Spring 2010

Analysis of boolean functions with high second order nonlinearity

Corneliu A. Bodea
University of Richmond

Analysis of Boolean Functions with High Second Order Nonlinearity

Corneliu A. Bodea
Honors Thesis [1]
Department of Mathematics and Computer Science
University of Richmond
Richmond, VA 23173
email : cornel.bodea@richmond.edu

April 26, 2010

[1] Under the direction of Dr. James A. Davis

Abstract

Highly nonlinear Boolean functions play a central role in the design and security analysis of high speed stream cyphers and block cyphers. We focus on analyzing the structure of Boolean functions that exhibit high second order nonlinearity. We commence with a theoretical overview of Boolean functions and Reed-Muller codes. We then introduce a new equivalence relation, 2-equivalence, for which we prove a number of important properties. Finally, we analyze the second order nonlinearity of concatenations of two Boolean functions.

Contents

1 Introduction

Symmetric (private key) cryptography involves the use of the same key to both encrypt and decrypt data. Symmetric systems are well suited to transmit large amounts of data very quickly, since the speed attained by symmetric systems is significantly higher than that of asymmetric methods. However, a major vulnerability of symmetric cryptography lies in the fact that the key necessary to decrypt a message must be shared with the recipient using a secure channel. In practice, both public key cryptography and conventional (private key) cryptography are combined to exchange large amounts of data securely. We study the Boolean functions used for making symmetric cryptosystems as nonlinear as possible, which enables them to be more resistant to known attacks. In particular, we focus on functions that exhibit high second order nonlinearity, and analyze properties of their concatenations.

2 Theoretical Overview of Boolean Functions

2.1 Representation of Boolean Functions

Boolean functions and their properties play a fundamental role in cryptography. We naturally proceed by providing an overview of these properties, starting with the definition of a Boolean function itself. In this paper, we denote vector addition over $\mathbb{F}_2$ by $\oplus$.

Definition 2.1 *Any function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, where $\mathbb{F}_2 = \{0, 1\}$ is the finite field of order two, is called a Boolean function.*

Since the order of $\mathbb{F}_2^n$ is 2^n, and every vector in $\mathbb{F}_2^n$ can be mapped to either 0 or 1, there are 2^{2^n} Boolean functions of n variables. Let B_n denote the set of all 2^{2^n} Boolean functions of n variables.

We can specify $f((x_1 \dots x_n)) \in B_n$ by a binary truth table, which contains the value of f for all 2^n arguments.

Example 2.2 *If $n = 3$, we can construct a function f with the following truth table:*

$$x_1 = (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1)$$
$$x_2 = (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1)$$
$$x_3 = (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1)$$
$$f = (0\ 0\ 1\ 1\ 1\ 1\ 0\ 0)$$

Thus, $f((0\ 1\ 0)) = 1$*, and* $f((1\ 1\ 0)) = 0$*.*

The above truth table specifies the value taken by f for all of the possible 2^3 input combinations, which make up the columns of the truth table. The last row of the truth table defines a binary vector of length 2^3, which contains the values taken by the Boolean function f, for all possible arguments in $\mathbb{F}_2^3$. The standard order of the arguments is the one presented in the above truth table. It is common to also denote the binary vector representing the last row of the truth table by f. This notation is generally accepted, since using a truth table (and observing the standard order of the arguments), we can uniquely define any Boolean function f just by specifying the associated vector f - the last row of the truth table. When working with Boolean functions, the context will clarify whether we refer to the Boolean function itself, or to its associated vector. However, it should be noted that these two interpretations are closely linked.

Definition 2.3 *A code C of length 2^n is any nonempty set of vectors $f \in \mathbb{F}_2^{2^n}$. The set $\mathbb{F}_2^{2^n}$ is the code space. The cardinality of C, denoted by $|C|$, is the size of the code.*

Example 2.4 *Consider the vectors*

$$0 = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$$
$$\mathbb{1} = (1\ 1\ 1\ 1\ 1\ 1\ 1\ 1)$$
$$x_1 = (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1)$$
$$x_2 = (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1)$$
$$x_3 = (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1)$$

Let $RM(1,3)$ be the code given by $\{0, \mathbb{1}, x_1, x_2, x_3, x_1 \oplus x_2, x_1 \oplus x_3, x_2 \oplus x_3, x_1 \oplus x_2 \oplus x_3, \mathbb{1} \oplus x_1, \mathbb{1} \oplus x_2, \mathbb{1} \oplus x_3, \mathbb{1} \oplus x_1 \oplus x_2, \mathbb{1} \oplus x_1 \oplus x_3, \mathbb{1} \oplus x_2 \oplus x_3, \mathbb{1} \oplus x_1 \oplus x_2 \oplus x_3\}$. $RM(1,3)$ is called the first order Reed-Muller code of length 8.

We will make extensive use of this and other Reed-Muller codes throughout this paper. The vector representation allows us to define two important characteristics of Boolean functions: Hamming weight and Hamming distance.

Definition 2.5 *The Hamming weight of a Boolean function f, denoted as $wt(f)$, is defined as the number of 1's in the vector representation of f.*

Definition 2.6 *The Hamming distance between two functions $f \in B_n$ and $g \in B_n$, denoted by $d(f, g)$, is defined as the number of positions in which the vectors differ.*

The Hamming distance can also be expressed in terms of the Hamming weight:

$$d(f, g) = wt(f \oplus g)$$

Here, $f \oplus g$ is defined as the elementwise binary addition of the vectors associated to the Boolean functions f and g. We can express our example function $f = (0\ 0\ 1\ 1\ 1\ 1\ 0\ 0)$ as $f = x_1 \oplus x_2$. This is true since $x_1 \oplus x_2 = (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1) \oplus (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1) = (0\ 0\ 1\ 1\ 1\ 1\ 0\ 0) = f$. Similarly, $\mathbb{1} \oplus f = (1\ 1\ 1\ 1\ 1\ 1\ 1\ 1) \oplus (0\ 0\ 1\ 1\ 1\ 1\ 0\ 0) = (1\ 1\ 0\ 0\ 0\ 0\ 1\ 1)$.

We denote the multiplication of Boolean functions f and g by $f \cdot g$, or simply fg. We define fg as the elementwise binary multiplication of the vectors associated to the Boolean functions f and g. For example, $x_1x_2 = (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1) \cdot (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1) = (0\ 0\ 0\ 0\ 0\ 0\ 1\ 1)$.

This notation is also called the disjunctive normal form of f. The disjunctive normal form is unique for every Boolean function. It can also be shown that the monomials $\mathbb{1}, x_1, x_2, x_3, x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3$ form a basis for B_3. Thus, any Boolean function in B_3 can be expressed in disjunctive normal form, and that representation is unique. Similarly, the monomials $\mathbb{1}, x_1, x_2, \cdots, x_n, x_1x_2, x_1x_3, \cdots, x_1x_2 \cdots x_n$ form a basis for B_n.

Example 2.7 *Let $f = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1)$ be the vector representation of a Boolean function f in B_4. Our observation suggests that f can be expressed in disjunctive normal form. This is true, since we can write $f = x_1 \oplus x_1x_2 \oplus x_1x_2x_3$. In this example, $wt(f) = 6$.*

Definition 2.8 *The algebraic degree of a Boolean function f, denoted by $d^\circ(f)$, is defined to be the maximum monomial degree among the monomials present in the disjunctive normal form of f. The degree of a monomial is defined to be the number of variables (distinct from $\mathbb{1}$) whose product represents the given monomial.*

Example 2.9 *The degree of the monomial $x_1x_2x_3 \in B_4$ is 3. If $f = x_1 \oplus x_1x_2 \in B_4$, then $d^\circ(f) = 2$. If $g = x_1 \oplus x_1x_2 \oplus x_1x_2x_3x_4 \in B_4$, then $d^\circ(g) = 4$.*

Notice that, if $f \in B_n$, then $d^\circ(f) \leq n$. Equality is achieved only when $f = x_1x_2 \cdots x_n \oplus g$, where $g \in B_n$, $d^\circ(g) < n$.

2.2 Affine Equivalence

Now we define affine equivalence classes so that when we study Boolean functions with high second order nonlinearity, patterns that would be lost by not grouping Boolean functions into such classes will be revealed.

Definition 2.10 *Denote by $GL(2, n)$ the general linear group of $n \times n$ invertible binary matrices.*

Definition 2.11 *An affine transform is a mapping from B_n to B_n that maps any function $f \in B_n$ to the function $g(x) = f(Dx \oplus a) \oplus b \cdot x \oplus c\mathbb{1}$, where $D \in GL(2, n)$, $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^n$, and $c \in \mathbb{F}_2$.*

Example 2.12 *Consider the affine transform that maps any function $f \in B_4$ to the function $g(x) = f(Dx \oplus a) \oplus b \cdot x \oplus c$, where*

$$D = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, a = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, b = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, c = \mathbb{1}$$

Then the function $f = \mathbb{1} \oplus x_1 \oplus x_2x_3 \oplus x_3x_4$ gets mapped to the function $g = \mathbb{1} \oplus x_2 \oplus x_3 \oplus x_1x_2 \oplus x_2x_3$. Similarly, the function $m = x_1x_2x_3x_4$ gets mapped to the function $n = \mathbb{1} \oplus x_1 \oplus x_4 \oplus x_1x_4 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_1x_2x_3x_4$. Under the specified affine transform, g is the image of f and n is the image of m.

Definition 2.13 *Two Boolean functions $f, g \in B_n$ are said to be affine equivalent if there exist $D \in GL(2, n)$, $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^n$, and $c \in \mathbb{F}_2$ such that $g(x) = f(Dx \oplus a) \oplus b \cdot x \oplus c$. In this case, f and g are in the same affine equivalence class. In the case when a is the zero vector, the two functions are called linearly equivalent.*

Example 2.14 *Let $f = x_1x_2 \oplus x_3x_4$ and $g = x_1x_3 \oplus x_2x_4$ be Boolean functions in B_4. Then f and g are linearly equivalent, since*

$$g(x) = f\left(\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}\right) = f\left(\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}\right)$$

Notice that in Example 2.14 there are multiple possible choices for the matrix D that define the affine equivalence relation between f and g. Secondly, notice that the locations of x_1 and x_3 are interchanged in the two functions f and g. We say that g is a permutation of f. Permutations are a particular type of affine transformations.

Definition 2.15 *An affine function is a Boolean function of the form*

$$f(x) = a_1x_1 \oplus \cdots \oplus a_nx_n \oplus a_0\mathbb{1}, \text{ where } a_i \in \mathbb{F}_2$$

Affine functions play an important role in cryptography, since nonlinear functions used in cryptosystems must behave as differently as possible from affine functions.

Theorems 2.16 and 4.2 highlight two important invariants of the affine equivalence relation.

Theorem 2.16 *Let $f, g \in B_n$ be affine equivalent. Then $d^\circ(f) = d^\circ(g)$.*

A concise proof of Theorem 2.16 is presented in Subsection 4.1.

Appendix C presents a summary of the equivalence classes of B_5. As stated in Theorem 2.16, all functions in an equivalence class share the same algebraic degree. Notice that not all functions of a given algebraic degree are contained in the same affine equivalence class. Section 5 presents a more general equivalence relationship that will organize all third degree functions of B_5 into only two distinct 2-equivalence classes, as opposed to 8 distinct affine equivalence classes.

2.3 Reed-Muller Codes

Definition 2.17 *The r^{th} order binary Reed-Muller (RM) code $R(r,n)$ of length 2^n, for $0 \leq r \leq n$, is the set of all vectors f in $\mathbb{F}_2^{2^n}$, where $f((x_1 \cdots x_n))$ is a Boolean function which is a polynomial of degree at most r.*

Corollary: $RM(r,m) \subset RM(r+1,m)$, where $r+1 \leq m$.

Refer to Example 2.4. The first order RM code of length 8, denoted $R(1,3)$, consists of the 16 codewords:

$$a_0\mathbb{1} \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3,\ a_i \in \mathbb{F}_2.$$

These codewords, along with their binary vector representation, are:

0	(0 0 0 0 0 0 0 0)
x_1	(0 0 0 0 1 1 1 1)
x_2	(0 0 1 1 0 0 1 1)
x_3	(0 1 0 1 0 1 0 1)
$x_1 \oplus x_2$	(0 0 1 1 1 1 0 0)
$x_2 \oplus x_3$	(0 1 1 0 0 1 1 0)
$x_1 \oplus x_3$	(0 1 0 1 1 0 1 0)
$x_1 \oplus x_2 \oplus x_3$	(0 1 1 0 1 0 0 1)
$\mathbb{1}$	(1 1 1 1 1 1 1 1)
$\mathbb{1} \oplus x_1$	(1 1 1 1 0 0 0 0)
$\mathbb{1} \oplus x_2$	(1 1 0 0 1 1 0 0)
$\mathbb{1} \oplus x_3$	(1 0 1 0 1 0 1 0)
$\mathbb{1} \oplus x_1 \oplus x_2$	(1 1 0 0 0 0 1 1)
$\mathbb{1} \oplus x_2 \oplus x_3$	(1 0 0 1 1 0 0 1)
$\mathbb{1} \oplus x_1 \oplus x_3$	(1 0 1 0 0 1 0 1)
$\mathbb{1} \oplus x_1 \oplus x_2 \oplus x_3$	(1 0 0 1 0 1 1 0)

In general, the r^{th} order RM code consists of all linear combinations of the vectors corresponding to the products $\mathbb{1}, x_1, \cdots, x_n, x_1x_2, x_1x_3, \cdots, x_{n-1}x_n, \cdots$ (up to degree r), which therefore form the basis of the code.

Notice that all codewords in $RM(1,3)$, except 0 and $\mathbb{1}$, have weight 4. We define the minimum weight of a code as the minimum Hamming weight of all nonzero codewords. The minimum weight of $RM(1,n)$ is 2^{n-1}. It can also be shown that the minimum weight of $RM(n-2,n)$ is 4. In general, the minimum weight of $RM(r,m)$ is 2^{m-r}, where $0 \leq r \leq m$.

2.4 The Discrete Fourier Transform

The discrete Fourier transform is an important tool in analyzing Boolean functions, since knowing it is equivalent to knowing the weights of all functions $f \oplus l$, where l is affine.

Example 2.18 *Refer to Example 2.4, where we defined the first order Reed-Muller code of length 8. Any affine function l coincides with one of the 16 codewords that make up the code. Consider a function $f \in B_3$. Knowing the weights of all functions $f \oplus l$, where l is affine, is equivalent to knowing the Hamming distance from f to any Boolean function in the code. This information is definitely helpful, especially when searching for functions that need to have large distances from all affine functions.*

Definition 2.19 *The discrete Fourier transform is a linear mapping from B_n to $\mathbb{Z}^{2^n}$, which maps any $\varphi \in B_n$ to $\hat{\varphi} \in \mathbb{Z}^{2^n}$, where $\hat{\varphi}(u_1, u_2, \cdots, u_n) = \sum_{(x_1,x_2,\cdots,x_n)\in\mathbb{Z}_2^n} \varphi(x_1, x_2, \cdots, x_n)(-1)^{(x_1,x_2,\cdots,x_n)\cdot(u_1,u_2,\cdots,u_n)}$, and $(x_1, x_2, \cdots, x_n)\cdot(u_1, u_2, \cdots, u_n)$ is the usual inner product. The discrete Fourier transform of a Boolean function is also known as the Walsh-Hadamard transform.*

Observation: $\hat{\varphi}(0) = \sum_{(x_1,x_2,\cdots,x_n)\in\mathbb{Z}_2^n} \varphi(x_1, x_2, \cdots, x_n)(-1)^0 = \sum_{(x_1,x_2,\cdots,x_n)\in\mathbb{Z}_2^n} \varphi(x_1, x_2, \cdots, x_n) = wt(\varphi)$.

Example 2.20 *Let $0, \mathbb{1}, x_1, x_2, x_3, x_4$ be the usual Boolean basis vectors of length 2^4. Consider the function $\varphi(x) = x_1 \oplus x_2 \in B_4$. To determine the Fourier transform of φ, we need to calculate $\hat{\varphi}(u)$ for every possible value of $u \in \mathbb{F}_2^4$.*

u_1	u_2	u_3	u_4	$\varphi(u)$	$\hat{\varphi}(u)$
0	*0*	*0*	*0*	*0*	*8*
0	*0*	*0*	*1*	*0*	*0*
0	*0*	*1*	*0*	*0*	*0*
0	*0*	*1*	*1*	*0*	*0*
0	*1*	*0*	*0*	*1*	*0*
0	*1*	*0*	*1*	*1*	*0*
0	*1*	*1*	*0*	*1*	*0*
0	*1*	*1*	*1*	*1*	*0*
1	*0*	*0*	*0*	*1*	*0*
1	*0*	*0*	*1*	*1*	*0*
1	*0*	*1*	*0*	*1*	*0*
1	*0*	*1*	*1*	*1*	*0*
1	*1*	*0*	*0*	*0*	*-8*
1	*1*	*0*	*1*	*0*	*0*
1	*1*	*1*	*0*	*0*	*0*
1	*1*	*1*	*1*	*0*	*0*

While analyzing the values of the Fourier transform, we make two observations:

1. $\hat{\varphi}(0) = wt(\varphi)$.
2. *The Fourier transform of* φ *takes only the value* 0*, except in the case* $u = 0$ *or* $u =$ `(1 1 0 0)`*. Also,* $\hat{\varphi}($`(1 1 0 0)`$) = -wt(\varphi)$

To explain observation 2, we write $\hat{\varphi}(u_1, u_2, u_3, u_4) =$
$\sum_{(x_1,x_2,x_3,x_4)\in\mathbb{Z}_2^n} \varphi(x_1, x_2, x_3, x_4)(-1)^{(x_1,x_2,x_3,x_4)\cdot(u_1,u_2,u_3,u_4)} =$
$(-1)^{(0\ 1\ 0\ 0)\cdot u} + (-1)^{(0\ 1\ 0\ 1)\cdot u} + (-1)^{(0\ 1\ 1\ 0)\cdot u} + (-1)^{(0\ 1\ 1\ 1)\cdot u} + (-1)^{(1\ 0\ 0\ 0)\cdot u} + (-1)^{(1\ 0\ 0\ 1)\cdot u} +$
$(-1)^{(1\ 0\ 1\ 0)\cdot u} + (-1)^{(1\ 0\ 1\ 1)\cdot u} = (-1)^{u_2} + (-1)^{u_2+u_4} + (-1)^{u_2+u_3} + (-1)^{u_2+u_3+u_4} + (-1)^{u_1} + (-1)^{u_1+u_4} +$
$(-1)^{u_1+u_3} + (-1)^{u_1+u_3+u_4}$. There exists exactly one string u for which all exponents become 1, namely $(u_1\ u_2\ u_3\ u_4) =$ `(1 1 0 0)`. This indicates that the Boolean function φ is $1 \cdot x_1 \oplus 1 \cdot x_2 \oplus 0 \cdot x_3 \oplus 0 \cdot x_4$. In all other cases (except $u = 0$), half of the exponents will be even, and half will be odd, which leads to $\hat{\varphi}(u) = 0$. This means that the vectors associated with the Boolean functions φ and $x \cdot u$ overlap in half of their positions and differ in the other half.

In general, the Fourier transform of any affine function will behave similarly, taking only values of 0, except in the case when $u = 0$ or $u_1x_1 \oplus u_2x_2 \oplus \cdots \oplus u_nx_n = \varphi$, where $x_1, x_2, \cdots, x_n$ are the usual Boolean basis

vectors of length 2^n.

One practical application of the Fourier transform is to identify and correct errors that may have affected the contents of a message. We take the example of NASA's Mariner 9 mission, which required the transmission of pictures of the Martian surface. Engineers chose $RM(1,5)$ codewords to determine a grayscale value for each 4-5 km^2 of Martian surface. Since there are 2^6 different codewords in $RM(1,5)$, the probe could return 64 different grayscale values. Since any information sent by the probe was subject to numerous interferences before being decoded on Earth, transmission errors could cause the codeword received to be different from the intended codeword. Applying the Fourier transform on the received codeword should produce the expected Fourier coefficients for affine functions (as in Example 2.20). If an error occurs and the received codeword is not part of $RM(1,5)$, then choosing the nonzero u that corresponds to the largest Fourier coefficient (in absolute terms) will indicate the affine codeword in $RM(1,5)$ that is closest to the received codeword. Thus, the error could be corrected in most cases, and the mission returned high-quality pictures of the Martian surface.

3 First Order Nonlinearity and Bent Functions

We now introduce the first order nonlinearity of Boolean functions. This concept is of great interest to the security of cryptosystems. Bent functions are a particularly important class of Boolean functions, since they offer good resistance to differential cryptanalysis, and, by definition, resistance to linear cryptanalysis. For an in-depth overview of current results, refer to [3].

Definition 3.1 *The first order nonlinearity of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, denoted by $nl_1(f)$, is the minimum Hamming distance from f to all affine functions.*

Definition 3.2 *A Boolean function f on $\mathbb{F}_2^n$ (for n even) is called bent if its Hamming distance to any Boolean function in $RM(1,n)$ equals $2^{n-1} - 2^{n/2-1}$, the covering radius of the RM code of order 1.*

Example 3.3 *Some classic examples of bent functions are $x_1x_2 \oplus x_3x_4 \in RM(2,4)$, $x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \in RM(2,6)$, and, in general, $x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-1}x_n \in RM(2,n)$, for n even.*

3.1 Discrete Fourier Transform of Bent Functions

The discrete Fourier transform is an efficient way to determine if a particular function is bent.

Theorem 3.4 *Let $f \in B_n$, n even, be a bent function. Then all coefficients of the Fourier transform of f, except $\hat{\varphi}(0) = wt(\varphi)$, take the values $\pm 2^{n/2-1}$.*

Example 3.5 *Consider the function $\varphi(x) = x_1x_2 \oplus x_3x_4 \in B_4$. To determine the Fourier transform of φ, we need to calculate $\hat{\varphi}(u)$ for every possible value of $u \in \mathbb{F}_2^4$.*

u_1	u_2	u_3	u_4	$\varphi(u)$	$\hat{\varphi}(u)$
0	0	0	0	0	6
0	0	0	1	0	-2
0	0	1	0	0	-2
0	0	1	1	1	2
0	1	0	0	0	-2
0	1	0	1	0	-2
0	1	1	0	0	-2
0	1	1	1	1	2
1	0	0	0	0	-2
1	0	0	1	0	-2
1	0	1	0	0	-2
1	0	1	1	1	2
1	1	0	0	1	2
1	1	0	1	1	2
1	1	1	0	1	2
1	1	1	1	0	-2

While analyzing the values of the Fourier transform, we make two observations, which follow from the assertions of Theorem 3.4:

1. *It is the case that $\hat{\varphi}(0) = wt(\varphi)$.*
2. *The Fourier transform of φ takes only the values ± 2, except in the case $u = 0$.*

In Example 2.20 we observed the behavior of the Fourier transform for an affine function. These two examples illustrate the importance of the Fourier transform in characterizing Boolean functions.

3.2 Primary Constructions

An important step towards understanding the structure of bent functions is to analyze known constructions of particular classes of bent functions. The following are primary constructions of the Maiorana-McFarland original class M and of the Partial Spreads class PS. Primary constructions, as opposed to secondary constructions, do not use previously known bent functions as inputs in the construction of new bent functions.

Maiorana-McFarland

Definition 3.6 *The Maiorana-McFarland original class M is the set of all Boolean functions on $\mathbb{F}_2^n = \{(x,y)|x,y \in \mathbb{F}_2^{n/2}\}$, of the form:*

$$f(x,y) = x \cdot \pi(y) \oplus g(y)$$

where π is any permutation on $\mathbb{F}_2^{n/2}$ and g is any Boolean function on $\mathbb{F}_2^{n/2}$. Any such function is bent.

Example 3.7 *Consider $\mathbb{F}_2^4 = \{(x,y)|x,y \in \mathbb{F}_2^2\}$, where $x = (x_1 \ x_2)$ and $y = (x_3 \ x_4)$, and let $\pi(y)$ be the identity permutation on y. Let $g = x_3x_4 \oplus x_3 \in RM(2,4)$. Then $f(x,y) = x_1x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_3$. This function is bent, since the distance from f to any function in $RM(1,4)$ is either $2^{4-1} - 2^{4/2-1} = 6$ or $2^{4-1} + 2^{4/2-1} = 10$.*

Example 3.8 *Consider $\mathbb{F}_2^4 = \{(x,y)|x,y \in \mathbb{F}_2^2\}$ and let $\pi(y)$ be the permutation*

$$\pi\left(\begin{bmatrix} x_3 \\ x_4 \end{bmatrix}\right) = \begin{bmatrix} x_4 \\ x_3 \end{bmatrix}$$

Let $g = x_3x_4 \oplus x_3 \in RM(2,4)$. Then $f(x,y) = x_1x_4 \oplus x_2x_3 \oplus x_3x_4 \oplus x_3$. This function is bent, since the distance from f to any function in $RM(1,4)$ is either $2^{4-1} - 2^{4/2-1} = 6$ or $2^{4-1} + 2^{4/2-1} = 10$.

Generalized Maiorana-McFarland Construction

Theorem 3.9 *Let $n = r + s$ $(r \leq s)$ be even. Let ϕ be any mapping from $\mathbb{F}_2^s$ to $\mathbb{F}_2^r$ such that, for every $a \in \mathbb{F}_2^r$, the set $\phi^{-1}(a)$ is an $(n-2r)-$dimensional affine subspace of $\mathbb{F}_2^s$. Let g be any Boolean function on $\mathbb{F}_2^s$ whose restriction to $\phi^{-1}(a)$ (viewed as a Boolean function on $\mathbb{F}_2^{n-2r}$ via an affine isomorphism between*

$\phi^{-1}(a)$ and this vector space) is bent for every $a \in \mathbb{F}_2^r$, if $n > 2r$ (no condition on g being imposed if $n = 2r$). Then the function $f_{\phi,g} = x \cdot \phi(y) \oplus g(y)$ is bent on $\mathbb{F}_2^n$.

Example 3.10 *Let $r = 2$ and $s = 4$, so ϕ is a mapping from $\mathbb{F}_2^2$ to $\mathbb{F}_2^4$. Consider*

$$\phi\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}\right) = x_1 x_2.$$

We first test that for every $a \in \mathbb{F}_2^2$, the set $\phi^{-1}(a)$ is a $2-$dimensional affine subspace of $\mathbb{F}_2^4$.

$$\phi^{-1}\left(\begin{bmatrix} 0 \\ 0 \end{bmatrix}\right) = \left\{\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}\right\}$$

$$\phi^{-1}\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \left\{\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}\right\}$$

$$\phi^{-1}\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \left\{\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}\right\}$$

$$\phi^{-1}\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = \left\{\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}\right\}$$

All of these four affine subspaces of $\mathbb{F}_2^4$ are two-dimensional, thus ϕ fulfills the condition required in Theorem 3.9.

Let

$$g\left(\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}\right) = x_6 \oplus x_5 x_6 \oplus x_3 x_4 x_5.$$

$g|_{\phi^{-1}((0\ \ 0))} = x_2 \oplus x_1 x_2 \in RM(2,2)$, *which is bent.*

$g|_{\phi^{-1}((0\ \ 1))} = x_2 \oplus x_1x_2 \in RM(2,2)$, *which is bent.*

$g|_{\phi^{-1}((1\ \ 0))} = x_2 \oplus x_1x_2 \in RM(2,2)$, *which is bent.*

$g|_{\phi^{-1}((1\ \ 1))} = x_1 \oplus x_2 \oplus x_1x_2 \in RM(2,2)$, *which is bent.*

Thus, g fulfills the condition stated in Theorem 3.9.

Now that we have two valid functions ϕ and g, we can construct the function $f_{\phi,g} = x \cdot \phi(y) \oplus g(y) =$

$$\left(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\right) \cdot \left(\begin{bmatrix} x_3 \\ x_4 \end{bmatrix}\right) \oplus x_6 \oplus x_5x_6 \oplus x_3x_4x_5 = x_6 \oplus x_1x_3 \oplus x_2x_4 \oplus x_5x_6 \oplus x_3x_4x_5.$$

As predicted by Theorem 3.9, f is indeed a bent function in $RM(3,6)$.

Partial Spreads

Definition 3.11 *The Partial Spreads class PS is the set of all the sums (modulo 2) of the indicators of* $2^{n/2-1}$ *or* $2^{n/2-1}+1$ *disjoint* $n/2-$*dimensional subspaces of* $\mathbb{F}_2^n$ *(disjoint meaning any two of these spaces intersect in 0 only, and therefore their sum is direct and equals* $\mathbb{F}_2^n$*). All such functions are bent.*

Example 3.12 *Consider*

$$\mathbb{F}_2^4 = \left\{ \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}, x_i \in \mathbb{F}_2 \right\}.$$

$$A = \left\langle \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \right\rangle \quad B = \left\langle \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \right\rangle \quad C = \left\langle \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right\rangle$$

are three disjoint 2-dimensional subspaces of $\mathbb{F}_2^4$.

The indicator function for A, denoted 1_A*, is* `(1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0)` $= \mathbb{1} \oplus x_1 \oplus x_2 \oplus x_1x_2$.

The indicator function for B, denoted 1_B*, is* `(1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0)` $= \mathbb{1} \oplus x_3 \oplus x_4 \oplus x_3x_4$.

The indicator function for C, denoted 1_C*, is* `(1 0 0 0 0 0 1 0 0 1 0 0 0 0 0 1)` $= \mathbb{1} \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_1x_2 \oplus x_3x_4 \oplus x_1x_3 \oplus x_2x_4$.

Then $1_A \oplus 1_B \oplus 1_C = \mathbb{1} \oplus x_1x_3 \oplus x_2x_4$*, which is a bent function in* $RM(2,4)$.

4 Higher Order Nonlinearity of Boolean Functions

4.1 Introduction

The higher order nonlinearity of Boolean functions is an important cryptographic criterion, since it measures the resistance against attacks to stream and block ciphers. Our work, as presented in the following sections, focuses on the properties of functions that exhibit large second order nonlinearity.

Definition 4.1 *The r^{th} order nonlinearity of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, denoted by $nl_r(f)$, is the minimum Hamming distance from f to all functions in $\mathbb{F}_2^n$ of algebraic degrees at most r, where r is a positive integer. Symbolically, $nl_r(f) = min_{g \in RM(r,n)} d(f, g)$.*

Observation: Notice that when $r = 1$ in Definition 4.1, we refer to the first order nonlinearity of Boolean functions, as per Section 3.

Theorem 4.2 presents a result that helps determine the r^{th} order nonlinearity of an entire class of Boolean functions, given the r^{th} order nonlinearity of a single Boolean function.

Theorem 4.2 *Let $f, g \in B_n$ be affine equivalent. Then $nl_r(f) = nl_r(g)$, where $r \leq n$.*

In Section 2.2, Theorem 2.16 stated that the algebraic degree is an affine invariant. Using the result in Theorem 4.2, we can now present a concise proof of this statement.

Proof: Let f and g be affine equivalent Boolean functions such that $d^\circ(f) = a$ and $d^\circ(g) = b$. Assume $a \neq b$.

1. If $a > b$, then $nl_b(g) = 0$, but $nl_b(f) > 0$. This contradicts the assumption that f and g are affine equivalent.
2. If $b > a$, then $nl_a(f) = 0$, but $nl_a(g) > 0$. This contradicts the assumption that f and g are affine equivalent.

We conclude that $a = b$, which implies that $d^\circ(f) = d^\circ(g)$. □

The following theorem provides an important property of nonlinearity that later forms the motivation for developing the notion of 2-equivalence classes described in Section 5.

Theorem 4.3 *Let $f, g \in B_n$, and $d^\circ(g) \leq r$. Then $nl_r(f \oplus g) = nl_r(f)$.*

Proof: Let $h \in B_n$, and $d^\circ(h) \leq r$. We know that $d(f \oplus g, h) = wt((f \oplus g) \oplus h) = wt(f \oplus (g \oplus h)) = d(f, g \oplus h) \geq nl_r(f)$, since $d^\circ(g \oplus h) \leq r$. Thus, $nl_r(f \oplus g) \geq nl_r(f)$. (1)
Let $a \in B_n$, with $d^\circ(a) \leq r$, such that $d(f, a) = nl_r(f)$. We know that $d^\circ(a \oplus g) \leq r$. Then, $d(f \oplus g, a \oplus g) = wt(f \oplus g \oplus a \oplus g) = wt(f \oplus a) = nl_r(f)$. Thus, $nl_r(f \oplus g) \leq nl_r(f)$. (2)
Inequalities (1) and (2) show that $nl_r(f \oplus g) = nl_r(f)$. □

In particular, if we wish to preserve the second order nonlinearity of a function, we can add to it any Boolean function of degree at most 2. The following theorem presents an upper bound on the first order nonlinearity of Boolean functions.

Theorem 4.4 *$nl_1(f) \leq 2^{n-1} - 2^{n/2-1}$ for every function $f \in RM(m, n)$. This bound is tight for n even.*

Since bent functions in $RM(m, n)$ possess a first order nonlinearity of $2^{n-1} - 2^{n/2-1}$, Theorem 4.4 states that there do not exist Boolean functions in $RM(m, n)$ of higher first order nonlinearity than bent functions. Bent functions, by definition, posses maximum first order nonlinearity. The bound in Theorem 4.4 is also called the covering radius bound (since it represents the covering radius of the Reed-Muller code of order 1 if n is even).

5 2-Equivalence and 2-Equivalence Classes

Our computer searches for functions that exhibit high second order nonlinearity have resulted in large amounts of data. For example, a search for Boolean functions in $RM(3, 6)$ that possess a second order nonlinearity of 18 yields thousands of functions. We quickly noticed that all these functions fall in just a few affine equivalence classes (in our case, 3 classes). Focusing on just one representative from each equivalence class of highly nonlinear functions allowed us to group functions with similar properties together and focus on the unique characteristics of the representatives. However, the need to group together functions with respect to their second order nonlinearity has led us to develop a more general classification than the one provided by affine equivalence classes.

Definition 5.1 *Let $f \in B_n$ and $g \in B_n$. We say that f and g are 2-equivalent, denoted by $f \equiv_2 g$, if*

$g(x) = f(Dx \oplus a) \oplus (Mx \cdot x) \oplus b \cdot x \oplus c$, *where* $D \in GL(2, n)$, M *is an* $n \times n$ *strictly upper triangular matrix,* $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^n$, *and* $c \in \mathbb{F}_2$. *Then* f *and* g *are said to be in the same 2-equivalence class.*

Example 5.2 *Let* $f, g \in RM(3, 4)$, $f = x_2x_3x_4$ *and* $g = x_3 \oplus x_1x_4 \oplus x_2x_3x_4$. *Notice that* $nl_1(f) = 2$, *and* $nl_1(g) = 4$. *Thus,* f *and* g *are not in the same affine equivalence class. However,* $f \equiv_2 g$, *since* $g(x) = f(Dx \oplus a) \oplus (Mx \cdot x) \oplus b \cdot x \oplus c$, *where* $D = I_4$, $a \in \mathbb{F}_2^n$ *is the zero vector,*

$$M = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, b = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, c = 0.$$

In general, if two Boolean functions differ only in their first and second degree terms, then the functions are 2-equivalent. This observation follows from Definition 5.1.

Theorem 5.3 *Let* A *denote the set of all pure degree two functions in* n *variables. Then the set* $S = \{Mx \cdot x |$ M *is a strictly upper triangular* $n \times n$ *matrix*$\} = A$.

Proof: This is a double inclusion proof. First we address $S \subseteq A$.
Let

$$f = \begin{bmatrix} 0 & a_{12} & a_{13} & a_{14} & \cdots & a_{1n} \\ 0 & 0 & a_{23} & a_{24} & \cdots & a_{2n} \\ 0 & 0 & 0 & a_{34} & \cdots & a_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \cdots \\ x_n \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \cdots \\ x_n \end{bmatrix} \in S.$$

Equivalently, $f = a_{12}x_1x_2 \oplus a_{13}x_1x_3 \oplus a_{14}x_1x_4 \oplus \cdots \oplus a_{1n}x_1x_n \oplus a_{23}x_2x_3 \oplus a_{24}x_2x_4 \oplus a_{25}x_2x_5 \oplus \cdots \oplus a_{2n}x_2x_n \oplus a_{34}x_3x_4 \oplus a_{35}x_3x_5 \oplus a_{36}x_3x_6 \oplus \cdots \oplus a_{3n}x_3x_n \oplus \cdots \oplus a_{n-1n}x_{n-1}x_n$.

Thus, $f \in A$. This proves that $S \subseteq A$.

Now we show that $A \subseteq S$. Let $f \in A$, $f = a_{12}x_1x_2 \oplus a_{13}x_1x_3 \oplus a_{14}x_1x_4 \oplus \cdots \oplus a_{1n}x_1x_n \oplus a_{23}x_2x_3 \oplus a_{24}x_2x_4 \oplus a_{25}x_2x_5 \oplus \cdots \oplus a_{2n}x_2x_n \oplus a_{34}x_3x_4 \oplus a_{35}x_3x_5 \oplus a_{36}x_3x_6 \oplus \cdots \oplus a_{3n}x_3x_n \oplus \cdots \oplus a_{n-1n}x_{n-1}x_n$.

Since f can be expressed in matrix form as above, $f \in S$. So $A \subseteq S$. This concludes the proof that $S = A$.

□

Theorem 5.4 *Let* $f, g \in RM(n, m)$, $f \equiv_2 g$. *Then* $nl_2(f) = nl_2(g)$.

Proof: Since $f \equiv_2 g$, there exist $D \in GL(2,m)$, M a strictly upper triangular $m \times m$ matrix, a and $b \in \mathbb{F}_2^m$, and $c \in \mathbb{F}_2$, such that $g(x) = f(Dx \oplus a) \oplus (Mx \cdot x) \oplus b \cdot x \oplus c$. We can rewrite this equality as $g(x) = [f(Dx \oplus a) \oplus b \cdot x \oplus c] \oplus (Mx \cdot x)$. We know that $f(Dx \oplus a) \oplus b \cdot x \oplus c$ is affine equivalent to f, and $Mx \cdot x \in RM(2,m)$ (by Theorem 5.3). Since affine equivalence preserves second order nonlinearity, and by applying the result in Theorem 4.3, we have $nl_2(f) = nl_2(g)$. □

Theorem 5.5 *2-equivalence is an equivalence relation.*

Proof: The proof of Theorem 5.5 is subdivided into three parts.

(1) Let $f \in RM(n,m)$. Then $f \equiv_2 f$ (reflexivity).

$f \equiv_2 f$ since $f(x) = f(Dx \oplus a) \oplus (Mx \cdot x) \oplus b \cdot x \oplus c$, where $D = I_m$, $a \in \mathbb{F}_2^n$ is the zero vector,

$$M = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, b = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, c = 0.$$

(2) Let $f, g \in RM(n,m)$. If $f \equiv_2 g$ then $g \equiv_2 f$ (symmetry).

Since $f \equiv_2 g$, $g(x) = f(Dx \oplus a) \oplus (Mx \cdot x) \oplus b \cdot x \oplus c$, where $D \in GL(2,n)$, M is an $n \times n$ strictly upper triangular matrix, $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^n$, and $c \in \mathbb{F}_2$. Then $f(x) = g(D^{-1}x \oplus D^{-1}a) \oplus M(D^{-1}x \oplus D^{-1}a) \cdot (D^{-1}x \oplus D^{-1}a) \oplus b \cdot (D^{-1}x \oplus D^{-1}a) \oplus c = g(D^{-1}x \oplus D^{-1}a) \oplus MD^{-1}x \cdot D^{-1}x \oplus MD^{-1}x \cdot D^{-1}a \oplus MD^{-1}a \cdot D^{-1}x \oplus MD^{-1}a \cdot D^{-1}a \oplus bD^{-1}x \oplus bD^{-1}a \oplus c$. Denote $D^{-1}a$ by $a^{'}$. Then $f(x) = g(D^{-1}x \oplus a^{'}) \oplus MD^{-1}x \cdot D^{-1}x \oplus MD^{-1}x \cdot a^{'} \oplus Ma^{'} \cdot D^{-1}x \oplus Ma^{'} \cdot a^{'} \oplus bD^{-1}x \oplus ba^{'} \oplus c$. Since $D^{-1} \in GL(2,n)$, $a^{'} \in \mathbb{F}_2^n$, $MD^{-1}x \cdot a^{'} \oplus Ma^{'} \cdot D^{-1}x \oplus bD^{-1}x \in RM(1,m)$, $Ma^{'} \cdot a^{'} \oplus ba^{'} \oplus c \in \mathbb{F}_2$, and $MD^{-1}x \cdot D^{-1}x \in RM(2,m)$, we can conclude that $g \equiv_2 f$.

(3) Let $f, g, h \in RM(n,m)$. If $f \equiv_2 g$ and $g \equiv_2 h$, then $f \equiv_2 h$ (transitivity).

$f \equiv_2 g \Rightarrow g(x) = f(Dx \oplus a) \oplus (Mx \cdot x) \oplus b \cdot x \oplus c$, $g \equiv h \Rightarrow h(x) = g(D^{'}x \oplus a^{'}) \oplus (M^{'}x \cdot x) \oplus b^{'} \cdot x \oplus c^{'}$. We can write $h(x) = g(D^{'}x \oplus a^{'}) \oplus (M^{'}x \cdot x) \oplus b^{'} \cdot x \oplus c^{'} = [f(D \cdot (D^{'}x \oplus a^{'}) \oplus a) \oplus (M(D^{'}x \oplus a^{'}) \cdot (D^{'}x \oplus a^{'})) \oplus b \cdot (D^{'}x \oplus a^{'}) \oplus c] \oplus (M^{'}x \cdot x) \oplus b^{'} \cdot x \oplus c^{'} = f(DD^{'}x \oplus (Da^{'} \oplus a)) \oplus [M(D^{'}x \oplus a^{'}) \cdot (D^{'}x \oplus a^{'}) \oplus M^{'}x \cdot x] \oplus (bD^{'} \oplus b^{'})x \oplus (ba^{'} \oplus c \oplus c^{'})$. Since $M(D^{'}x \oplus a^{'}) \cdot (D^{'}x \oplus a^{'}) \oplus M^{'}x \cdot x \in RM(\bar{2},m)$, $ba^{'} \oplus c \oplus c^{'} \in \mathbb{F}_2$, $DD^{'} \in GL(2,m)$, and $Da^{'} \oplus a \in \mathbb{F}_2^m$,

we conclude, by Definition 5.1, that $f \equiv_2 h$.

Results (1), (2), and (3) imply that 2-equivalence is an equivalence relation. □

Example 5.6 *Let $f = x_1x_2x_3$ and $g = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4$ be Boolean functions in B_4. It is known that f and g are not affine equivalent, since they have different first order nonlinearity (2 and 4 respectively). However, we can prove that these two functions are 2-equivalent: $f = x_1x_2x_3$ is affine equivalent (thus, also 2-equivalent) to $(x_1 \oplus x_2)(x_2 \oplus x_3)(x_3 \oplus x_4) = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus (x_1x_3 \oplus x_2x_4)$ which is 2-equivalent to $x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 = g$ (the two functions only differ by second degree terms). By Theorem 5.5 we can conclude that $f \equiv_2 g$.*

Theorem 5.7 *Let $f, g \in B_n$. If $f \equiv_2 g$ and $d^\circ(f) \geq 3$, then $d^\circ(f) = d^\circ(g)$.*

Proof: Follows directly from the construction of g. □

6 Concatenation Analysis of Functions With High Second Order Nonlinearity

Concatenating Boolean functions with high nonlinearity can be a useful way to construct new highly nonlinear functions of greater lengths. One of the main focuses of our work was to develop such concatenation constructions and explain why some concatenations yield functions of maximum second order nonlinearity. Before touching on our work, we present the basic properties of concatenations.

6.1 Properties of Concatenations

Definition 6.1 *$(f|g)$ denotes the concatenation of the two Boolean functions f and g, in this order.*

Example 6.2 *Let $f, g \in RM(1,4)$, $f =$* (0 0 0 0 1 1 1 1), *$g =$* (0 0 1 1 0 0 1 1).
Then $(f|g) =$ (0 0 0 0 1 1 1 1 0 0 1 1 0 0 1 1) $\in RM(2,5)$.

The following is a list of formulas that explain the Boolean function notation of concatenations.

Theorem 6.3 *Let $0, \mathbb{1}, x_1, x_2, \cdots, x_n$ be the usual Boolean basis vectors of length 2^n, and $0', \mathbb{1}', x_1', x_2', \cdots, x_{n+1}'$ be the usual Boolean basis vectors of length 2^{n+1}. Then the following formulas hold:*

1. $(x_i|x_j) \cdot (x_k|x_l) = (x_i x_k | x_j x_l)$
2. $(x_i|x_j) \oplus (x_k|x_l) = (x_i \oplus x_k | x_j \oplus x_l)$
3. $(0|\mathbb{1}) = x_1'$
4. $(\mathbb{1}|\mathbb{1}) = \mathbb{1}'$
5. $(x_n|x_n) = x_{n+1}'$
6. $(0|x_n) = x_1' x_{n+1}'$
7. $(x_n|0) = x_1' x_{n+1}' \oplus x_{n+1}'$

Proof: Formulas $1, 2, 3, 4$ and 5 follow directly form the definition of Boolean function addition and multiplication, and from the definition of the basis vectors $x_1', \mathbb{1}'$, and x_{n+1}'.
Formula 6: $(0|x_n) = (0|\mathbb{1}) \cdot (x_n|x_n) = x_1' x_{n+1}'$.
Formula 7: $(x_n|0) = (0|\mathbb{1}) \cdot (x_n|x_n) \oplus (x_n|x_n) = x_1' x_{n+1}' \oplus x_{n+1}'$. □

Consider $f, g \in RM(2,6)$, $d^\circ(f) = d^\circ(g) = 2$ (equivalently, we could have said $f, g \in RM(2,6) \backslash RM(1,6)$). An important characteristic of $(f|g)$ that we want to determine is $d^\circ((f|g))$. In our case, depending on the specific form of f and g, $d^\circ((f|g))$ can be either 2 or 3. The concatenation formulas presented in Theorem 6.3 allow us to gain a deeper understanding of this issue.

Definition 6.4 *Let $f, g \in RM(n,m)$, with $d^\circ(f) = d^\circ(g)$. We say that f and g have the same n^{th} degree terms if $f - g \in RM(n-1, m)$.*

Theorem 6.5 *Let $f, g \in RM(n,m)$, $d^\circ(f) = d^\circ(g) = n$. Then $d^\circ((f|g)) = n$ iff $d^\circ(f - g) < n$.*

Proof: Let $f, g \in RM(n,m)$ with $d^\circ(f) = d^\circ(g) = n$.

Assume that $d^\circ((f|g)) = n$, and f and g do not have the same n^{th} degree terms. Without loss of generality, let $x_{i_1}x_{i_2}\cdots x_{i_n}$ be a term in the polynomial g, but not in the polynomial f. Thus, the term $(0|x_{i_1}x_{i_2}\cdots x_{i_n})$ will appear in the polynomial $(f|g)$. Consequently, $(0|x_{i_1}x_{i_2}\cdots x_{i_n}) = x_1^{'}x_{i_1+1}^{'}x_{i_2+1}^{'}\cdots x_{i_n+1}^{'}$ will be a degree $n+1$ term appearing in the polynomial $(f|g)$, which means that $d^\circ((f|g)) = n+1$. This contradicts our original assumption that $d^\circ((f|g)) = n$. Thus, $d^\circ((f|g)) = n \Rightarrow f$ and g have the same n^{th} degree terms.

Now assume that f and g have the same n^{th} degree terms, but $d^\circ((f|g)) \neq n$. Let $x_{i_1}x_{i_2}\cdots x_{i_n}$ be an n^{th} degree term shared by f and g (at least one such term must exist). Then $x_{i_1}x_{i_2}\cdots x_{i_n}|x_{i_1}x_{i_2}\cdots x_{i_n}$ will appear in the polynomial $(f|g)$. But $x_{i_1}x_{i_2}\cdots x_{i_n}|x_{i_1}x_{i_2}\cdots x_{i_n} = x_{i_1+1}^{'}x_{i_2+1}^{'}\cdots x_{i_n+1}^{'}$ is an n^{th} degree term. Thus, $d^\circ((f|g)) \geq n$. Consequently,the shared n^{th} degree terms of f and g will only contribute n^{th} degree terms to the polynomial $(f|g)$. Since concatenating $n-1^{th}$ degree terms or below will never result in a term of degree greater than n, we know that $d^\circ((f|g)) = n$, contradicting our original assumption that $d^\circ((f|g)) \neq n$. So f and g have the same n^{th} degree terms $\Rightarrow d^\circ((f|g)) = n$.

Combining the two results, we get that $d^\circ((f|g)) = n$ iff f and g have the same n^{th} degree terms. □

6.2 Concatenation Constructions

One of our initial approaches to constructing new Boolean functions of high second order nonlinearity was to concatenate two functions that are known to exhibit high second order nonlinearity. The resulting concatenation can, under special conditions, achieve more than double the second order nonlinearity of the original pieces. Theorem 6.7 summarizes the theoretical basis of this approach. We commence by proving the result in Lemma 6.6.

Lemma 6.6 *Let $f \in RM(2,n)$. Then there exist Boolean functions f_1 and f_2 in $RM(2,n-1)$ that have the same second degree terms, and for which $f = (f_1|f_2)$.*

Proof: Since $RM(n-1,n-1) = B_{n-1}$ contains all binary vectors of length 2^{n-1}, the two halves of the binary vector associated with the function f, call them f_1 and f_2, will be Boolean functions in $RM(n-1,n-1)$. Assume that $d^\circ(f_1) = k > 2$. Then the disjunctive normal form of f_1 contains the term $x_{i_1}x_{i_2}\cdots x_{i_k}$. If the disjunctive normal form of f_2 does not contain the element $x_{i_1}x_{i_2}\cdots x_{i_k}$, then $(x_{i_1}x_{i_2}\cdots x_{i_k}|0) = x_1^{'}x_{i_1+1}^{'}x_{i_2+1}^{'}\cdots x_{i_k+1}^{'} \oplus x_{i_1+1}^{'}x_{i_2+1}^{'}\cdots x_{i_k+1}^{'}$ will be a $k+1^{th}$ degree term appearing in the polynomial

$(f_1|f_2) = f$. If f_2 also contains the term $x_{i_1}x_{i_2}\cdots x_{i_k}$, the polynomial $(f_1|f_2)$ will contain the term $(x_{i_1}x_{i_2}\cdots x_{i_k}|x_{i_1}x_{i_2}\cdots x_{i_k}) = x'_{i_1+1}x'_{i_2+1}\cdots x'_{i_k+1}$ of degree k. Thus, $d^\circ(f) \geq k > 2$. Similarly, $d^\circ(f) > 2$ if $d^\circ(f_2) > 2$. But since $d^\circ(f) \leq 2$, we conclude that $d^\circ(f_1) \leq 2$ and $d^\circ(f_2) \leq 2$. So f_1, f_2 must be Boolean functions in $RM(2, n-1)$. However, this condition is necessary but not sufficient for $(f_1|f_2)$ to be in $RM(2, n)$. By Theorem 6.5, it must also be the case that f_1 and f_2 have the same second degree terms. Thus, there exist Boolean functions f_1 and f_2 in $RM(2, n-1)$ that have the same second degree terms, and for which $f = (f_1|f_2)$. □

Theorem 6.7 *Let $f_1, f_2 \in B_n$ satisfy $nl_2(f_1) = nl_2(f_2) = k$. Then $nl_2((f_1|f_2)) \geq 2 \cdot k$.*

Proof: Let $g \in RM(2, n+1)$. Then, by Lemma 6.6, $g = (g_1|g_2)$ for some $g_1, g_2 \in RM(2, n)$ that have the same second degree terms. This implies that $d(f_1, g_1) \geq k$ and $d(f_2, g_2) \geq k$. Thus, $d((f_1|f_2), g) = d((f_1|f_2), (g_1|g_2)) = d(f_1, g_1) + d(f_2, g_2) \geq 2 \cdot k$. Since this inequality holds for any $g \in RM(2, n+1)$ we can conclude that $nl_2((f_1|f_2)) \geq 2 \cdot k$. □

Observation: Equality does not always hold. If none of the functions $g_1 \in RM(2, n)$ that are distance k away from f_1 have the same second degree terms as a function $g_2 \in RM(2, n)$ that is distance k away from f_2, then $nl_2((f_1|f_2)) > 2 \cdot k$.

An analysis of the affine equivalence classes of $RM(3, 7)$ suggests that the highest second order nonlinearity present in $RM(3, 7)$ is 40. Similarly, the highest second order nonlinearity present in $RM(3, 6)$ is 18.

Corollary: If $f_1, f_2 \in RM(3, 6)$ satisfy $nl_2(f_1) = nl_2(f_2) = 18$, then $nl_2((f_1|f_2)) \geq 36$.

This result led us to expect that most functions in $RM(3, 7)$ that have a second order nonlinearity of 40 should result from concatenations of two functions in $RM(3, 6)$ that have the same third degree terms and that have a second order nonlinearity of 18. To test our assumption, we analyze the function $f = x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_1x_6x_7 \in RM(3, 7)$, $nl_2(f) = 40$. Separating f into two halves results in $f = (x_1x_3x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_5|x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_1x_3x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_5) = (f_1|f_2)$. Note that f_1 and f_2 have the same third degree terms. If this had not been the case, $(f_1|f_2)$ would have been a function in $RM(4, 7)$ instead of $RM(3, 7)$. Using a computer program, we find that $nl_2(f_1) = nl_2(f_2) = 12$. This result is surprising, since Theorem 6.7 only guarantees a second order nonlinearity of at least 24 for $(f_1|f_2)$ when $nl_2(f_1) = nl_2(f_2) = 12$. Also, notice that $f_1 \oplus f_2 = x_1x_2 \oplus x_3x_4 \oplus x_5x_6$ is a bent function

in $RM(3,6)$ (its minimum Hamming distance to all functions in RM(2,6) is $2^{6-1} - 2^{6/2-1} = 28$). The observation that the two halves of f differ by a bent function is another puzzling aspect. The following result explains part of f's large second order nonlinearity, given that the two halves of f differ by a bent function.

Theorem 6.8 *Let $f \in RM(3,6)$ with $nl_2(f) = 12$, and let $b \in RM(2,6)$ be a bent function. Then $(f|f \oplus b) \in RM(3,7)$ and $nl_2((f|f \oplus b)) > 2 \cdot 12$.*

Proof: Since f and $f \oplus b$ have the same third degree terms, $(f|f \oplus b) \in RM(3,7)$, and $nl_2(f) = nl_2(f \oplus b) = 12$. Theorem 6.7 states that $nl_2((f|f \oplus b)) \geq 2 \cdot 12$. Assume there exist $a \in RM(2,6)$ and $m \in RM(1,6)$, such that $d((f|f \oplus b), (a|a \oplus m)) = 2 \cdot 12$. Then $d(f,a) = 12$ and $d(f \oplus b, a \oplus m) = 12$. Thus, $12 = d(f,a) = wt(f \oplus a) = wt(f \oplus a \oplus b \oplus m) = d(f \oplus a, b \oplus m)$. Since $b \oplus m$ is a bent function, $wt(b \oplus m) = 2^{6-1} \pm 2^{6/2-1} = 28$ or 36. This implies that $wt(f \oplus a) \geq 16$, contradicting the fact that $wt(f \oplus a) = 12$. This proves that there does not exist a function in $RM(2,6)$ distance 12 away from $(f|f \oplus b)$. So $nl_2((f|f \oplus b)) > 2 \cdot 12$. □

Theorem 6.8 only explains why the second order nonlinearity of the concatenation is more than twice the second order nonlinearity of the halves. However, it does not explain why the second order nonlinearity of the concatenation jumps from $2 \cdot 12 = 24$ to 40. Theorem 6.9 presents a generalization of Theorem 6.8.

Theorem 6.9 *Let $f \in RM(m,n)$, and let $b \in RM(2,n)$ be a bent function. If $nl_2(f) < 2^{n-2} - 2^{n/2-2}$, then $nl_2((f|f \oplus b)) > 2 \cdot nl_2(f)$.*

Proof: Assume there exist $a \in RM(2,n)$ and $p \in RM(1,n)$ such that $d((f|f \oplus b), (a|a \oplus p)) = 2 \cdot nl_2(f)$. Then $d(f,a) = nl_2(f)$ and $d(f \oplus b, a \oplus p) = nl_2(f)$. Thus, $nl_2(f) = wt(f \oplus a) = wt(f \oplus a \oplus b \oplus p) = d(f \oplus a, b \oplus p)$. Since $b \oplus p$ is a bent function, $wt(b \oplus p) = 2^{n-1} \pm 2^{n/2-1}$. Thus, $wt(f \oplus a) \geq 2^{n-1} - 2^{n/2-1} - nl_2(f) > 2^{n-2} - 2^{n/2-2}$. This contradicts the assumption that $nl_2(f) < 2^{n-2} - 2^{n/2-2}$. Thus, $nl_2((f|f \oplus b)) > 2 \cdot nl_2(f)$. □

The result in Theorem 6.9 depends heavily upon the bent function b used in the concatenation construction. More precisely, Theorem 6.9 makes use of the relatively high weight of bent functions. Other functions that play the role of b can be applied in the above construction, as long as $wt(b \oplus p)$ is high for all $p \in RM(1,n)$. A more general (but somewhat less practical) result that does not require functions of high weights is presented in Theorem 6.10 and the next corollary.

Theorem 6.10 *Let $f, g \in RM(n,m)$, $nl_2(f) = nl_2(g) = p$. Let $F = \{a \in RM(2,m) | d(a,f) = p\}$ and $G = \{b \in RM(2,m) | d(b,g) = p\}$. If there exist $f' \in F$ and $g' \in G$ that have the same second degree terms, then $nl_2(f|g) = 2p$. Otherwise, $nl_2(f|g) > 2p$.*

Proof: If there exist functions $f' \in F$ and $g' \in G$ that have the same second degree terms, then, according to Theorem 6.5, $d^\circ((f|g)) = 2$, and $(f|g) \in RM(2, m+1)$. Since $d(f, f_1) = d(g, g_1) = p$, we know that $d((f|g), (f_1 g_1)) = 2p$. Thus, there exists a function in $RM(2, m+1)$ that is $2p$ away from $(f|g)$. According to Theorem 6.7, since $nl_2(f) = nl_2(g) = p$, there cannot exist any functions in $RM(2, m+1)$ whose distance to $(f|g)$ is less than $2p$. Thus, $nl_2(f|g) = 2p$.
If there do not exist functions $f' \in F$ and $g' \in G$ that have the same second degree terms, then, according to Theorem 6.5, $(f'|g') \in RM(3,m) \backslash RM(2,m)$. Therefore, although the distance from $(f|g)$ to $(f'|g')$ is $2p$, it does not influence the second order nonlinearity of $(f|g)$. Since $nl_2(f|g) \neq 2p$, we have that $nl_2(f|g) > 2p$.
□

Corollary: Let $f, g \in RM(n,m)$. $nl_2((f,g))$ is $\min\{d(f,a) + d(f,b)\}$, where $a, b \in RM(2,m) \backslash RM(1,m)$ and have the same second degree terms, or $a, b \in RM(1,m)$ and $a \neq b$. The proof of this corollary follows directly from Theorem 6.10 and Theorem 6.5.

7 Future Work

As we have seen in Section 6 on Concatenation Constructions, there exist functions in $RM(3,7)$ with maximal second order nonlinearity (40) that result as a concatenation of two functions in $RM(3,6)$ whose second order nonlinearity is only 12. Moreover, the two functions in $RM(3,6)$ differ almost always by a bent function in $RM(2,6)$. Future work will seek to answer a series of questions:

1. What role do bent functions play in concatenation constructions of high second order nonlinearity functions? Can bent functions be replaced by other high-weight functions, as suggested in the commentary to Theorem 6.9?

2. We found one affine equivalence class of functions in $RM(3,5)$ that exhibit maximum second order nonlinearity (6), but are formed by concatenating two functions in $RM(3,4)$ that differ by a non-bent function. Thus, there exist constructions of high second order nonlinearity functions that do not

depend on bent functions. What are these constructions?

3. While analyzing the function $f = x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_1x_6x_7 \in RM(3,7)$ presented in the introduction to Theorem 6.8, a computer search revealed that f is distance 40 from functions in $RM(2,7)$ that are formed by concatenating two bent functions in $RM(2,6)$ (for example $(\mathbb{1} \oplus x_1 \oplus x_2 \oplus x_1x_2 \oplus x_3x_4 \oplus x_5x_6 | x_1x_2 \oplus x_3x_4 \oplus x_5x_6)$). What is the role of bent functions in this case?

4. Why does concatenating two functions in $RM(3,6)$ whose second order nonlinearity is 12 result in a function in $RM(3,7)$ whose second order nonlinearity is 40, much greater than $2 \cdot 12 = 24$? How can we replicate this process to construct other highly nonlinear functions?

We were led to another interesting line of observations while analyzing the set A of Boolean functions in $RM(2,7)$ that are distance 40 from the function $f = x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_1x_6x_7 \in RM(3,7)$. We know that $nl_2(f) = 40$ and that $wt(f) = 40$. After an exhaustive computer search, we found that the set A contains $11264 = 11 \cdot 2^{10}$ elements. Define a good sum as a binary sum of two elements in A that is also contained in A. For each function in A, we count the number of times that function is a term in a good sum. Since the zero codeword is an element in A, each function will appear at least once as a term in a good sum. Also, the zero codeword will appear in 11264 good sums. The distinct numbers of our count are: $4, 7, 12, 16, 32, 40, 48, 64, 92, 160, 164, 256, 416, 576, 1024, 1536, 2816, 11264$. The most striking pattern (for which we have not yet found an explanation) is that for each function $m \in A$, there exists a function $n \in A$ that satisfies $n \neq m$ and $n \neq 0$, such that $m \oplus n \in A$. Secondly, each nonzero function $a \in A$ pairs with an even number of distinct nonzero functions in A to create a good sum. An explanation for this second observation is the following: consider the function $b \in A$ that satisfies $b \neq a$ and $b \neq 0$, such that $a \oplus b \in A$. Then $a \oplus b \neq a$ and $a \oplus b \neq b$. Thus, $a \oplus (a \oplus b) = b \in A$ and $a \oplus (a \oplus b)$ is a distinct good sum from $a \oplus b$.

Similarly, we ran an exhaustive computer search for all Boolean functions in $RM(2,6)$ that are distance 18 away from the function $f = x_1x_2x_3 \oplus x_1x_2x_6 \oplus x_1x_4x_6 \oplus x_2x_5x_6 \oplus x_3x_4x_5 \in RM(3,6)$ (call this set A). We know that $nl_2(f) = 18$ and that $wt(f) = 18$ (as in the previous paragraph, notice that the zero codeword is an element of A). The cardinality of A is $3584 = 7 \cdot 2^9$ (in the previous paragraph, the cardinality of A was $11264 = 11 \cdot 2^{10}$). Why is the cardinality of the sets A a multiple of such high powers of two?

Another attractive area of future work is finding an easy way to identify Boolean functions that exhibit high second order nonlinearity. As presented in Example 2.20 and Example 3.5, the Fourier transform offers a convenient way to determine whether a particular Boolean function is bent. Can we find similar approaches that relate to second order nonlinearity?

Bibliography

[1] F.J.MacWilliams, N.J.A.Sloane, "The Theory of Error-Correcting Codes", *North-Holland Publishing Company*, Amsterdam, 1986.

[2] Claude Carlet, "Boolean Functions for Cryptography and Error Correcting Codes",*Cambridge University Press*, http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.

[3] Claude Carlet, "On the Higher Order Nonlinearities of Boolean Functions and S-Boxes, and Their Generalizations", http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.

[4] Joanne Elizabeth Fuller, "Analysis of Affine Equivalent Boolean Functions for Cryptography", *Queensland University of Technology*, 2003.

[5] An Braeken, Yuri Borissov, Svetla Nikova, Bart Preneel, "Classification of Boolean Functions of 6 Variables or Less with Respect to Some Cryptographic Properties", *Springer Berlin / Heidelberg*, Lecture Notes in Computer Science, Volume 3580/2005, pp. 324-334, 2005.

Appendix A

Equivalence Classes of B_3

The following table contains the affine equivalence classes of B_3 [4].

Class	Representative Function	Degree	Nonlinearity
1	$1 \oplus x_3$	1	0
2	$1 \oplus x_3 \oplus x_1x_2x_3$	3	1
3	$1 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3$	2	2

Each of these three affine equivalence classes also represents a distinct 2-equivalence class.

Appendix B

Equivalence Classes of B_4

The following table contains the affine equivalence classes of B_4 [4].

Class	Representative Function	Degree	Nonlinearity	Second Order Nonlinearity
1	$1 \oplus x_1 \oplus x_4$	1	0	0
2	$1 \oplus x_1 \oplus x_4 \oplus x_2x_3x_4 \oplus x_1x_2x_3x_4$	4	1	1
3	$1 \oplus x_1 \oplus x_4 \oplus x_3x_4 \oplus x_1x_3x_4$	3	2	2
4	$1 \oplus x_4 \oplus x_1x_2 \oplus x_2x_3x_4 \oplus x_1x_2x_3x_4$	4	3	1
5	$1 \oplus x_4 \oplus x_1x_4$	2	4	0
6	$1 \oplus x_4 \oplus x_1x_2 \oplus x_2x_3x_4$	3	4	2
7	$1 \oplus x_1 \oplus x_4 \oplus x_1x_4 \oplus x_1x_2x_3 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2x_3x_4$	4	5	1
8	$1 \oplus x_4 \oplus x_1x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_2x_4$	2	6	0

The following table contains the 2-equivalence classes of B_4.

Class	Representative Function	Degree	Nonlinearity	Second Order Nonlinearity
1	$1 \oplus x_1 \oplus x_4$	1	0	0
2	$1 \oplus x_1 \oplus x_4 \oplus x_2x_3x_4 \oplus x_1x_2x_3x_4$	4	1	1
3	$1 \oplus x_1 \oplus x_4 \oplus x_3x_4 \oplus x_1x_3x_4$	3	2	2

Appendix C

Affine Equivalence Classes of B_5

The following table presents the 48 affine equivalence classes of B_5 [4].

class	example	**ord**	$\mathcal{N}$	$\lvert\hat{\mathcal{F}}(\omega)\rvert$ distribution	$\lvert\hat{\mathcal{R}}(\omega)\rvert$ distribution
1	0xaa55aa55	1	0	(0,31),(32,1)	(32,32)
2	0xaa55ab55	5	1	(2,31),(30,1)	(28,31),(32,1)
3	0xaa55bb55	4	2	(0,16),(4,15),(28,1)	(24,30),(32,2)
4	0xaa5dbb55	5	3	(2,24),(6,7),(26,1)	(20,28),(28,3),(32,1)
5	0xaaddbb55	3	4	(0,24),(8,7),(24,1)	(16,28),(32,4)
6	0xaa5dbb51	4	4	(0,12),(4,16),(8,3),(24,1)	(16,25),(24,6),(32,1)
7	0x2a5dbb51	5	5	(2,20),(6,10),(10,1),(22,1)	(12,21),(20,10),(32,1)
8	0xaaddbb51	5	5	(2,24),(6,4),(10,3),(22,1)	(12,24),(20,4),(28,3),(32,1)
9	0x2a5dbf51	3	6	(4,30),(12,1),(20,1)	(8,16),(16,15),(32,1)
10	0x6a5dbb51	4	6	(0,10),(4,15),(8,6),(20,1)	(8,16),(16,15),(32,1)
11	0x2addbb51	4	6	(0,12),(4,14),(8,4),(12,1),(20,1)	(8,19),(16,9),(24,3),(32,1)
12	0xa8ddbb51	4	6	(0,16),(4,12),(12,3),(20,1)	(8,24),(24,6),(32,2)
13	0xaeddda51	5	7	(2,15),(6,15),(10,1),(18,1)	(4,10),(12,21),(32,1)
14	0x0a5dbf51	5	7	(2,18),(6,12),(14,1),(18,1)	(4,16),(12,9),(20,6),(32,1)
15	0x8addda51	5	7	(2,19),(6,9),(10,3),(18,1)	(4,13),(12,15),(20,3),(32,1)
16	0xa8dd9b51	5	7	(2,22),(6,6),(10,2),(14,1),(18,1)	(4,18),(12,6),(20,6),(28,1),(32,1)
17	0x88ddbb51	5	7	(2,28),(14,3),(18,1)	(4,24),(28,7),(32,1)
18	0x88ddbb11	2	8	(0,28),(16,4)	(0,24),(32,8)

class	example	**ord**	$\mathcal{N}$	$\lvert\hat{\mathcal{F}}(\omega)\rvert$ distribution	$\lvert\hat{\mathcal{R}}(\omega)\rvert$ distribution
19	0x8c5dda51	3	8	(0,19),(8,12),(16,1)	(0,9),(8,16),(16,6),(32,1)
20	0xa89d9b51	3	8	(0,22),(8,8),(16,2)	(0,18),(16,12),(32,2)
21	0x8eddda51	4	8	(0,7),(4,16),(8,8),(16,1)	(0,6),(8,22),(16,3),(32,1)
22	0xaefdda51	4	8	(0,9),(4,15),(8,6),(12,1),(16,1)	(0,9),(8,16),(16,6),(32,1)
23	0x025dbf51	4	8	(0,10),(4,16),(8,4),(16,2)	(0,16),(8,4),(16,9),(24,2),(32,1)
24	0x88ddda51	4	8	(0,11),(4,14),(8,4),(12,2),(16,1)	(0,11),(8,13),(16,6),(24,1),(32,1)
25	0x88dd9b51	4	8	(0,14),(4,14),(12,2),(16,2)	(0,17),(8,7),(24,7),(32,1)
26	0xceddda51	5	9	(2,15),(6,13),(10,3),(14,1)	(4,22),(12,9),(32,1)
27	0x0eddda51	5	9	(2,15),(6,13),(10,3),(14,1)	(4,24),(12,6),(20,1),(32,1)
28	0x425dbf51	5	9	(2,18),(6,10),(10,2),(14,2)	(4,20),(12,9),(20,2),(32,1)
29	0x8cddda51	5	9	(2,19),(6,7),(10,5),(14,1)	(4,21),(12,9),(20,1),(32,1)
30	0x88dddb51	5	9	(2,21),(6,7),(10,1),(14,3)	(4,24),(20,7),(32,1)
31	0x289d9b51	5	9	(2,22),(6,4),(10,4),(14,2)	(4,18),(12,12),(28,1),(32,1)
32	0x86fdda51	3	10	(4,28),(12,4)	(0,12),(8,16),(16,3),(32,1)
33	0x88dddb71	3	10	(4,28),(12,4)	(0,24),(16,7),(32,1)
34	0xcefdda51	4	10	(0,6),(4,15),(8,10),(12,1)	(0,15),(8,16),(32,1)
35	0x0efdda51	4	10	(0,8),(4,14),(8,8),(12,2)	(0,15),(8,14),(16,2),(32,1)
36	0x288d9b51	4	10	(0,8),(4,14),(8,8),(12,2)	(0,17),(8,13),(24,1),(32,1)
37	0x8cfdda51	4	10	(0,10),(4,13),(8,6),(12,3)	(0,12),(8,16),(16,3),(32,1)
38	0x8cdddb51	4	10	(0,12),(4,12),(8,4),(12,4)	(0,18),(8,6),(16,7),(32,1)
39	0x8ccdda51	4	10	(0,12),(4,12),(8,4),(12,4)	(0,8),(8,21),(16,1),(24,1),(32,1)
40	0x289d9b41	4	10	(0,16),(4,10),(12,6)	(8,30),(32,2)
41	0x488ddb51	5	11	(2,12),(6,16),(10,4)	(4,28),(12,3),(32,1)
42	0xccfdda51	5	11	(2,16),(6,10),(10,6)	(4,25),(12,6),(32,1)
43	0x688d9b51	5	11	(2,16),(6,10),(10,6)	(4,27),(12,3),(20,1),(32,1)
44	0x288d9b41	5	11	(2,16),(6,10),(10,6)	(4,30),(28,1),(32,1)
45	0x288d1b41	2	12	(0,16),(8,16)	(0,30),(32,2)
46	0xdcfdda51	3	12	(0,16),(8,16)	(0,15),(8,16),(32,1)
47	0x68ad9b51	3	12	(0,16),(8,16)	(0,27),(16,4),(32,1)
48	0x688ddb51	4	12	(0,4),(4,16),(8,12)	(0,24),(8,6),(16,1),(32,1)

Appendix D

Equivalence Classes of $RM(3,6)\backslash RM(1,6)$

The six representatives of $RM(3,6)\backslash RM(2,6)$ are:

$f_1 = 0$
$f_2 = 123$
$f_3 = 123 \oplus 245$
$f_4 = 123 \oplus 456$
$f_5 = 123 \oplus 245 \oplus 346$
$f_6 = 123 \oplus 145 \oplus 246 \oplus 356 \oplus 456$

The following table contains the 34 affine equivalence classes of $RM(3,6)\backslash RM(1,6)$ [5].

	Representative	Number of Cosets	Walsh transform	Autocorrelation Transform
f_1	0	1	(0,63),(64,1)	(0,63),(64,1)
	12	651	(0,60),(32,4)	(0,48),(64,16)
	14+23	18 228	(0,48),(16,16)	(0,60),(64,16)
	16+25+34	13 888	(8,64)	(0,63),(64,1)
f_2	0	$1\,395 \times 8$	(0,56),(16,7),(48,1)	(32,56),(64,8)
	14	$1\,395 \times 392$	(0,54),(16,8),(32,2)	(0,36),(32,24),(64,4)
	24+15	$1\,395 \times 2\,352$	(0,48),(16,16)	(0,54),(32,8),(64,2)
	16+25+34	$1\,395 \times 1\,344$	(64,8)	(0,63),(64,1)
	45	$1\,395 \times 3\,584$	(0,32),(8,28),(24,2)	(0,48),(32,14),(64,2)
	16+45	$1\,395 \times 25\,088$	(0,24),(8,32),(16,8)	(0,57),(32,6),(64,1)
f_3	0	$54\,684 \times 32$	(0,32),(8,30),(24,1),(40,1)	(16,32),(32,30),(64,2)
	13	$54\,684 \times 320$	(0,51),(16,12),(32,1)	(0,18),(16,32),(32,12),(64,2)
	14	$54\,684 \times 480$	(0,32),(8,28),(24,4)	(0,24),(16,32),(32,6),(64,2)
	16	$54\,684 \times 7\,680$	(0,28),(8,30),(16,4),(24,2)	(0,39),(16,16),(32,8),(64,1)
	26	$54\,684 \times 32$	(0,30),(8,32),(32,2)	(0,32),(32,30),(64,2)
	26+13	$54\,684 \times 320$	(0,48),(16,16)	(0,51),(32,12),(64,1)
	26+14	$54\,684 \times 480$	(0,24),(8,32),(16,8)	(0,57),(32,6),(64,1)
	13+15+26+34	$54\,684 \times 192$	(8,64)	(0,63),(64,1)
	34+13+15	$54\,684 \times 23\,040$	(0,48),(16,16)	(0,30),(16,32),(64,2)
	34+16	$54\,684 \times 192$	(0,24),(8,32),(16,8)	(0,45),(16,16),(64,1)
f_4	0	$357\,120 \times 64$	(4,49),(12,14),(36,1)	(16,49),(32,14),(64,1)
	14	$357\,120 \times 3\,136$	(4,49),(12,12),(28,1),(20,2)	(0,24),(16,33),(32,6),(64,1)
	15+24	$357\,120 \times 64$	(4,46),(20,3),(12,15)	(0,36),(16,25),(32,2),(64,1)
	34+25+16	$357\,120 \times 64$	(4,42),(12,21),(20,1)	(0,42),(16,21),(64,1)
f_5	0	$468\,720 \times 448$	(0,27),(8,32),(16,4),(32,1)	(0,9),(16,48),(32,6),(64,1)
	12+13	$468\,720 \times 18$	(0,28),(8,30),(16,4),(24,2)	(0,27),(16,32),(32,4),(64,1)
	15	$468\,720 \times 14\,336$	(0,26),(8,31),(24,1),(16,6)	(0,30),(16,32),(32,1),(64,1)
	12+13+25	$468\,720 \times 2\,222$	(0,48),(16,16)	(0,27),(16,32),(32,4),(64,1)
	14+25	$468\,720 \times 1\,344$	(0,24),(8,32),(16,8)	(0,45),(16,16),(64,1)
	35+26+25+12	$468\,720 \times 14\,336$	(8,64)	(0,63),(64,1)
	25+15+16	$468\,720 \times 64$	(0,24),(8,32),(16,8)	(0,39),(16,24),(64,1)
f_6	0	$166\,656 \times 3\,584$	(4,45),(12,18),(28,1)	(0,18),(16,45),(64,1)
	12+13	$166\,656 \times 21\,504$	(4,46),(12,15),(20,3)	(0,30),(16,33),(64,1)
	23+15+14	$166\,656 \times 7\,680$	(4,42),(12,21),(20,1)	(0,42),(16,21),(64,1)

All affine equivalence classes that have the same f_i representative are part of the same 2-equivalence class.

Appendix E

Equivalence Classes of $RM(3,7)\backslash RM(1,7)$

The six representatives of $RM(3,7)\backslash RM(2,7)$ are:

$f_1 = 0$
$f_2 = 123$
$f_3 = 123 \oplus 245$
$f_4 = 123 \oplus 456$
$f_5 = 123 \oplus 245 \oplus 346$
$f_6 = 123 \oplus 145 \oplus 246 \oplus 356 \oplus 456$
$f_7 = 127 \oplus 347 \oplus 567$
$f_8 = 123 \oplus 456 \oplus 147$
$f_9 = 123 \oplus 245 \oplus 346 \oplus 147$
$f_{10} = 123 \oplus 456 \oplus 147 \oplus 257$
$f_{11} = 123 \oplus 145 \oplus 246 \oplus 356 \oplus 456 \oplus 167$
$f_{12} = 123 \oplus 145 \oplus 246 \oplus 356 \oplus 456 \oplus 167 \oplus 247$

The following table contains the affine equivalence classes of $RM(3,7)\backslash RM(1,7)$ [5].

	Coset of $RM(3,7)$	Number of Cosets ($\times\nu(7,3,f)$)	Walsh transform	Autocorrelation Transform
f_1	0	1	(0,127),(128,1)	(128,128)
	12	2 667	(0,124),(64,4)	(0,96),(128,32)
	14+23	330 708	(0,112),(32,16)	(0,120),(128,32)
	16+25+34	1 763 776	(0,64),(16,64)	(0,126),(128,2)
f_2	0	8	(0,120),(32,7),(96,1)	(64,112),(128,16)
	14	840	(0,118),(32,8),(64,2)	(0,72),(64,48),(128,8)
	24+15	11760	(0,112),(32,16)	(0,108),(64,16),(128,4)
	16+24+34	20 160	(0,64),(16,64)	(0,126),(128,2)
	45	17920	(0,96),(16,28),(48,2)	(0,96),(64,28),(128,4)
	16+45	3766320	(0,88),(16,32),(32,8)	(0,114),(64,12),(128,2)
	45+17+26	752 640	(0,64),(16,64)	(0,123),(64,4),(128,1)
	47+56	917 504	(8,112),(24,16)	(0,120),(64,7),(128,1)
f_3	0	32	(0,96),(16,30),(48,1),(80,1)	(32,64),(64,60),(128,4)
	13	320	(0,115),(32,12),(64,1)	(0,36),(32,64),(64,24),(128,4)
	14	480	(0,92),(16,28),(48,4)	(0,48),(32,64),(64,12),(128,4)
	16	23040	(0,92),(16,30),(32,4),(48,2)	(0,78),(32,32),(64,16),(128,2)
	26	96	(0,94),(16,32),(64,2)	(0,66),(64,60),(128,4)
	26+13	960	(0,112),(32,16)	(0,102),(64,24),(128,2)
	26+14	1440	(0,88),(16,32),(32,8)	(0,114),(64,12),(128,2)
	26+17	23 040	(0,88),(16,32),(32,8)	(0,60),(32,64),(128,1)
	34+13+15	192	(0,112),(32,16)	(0,60),(32,64),(128,4)
	34+16	69120	(0,88),(16,32),(32,8)	(0,90),(32,32),(128,2)
	13+15+26+34	576	(0,64),(16,64)	(0,126),(128,2)
	34+26+17	69 120	(0,64),(16,64)	(0,123),(64,4),(128,1)
	36+17	983 040	(8,112),(24,16)	(0,108),(32,16),(64,3),(128,1)
	46+17	491 520	(0,76),(16,48),(32,4)	(0,105),(32,16),(64,6),(128,1)
	46+35+17	184 320	(0,64),(16,64)	(0,111),(32,16),(128,1)
	67	184 320	(8,120),(24,4),(40,4)	(0,96),(32,16),(64,15),(128,1)
	67+13	327 680	(0,64),(16,64)	(0,111),(32,16),(128,1)
	67+14	491 520	(0,76),(16,48),(32,4)	(0,105),(32,16),(64,6),(128,1)
	6+34+14+137	196 608	(8,120),(24,4),(40,4)	(0,96),(32,16),(64,15),(128,1)
f_4	0	64	(0,64),(8,49),(24,14),(72,1)	(32,98),(64,28),(128,2)
	14	3, 136	(0,64),(8,49),(24,12),(40,2),(56,1)	(0,48),(32,66),(64,12),(128,2)
	17	7 168	(0,48),(8,56),(16,14),(24,8),(48,2)	(0,72),(32,42),(64,13),(128,1)
	15+24	18816	(0,64),(8,46),(24,15),(40,3)	(0,72),(32,50),(64,4),(128,2)
	24+17	150 528	(0,44),(8,56),(16,16),(24,8),(32,4)	(0,96),(32,26),(64,5),(128,1)
	34+25+16	10752	(0,64),(8,42),(24,21),(40,1)	(0,84),(32,42),(128,2)
	34+25+17	301 056	(0,32),(8,56),(16,32),(24,8)	(0,108),(32,18),(64,1),(128,1)
	47+17	100 352	(0,38),(8,60),(16,24),(24,2),(32,2),(40,2)	(0,87),(32,34),(64,6),(128,1)
	47+25+17	131 360	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,99),(32,26),(64,2),(128,1)
	47+35+26+16	602 112	(0,32),(8,56),(16,32),(24,8)	(0,105),(32,22),(128,1)

f_5	0	448	(0,91),(16,32),(32,4),(64,1)	(0,18),(32,96),(64,12),(128,2)
	12+13	1792	(0,92),(16,30),(32,4),(48,2)	(0,54),(32,64),(64,8),(128,2)
	15	14336	(0,90),(16,31),(32,6),(48,1)	(0,60),(32,64),(64,2),(128,2)
	17	114 688	(8,116),(24,10),(40,2)	(0,84),(32,40),(64,3),(128,1)
	12+13+25	448	(0,112),(32,16)	(0,54),(32,64),(64,8),(128,2)
	14+25	1344	(0,88),(16,32),(32,8)	(0,90),(32,32),(64,4),(128,2)
	25+15+16	14336	(0,88),(16,32),(32,8)	(0,78),(32,48),(128,2)
	25+17	344 064	(0,76),(16,48),(32,4)	(0,93),(32,32),(64,2),(128,1)
	26+17	344 064	(8,112),(24,16)	(0,102),(32,24),(64,1),(128,1)
	27	3 584	(0,80),(16,46),(48,2)	(0,69),(32,48),(64,10),(128,1)
	27+13	10 752	(0,88),(16,32),(32,8)	(0,87),(32,32),(64,8),(128,1)
	27+14	10 752	(0,76),(16,48),(32,4)	(0,105),(32,16),(64,6),(128,1)
	27+15	114 688	(8,112),(24,16)	(0,102),(32,24),(64,1),(128,1)
	27+16	43 008	(0,76),(16,48),(32,4)	(0,93),(32,32),(64,2),(128,1)
	35+26+25+12+13+14	64	(0,64),(16,64)	(0,126),(128,2)
	35+26+25+17	114 688	(0,64),(16,64)	(0,111),(32,16),(128,1)
	35+27+13+14	3 584	(0,64),(16,64)	(0,123),(64,4),(128,1)
	35+27+16	43 008	(0,64),(16,64)	(0,111),(32,16),(128,1)
	56+17	458 752	(8,112),(24,16)	(0,99),(32,28),(128,1)
	56+25+17	458 752	(0,70),(16,56),(32,2)	(0,99),(32,28),(128,1)
f_6	0	3584	(0,64),(8,45),(24,18),(56,1)	(0,36),(32,90),(128,2)
	12+13	21504	(0,64),(8,46),(24,15),(40,3)	(0,60),(32,66),(128,2)
	17	129 024	(0,32),(8,60),(16,32),(24,2),(40,2)	(0,81),(32,46),(128,1)
	23+15+14	7680	(0,64),(8,42),(24,21),(40,1)	(0,84),(32,42),(128,2)
	23+16	1 290 240	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,93),(32,34),(128,1)
	25+17	645 120	(0,32),(8,56),(16,32),(24,8)	(0,105),(32,22),(128,1)
f_7	0	128	(8,126), (56,1), (72,1)	(16,64), (64,63), (128,1)
	12	43 008	(0,90), (16,31), (32,6), (48,1)	(0,45), (16,64), (64,18), (128,1)
	13	40 320	(8,120), (24,4), (40,4)	(0,48), (16,64), (64,15), (128,1)
	23+14	645 120	(0,76),(16,48), (32,4)	(0,57), (16,64), (64,6), (128,1)
	23+14+12	516 096	(8,112), (24,16)	(0,60), (16,64), (64,3), (128,1)
	23+15	483 840	(8,112), (24,16)	(0,60), (16,64), (64,3), (128,1)
	34+25+23+16+14	368 640	(0,64), (16,64)	(0,63), (16,64), (128,1)
f_8	0	128	(0,37),(8,64),(16,24),(32,2),(64,1)	(16,32),(32,82),(64,13),(128,1)
	15	768	(0,38),(8,64),(16,22),(32,2),(48,2)	(0,36),(16,32),(32,50),(64,9),(128,1)
	17	1 024	(0,48),(8,55),(16,16),(24,7),(40,1),(56,1)	(0,27),(16,32),(32,58),(64,10),(128,1)
	15+23	3 072	(0,48),(8,52),(16,16),(24,10),(40,2)	(0,63),(16,32),(32,26),(64,6),(128,1)
	23+17	2 048	(0,60),(8,50),(24,13),(32,4),(40,1)	(0,54),(16,32),(32,34),(64,7),(128,1)
	15+24	1 152	(0,34),(8,64),(16,24),(32,6)	(0,72),(16,32),(32,18),(64,5),(128,1)
	25	4608	(0,36),(8,64),(16,23),(32,4),(48,1)	(0,48),(16,32),(32,42),(64,5),(128,1)
	25+16	9 216	(0,34),(8,64),(16,24),(32,6)	(0,66),(16,32),(32,26),(64,3),(128,1)
	25+17	18 432	(0,48),(8,52),(16,16),(24,10),(40,2)	(0,57),(16,32),(32,34),(64,4),(128,1)
	25+23+16	18 432	(0,48),(8,48),(16,16),(24,16)	(0,75),(16,32),(32,18),(64,2),(128,1)
	25+23+17	18 423	(0,48),(8,50),(16,16),(24,13),(40,1)	(0,66),(16,32),(32,26),(64,3),(128,1)
	27	24 576	(0,38),(8,60),(16,24),(24,2),(32,2),(40,2)	(0,57),(16,32),(32,34),(64,4),(128,1)
	27+15	73 728	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,75),(16,32),(32,18),(64,2),(128,1)
	27+23	12 288	(0,46),(8,56),(16,15),(24,8),(32,2),(48,1)	(0,48),(16,32),(32,42),(64,5),(128,1)
	27+15+23	36 684	(0,44),(8,56),(16,16),(24,8),(32,4)	(0,66),(16,32),(32,26),(64,3),(128,1)
	34+25+16	4608	(0,22),(8,64),(16,40),(32,2)	(0,84),(16,32),(32,10),(64,1),(128,1)
	34+27+23	12 288	(0,44),(8,56),(16,16),(24,8),(32,4)	(0,66),(16,32),(32,26),(64,3),(128,1)
	34+27+23+15	36 864	(0,32),(8,56),(16,32),(24,8)	(0,84),(16,32),(32,10),(64,1),(128,1)
	35+26	12 288	(0,48),(8,48),(16,16),(24,16)	(0,72),(16,32),(32,22),(64,1),(128,1)
	35+26+17	36 864	(0,28),(8,64),(16,32),(32,4)	(0,72),(16,32),(32,22),(64,1),(128,1)
	35+26+23+17	12 288	(0,28),(8,64),(16,32),(32,4)	(0,72),(16,32),(32,22),(64,1),(128,1)

	27+35	147 456	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,72),(16,32),(32,22),(64,1),(128,1)
	35+27+16	147 456	(0,32),(8,56),(16,32),(24,8)	(0,81),(16,32),(32,14),(128,1)
	35+27+34	147 456	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,72),(16,32),(32,22),(64,1),(128,1)
	35+27+23+16	147 456	(0,32),(8,56),(16,32),(24,8)	(0,81),(16,32),(32,14),(128,1)
	57+27	147 456	(0,38),(8,58),(16,24),(24,5),(32,2),(40,1)	(0,63),(16,32),(32,30),(64,2),(128,1)
	57+27+16	294 912	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,72),(16,32),(32,22),(64,1),(128,1)
	57+34+27+16	147 456	(0,32),(8,56),(16,32),(24,8)	(0,81),(16,32),(32,14),(128,1)
	57+36+27	589 824	(0,35),(8,56),(16,28),(24,8),(32,1)	(0,75),(16,32),(32,20),(128,1)
f_9	0	1 024	(8,119),(24,7),(40,1),(56,1)	(16,64),(32,56),(64,7),(128,1)
	15	21 504	(8,116),(24,10),(40,2)	(0,36),(16,64),(32,24),(64,3),(128,1)
	17	14 336	(0,78),(16,47),(32,2),(48,1)	(0,27),(16,64),(32,32),(64,4),(128,1)
	23+17	14 336	(0,88),(16,32),(32,8)	(0,27),(16,64),(32,32),(64,4),(128,1)
	25+16	86 016	(0,76),(16,48),(32,4)	(0,45),(16,64),(32,16),(64,2),(128,1)
	26+15	43 008	(8,112),(24,16)	(0,54),(16,64),(32,8),(64,1),(128,1)
	27+17+15	57 344	(8,112),(24,16)	(0,54),(16,64),(32,8),(64,1),(128,1)
	35+27+16+15	24 576	(0,64),(16,64)	(0,63),(16,64),(128,1)
	56	229 376	(0,76),(16,48),(32,4)	(0,42),(16,64),(32,20),(64,1),(128,1)
	56+17	229 376	(8,114),(24,13),(40,1)	(0,42),(16,64),(32,20),(64,1),(128,1)
	56+16+15	688 128	(0,76),(16,48),(32,4)	(0,42),(16,64),(32,20),(64,1),(128,1)
	56+27+15	688 128	(8,112),(24,16)	(0,51),(16,64),(32,12),(128,1)
f_{10}	0	768	(0,40),(8,57),(16,24),(24,6),(56,1)	(0,12),(16,48),(32,64),(64,3),(128,1)
	13	9216	(0,38),(8,60),(16,23),(24,4),(32,2),(48,1)	(0,33),(16,48),(32,44),(64,2),(128,1)
	15	1 536	(0,40),(8,58),(16,24),(24,3),(40,3)	(0,36),(16,48),(32,40),(64,3),(128,1)
	16	9 216	(0,40),(8,56),(16,24),(24,6),(40,2)	(0,42),(16,48),(32,36),(64,1),(128,1)
	23+14	18 432	(0,46),(8,54),(16,16),(24,9),(32,2),(40,1)	(0,45),(16,48),(32,32),(64,2),(128,1)
	15+23	9 216	(0,36),(8,60),(16,24),(24,4),(32,4)	(0,57),(16,48),(32,20),(64,2),(128,1)
	23+16	36 864	(0,36),(8,60),(16,24),(24,4),(32,4)	(0,54),(16,48),(32,24),(64,1),(128,1)
	23+16+13	18 432	(0,46),(8,52),(16,16),(24,12),(32,2)	(0,54),(16,48),(32,24),(64,1),(128,1)
	24+15	768	(0,40),(8,54),(16,24),(24,9),(40,1)	(0,60),(16,48),(32,16),(64,3),(128,1)
	24+16	9 216	(0,40),(8,52),(16,24),(24,12)	(0,66),(16,48),(32,12),(64,1),(128,1)
	26+16	9 216	(0,40),(8,54),(16,24),(24,9),(40,1)	(0,54),(16,48),(32,24),(64,1),(128,1)
	27+17+16	18 432	(0,40),(8,54),(16,24),(24,9),(40,1)	(0,54),(16,48),(32,24),(64,1),(128,1)
	27+23+17+13	512	(0,48),(8,52),(16,15),(24,12),(48,1)	(0,36),(16,48),(32,40),(64,3),(128,1)
	27+23+17+13	512	(0,58),(8,52),(24,12),(32,6)	(0,36),(16,48),(32,40),(64,3),(128,1)
	27+23+17+16+13	9 216	(0,46),(8,52),(16,16),(24,12),(32,2)	(0,54),(16,48),(32,24),(64,1),(128,1)
	34+16	6 144	(0,30),(8,60),(16,32),(24,4),(32,2)	(0,63),(16,48),(32,16),(128,1)
	34+16+13	36 864	(0,40),(8,52),(16,24),(24,12)	(0,63),(16,48),(32,16),(128,1)
	34+17+16+13	18 432	(0,30),(8,60),(16,32),(24,4),(32,2)	(0,63),(16,48),(32,16),(128,1)
	34+23+17+16+13	36 864	(0,30),(8,60),(16,32),(24,4),(32,2)	(0,63),(16,48),(32,16),(128,1)
	34+26+23	3 072	(0,36),(8,60),(16,24),(24,4),(32,4)	(0,51),(16,48),(32,28),(128,1)
	34+26+23+14	3 072	(0,24),(8,60),(16,40),(24,4)	(0,75),(16,48),(32,4),(128,1)
	34+26+23+17+13	6 144	(0,40),(8,52),(16,24),(24,12)	(0,63),(16,48),(32,16),(128,1)
	36	98 304	(0,33),(8,60),(16,28),(24,4),(32,3)	(0,57),(16,48),(32,22),(128,1)
	36+13	32 768	(0,40),(8,54),(16,24),(24,9),(40,1)	(0,51),(16,48),(32,28),(128,1)
	36+15+13	98 304	(0,40),(8,52),(16,24),(24,12)	(0,63),(16,48),(32,16),(128,1)
	36+24+15	32 768	(0,27),(8,60),(16,36),(24,4),(32,1)	(0,69),(16,48),(32,10),(128,1)
	37	73 728	(0,38),(8,58),(16,24),(24,5),(32,2),(40,1)	(0,48),(16,48),(32,30),(64,1),(128,1)
	37+14	73 728	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,60),(16,48),(32,18),(64,1),(128,1)
	37+16	294 912	(0,35),(8,56),(16,28),(24,8),(32,1)	(0,63),(16,48),(32,16),(128,1)
	37+25+13	6 144	(0,40),(8,56),(16,23),(24,8),(48,1)	(0,36),(16,48),(32,42),(64,1),(128,1)
	37+25+13+14	18 432	(0,44),(8,56),(16,16),(24,8),(32,4)	(0,48),(16,48),(32,30),(64,1),(128,1)
	37+23+15+13	18 432	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,60),(16,48),(32,18),(64,1),(128,1)
	37+23+16	147 456	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,57),(16,48),(32,22),(128,1)
	37+25+24+15+14+13	6 144	(0,32),(8,56),(16,32),(24,8)	(0,72),(16,48),(32,6),(64,1),(128,1)
	37+24+23+16	147 456	(0,32),(8,56),(16,32),(24,8)	(0,69),(16,48),(32,10),(128,1)
	37+36	98304	(0,35),(8,58),(16,28),(24,5),(32,1),(40,1)	(0,51),(16,48),(32,28),(128,1)
	37+36+13	294 912	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,57),(16,48),(32,22),(128,1)
	37+36+15	294 912	(0,35),(8,56),(16,28),(24,8),(32,1)	(0,63),(16,48),(32,16),(128,1)
	37+36+24+15+13	98 304	(0,32),(8,56),(16,32),(24,8)	(0,69),(16,48),(32,10),(128,1)

f_{11}	0	6 144	(0,30),(8,64),(16,31),(32,2),(48,1)	(16,96),(32,30),(64,1),(128,1)
	23	5 120	(0,24),(8,64),(16,39),(48,1)	(0,12),(16,96),(32,18),(64,1),(128,1)
	23+12	15 360	(0,34),(8,64),(16,24),(32,6)	(0,12),(16,96),(32,18),(64,1),(128,1)
	23+17	61 440	(0,48),(8,50),(16,16),(24,13),(40,1)	(0,12),(16,96),(32,18),(64,1),(128,1)
	25	30 720	(0,28),(8,64),(16,32),(32,4)	(0,24),(16,96),(32,6),(64,1),(128,1)
	27	737 280	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,21),(16,96),(32,10),(128,1)
	27+14	245 760	(0,32),(8,58),(16,32),(24,5),(40,1)	(0,21),(16,96),(32,10),(128,1)
	34+25+17+16+14	10 240	(0,48),(8,48),(16,16),(24,16)	(0,24),(16,96),(32,6),(64,1),(128,1)
	27+34	983 040	(0,35),(8,56),(16,28),(24,8),(32,1)	(0,27),(16,96),(32,4),(128,1)
	27+23+24	2 048	(0,60),(8,48),(24,16),(32,4)	(16,96),(32,30),(64,1),(128,1)
f_{12}	0	129 024	(0,39),(8,56),(16,24),(24,7),(32,1),(40,1)	(0,36),(16,64),(32,27),(128,1)
	12	16 128	(0,36),(8,58),(16,27),(24,6),(48,1)	(0,24),(16,64),(32,39),(128,1)
	16+15+13	32 256	(0,34),(8,60),(16,28),(24,3),(32,2),(40,1)	(0,36),(16,64),(32,27),(128,1)
	17+15+13+12	128	(0,28),(8,63),(16,36),(56,1)	(16,64),(32,63),(128,1)
	23	110 592	(0,36),(8,56),(16,28),(24,7),(40,1)	(0,42),(16,64),(32,21),(128,1)
	23+12	258 048	(0,37),(8,58),(16,24),(24,6),(32,3)	(0,42),(16,64),(32,21),(128,1)
	23+12+13	129 024	(0,39),(8,54),(16,24),(24,10),(32,1)	(0,48),(16,64),(32,15),(128,1)
	23+15	387 072	(0,34),(8,58),(16,28),(24,6),(32,2)	(0,48),(16,64),(32,15),(128,1)
	23+15+13	387 072	(0,39),(8,54),(16,24),(24,10),(32,1)	(0,48),(16,64),(32,15),(128,1)
	23+15+13+12	43 008	(0,45),(8,54),(16,16),(24,10),(32,3)	(0,36),(16,64),(32,27),(128,1)
	25+16+13	48 384	(0,34),(8,58),(16,28),(24,6),(32,2)	(0,48),(16,64),(32,15),(128,1)
	25+17+15+12+13	8 064	(0,28),(8,60),(16,36),(24,3),(40,1)	(0,48),(16,64),(32,15),(128,1)
	34+25+12	258 048	(0,36),(8,54),(16,28),(24,10)	(0,54),(16,64),(32,9),(128,1)
	34+25+16+12	258 048	(0,31),(8,58),(16,32),(24,6),(32,1)	(0,54),(16,64),(32,9),(128,1)
	34+26+17+15+14+13+12	32 256	(0,28),(8,58),(16,36),(24,6)	(0,60),(16,64),(32,3),(128,1)

All affine equivalence classes that share the same f_i representative are part of the same 2-equivalence class.

Appendix F

Software

We developed numerous software packages to increase the speed and efficiency of our search for highly nonlinear Boolean functions. The following are some of the features we implemented:

1. Compute the second order nonlinearity of a given Boolean function
2. Generate affine equivalent functions to a given Boolean function
3. Determine if a given Boolean function is bent using the Fourier transform
4. Determine if two given Boolean functions are permutations of one another

The software is written in Java and Prolog.