}$. Our approach is to construct a parent class called VBF, and this parent class will serve as an abstract representation of what a vectorial Boolean function is. Note that we will be working completely in Python, unless otherwise stated.

We identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$, so we assume all such functions are over a finite field. In order to work over finite fields, we use the pyfinite package, which will be our primary tool for working over finite fields (see [35]). To create a field in pyfinite, we simply can do the following,

```
1 from pyfinite import ffield
2 field = ffield.FField(n)
```

where n is some positive integer.

6.1.1 Abstract vectorial Boolean functions

Recall that a vectorial Boolean function is simply a function from F_2^n to F_2^n. Hence, representing vectorial Boolean functions $F : F_2^n \to F_2^n$ can be done quite naturally since F is, in short, a map sending bitstrings to bitstrings. When working in py nite, we treat elements of F_2^n as elements of F_{2^n}.

For representing a function $F : F_2^n \to F_2^n$, we create a VBF class, which de nes a vectorial Boolean function to be a lambda function along with an instance of a eld. For example, the identity function can be written as id_fcn = VBF(eld, lambda x: x). Depending on the complexity of the given lambda function, it is only sensible to allow for caching, that is, we can store computed values of a given vectorial Boolean function in a dictionary to reduce future computations to $O(1)$ runtime. One can enable caching by setting the use_caching optional parameter to True. Also, if we know ahead of time whether the given function is APN or AB, we are able to pass this parameter to the VBF object to prevent redundancy. We now provide our object representation of vectorial Boolean functions.

Listing 6.1: Representing a vectorial Boolean function in Python.

```
1  class VBF:
2      def __init__(self, field, function, use_caching=True, apn=None, ab=None):
3          self.field = field
4          self.n = field.n
5          self.function = function
6          self.use_caching = use_caching
7          if use_caching:
8              self.cache = fg
9          self.apn = apn
10         self.ab = ab
11
12     def apply_function(self, x):
13         if self.use_caching:
14             if x in self.cache:
15                 return self.cache[x]
16             else:
17                 self.cache[x] = self.function(x)
18                 return self.cache[x]
19         return self.function(x)
20
21     def walsh_spectrum(self):
22         to_return = set()
23         for a in range(2 □□ self.n):
```

```
24              for b in range(1, 2 □□ self.n):
25                  to_return.add(walsh(self, a, b, self.field))
26          return to_return
27
28      def is_apn(self):
29          if self.apn is not None:
30              return self.apn
31          n = self.n
32          for a in range(1, 2 □□ n):
33              sol_range = set()
34              for x in range(0, 2 □□ n):
35                  sol_range.add(self.apply_function(x) ^ self.apply_function(x ^
                        a))
36              if len(sol_range) != 2 □□ (n - 1):
37                  self.apn = False
38                  return False
39          self.apn = True
40          return True
41
42      def is_ab(self):
43          # AB functions cannot exist in even dimensions (Canteaut, Charpin, and
                Dobbertin, '99)
44          if self.ab is not None:
45              return self.ab
46          n = self.n
47          if n % 2 == 0:
48              return False
49          m = 2 □□ ((n + 1) / 2)
50          return self.walsh_spectrum() == f0, -m, mg
51
52
53      def is_permutation(self):
54          output = set()
55          for x in range(2 □□ self.n):
56              eval_at_x = self.apply_function(x)
57              if eval_at_x in output:
58                  return False
59              output.add(eval_at_x)
60          return True
61
62      def is_plateaued(self):
63          for v in range(2 □□ self.n):
64              outputs = fwalsh(self, u, v, self.field) for u in range(2 □□ self.
                    n)g
65              if len(outputs) < 3 or (len(outputs) == 3 and 0 in outputs and min
                    (outputs) == -max(outputs)):
66                  continue
67              return False
68          return True
69
70      def all_component_functions_unbalanced(self):
71          for v in range(1, 2 □□ self.n):
72              if walsh(self, 0, v, self.field) == 0:
73                  return False
74          return True
```

To verify if $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ is APN, we compute the sizes of the sets $\operatorname{im} D_a F$ for all $a \in (\mathrm{F}_2^n)^*$. It is equivalent to say that F is APN if and only if $|\operatorname{im} D_a F| = 2^{n-1}$ for all $a \in (\mathrm{F}_2^n)^*$. The algorithm we use is $O(2^n(2^n - 1)) = O(2^{2n})$, but it would be desirable to increase the speed of this, especially for examples in higher dimensions.

To compute whether or not a function $F : \mathrm{F}_2^n \to \mathrm{F}_2^n$ is AB, we compute the Walsh spectrum, the set of all possible values of $W_F(a, b)$ where $b \neq 0$, and verify that it is equal to $\left\{0, 2^{\frac{n+1}{2}}\right\}$. Similar to before, this algorithm runs in $O(n^2)$ time, but we believe it to be difficult to find a faster generic algorithm.

The VBF class also has a method for seeing if a vectorial Boolean function is plateaued or not. This involves only simply checking if F satisfies the definition provided in Chapter 5 on plateaued functions. Also, to see if all the component functions $v \cdot F$, $v \neq 0$, are unbalanced, it is sufficient to check if $W_F(0, v) \neq 0$ because $W_F(0, v) = \sum_{x \in \mathrm{F}_2^n} (-1)^{v \cdot F(x)}$.

6.1.2 The power function case

We now consider functions $F : \mathrm{F}_{2^n} \to \mathrm{F}_{2^n}$ of the form $F(x) = x^d$. Recall from Table 2.2.1 that there are very few known families of APN power functions over F_{2^n}.

Since most of our known examples are with d large, it is wise to use a fast exponentiation algorithm. We use an algorithm that computes x^d in $O(\log d)$ operations, and this algorithm is often referred to as "exponentiation by squaring" (see [21, Ch. 9]).

Listing 6.2: Exponentiation by squaring in F_{2^n}.

```
1  def field_exp(x, exp, field):
2      '''
3      Computes an exponential power. Runs in logarithmic time.
4      :param x: the base of the exponent
5      :param exp: the power to raise x to
6      :param field: the field x belongs in
7      :return: the result of x^{exp}
8      '''
9
10     a = x
11     d = exp
12
13     # Base Cases
14     if a == 0:
15         return 0
16     if d < 0:
```

```
17          a = field.Inverse(a)
18          d = -d
19      if d == 0:
20          return 1
21
22      y = 1
23      while d > 1:
24          if d % 2 == 1:
25              y = field.Multiply(a, y)
26              d -= 1
27          a = field.Multiply(a, a)
28          d = d / 2
29      return field.Multiply(a, y)
```

We now provide our abstract representation of power functions over F_{2^n} in Python.

Listing 6.3: Representing a power function over F_{2^n}.

```
1  class PowerVBF(VBF):
2      """
3      Represents a function F from GF(2^n) to itself of the form F(x) = x^d.
4      This is known as a power vectorial Boolean function.
5      """
6
7      def __init__(self, exponent, field, use_caching=True, apn=None, ab=None):
8          super().__init__(field, lambda x: field_exp(x, int(exponent), field),
               use_caching, apn, ab)
9          self.exponent = int(exponent)
10
11     def algebraic_degree(self):
12         """
13         Computes the algebraic degree of this function.
14         Since this is a vectorial Boolean power function, the algebraic degree
               is the 2-weight of the exponent.
15         :return: The algebraic degree of F.
16         """
17         return bin(self.exponent).count('1')
18
19     def get_exponent(self):
20         """
21         Get d where F(x) = x^d.
22         :return: The exponent of this power function.
23         """
24         return self.exponent
25
26     def walsh_spectrum(self):
27         # Since F is a power function, it suffices to compute for a =0,1 and b
               nneq 0
28         # because W_F(a,b) = W_F(1, a^{-d} b) for a nneq 0.
29         to_return = set()
30         for a in range(2):
31             for b in range(1, 2 □□ self.n):
32                 to_return.add(walsh(self, a, b, self.field))
33         return to_return
34
35     def cyclotomic_equivalent(self, power_vbf_function):
36         d1 = self.get_exponent()
37         d2 = power_vbf_function.get_exponent()
38         n = self.n
```

```
39          if math.gcd(d1, int(2 □□ n) - 1) == 1:
40              # This is the case when F is a permutation
41              for i in range(n):
42                  if (d2 == (i □ d1) % (int(2 □□ n) - 1)
43                          or (d1 □ d2) % (int(2 □□ n) - 1) == int(2 □□ i)):
44                      return True
45          else:
46              for i in range(n):
47                  if d2 == ((i □ d1) % (int(2 □□ n) - 1)):
48                      return True
49
50          return False
```

Notice that we include a method for checking if two APN power functions are cyclotomic equivalent. This is particularly useful because if two APN power functions are cyclotomic equivalent, then they are also CCZ equivalent because of Dempwol 's result from [24]. In general, computing if two APN functions are CCZ equivalent is quite di cult, but this result allows the power function case to be easily computed.

6.1.3 Common examples of APN functions

We now provide methods for creating the APN functions listed in Table 2.2.1, the APN permutation over F_{2^6} discussed on page 18 which we refer to as \Dillon's permutation", and the following two additional quadratic APN functions:

Function	Condition	Reference
$x^3 + a^{\ 1}\mathrm{tr}_n(a^3x^9)$	$a \neq 0$	[13]
$x^3 + a^{\ 1}\mathrm{tr}_n^3(a^3x^9 + a^6x^{18})$	$3jn$, $a \neq 0$	[14]

Table 6.1.1: Two quadratic APN functions $F_{2^n} \to F_{2^n}$.

Listing 6.4: Methods to generate APN functions.

```
1  def gold(field, k=1, find_nontrivial_k=False, use_caching=True):
2      n = field.n
3      assert math.gcd(n, k) == 1
4      if find_nontrivial_k:
5          # k can always be taken less than n/2 due to conjugacy [c.f. Carlet,
               Picek]
6          for l in range(2, n // 2 + 1):
7              if math.gcd(n, l) == 1:
8                  k = l
9                  break
10     d = int(2 □□ k) + 1
11     return PowerVBF(d, field, use_caching, apn=True, ab=(n % 2 == 1))
12
13
```

```
14 def kasami(field, k=1, find_nontrivial_k=False, use_caching=True):
15     n = field.n
16     k_exp = k
17     if find_nontrivial_k:
18         # k can always be taken less than n/2 due to conjugacy
19         # See "On the exponents of APN power functions and Sidon sets,
20         # sum-free sets, and Dickson polynomials" by Carlet, Picek).
21         for l in range(2, n // 2 + 1):
22             if math.gcd(n, l) == 1:
23                 k_exp = l
24     exp = int(2 □□ (2 □ k_exp)) - int(2 □□ k_exp) + 1
25     return PowerVBF(exp, field, use_caching, apn=True, ab=(n % 2 == 1))
26
27
28 def welch(field, use_caching=True):
29     n = field.n
30     assert n % 2 == 1
31     m = (n - 1) / 2
32     exp = int(2 □□ m) + 3
33     return PowerVBF(exp, field, use_caching, apn=True, ab=True)
34
35
36 def niho(field, use_caching=True):
37     n = field.n
38     assert n % 2 == 1
39     t = (n - 1) // 2
40     if t % 2 == 0:
41         d = int(2 □□ t + 2 □□ (t / 2) - 1)
42     else:
43         d = int(2 □□ t + 2 □□ ((3 □ t + 1) / 2) - 1)
44     return PowerVBF(d, field, use_caching, apn=True, ab=True)
45
46
47 def inverse(field):
48     n = field.n
49     assert field.n % 2 == 1
50     m = (n - 1) / 2
51     return PowerVBF(int(2 □□ (2 □ m)) - 1, field, use_caching=True, apn=True,
           ab=False)
52
53
54 def dobbertin(field, use_caching=True):
55     n = field.n
56     assert n % 5 == 0
57     t = n / 5
58     d = int(2 □□ (4 □ t) + 2 □□ (3 □ t) + 2 □□ (2 □ t) + 2 □□ t - 1)
59     return PowerVBF(d, field, use_caching, apn=True, ab=False)
60
61
62 def quadratic_CCZ_inquiv_to_power(field, a=1, use_caching=True):
63     """
64     This function is inquivalent to any Gold function for n >= 7, and for n=7,
           it's inequivalent to any power mapping.
65     :param field:
66     :param a:
67     :param use_caching:
68     :return:
69     """
70     assert a != 0
```

```
71      a_inv = field.Inverse(a)
72      a3 = field_exp(a, 3, field)
73      trace_of_a3x9 = lambda x: (
74          trace(field.Multiply(a3, field_exp(x, 9, field)), field))
75      fcn = lambda x: (field_exp(x, 3, field) ^
76                       field.Multiply(a_inv, trace_of_a3x9(x)))
77      return VBF(field, fcn, use_caching, ab=(n % 2 == 1))
78
79
80  def quadratic_CCZ_inquiv_to_power2(field, a=1, use_caching=True):
81      assert a != 0
82      assert n % 3 == 0
83      a_inv = field.Inverse(a)
84      a3 = field_exp(a, 3, field)
85      a6 = field_exp(a, 6, field)
86      trace3_of_a3x9_plus_a6x18 = lambda x: (
87          trace(field.Multiply(a3, field_exp(x, 9, field)) ^ field.Multiply(a6,
                field_exp(x, 18, field)),
88                field, m=3))
89      fcn = lambda x: field_exp(x, 3, field) ^ field.Multiply(a_inv,
            trace3_of_a3x9_plus_a6x18(x))
90      return VBF(field, fcn, use_caching, ab=(n % 2 == 1))
91
92
93  def dillion_APN_permutation_dim6(field, use_caching=True):
94      assert field.n == 6
95      c_powers = [25, 30, 32, 37, 23, 39, 44, 4, 18, 46, 51, 52, 18, 56, 53, 30,
             1, 58, 60, 37, 51, 1, 2, 4, 44, 32, 18,
96                  1, 9, 17, 51, 17, 18, 0, 16, 13]
97      x_powers = [57, 56, 50, 49, 48, 43, 42, 41, 40, 36, 35, 34, 33, 32, 29,
            28, 25, 24, 22, 21, 20, 18, 17, 15, 14, 13,
98                  12, 11, 10, 8, 7, 6, 5, 4, 3, 1]
99
100     c = find_primitive_element(field)
101     return VBF(field, lambda x: compute_polynomial(x, c, x_powers, c_powers,
            field), use_caching, apn=True, ab=False)
```

6.1.4 *More general polynomials*

Upon observation of the code above, one may notice that we use a method called compute_polynomial in the method called dillon_APN_permutation_dim6 which refers to Dillon's permutation. The method compute_polynomial is used to compute a 2-variable polynomial in general and is done so by providing the input and coe cients by using a primitive element of F_{2^n}. In short, compute_polynomial can be used to compute the value of $\sum_{i2I} c^i y^i$ for some index set $I \quad f0;:::;2^n \quad 1g$. If $c \ 2 \ F_{2^n}$ is primitive, then by de nition, for all $x \ 2 \ F_{2^n}$ there exist some $i \ 2 \ f0;:::;2^n \quad 1g$ such that $c^i = x$. For this reason, compute_polynomial is particularly useful for computing polynomials of $\sum_{i2I} c^i x^i$ where c is primitive.

Listing 6.5: Method to compute polynomials over F_{2^n}.

```
def compute_polynomial(x, c, x_powers, c_powers, field):
    """
    Computes a polynomial given P(x) = Sum[c^(a_i) x^(b_i)]
        where a_i is the ith entry of x_powers and b_i is the ith entry of
            c_powers
    :param x: The input to the polynomial
    :param c: Used to define coefficients of the polynomial. If primitive, c^d
         can be any element non-zero element
    :param x_powers: The powers of x to evaluate, the ith entry will
        correspond to the ith power of x
    :param c_powers: The powers of c to evaluate, the ith entry will
        correspond to the ith power of c
    :param field: The field that x and c belong to
    :return:
    """
    result = 0
    for x_power, c_power in zip(x_powers, c_powers):
        result ^= field.Multiply(field_exp(x, x_power, field), field_exp(c,
            c_power, field))
    return result
```

6.2 Creating the graph of F

For a vectorial Boolean function $F : F_2^n \to F_2^n$, we want to represent its graph as a set within $F_2^n \times F_2^n$. Recall that the graph of F is defined as $G_F = \{(x; F(x)) : x \in F_2^n\}$. So, in order to represent F, we can concatenate the binary strings of x and $F(x)$, both of which are of length n, to create a binary string of length $2n$.

Example 6.2.1. Suppose F is the identity function $F(x) = x$, and suppose $n = 2$. Then

$$G_F = \{(0;0);(0;0)); ((0;1);(0;1)); ((1;0);(1;0)); ((1;1);(1;1))\}:$$

We can simplify notation by writing vectors in F_2^n as bitstrings, so G_F is

$$G_F = \{0000; 0101; 1010; 1111\}:$$

So, in order to concatenate we use a very simple method.

Listing 6.6: Method to concatenate two binary strings in Python.

```
def concatenate_binary_strings(left, right, n):
    """
    Stitches the two binary strings of the given integers together to create a
         new integer.
    Given two integers p1 and p2, we return the point (p1, p2).
    :param left: p1
```

```
    :param right: p2
    :param n: The dimension of the field which both p1 and p2 lie in.
    :return: The newly constructed point which lies in dimension 2n.
    """
    return int(f"{left:0{n}b}{right:0{n}b}", 2)
```

Now, we are able to construct the graph of a vectorial Boolean function by using the concatenation of two binary strings. Furthermore, we also are able to construct T_F by using an additional method called translate_set which simply adds a given point to all points to the given set.

Listing 6.7: Constructing G_F and T_F in Python.

```

def build_graph(vbf):
    """
    Builds the graph of the function F: F_{2^n} to F_{2^n}.
    The graph of a function F is defined to be the set of all ordered pairs (x
        ,F(x)) for all x in F_{2^n}.
    :param F: The function.
    :param n: The dimension of the field F is over
    :return:
    """
    n = vbf.field.n
    to_return = []
    for p in range(int(2 □□ n)):
        to_return.append(concatenate_binary_strings(p, vbf.apply_function(p),
            n))
    return to_return

def get_all_graph_translations(F):
    n = F.field.n
    graph = build_graph(F)
    # return [tuple(translate_set(graph, t)) for t in range(0, 2 □□ (2 □ n))]
    return list(set([tuple(sorted(translate_set(graph, t))) for t in range(0,
        2 □□ (2 □ n))]))
```

One may wonder why we first sort translations, convert them into tuples, then sets, and back into a list. The reason for this is to prevent duplicate translations because when $_F = 2^n$, there exist $(a;b);(c;d)\ 2\ (\mathrm{F}_2^n)^2$ such that $_{a;b}(G_F) = _{c;d}(G_F)$ (see Lemma 4.3.3).

6.3 Representing the Kneser graph of all translations

In this section, we consider computing the Kneser graph of all translations of G_F where $F : \mathrm{F}_2^n \ ! \ \mathrm{F}_2^n$ is a vectorial Boolean function. In order to construct the graph, we use the networkx package

in Python (see [40]). Since we have already de ned the get_all_translations method, creating the Kneser graph of T_F is straightforward.

Listing 6.8: Generating the Kneser graph of T_F.

```
import networkx as nx

def kneser_graph(sets):
    G = nx.Graph()
    # Add nodes to the graph
    G.add_nodes_from(sets)

    # Add edges to the graph for disjoint k-subsets
    for i, subset1 in enumerate(sets):
        for subset2 in sets[i + 1:]:
            # if subset1 != subset2:
            if not any(item in subset2 for item in subset1):
                G.add_edge(subset1, subset2)
    return G

KGTF = kneser_graph(all_translations)
```

6.4 Computing the exclude distribution of a Sidon set

Now, we consider the exclude distribution of a Sidon set S $\mathbb{F}_2^n$. The exclude distribution contains information about how many points in $\mathbb{F}_2^n n S$ have exclude multiplicity k as the number of such points is equal to $jd_S{}^1(fkg)j$. However, computing the exclude multiplicities of all points in $\mathbb{F}_2^n \, n \, S$ is computationally expensive. Regarding runtime, assigning each point its exclude multiplicity is $O(\,{}^{jSj}_{3}\,) = O(jSj^3)$.

When S is the graph of an APN function $F : \mathbb{F}_2^n \; ! \; \mathbb{F}_2^n$, then it is possible to compute the exclude multiplicity of a single point in $(\mathbb{F}_2^n)^2 \, n \, G_F$. This is because Corollary 5.3.3 states that any point $(a; b) \; 2 \; (\mathbb{F}_2^n)^2 \, n \, G_F$ has exclude multiplicity

$$\frac{1}{3 \;\; 2^{2n+1}} \sum_{(u;v)2(\mathbb{F}_2^n)^2} (\;\; 1)^{v \, b+u \, a} W_F^3(u; v):$$

Therefore, in case $S = G_F$ for an APN function F, we are able to compute the exclude multiplicity of a single point in $(\mathbb{F}_2^n)^2 n G_F$. However, the obvious algorithm still has $O(2^{3n})$ runtime. It would be interesting to nd a faster algorithm for computing the exclude multiplicity of a single point in the complement of G_F.

Since computing the exclude multiplicities of all points in $F_2^n nS$ is computationally expensive, we provide code written in C rather than Python. This allows us to compute the distribution of exclude multiplicities distribution signi cantly faster. We provide our code now.

Listing 6.9: Computing the exclude distribution of a given Sidon set in C.

```
#include <stdio.h>
#include <stdlib.h>

int max(int arr[], int size)
{
    int max = arr[0];
    for (int i = 1; i < size; i++)
    {
        if (arr[i] > max)
        {
            max = arr[i];
        }
    }
    return max;
}

int main()
{
    // INPUT
    int dim;
    printf("Enter the dimension of the set: ");
    scanf("%d", &dim);
    int spaceSize = 1 << dim; // 2^d

    int sizeOfSet;
    printf("Enter the size of the set: ");
    scanf("%d", &sizeOfSet);

    int *sidonSet = (int *)malloc(sizeOfSet * sizeof(int));
    printf("Enter %d values for set:\n", sizeOfSet);
    for (int i = 0; i < sizeOfSet; ++i)
    {
        scanf("%d", &sidonSet[i]);
    }

    printf("Sidon set:\n");
    for (int i = 0; i < sizeOfSet; i++)
    {
        printf("%d ", sidonSet[i]);
    }
    printf("\n");

    printf("Values stored\n");

    // Table:
    // Key = Point in \nF_2^{2n}, Value = Exclude Multiplicity
    int *excludeMultiplicties = (int *)malloc(spaceSize * sizeof(int));

    for (int i = 0; i < sizeOfSet; i++)
    {
        for (int j = i + 1; j < sizeOfSet; j++)
```

```
52          {
53              for (int k = j + 1; k < sizeOfSet; k++)
54              {
55                  excludeMultiplicties[sidonSet[i] ^ sidonSet[j] ^ sidonSet[k
                        ]]++;
56              }
57          }
58      }
59
60      free(sidonSet);
61
62      int maxExcludeMult = max(excludeMultiplicties, spaceSize);
63      printf("\n\nExclude Distribution:\n\n");
64      printf("Mult\t\tFreq\n\n");
65      for (int mult = 0; mult <= maxExcludeMult; mult++)
66      {
67          int count = (mult == 0) ? -sizeOfSet : 0;
68          for (int point = 0; point < spaceSize; point++)
69          {
70              if (excludeMultiplicties[point] == mult)
71              {
72                  count++;
73              }
74          }
75          if (count > 0)
76          {
77              printf("%d\t\t%d\n\n", mult, count);
78          }
79      }
80      free(excludeMultiplicties);
81      return 0;
82  }
```

Bibliography

[1] T. D. Bending and D. Fon-Der-Flaass. \Crooked functions, bent functions, and distance regular graphs". In: *The Electronic Journal of Combinatorics* 5.1 (June 1998). doi: 10.37236/1372.

[2] A. Bernasconi and B. Codenotti. \Spectral analysis of Boolean functions as a graph eigenvalue problem". In: *IEEE Transactions on Computers* 48.3 (1999), pp. 345{351. doi: 10.1109/12.755000.

[3] A. Bernasconi, B. Codenotti, and J.M. Vanderkam. \A characterization of bent functions in terms of strongly regular graphs". In: *IEEE Transactions on Computers* 50.9 (2001), pp. 984{985. doi: 10.1109/12.954512.

[4] T. Beth and C. Ding. \On Almost Perfect Nonlinear Permutations". In: *Advances in Cryptology | EUROCRYPT '93*. Ed. by Tor Helleseth. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 65{76. isbn: 978-3-540-48285-7.

[5] Eli Biham and Adi Shamir. \Di erential cryptanalysis of DES-like cryptosystems". In: *Journal of Cryptology* 4.1 (Jan. 1991), pp. 3{72. issn: 1432-1378. doi: 10.1007/BF00630563. url: https://doi.org/10.1007/BF00630563.

[6] Celine Blondeau and Kaisa Nyberg. \Perfect nonlinear functions and cryptography". In: *Finite Fields and Their Applications* 32 (2015). Special Issue : Second Decade of FFA, pp. 120{147. issn: 1071-5797. doi: https://doi.org/10.1016/j.ffa.2014.10.007. url: https://www.sciencedirect.com/science/article/pii/S1071579714001208.

[7] Andries E. Brouwer, Arjeh M. Cohen, and Arnold Neumaier. *Distance-Regular Graphs*. 1st ed. Springer Berlin, Heidelberg, 1989. isbn: 9783642743436. doi: 10.1007/978-3-642-74341-2.

[8] K.A. Browning, J.F. Dillion, M.T. McQuistan, and A.J. Wolfe. \An APN permutation in dimension six". In: *Finite Fields: Theory and Applications* S18.FQ9 (2010), pp. 33{42.

[9] L. Budaghyan, C. Carlet, and A. Pott. \New classes of almost bent and almost perfect nonlinear polynomials". In: *IEEE Transactions on Information Theory* 52.3 (Mar. 2006), pp. 1141{1152. issn: 1557-9654. doi: 10.1109/TIT.2005.864481.

[10] Lilya Budaghyan. *Construction and Analysis of Cryptographic Functions*. 1st ed. Springer International Publishing, 2014.

[11] Lilya Budaghyan, Claude Carlet, and Tor Helleseth. \On bent functions associated to AB functions". In: *2011 IEEE Information Theory Workshop*. Oct. 2011, pp. 150{154. doi: 10.1109/ITW.2011.6089365.

[12] Lilya Budaghyan, Claude Carlet, Tor Helleseth, Nian Li, and Bo Sun. \On Upper Bounds for Algebraic Degrees of APN Functions". In: *IEEE Transactions on Information Theory* 64.6 (2018), pp. 4399{4411. doi: 10.1109/TIT.2017.2757938.

[13] Lilya Budaghyan, Claude Carlet, and Gregor Leander. \Constructing new APN functions from known ones". In: *Finite Fields and Their Applications* 15.2 (2009), pp. 150{159. issn: 1071-5797. doi: https://doi.org/10.1016/j.ffa.2008.10.001. url: https://www.sciencedirect.com/science/article/pii/S1071579708000622.

[14] Lilya Budaghyan, Claude Carlet, and Gregor Leander. \On a construction of quadratic APN functions". In: *2009 IEEE Information Theory Workshop*. 2009, pp. 374{378. doi: 10.1109/ITW.2009.5351383.

[15] A. Canteaut, P. Charpin, and H. Dobbertin. \Binary m-sequences with three-valued cross-correlation: a proof of Welch's conjecture". In: *IEEE Transactions on Information Theory* 46.1 (2000), pp. 4{8. doi: 10.1109/18.817504.

[16] Anne Canteaut, Pascale Charpin, and Hans Dobbertin. \Weight Divisibility of Cyclic Codes, Highly Nonlinear Functions on F2m, and Crosscorrelation of Maximum-Length Sequences". In: *SIAM Journal on Discrete Mathematics* 13.1 (2000), pp. 105{138. doi: 10.1137/S0895480198350057. eprint: https://doi.org/10.1137/S0895480198350057. url: https://doi.org/10.1137/S0895480198350057.

[17] Claude Carlet. \On APN Functions Whose Graphs are Maximal Sidon Sets". In: *LATIN 2022: Theoretical Informatics*. Ed. by Armando Castaneda and Francisco Rodr guez-Henr quez. Cham: Springer International Publishing, 2022, pp. 243{254. isbn: 978-3-031-20624-5.

[18] Claude Carlet, Pascale Charpin, and Victor Zinoviev. \Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems". In: *Des. Codes Cryptography* 15 (Nov. 1998), pp. 125{156. doi: 10.1023/A:1008344232130.

[19] Claude Carlet and Stjepan Picek. *On the exponents of APN power functions and Sidon sets, sum-free sets, and Dickson polynomials*. Cryptology ePrint Archive, Paper 2017/1179. https://eprint.iacr.org/2017/1179. 2017. url: https://eprint.iacr.org/2017/1179.

[20] Florent Chabaud and Serge Vaudenay. \Links between di erential and linear cryptanalysis". In: *Advances in Cryptology | EUROCRYPT'94* (1995), pp. 356{365. doi: 10.1007/bfb0053450.

[21] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography, Second Edition*. 2nd. Chapman & Hall/CRC, 2012. isbn: 1439840008.

[22] Julia Crager, Felicia Flores, Timothy E. Goldberg, Lauren L. Rose, Daniel Rose-Levine, Darrion Thornburgh, and Raphael Walker. \How Many Cards Should You Lay Out in a Game of EvenQuads: A Detailed Study of Caps in AG(n,2)". In: *La Matematica* (May 2023). doi: 10.1007/s44007-023-00047-0. url: https://doi.org/10.1007/s44007-023-00047-0.

[23] Ingo Czerwinski and Alexander Pott. *Sidon sets, sum-free sets and linear codes*. 2023. arXiv: 2304.07906 [math.CO].

[24] Ulrich Dempwol . \CCZ equivalence of power functions". In: *Designs, Codes and Cryptography* 86 (Mar. 2018). doi: 10.1007/s10623-017-0350-8.

[25] H. Dobbertin. \Almost perfect nonlinear power functions on *GF*(2^n): the Welch case". In: *IEEE Transactions on Information Theory* 45.4 (1999), pp. 1271{1275. doi: 10.1109/18.761283.

[26] Hans Dobbertin. \Almost Perfect Nonlinear Power Functions on *GF*(2^n): A New Case for *n* Divisible by 5". In: *Finite Fields and Applications*. Ed. by Dieter Jungnickel and Harald Niederreiter. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 113{121. isbn: 978-3-642-56755-1.

[27] Hans Dobbertin. \Almost Perfect Nonlinear Power Functions on *GF*(2^n): The Niho Case". In: *Information and Computation* 151.1 (1999), pp. 57{72. issn: 0890-5401. doi: https://doi.org/10.1006/inco.1998.2764. url: https://www.sciencedirect.com/science/article/pii/S089054019892764X.

[28] Hans Dobbertin. \Almost perfect nonlinear power functions on *GF*(2^n): the Welch case". In: *IEEE Transactions on Information Theory* 45.4 (1999), pp. 1271{1275. doi: 10.1109/18.761283.

[29] Michael Follett, Kyle Kalail, Elizabeth McMahon, Catherine Pelland, and Robert Won. \Partitions of AG(4,3) into maximal caps". In: *Discrete Mathematics* 337 (2014), pp. 1{8. issn: 0012-365X. doi: https://doi.org/10.1016/j.disc.2014.08.002. url: https://www.sciencedirect.com/science/article/pii/S0012365X14003069.

[30] R. Gold. \Maximal recursive sequences with 3-valued recursive cross-correlation functions". In: *IEEE Transactions on Information Theory* 14.1 (Jan. 1968), pp. 154{156. issn: 1557-9654. doi: 10.1109/TIT.1968.1054106.

[31] Henk D.L. Hollmann and Qing Xiang. \A Proof of the Welch and Niho Conjectures on Cross-Correlations of Binary m-Sequences". In: *Finite Fields and Their Applications* 7.2 (2001), pp. 253{286. issn: 1071-5797. doi: https://doi.org/10.1006/ffta.2000.0281. url: https://www.sciencedirect.com/science/article/pii/S1071579700902818.

[32] H. Janwa and R. M. Wilson. \Hyperplane sections of fermat varieties in P3 in char. 2 and some applications to cyclic codes". In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. Ed. by Gerard Cohen, Teo Mora, and Oscar Moreno. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, pp. 180{194. isbn: 978-3-540-47630-6.

[33] T. Kasami. \The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes". In: *Information and Control* 18.4 (1971), pp. 369{394. issn: 0019-9958. doi: https://doi.org/10.1016/S0019-9958(71)90473-6. url: https://www.sciencedirect.com/science/article/pii/S0019995871904736.

[34] Gohar M. Kyureghyan. \Crooked maps in F_2^n". In: *Finite Fields and Their Applications* 13.3 (2007), pp. 713{726. issn: 1071-5797. doi: https://doi.org/10.1016/j.ffa.2006.03.003. url: https://www.sciencedirect.com/science/article/pii/S1071579706000207.

[35] Emin Martinian. *py nite*. Nov. 2022. url: https://github.com/emin63/pyfinite/.

[36] Mitsuru Matsui. \Linear Cryptanalysis Method for DES Cipher". In: *Advances in Cryptology | EUROCRYPT '93*. Ed. by Tor Helleseth. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 386{397. isbn: 978-3-540-48285-7.

[37] Willi Meier and Othmar Sta elbach. \Nonlinearity Criteria for Cryptographic Functions". In: *Advances in Cryptology | EUROCRYPT '89*. Ed. by Jean-Jacques Quisquater and Joos Vandewalle. Berlin, Heidelberg: Springer Berlin Heidelberg, 1990, pp. 549{562. isbn: 978-3-540-46885-1.

[38] Tim Mussche. \Extremal combinatorics in generalized Kneser graphs". In: *Nano Letters - NANO LETT* (Jan. 2009).

[39] Gabor Nagy. *Thin Sidon sets and the nonlinearity of vectorial Boolean functions*. Dec. 2022. doi: 10.48550/arXiv.2212.05887.

[40] *NetworkX*. Nov. 2022. url: https://networkx.org/.

[41] Ahmed Noubi Elsawy. *Paley Graphs and Their Generalizations*. Mar. 2012. doi: 10.48550/arXiv.1203.1818.

[42] Kaisa Nyberg. \Di erentially uniform mappings for cryptography". In: *Advances in Cryptology | EUROCRYPT '93*. Ed. by Tor Helleseth. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 55{64. isbn: 978-3-540-48285-7.

[43] Maximus Redman, Lauren Rose, and Raphael Walker. \A Small Maximal Sidon Set in Z_2^n". In: *SIAM J. Discrete Math.* 36.3 (2022), pp. 1861{1867. issn: 0895-4801. doi: 10.1137/21M1454663. url: https://doi.org/10.1137/21M1454663.

[44] Michael Tait and Robert Won. \Improved bounds on sizes of generalized caps in $AG(n;q)$". In: *SIAM J. Discrete Math.* 35.1 (2021), pp. 521{531. issn: 0895-4801. doi: 10.1137/20M1369439. url: https://doi.org/10.1137/20M1369439.

[45] E.R. van Dam and D. Fon-Der-Flaass. \Codes, graphs, and schemes from nonlinear functions". In: *European Journal of Combinatorics* 24.1 (2003), pp. 85{98. issn: 0195-6698. doi: https://doi.org/10.1016/S0195-6698(02)00116-6. url: https://www.sciencedirect.com/science/article/pii/S0195669802001166.

[46] Raphael Walker. *Qap Visualizer*. https://slickytail.github.io/QuadsVis/index.html.

[47] Association for Women in Math. *EvenQuads Website: https://awm-math.org/publications/playing-cards/*. 2020. url: https://awm-math.org/publications/playing-cards/evenquads/.