ON NONLINEARITY AND HAMMING WEIGHT PRESERVING BIJECTIVE MAPPINGS ACTING ON BOOLEAN FUNCTIONS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

İSA SERTKAYA

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

AUGUST 2014

Approval of the thesis:

ON NONLINEARITY AND HAMMING WEIGHT PRESERVING BIJECTIVE MAPPINGS ACTING ON BOOLEAN FUNCTIONS

submitted by **İSA SERTKAYA** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Bülent Karasözen
Director, Graduate School of **Applied Mathematics** _____

Prof. Dr. Ferruh Özbudak
Head of Department, **Cryptography** _____

Assoc. Prof. Dr. Ali Doğanaksoy
Supervisor, **Department of Mathematics** _____

Examining Committee Members:

Prof. Dr. İsmail Ş. Güloğlu
Department of Mathematics, Doğuş University _____

Prof. Dr. Ersan Akyıldız
Department of Mathematics, METU _____

Prof. Dr. Ferruh Özbudak
Department of Mathematics, METU _____

Prof. Dr. Ali Aydın Selçuk
Department of Computer Engineering, TOBB ETU _____

Assoc. Prof. Dr. Ali Doğanaksoy
Department of Mathematics, METU _____

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: İSA SERTKAYA

Signature :

ABSTRACT

ON NONLINEARITY AND HAMMING WEIGHT PRESERVING BIJECTIVE MAPPINGS ACTING ON BOOLEAN FUNCTIONS

Sertkaya, İsa

Ph.D., Department of Cryptography

Supervisor : Assoc. Prof. Dr. Ali Doğanaksoy

August 2014, 86 pages

Boolean functions are widely studied in cryptography due to their key role and applications in various cryptographic schemes. Particularly in order to make symmetric crypto-systems resistant against cryptanalytic attacks, Boolean functions are associated some cryptographic design criteria. As a result of Shannon's similarity of secrecy systems theory, cryptographic design criteria should be at least preserved under the action of basic transformations. Among these design criteria, Meier and Staffelbach analyzed behavior of the nonlinearity criteria under the action of bijective mappings defined on input values of the functions. Later, Preneel proved that nonlinearity still remains invariant under the action of affine equivalence mappings. Motivated by the previous studies, in his master thesis, the author showed the existence of new nonlinearity preserving bijective mappings.

In this thesis, we first give definition of the maximal group that can act on Boolean functions. This maximal group is the symmetric group of the vector space that corresponds to the set comprised of the truth table of the Boolean functions. We give a representation, based on the coordinate functions' algebraic normal form, for the elements of this symmetric group and then we list its subgroups that we mainly focus on. Regarding these subgroups, our aim is to enumerate or classify these bijective mappings with respect to preserving a cryptographic design criterion. After the necessary definitions and notions, we mainly investigate the nonlinearity preserving bijective mappings. Then we apply the procedures constructed on nonlinearity preservability

to another cryptographic design criterion, namely the Hamming weight. From a theoretical viewpoint, our basic result is that we show the existence of new families of bijective mappings that leaves nonlinearity (respectively, Hamming weight) invariant.

Under the action of linear and affine bijective mappings we give the necessary and sufficient conditions to keep nonlinearity invariant. We explicitly construct an isomorphism between the affine equivalency mappings subgroup and the automorphism group of the Sylvester Hadamard matrices and give the order of this automorphism group. Next we construct a family of non-affine nonlinearity preserving bijective mappings explicitly. However, we also show that all of these explicitly constructed nonlinearity preserving bijective mappings produce the same orbit structure as the affine equivalency mappings. On the other hand, we give the exact number of nonlinearity preserving bijective mappings for the functions with $n \leq 6$ variables. Then, based on these cardinalities, we prove the existence of new non-affine nonlinearity preserving mappings, without constructing explicitly. We demonstrate some examples for these non-affine mappings.

Following the results obtained for nonlinearity preserving bijective mappings, we extend our study to the Hamming weight preserving bijective mappings. First we completely solve the enumeration problem of Hamming weight preserving bijective mappings, and give the exact number of the Hamming weight preserving bijective mappings for all Boolean functions. Afterwards, we study the classification problem and give partial results. Lechner proved that the Hamming weight property is preserved under the action of symmetric group of input vector space. We further prove that among the affine bijective mappings only these mappings preserve the Hamming weight. Finally, again based on the enumeration of the Hamming weight preserving bijective mappings we proved the existence of Hamming weight preserving non-affine bijective mappings.

Keywords: Boolean functions, Nonlinearity, Hamming weight, Affine equivalence, Sylvester Hadamard matrices

ÖZ

BOOLE FONKSİYONLARI ÜZERİNE TANIMLI NONLİNEERİTE VE HAMMING AĞIRLIĞINI KORUYAN TERSİNİR DÖNÜŞÜMLER

Sertkaya, İsa

Doktora, Kriptografi Bölümü

Tez Yöneticisi : Assoc. Prof. Dr. Ali Doğanaksoy

Ağustos 2014, 86 sayfa

Kriptografik literatürde Boole fonksiyonları, türlü kriptografik projelerdeki rolleri ve uygulamaları nedeniyle, oldukça sık çalışılmaktadır. Özellikle simetrik kripto sistemlerinin kriptografik saldırılara dayanıklı olması için Boole fonksiyonları birkaç kriptografik tasarım kriterleri ile ilişkilendirilir. Shannon?ın gizlilik sistemlerinin benzerliği teorisi gereği, kriptografik tasarım kriterleri en azından temel dönüşümlerin etkisi altında korunmalıdır. Bu tasarım kriterleri arasından nonlineerite kriterleri, Meier ve Staffelbach tarafından fonksiyonların girdileri üzerine tanımlı tersinir dönüşümlerin etkisi altında incelenmiştir. Daha sonra, Preneel nonlineeritenin afin denklik dönüşümlerinin etkisi altında da sabit kaldığını ispatlamıştır. Önceki çalışmalardan hareketle, yazar, yüksek lisans tezinde nonlineeriteyi koruyan yeni tersinir dönüşümlerin varlığını göstermiştir.

Bu çalışmada öncelikle, Boole fonksiyonları üzerine etki edebilecek maksimal grubun tanımını vermekteyiz. Bu maksimal grup Boole fonksiyonlarının doğruluk tablolarının oluşturduğu kümeye karşılık gelen vektör uzayının simetrik grubuna tekabül eder. Koordinat fonksiyonlarının cebirsel normal formlarını baz alarak bu simetrik grubun öğelerine bir gösterim veriyor ve sonrasında bu sismetrik grubun çalışmada odaklanacağımız altgruplarını listeliyoruz. Bu altgrupları dikkate alarak; amacımız bu tersinir dönüşümlerin içinden bir kriptografik tasarım kriterini koruyanlarını saymak veya sınıflandırmakdır. Gerekli tanım ve nosyonlardan sonra, çoğunlukla nonlineeriteyi koruyan tersinir dönüşümleri incelemekteyiz. Ardından nonlineeritenin korunması

üzerine oluşturulan prosedürleri diğer bir kriptografik tasarım kriteri olan Hamming ağırlığı için uygulamaktayız. Teorik bakış açısıyla, temelde nonlineeriteyi (benzer şekilde Hamming ağırlığını) sabit bırakan yeni tersinir dönüşümler ailesinin varlığını göstermekteyiz.

Lineer ve afin tersinir dönüşümlerin etkisi altında, nonlineeritenin sabit kalması için gerek ve yeter şartları veriyoruz. Afin denklik dönüşümler altgrubu ile Sylvester Hadamard matrislerinin otomorfizma grubu arasında açıkca bir izomorfizma oluşturuyor ve bu otomorfizma grubunun eleman sayısını veriyoruz. Devamında nonlineeriteyi koruyan afin olmayan bir tersinir dönüşümler ailesini açıkca oluşturuyoruz. Fakat, açıkca bilinen nonlineeriteyi koruyan tersinir dönüşümlerin tamamının afin denklik dönüşümler ile aynı yörünge yapısını ürettiklerini gösteriyoruz. Öte yandan, $n \leq 6$ değişkenli fonksiyonlar için nonlineeriteyi koruyan dönüşümlerin tam sayılarını veriyoruz. Ondan sonra bu sayılardan hareketle, açıkca oluşturmadan afin olmayan nonlineeriteyi koruyan yeni tersinir dönüşümlerin varlığını ispatlıyoruz. Bu afin olmayan dönüşümlerin bazı örneklerini veriyoruz.

Nonlineeriteyi koruyan tersinir dönüşümler için elde edilen sonuçları izleyerek; çalışmamızı Hamming ağırlığını koruyan tersinir dönüşümleri de kapsayacak şekilde genişletiyoruz. Öncelikle Hamming ağırlığını koruyan dönüşümlerin sayılması problemini tamamıyla çözümlüyor ve tüm Boole fonksiyonları için Hamming ağırlığını koruyan tersinir dönüşümlerin sayısını veriyoruz. Sonrasında sınıflandırma problemi üzerine çalışıyor ve kısmi sonuçlar veriyoruz. Lechner Hamming ağırlığı özelliğinin girdi vektör uzayının simetrik grubunun etkisi altında korunduğunu göstermiştir. Biz afin tersinir dönüşümlerin içinde de sadece bu dönüşümlerin Hamming ağırlığını koruduğunu kanıtladık. Son olarak ise yine Hamming ağırlığını koruyan dönüşümlerin sayısından hareketle afin olmayan Hamming ağırlığını koruyan dönüşümlerin varlığını ispatlıyoruz.

Anahtar Kelimeler: Boolea fonksiyonları, Nonlineerite, Hamming ağırlığı, Afin denklikler, Sylvester Hadamard matrisleri

Tüm Aileme,
özellikle
Annem, Babam, Eşim ve
biricik İpek'ime

ACKNOWLEDGMENTS

"Hamd ve övgü Allah'a mahsustur."

To this position in my academic career pursuit, there are many many people to whom I owe at least a sincere gratefulness or a "Thank you". A try will be given to be as complete as possible even if some will unwillingly and eventually left out.

First, I would like to express my sincerest gratitude and acknowledgment to my supervisor Ali Doğanaksoy. Although I tried to quit several times and give up, he guided me in a very patient way and directed all of my excuses to a motivation. As I already acknowledged him before:

> "My first, and the most earnest, acknowledgment must go to my supervisor Assoc. Prof. Dr. Ali Doğanaksoy not only for patiently guiding, motivating, and encouraging me throughout this study, but also for being instrumental in ensuring my academic, professional and moral wellbeing ever since. In every sense, none of this work would have been possible without him."

His encouragement and both professional and moral perspective, not only throughout this thesis but also in daily life matters, have been irreplaceable. I would not have asked for any other supervisor, he deserve far more credit than I can ever give.

I would like to thank my committee members, İsmail Ş. Güloğlu, Ersan Akyıldız, Ferruh Özbudak and Ali Aydın Selçuk for serving as my committee members, letting my defense be an enjoyable moment, brilliant comments and suggestions.

Special thanks must go to my colleagues at BİLGEM UEKAE for creating an enjoyable atmosphere. In particular, I want to acknowledge my managers and Özkan, Emrah, Birnur, Mehmet, Osmanbey, Şükran and Hüseyin for the moments we share. It is also a pleasure to thank to my former managers and colleagues Önder Yetiş, Alparslan Babaoğlu and Nezih Geçkinli.

I also would like to thank to all people at IAM, especially to Dr. Muhiddin Uğuz for his valuable comments and suggestions.

My appreciation to my wife Meltem is immense. Her support, encouragement, quiet patience and unwavering love were in the end what made this dissertation possible. Especially during the dissertation writing period, she had to take care of almost everything and make our beloved daughter İpek feel comfortable. And of course, –̇pek

who makes everything else almost meaningless. I always pray to be able fulfill every moment and my responsibilities for both of you.

Last but certainly not the least, I want to express my genuine appreciation and warm thanks for my father Ali, my mother Şerife, my sisters Mümine and Gülsün, my brothers Hasan and İsmail and my in-laws for their unconditional support. Not only during the time spent on this thesis, but also throughout the many preceding years of education, they always cheered me up and were there for me. Words would never be enough how grateful I am.

Above all, I praise Allah for each and every bit of my life.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

$\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$	Natural, Integer, Real, Complex Numbers, resp.
$\mathsf{Sym}(\cdot)$	The symmetric group of a set
$\mathscr{S}_n$	The symmetric group of order $n!$, $n \times n$ permutation matrices
π_ψ	Permutation representation of a bijective mapping ψ
1_G	The identity element of a group G
$\#(\cdot)$	The cardinality of, the order of, or equivalently, the number of elements in.
$\mathsf{Aut}(\cdot)$	The automorphism group
$\mathbb{F}_q$	Finite field of order q
$\mathbb{F}_2^n$	n dimensional $\mathbb{F}_2$–vector space
$\mathsf{sup}(\cdot)$	The support of, i.e. the set of components for which $(.)$ has non-zero value
$\mathsf{w}(\cdot)$	The Hamming weight
w_t	The set comprised of Boolean function with Hamming weight t
$\mathsf{d}(\cdot,\cdot)$	The Hamming distance
$\mathscr{T}_n$	The group of translations acting on $\mathbb{F}_2^n$.
I_n	The identity matrix of order n
GL_n	General linear group of order n over $\mathbb{F}_2$
$\mathscr{D}_n$	$n \times n$ Diagonal matrices having only $\{\pm 1\}$ in main diagonal
$\times, \ltimes$	Direct product, Semi-direct product (reap.)
$\mathscr{S}_n^{\pm}$	Signed permutations, i.e. $\mathscr{S}_n \ltimes \mathscr{D}_n$
AGL_n	General Affine group of order n over $\mathbb{F}_2$
H_n	Sylvester Hadamard matrix of order 2^n
$\mathscr{F}_n$	The set of all n variable Boolean functions
T_f	The truth table of a Boolean function f
$\mathscr{E}_n$	The set of all n variable balanced functions
$\chi(\cdot)$	The additive character
$\chi_f(\cdot)$	The sign function or character form of a Boolean function f
ζ_f	The sequence of a Boolean function f
ANF	The algebraic normal form of a Boolean function
A_f	The algebraic normal form coefficients of a Boolean function f

A_n	The algebraic normal form matrix of order n
$\mathsf{deg}(f)$	The degree of ANF of a Boolean function f
$\ell_\alpha(\cdot)$	The linear Boolean function $\ell_\alpha : x \mapsto \langle x, \alpha \rangle$
$\mathscr{L}_n$	The set of all n variable linear functions
$\ell_{\alpha,a}(\cdot)$	The affine Boolean function $\ell_{\alpha,a} : x \mapsto \langle x, \alpha \rangle \oplus a$
$\mathscr{A}_n$	The set of all n variable affine functions
WHT	The Walsh Hadamard transform of a Boolean function
W_f	The Walsh spectra of a Boolean function f
$\delta(\cdot)$	The Kronecker delta function
$\lvert . \rvert$	The absolute value
N_f	The nonlinearity value of a Boolean function f
N_t	The set comprised of Booelan functions with nonlinearity t
$\mathscr{B}_n$	The set of all n variable bent functions
$\mathsf{AGL}_n \ltimes \mathscr{A}_n$	The group of affine equivalency mappings acting on n variable functions
$n!$	For $n \in \mathbb{N}$, $n! = 1\,2\,3 \cdots (n-1)\,n$
$\binom{n}{k}$	n chooses k
$\mathscr{P}_n(\mathsf{N})$	The group of nonlinearity preserving bijective mappings acting on n variable functions
$A - B$	Set difference of A and B
$\ggg$	very much greater than
$\mathscr{P}_n(\mathsf{w})$	The group of Hamming weight preserving bijective mappings acting on n variable functions

CHAPTER 1

INTRODUCTION

Main problem studied within this thesis is to analyze the action of bijective mappings on the Boolean functions and additionally try to classify or enumerate the ones that keep certain cryptographic design criteria invariant especially the nonlinearity and Hamming weight. Further to investigate outcome of these mappings mainly for cryptographic research. Up to the author knowledge, even if some well-known transformations are widely studied, this generalized problem did not gather much attention. In this chapter, we first give an overview and related work, then continue with the our objectives and contributions, finally give the outline.

1.1 Overview

Boolean functions are named after the British mathematician George Boole who is known to be the founder of mathematical logic (Boolean algebra) due to his seminal books [12, 13]. Even if the Boole's studies were well credited, it was Claude E. Shannon who ported the work of Boole into electronic circuits, which is mostly credited as foundations of digital engineering, and used them as switching functions [130].

Basically, Boolean function are $\{0,1\}$-valued functions of finitely many of $\{0,1\}$-valued input variables [35]. Boolean functions, or hereinafter shortly functions, and its applications spread to a diverse number of fields such as logic, proof theory, learning theory, game theory, combinatorics, switching theory, computational complexity theory, harmonic analysis, theoretical computer science, electronical engineering, cryptography and coding theory. For a comprehensive list and therein list of recent studies, reader may refer to [34, 35].

In coding theory the basic aim is to transmit a codeword, which is mostly a binary string, on a noisy communication channel and in case of an error detected correct them if possible. Hence, Boolean functions are naturally play important roles in coding theory [95]. Actually one of the oldest family of codes Reed-Muller codes, named after Reed [115] and Muller [105], are basically defined by Boolean functions.

On the contrary to the coding theory, main concern in classical cryptography is to conceal and/or break the secret information which is needed to be transmitted between at

least two parties. With the information age, cryptography evolved from classical cryptography into larger perimeter where confidentiality, privacy, secrecy, data integrity, authentication, undeniability, access control and non-repudiative concerns are all included. For further reading please refer to [104, 121, 49].

Cryptographic systems are generally classified into two schemes such as secret (symmetric) key and public (asymmetric) key crypto systems. In public key cryptography, [41], two different keys are used for encryption and decryption whereas in secret key cryptography both parties share only a secret key that is used both for encryption and decryption process. Secret key cryptography can further be decomposed into two different schemes as block ciphers and streams ciphers. In the block cipher schemes, secret message so called *plaintext* are partitioned into a fixed larger length of blocks and encrypted to get *ciphertext* where in stream ciphers process generally each bit of plaintext with an internally updated algorithms [15].

In the classical cryptography, encryption and decryption is made by porting the plaintext into a function with a secret key and sending its image as a ciphertext. Shannon in his seminal work [131], with an information theoretical approach, proved that the *one time pad*, also known as Vernam cipher named in the honor of G. Vernam [139], has the perfect secrecy under the cipher-text only attack. The necessary condition is to use a random key whose length is as long as the plaintext only once. These conditions make the system usage nearly impossible due to key distribution and management problems. Shannon further proposed that any secret key scheme should possess the *confusion* property to maximize the system complexity and the *diffusion* property to minimize effect of the plaintext redundancy on the ciphertext.

Based on the confusion and diffusion design principles, in modern block ciphers encryption process evolved into applying so called *round function* with the *round key* obtained from the secret key, repeatedly where the procedure is either based on either Feistel or substitution-permutation network structure, see [48, 106] and [75, 107, 38], respectively. For recent developments in block ciphers and related cryptanalysis techniques please see [83, 8].

Meanwhile, the promising property of the one time pad led many researches to build a stream cipher where the encryption is pursued by xoring the plaintext with a pseudo random key generated in a deterministic way from the initial secret state. Stream ciphers evolved from rotor based machines into *linear feedback shift registers* (LFSR) based stream ciphers such as nonlinear feedback shift registers, nonlinear filter generator, clock controlled stop/go generators [53], shrinking generators [32, 103], alternating step generators [55] and look up based stream ciphers [116]. For a then and now reading, please refer to [54, 36, 117, 82] respectively.

Cryptology has mainly two branches, *cryptography* the art of designing crypto systems and *cryptanalysis* the art of breaking the crypto systems. Kerchoff's design principle recommends consider all building components are public and to build an enciphering scheme security solely on the secret key [80]. Except the one time pad, the security of each enciphering scheme relies on the computational complexity which is mostly the cardinality of the enciphering key space. The aim of cryptography is to prove that the system satisfies the necessary security conditions whereas the aim of cryptanalysis

prove it otherwise even with slightly reducing key space. In a nutshell, this rivalry leads to every research and development in cryptology.

Most of the well-known cryptanalysis techniques led to new cryptographic design criteria. For instance, statistical attacks to *balancedness*, correlation attack [132] to *correlation immunity* and *resiliency*, differential cryptanalysis [9, 11, 10] to *strict avalanche criterion* [140], *propagation criterion* [114] and *differential uniformity*, linear cryptanalysis [99, 98] to *nonlinearity* [111], algebraic attack [33] to *algebraic immunity* [101].

Due to the Shannon's similarity of secrecy systems theory, proposed design criteria should remain invariant under simple transformations [131, Chapter 8]. Two crypto systems are considered to be the same if one can be obtained from the other by applying a series of simple transformations.

The design criteria should provide adequate level of confusion and diffusion for resisting the cryptanalytic attacks. Thus the design of enciphering scheme should be proven to satisfy the design criteria for the whole routine of the enciphering scheme. However, in many cases giving such a proof may become impossible. Therefore, these design criteria are examined or analyzed for the building blocks of ciphers. Intentionally it is expected that if the building blocks of the scheme are shown to satisfying the design margin, it would lead to the satisfaction for the whole scheme.

Block ciphers mostly contains *S-Boxes* for satisfying the confusion property which are in fact can be represented as *vectorial Boolean functions*, i.e. maps $\{0,1\}^n$ values to $\{0,1\}^m$ values. Vectorial Boolean functions, sometimes also called multi output Boolean functions can be easily reviewed by a collection of Boolean functions called *component* or *coordinate* functions. Similarly, stream ciphers like nonlinearly filtered LFSRs, nonlinear combiners and nonlinear feedback shift registers are also utilize the applications of the Boolean functions.

1.2 Motivation

Both stream and block ciphers are actively studied research area, since the symmetric crypto systems play the key role almost every cryptographic scheme. Therefore, research on vectorial Boolean and/or Boolean functions are actively pursued. In many of the cases, constructing a symmetric cipher scheme and later proving its security margins with respect to the cryptographic design criteria may deduce to the construction and analysis of Boolean functions. Maximal values or upper bounds of certain design criteria, constructions of Boolean function families attaining maximal design criteria values, the tradeoffs in-between the design criteria, classification of Boolean functions regarding a design criterion problems have great importance both in theoretical and practical cryptographic purposes. For extensive surveys and recent research on Boolean functions and their applications in cryptography, the reader may refer to [24, 25, 37, 113].

For instance, the underlying point of the Matsui's linear cryptanalysis is the existence

of highly probable linear relation among the plaintexts, ciphertexts and secret key [99]. S-boxes and so is the Boolean functions with low nonlinearity would lead such linear relations. Meier and Staffelbach analyzed the proposed nonlinearity notions and showed that for the Boolean functions with even number variables, highest nonlinearity and maximal order of propagation criterion coincides [102]. Further, they presented that the *bent functions* given by Rothaus [118] possess these maximal properties. Due to their applications in various area, many studies pursued on constructions, classifications and enumerations of bent functions, some of them are [42, 100, 43, 44, 84].

Bent functions exist only for even numbered variables, but much worse of that is their unbalancedness. Highly nonlinear balanced Boolean functions for both even and odd numbered variables is still an open problem. On the one hand recursive constructions and on the other hand heuristic computer search based studies are deeply carried on [79, 97]. During these search, when a Boolean function is found or constructed, one basic question rises: Does this function belong to the previously known families or not? To answer this question one first needs to define an equivalence relation between the functions.

The study of equivalencies on Boolean functions dates back to switching theory. In 1950s, S. W. Golomb published a paper concerning the classification of Boolean functions with respect to the equivalence relation composed of only permutations and negations of input variables based on the work of Slepian [133]. Later, the equivalence relation is extended to the general linear and affine groups acting on input variables of Boolean functions by Harrison [63, 62, 64, 61, 65, 66], Lorenz [92], Lechner [85, 86]. Furthermore, asymptotic estimates for the number of equivalence classes are also studied [67, 40]. We refer to [135] and [120, Chapter 1] for further reading.

In coding theory, equivalence of codes, based on these equivalencies the automorphism group of a code has great importance both for understanding the code and constructing effective decoding procedures. The automorphism of a code is in fact an equivalence relation that maps the code into itself and hence keeping its properties invariant. Generally, we refer to the book of Macwilliams and Sloane [95] for an excellent survey. In particular, the automorphism group of Reed-Muller codes and generalized Reed-Muller codes is given [95, Chapter 13, Theorem 24],[5], respectively. In the pursue of the coset classification, covering radius of Reed-Muller codes, Hou also studied the action of certain general linear and affine transformations [45, 70, 71, 46]. Furthermore, following the work of Lechner, Berlekamp and Welch partitioned 5 variables Boolean functions into equivalence classes and later Maiorana with aid of computer based search gave the equivalence classes of 6 variables Boolean functions, see [85], [6] and [96], respectively.

Partitioning the Boolean functions set into equivalence classes has great importance. For $n \geq 6$, scanning each of n variable Boolean functions and looking their specific properties may become infeasible. Hence, instead of a whole scan, dividing the set of all functions into disjoint equivalence classes where each function in the same class possesses the same design criterion value becomes handy and makes some searches feasible.

In 1988 Forré proved that the strict avalanche criterion, which was proposed by Web-

ster and Tavares [140], remains invariant under the action of the transformations composed of permuting the coordinates and translating with a fixed vector on the input variables [50].

Meier and Staffelbach, in their seminal work [102], showed that the algebraic degree, the distance to the affine functions which the nonlinearity and to the linear structures defined in [30, 47] remains invariant under the action of general affine group on the input variables of the functions. Meier and Staffelbach additionally proved that correlation immunity is invariant under the mappings consisting only the permutation and/or complementation of input variables. Seberry, Zhang and Zheng further given that the algebraic degree, Hamming weight, nonlinearity and the number of vectors to which propagation criterion satisfied are all remains invariant under the action of general affine group acting on the input variables of the functions [122]. Meanwhile, Preneel extended the group of transformations to the group, so called affine equivalence, constructed by the semi-direct product of general affine group and affine Boolean functions, showed that nonlinearity is still remains invariant [112]. Later, Braeken, Borissov, Nikova, and Preneel showed that algebraic immunity is invariant under affine transformations acting on input arguments [16]. For an extensive studies of the action of so called affine equivalence relations on Boolean functions please refer to [85, 63, 52, 15]. Actual consequences of studying the affine equivalences are enumeration of Boolean functions with respect to their cryptographic design criteria values, see [17, 14, 84].

Same approach and problems are also exist for vectorial Boolean functions. Besides of the affine and extended affine equivalences, in 1998 Carlet, Charpin and Zinoev proposed so called *CCZ equivalence* and in 2004 Breveglieri, Cherubini and Macchetti defined generalized linear equivalence, see [26] and [18, 93, 94], respectively. The equivalence proposed for vectorial Boolean functions can be also analyzed for the Boolean functions. For instance, Budagyhan and Carlet proved that for Boolean function case, the CCZ equivalence reduces to the affine equivalence [20].

1.3 Objectives and Accomplishments

Any bijective mapping defined on a set onto itself is in fact a permutation of the elements of the set. The set of all such permutations forms a group with the group law being the composition. For a set consisting only n elements, largest group consisting of all permutations of the set is called *symmetric group* and it has $n!$ permutations, i.e. its cardinality is $n!$.

The set of all Boolean functions with n variables, consists of only 2^{2^n} elements. Hence, the symmetric group consisting of all bijective mappings, namely the group of permutations of all of the Boolean functions with n variables, has $2^{2^n}!$ elements.

Defining an equivalence relation between two Boolean functions is in fact a natural result of construction of an action of a group consisting of only bijective mappings on the set of Boolean functions. Maximal group of bijective mappings for which an action on Boolean functions with n variable can be defined is the symmetric group

consisting of $2^{2^n}!$ elements. However, all of the aforementioned transformation groups in the previous section are just a proper subgroup of this symmetric group. Therefore, some natural questions arise, such as, are those proper subgroups only the ones that keep certain design criterion invariant, if not is it possible to construct new bijective mappings, is it possible to enumerate, classify or explicitly construct all of the bijective mappings that keep certain criterion invariant.

Under the supervising of Doğanaksoy, in his master thesis, the author studied the above questions for the nonlinearity criterion and proved the existence of new nonlinearity preserving bijective transformations [124].

In this thesis, main objective is to formally define and analyze the maximal group of bijective mappings, namely the symmetric group, with respect to invariance of the nonlinearity and the Hamming weight criteria by defining a formal action on the set of Boolean functions and try to find the answers of the following problems:

- classify, enumerate and explicitly construct the group of all nonlinearity preserving bijective mappings,
- classify, enumerate and explicitly construct the group of all Hamming weight preserving bijective mappings.

In the pursue of the answers of these problems, we first revisit the group of all affine equivalency mappings and give a proof of an isomorphism between the automorphism group of Sylvester Hadamard matrices and the group of affine equivalence relations. Next, for $n = 2$, we exactly determine the group of all nonlinearity preserving bijective mappings. For $n \leq 6$, we enumerate all of the nonlinearity preserving bijective mappings. We construct some new families of nonlinearity preserving bijective mappings and further we prove existence of nonlinearity preserving bijective mappings without constructing explicitly based on the enumerations. Following these results, we analyze the notion of automorphism group of nonlinearity classes and propose that studying the automorphism group of nonlinearity classes as a subgroup of the symmetric group is more insightful for cryptographic design purposes, since it contains transformations which do not belong to the group of affine equivalence relations.

Besides the nonlinearity preserving bijective mappings, we have another focal point. We also studied the Hamming weight preserving bijective mappings. For the Hamming weight of the Boolean functions, first we give the exact number of Hamming weight preserving bijective mappings. Second, we present that the affine Hamming weight preserving bijective mappings are comprised of the bijective mappings acting on input variables. Next we prove that there also exist non-affine Hamming weight pressuring bijective mappings.

The results for the nonlinearity preserving bijective mappings which are included in this thesis are published and/or accepted in various conferences, see [126, 127, 128, 129, 125]. However, the results on Hamming weight preserving bijective mappings are not yet published but are in preprint.

1.4 Outline of the Thesis

In Chapter 2, we first give some notations. preliminaries and mention the definitions and propositions which will be used in the following sections.

In Chapter 3, we prove that the group of affine equivalence relations is isomorphic to the automorphism group of Sylvester Hadamard matrices. we give the exact number of nonlinearity preserving bijective mappings for $n \leq 6$, prove existence of new nonlinearity preserving non-affine mappings, and give some new examples. We discuss the main concerns about the automorphism group of nonlinearity classes.

In Chapter 4, we completely solve the enumeration problem for the Hamming weight preserving bijective mappings. We characterize the affine Hamming weight preserving bijective mappings. Moreover, we show the existence of non-affine bijective mappings that leave Hamming weight invariant.

Finally, Chapter 5 summarizes and concludes the thesis and points out some open problems for future studies.

CHAPTER 2

PRELIMINARIES

In this chapter, we are going to state the notations, recall the definitions and theorems that will be used throughout the thesis. The thesis is organized to be self-contained as much as possible. For details and further reading of the fundamental theory and concepts, the reader may refer to; [72, 21] for group theory and permutation groups, [24, 25, 37] for Boolean and vectorial Boolean functions, [59, 39, 1, 69] for combinatorics, design theory and Hadamard matrices, [90, 91, 88, 4] for Fourier and Walsh Hadamard transforms and [51, 15] for affine equivalence relations.

2.1 Symmetric Group

In this section, we give basic group theory definitions and notions, unless otherwise stated we will follow the notations and order of the topics as in [2, Chapter 1] as much as possible.

Let Ω be a non-empty finite set. A one-to-one and onto (namely *bijective*) mapping of Ω onto itself is called a *permutation* of Ω. The *symmetric group* $\mathsf{Sym}(\Omega)$ on Ω is the set of all permutations of Ω with the group law being the composition. We write permutations on the left and composition from right to left. The image of $x \in \Omega$ under the permutation π will interchangeably be denoted by $\pi(x)$ or πx and the composition of the permutations π and σ as $\pi \circ \sigma$ with $(\pi \circ \sigma)x := \pi(\sigma(x))$ or shortly $(\pi\sigma)x := \pi(\sigma x)$ if the context permits.

In a specific case where $\Omega = \{1, 2, \ldots, n\}$ with $n \in \mathbb{N}$ being a positive integer, $\mathscr{S}_n$ will be used to denote the symmetric group $\mathsf{Sym}(\Omega)$. Indeed, for $\#(\Omega) = n$ the cardinality of $\mathscr{S}_n$ is

$$\#(\mathscr{S}_n) = n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n \ .$$

There are common ways to write the permutations. Any permutation $\pi \in \mathsf{Sym}(\Omega)$ with $\#(\Omega) = n$ can be written as follows.

– As an explicit sequence of preimage and image pairs:

$$\pi := \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_{n-1} & x_n \\ \pi(x_1) & \pi(x_2) & \pi(x_3) & \cdots & \pi(x_{n-1}) & \pi(x_n) \end{pmatrix}$$

where the first row is an enumeration of elements of Ω, and the second row is the image of those elements ordered respectively under π.

– As products of disjoint cycles (disjoint cycle decomposition): A permutation π is called *cycle of length k* if there are distinct integers $1 \leq x_1, x_2, \ldots, x_k \leq n$ such that $\pi(x_i) = x_{i+1}$ for all $1 \leq i < k$, $\pi(x_k) = x_1$, and $\pi(y) = y$ for any $1 \leq y \leq n$ which is not equal to some x_i. In this case, π is written as $(x_1\ x_2\ \cdots\ x_k)$.

– As product of (not necessarily disjoint) transpositions: A *transposition* is a cycle of length 2.

Example 2.1. Let $\Omega = \{1, 2, \ldots, 8\}$, the following define the same permutation.

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 1 & 3 & 5 & 8 & 7 & 6 \end{pmatrix}$, (1 2 4 3)(5)(6 8)(7), (1 2 4 3)(6 8), (1 2)(2 4)(4 3)(6 8)

Let G and H be groups, we have the following definitions.

– A *homomorphism* is a map φ from G to H preserving the respective group structure, that is $\varphi : G \to H$ satisfying $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$.

– Additionally, if φ is bijective, then it is called an *isomorphism*. In this case, we say that G and H are *isomorphic* and denote by $G \cong H$.

– A homomorphism $\varphi : G \to G$ is called an *endomorphism* of G.

– A bijective endomorphism is called an *automorphism* of G. The set of all automorphisms of G, denoted by $\mathsf{Aut}(G)$, forms a group where the group operation is composition of the mappings.

Definition & Proposition 2.1. Let G_1 and G_2 be groups. The set constructed with the *Cartesian product* $G_1 \times G_2$ and associated with the binary operation named componentwise multiplication which is defined as $(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$ for all $g_1, g_1' \in G_1$ and $g_2, g_2' \in G_2$, is called the *direct product* of G_1 and G_2. It can be easily proved that $G_1 \times G_2$ possesses a group structure with the given operation.

Similarly,

Definition & Proposition 2.2. Let H and N be groups with a given (conjugation) homomorphism $\varphi : H \to \mathsf{Aut}(N)$ satisfying $\varphi(h)(n) := hnh^{-1}$. One can construct the group $G := H \ltimes_\varphi N$ that is the *(internal) semi-direct product* of a normal subgroup isomorphic with N by a subgroup isomorphic with H. Then we have

$$G = H \ltimes_\varphi N := \{hn \mid h \in H, n \in N\}$$

where the group operation is defined by

$$(h_1 n_1)(h_2 n_2) := h_1 h_2 n_1 \varphi(h_1)(n_2) := h_1 h_2 n_1 h_1 n_2 h_1^{-1},$$

for all $h_1, h_2 \in H$ and $n_1, n_2 \in N$.

Provided that the context permits, we sometimes use $G = H \ltimes N$ instead of $G = H \ltimes_\varphi N$.

2.1.1 Group Actions

Definition 2.1. Let G be a group and Ω any nonempty set. A *(left) action* of G on Ω is a map from $G \times \Omega$ to Ω such as $(g,x) \mapsto gx$ satisfying the following conditions:

- $1x = x$ for all $x \in \Omega$ where 1 is the identity element of G.
- $(g_1g_2)x = g_1(g_2x)$, for every $x \in \Omega$ and $g_1, g_2 \in G$.

Whenever, there exists an action of G on Ω, we say G acts on Ω or Ω is a G–set.

Suppose G acts on Ω, then one can easily show that, for an arbitrary element $g \in G$, the mapping $\pi_g : \Omega \to \Omega$ defined by $\pi_g(x) := gx$ has an inverse, and thus π_g is a permutation of the set Ω, i.e. $\pi_g \in \mathsf{Sym}(\Omega)$. In fact, the map $g \mapsto \pi_g$ is a homomorphism from G to $\mathsf{Sym}(\Omega)$. This homomorphism is called a *permutation representation* of G. Any subgroup G of $\mathsf{Sym}(\Omega)$ is called *permutation group* on Ω.

Theorem 2.3 (Cayley's Theorem)**.** *[29] Let G be an arbitrary group. Then G is isomorphic to a subgroup of $\mathsf{Sym}(G)$. In particular, if G is finite with $\#(G) = n$, then G is isomorphic to a subgroup of $\mathscr{S}_n$.*

Definition 2.2. Given a permutation group G on Ω. For each $x \in \Omega$, the *orbit* Gx of the x is the subset $Gx := \{gx \mid g \in G\}$ of Ω. The *stabilizer* of x is the subgroup $G_x := \{g \in G \mid gx = x\}$ of G.

Throughout the thesis, we mostly cope with the $\mathbb{F}_2$–vector spaces and their set property. Thus, for the rest of this section, hereinafter if possible, group theory related definitions will be given for $\mathbb{F}_2$–vector spaces even if they hold more generally.

2.2 $\mathbb{F}_2$–Vector Spaces

We denote the Galois field of order two by $\mathbb{F}_2$, use $\oplus$, $\bigoplus$ for addition in characteristic 2 and $+$, $\sum$ for addition in characteristic 0. The *Kronecker product* of two matrices will be denoted by $\otimes$, and the k^{th} Kronecker product power of a matrix M by M_k.

Let $\mathbb{F}_2^n$ be the set of all n-tuples, $\alpha = (a_1, a_2, \ldots, a_n)$, whose elements from $\mathbb{F}_2$. It is trivially easy to prove that $\mathbb{F}_2^n$ has the n dimensional vector space structure over $\mathbb{F}_2$. $\mathbb{F}_2^n$ possesses the *lexicographic ordering* [22, 23], as follows: for any $\alpha, \beta \in \mathbb{F}_2^n$, $\alpha < \beta$ if and only if there exists $i \in \{1, 2, \ldots, n\}$, such that $a_1 = b_1, \ldots, a_{i-1} = b_{i-1}$ and $a_i < b_i$.

We index the elements $\alpha_k = (a_1, a_2, \ldots, a_n)$ in $\mathbb{F}_2^n$, with representing them by the integer k from $\mathbb{Z}_{2^n}$, ring of integers modulo 2^n, by defining the map

$$\alpha_k = (a_1, a_2, \ldots, a_n) \mapsto k = \sum_{i=1}^{n} a_i 2^{n-i}.$$

It can be easily checked that the above map is indeed a bijection, thus we can mention about a one to one correspondence between $\mathbb{F}_2^n$ and $\mathbb{Z}_{2^n}$. Obviously, under this correspondence, lexicographic ordering coincides natural ordering of integers. The standard basis of $\mathbb{F}_2^n$ is denoted by $\{e_1, e_2, \ldots, e_n\}$, where e_i stands for the vector having all zero's except 1 on the i-th position. In fact, following the lexicographic ordering and indexing above, each e_i will be a short denotation for $\alpha_{2^{n-i}}$.

When the context permits,we use α_k or simply $k \in [0, 1, \ldots, 2^n - 1]$ to identify the elements of $\mathbb{F}_2^n$. We will use $[\alpha]$ to denote an element $\alpha \in \mathbb{F}_2^n$ as an $n \times 1$ column matrix.

The *standard inner product* or *scalar product* of α and β on $\mathbb{F}_2^n$ is defined as,

$$\langle \alpha \cdot \beta \rangle := \bigoplus_{i=1}^{n} a_i b_i = a_1 b_1 \oplus a_2 b_2 \oplus \cdots a_n b_n$$

.

The *support* $\mathsf{sup}(\alpha)$ of a vector $\alpha \in \mathbb{F}_2^n$ is the set of its nonzero coordinates, that is

$$\mathsf{sup}(\alpha) = \{i = 1, 2, \ldots, n \mid a_i \neq 0\} = \{i = 1, 2, \ldots, n \mid a_i = 1\}$$

.

The *Hamming weight*, named after R. W. Hamming, of $\alpha \in \mathbb{F}_2^n$ is the number of its nonzero coordinates [60]. We denote the Hamming weight or hereafter shortly weight by $\mathsf{w}(\alpha)$. Then we have,

$$\mathsf{w}(\alpha) = \#(\mathsf{sup}(\alpha)),$$

where # denotes the cardinality of the set.

Additionally, the *Hamming distance* between α and β on $\mathbb{F}_2^n$, denoted by $\mathsf{d}(\alpha, \beta)$, is the number of coordinates in which they differ, hence $\mathsf{d}(\alpha, \beta) = \mathsf{w}(\alpha \oplus \beta)$ [60]. In fact, Hamming proved that for any $\alpha, \beta, \gamma \in \mathbb{F}_2^n$, the Hamming distance function $d : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{R}$ satisfies the usual conditions for a *metric*:

- $\mathsf{d}(\alpha, \beta) = 0$ if and only if $\alpha = \beta$,
- $\mathsf{d}(\alpha, \beta) = \mathsf{d}(\beta, \alpha)$,
- $\mathsf{d}(\alpha, \gamma) \leq \mathsf{d}(\alpha, \beta) + \mathsf{d}(\beta, \gamma)$.

Thus one can conclude that the $\mathbb{F}_2^n$ together with the Hamming distance is in fact a *metric space*.

Definition 2.3. [96] Let $\alpha, \beta, \gamma \in \mathbb{F}_2^n$ and the map $\upsilon_\beta : \mathbb{F}_2^n \to \mathbb{F}_2^n$ defined by $\upsilon_\beta(\alpha) = \alpha \oplus \beta$ is called a *translation*. Since $\upsilon_\beta \upsilon_\gamma = \upsilon_{\beta \oplus \gamma}$, the collection of translations forms a group $\mathscr{T}_n$ and $\mathscr{T}_n$ is isomorphic to $\mathbb{F}_2^n$.

2.2.1 General Linear Group

We use the notation $\varphi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ for any mapping or transformation from $\mathbb{F}_2^n$ onto itself. We interchangeably use $\varphi(\alpha)$ or $\varphi\alpha$ for the image of $\alpha \in \mathbb{F}_2^n$ under φ and $\varphi : \alpha \mapsto \varphi(\alpha)$ or $\varphi : \alpha \mapsto \varphi\alpha$ to represent the effect of φ on α.

Let $\{v_1, v_2, \ldots, v_n\}$ be another basis for $\mathbb{F}_2^n$. Then, we can define a *linear transformation* $\varphi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that

$$\varphi : e_i \mapsto v_j = \bigoplus_{i=1}^{n} m_{ij} e_i$$

with $m_{ij} \in \mathbb{F}_2$ for all $1 \leq i, j \leq n$. In fact, m_{ij} are called called the *matrix coefficients* of the linear transformation φ and the $n \times n$ array

$$M = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1n} \\ m_{21} & m_{12} & \cdots & m_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{nn} \end{bmatrix}$$

is the *matrix* of φ with respect to the basis $\{e_1, e_2, \ldots, e_n\}$.

We denote the set of all $n \times n$ matrices with entries in the $\mathbb{F}_2$ by $\mathscr{M}_n(\mathbb{F}_2)$ and often use shortly $\mathscr{M}_n$. We write any matrix $M \in \mathscr{M}_n$ as follows.

- Entry based: $M := (m_{ij})$ where $m_{ij} \in \mathbb{F}_q$ denotes the (i, j)–entry of M where $1 \leq i, j \leq n$.
- Coloumn based: $M := [C_1\ C_2\ C_3\ \ldots\ C_n]$ where each C_i is $n \times 1$ matrix with entries in the $\mathbb{F}_q$ for $1 \leq i \leq n$.
- Row based: $M := \begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ \vdots \\ R_n \end{bmatrix}$ where each R_i is $1 \times n$ matrix with entries in the $\mathbb{F}_q$ for $1 \leq i \leq n$.

We use M^t and M^{-1} to denote the transpose and the inverse (provided that it exists) of a matrix $M \in \mathscr{M}_n$, respectively.

The set of all invertible linear transformations of $\mathbb{F}_2^n$ to itself will be denoted by $\mathsf{GL}(\mathbb{F}_2^n)$. In fact, this set owns a group structure under the composition of transformations with identity element is the identity transformation that maps each α to itself for all $\alpha \in \mathbb{F}_2^n$.

Definition & Proposition 2.4. The subset $\mathsf{GL}(n, \mathbb{F}_2)$ (shortly GL_n) of $\mathscr{M}_n$ consisting only of all invertible matrices, that is all matrices having non-zero determinant, is called the *general linear group*. GL_n forms a group under the usual matrix multiplication and we denote the identity element by I_n.

Indeed, given a finite dimensional vector space $\mathbb{F}_2^n$ with a basis , it is possible to construct the general linear group $\mathsf{GL}(\mathbb{F}_2^n)$ as the group of all invertible linear transformations of $\mathbb{F}_2^n$ with the group law being composition of the mappings. Thus GL_n is isomorphic in an obvious way with the general linear group defined as to be the group of all invertible linear transformations of $\mathbb{F}_2^n$ where composition of transformations being the group operation. Moreover, since GL_n is the automorphism group of $\mathbb{F}_2^n$, we regard GL_n as $\mathsf{Aut}(\mathbb{F}_2^n)$.

Proposition 2.5. *[3, p.169] Let $n \in \mathbb{N}$. Then*

$$\#(\mathsf{GL}_n) = \prod_{i=0}^{n-1}(2^n - 2^i) \ .$$

Proof. Counting the number of $n \times n$ matrices whose rows are linearly independent over $\mathbb{F}_2$ will be sufficient. For the first row there exist $2^n - 1$, namely the non-zero vectors in $\mathbb{F}_2^n$. For $1 < i \leq n$, the ith row can be any vector in $\mathbb{F}_2^n$ except for the 2^{i-1} linear combinations of the previous $i-1$ rows, thus for ith row there are $2^n - 2^{i-1}$ choices, from which the assertion follows. □

For a moment, let us consider the set $M \in \mathscr{M}_n(\mathbb{F})$ with $M = (m_{ij})$ over any field $\mathbb{F}$. The *main diagonal* of M consists of the entries m_{ii} for $1 \leq i \leq n$. The matrices whose only non-zero entries appear on the main diagonal are called *diagonal matrices*. Additional to the above representations, diagonal matrices can further be written or denoted as $M := diag(m_{11}, m_{22}, m_{33}, \ldots, m_{nn})$.

Proposition 2.6. *The subset of $\mathsf{D}(n,\mathbb{F})$ of $\mathscr{M}_n(\mathbb{F})$ consisting only of all diagonal matrices is a subgroup of $\mathsf{GL}(n,\mathbb{F})$.*

Proof. Let $D, D' \in \mathsf{D}(n,\mathbb{F})$ and write them as $D = diag(d_{11}, d_{22}, d_{33}, \ldots, d_{nn})$ and $D' = diag(d'_{11}, d'_{22}, d'_{33}, \ldots, d'_{nn})$. Then, by computing the multiplication directly, we get

$$DD' = diag(d_{11}d'_{11}, d_{22}d'_{22}, d_{33}d'_{33}, \ldots, d_{nn}d'_{nn}) \ .$$

Further in a similar way, one can easily prove that any diagonal matrix $D \in \mathsf{D}(n,\mathbb{F}_q)$ with $D = diag(d_{11}, d_{22}, d_{33}, \ldots, d_{nn})$ has the matrix

$$D^{-1} = diag(d_{11}^{-1}, d_{22}^{-1}, d_{33}^{-1}, \ldots, d_{nn}^{-1})$$

as its inverse where each d_{jj}^{-1} stands for multiplicative inverse of d_{ii}^{-1}. Hence the statement now follows. □

For the finite field $\mathbb{F}_2$, $\mathsf{D}(n,\mathbb{F}_2)$ is trivial since $\mathsf{D}(n,\mathbb{F}_2) = \{\mathsf{I}_n\}$.

We further continue to construct subgroups of GL_n. A *permutation matrix* is a matrix in which every row and column has a unique non-zero entry equal to 1. For instance I_n is a permutation matrix. Since every permutation matrix is orthogonal, it has an inverse which is equal to its transpose.

Proposition 2.7. *The set of all permutation matrices is a subgroup*[1] *of* GL_n.

Proof. Showing the closedness under matrix multiplication will be sufficient.

Let $P = (p_{ij})$ and $P' = (p'_{ij})$ be two permutation matrices and $M = PP' = (m_{ij})$. For any $1 \leq i, j, k, \leq n$, we have

$$m_{ij} = \begin{cases} 1 & \text{if } p_{ik} = p'_{kj} = 1 \text{ for some k} \\ 0 & \text{otherwise} \end{cases}$$

Indeed, by definition given i, there exists unique k such that $p_{ik} = 1$ and there is a unique j such that $p'_{kj} = 1$, thus $m_{ij} = 1$ for only one j. Similarly this also holds for a given j. Hence, M is also a permutation matrix, from which the assertion follows. □

Proposition 2.8. *The subgroup composed of all the permutation matrices of* GL_n *is isomorphic to* $\mathscr{S}_n$.

Proof. From Cayley's Theorem (Theorem 2.3), we know that any group of finite order n is isomorphic with a subgroup of $\mathscr{S}_n$. With simple counting, we see that the number of $n \times n$ permutation matrices is $n!$. Hence, we conclude that the group of $n \times n$ permutation matrices is isomorphic to $\mathscr{S}_n$. □

We will implicitly regard elements of $\mathscr{S}_n$ as being a permutation matrix, henceforth by abusing the notation, we will denote the group of $n \times n$ permutation matrices with also $\mathscr{S}_n$.

In fact, it is possible to construct *generalized permutation matrices* in order to represent the *generalized symmetric group* which is the *wreath product* $\mathscr{S}(m,n) := \mathbb{Z}_m \wr \mathscr{S}_n$ of the cyclic group of order m and $\mathscr{S}_n$. Equivalently, $\mathscr{S}(m,n)$ is the subgroup of the general linear group $\mathsf{GL}(n,\mathbb{C})$ over the complex numbers field comprising monomial matrices where all the non-zero entries are m^{th} roots of unity. In this general context, for $m = 1$, we have $\mathscr{S}(1,n) = \mathscr{S}_n$. Without going much further, we will only consider $\mathscr{S}(2,n) := \mathbb{Z}_2 \wr \mathscr{S}_n$ which is also called *signed symmetric group* or *signed permutations*, shortly we will denote by $\mathscr{S}_n^{\pm}$.

Definition & Proposition 2.9. Let $\mathscr{S}_n$ be the group of all permutation matrices of order n and $\mathscr{D}_n$ be the group of all diagonal matrices of order n with having only non-zero values at diagonal entries equal either to 1 or -1. Then, the elements of the semi-direct product $\mathscr{S}_n^{\pm} := \mathscr{S}_n \ltimes \mathscr{D}_n$ are called monomial matrices.
$\mathscr{S}_n^{\pm}$ forms a group under the operation $\cdot$ given by

$$P_1 \cdot P_2 = P'_1 P'_2 D_1 P'_1 D_2 (P'_1)^{-1} \tag{2.1}$$

where $P_1 = P'_1 D_1$ and $P_2 = P'_2 D_2$ with $P'_1, P'_2 \in \mathscr{S}_n$ and $D_1, D_2 \in \mathscr{D}_n$.

[1] also called Weyl subgroup [2, p. 42]

Proof. We have $\mathscr{D}_n \cap \mathscr{S}_n = I_n$. Furthermore, we have a homomorphism $\varphi : \mathscr{S}_n \to \mathsf{Aut}(\mathscr{D}_n)$ such that

$$\varphi(P)(D) := PDP^{-1}$$

for any $P \in \mathscr{S}_n$ and $D \in \mathscr{D}_n$. So we get $\mathscr{D}_n$ is a normal subgroup of $\mathscr{S}_n^{\pm}$. Hence the statement now follows. □

2.2.2 General Affine Group

We now extend the general linear group into the general affine group by constructing a group as a semi-direct product of GL_n with $\mathbb{F}_2^n$.

Proposition 2.10. *[96] Let the notations be as above. Let further* $\mathsf{AGL}(n, \mathbb{F}_2)$ *(shortly* AGL_n*) be the set*

$$\mathsf{GL}_n \ltimes \mathscr{T}_n := \{(A, \alpha) |\, A \in \mathsf{GL}_n,\ \alpha \in \mathbb{F}_2^n\}.$$

Then AGL_n *is a group with respect to the operation* $\bullet$*. The group law and its inverse are given by*

$$(A, \alpha) \bullet (A', \alpha') := (A'A, \alpha' A + \alpha),$$
$$(A, \alpha)^{-1} := (A^{-1}, \alpha A^{-1})$$

for all $(A, \alpha), (A', \alpha') \in \mathsf{AGL}_n$.

Proof. $A = I_n, \alpha = \alpha_0$ is the identity element of AGL_n. Closedness, existence of inverse elements and associativity follows immediately from the same properties of the underlying group structure of the components. □

2.3 Sylvester Hadamard Matrices

In this section, we leave $\mathbb{F}_2$-vector spaces for a moment and recall the Sylvester-Hadamard matrices defined over the field of real numbers $\mathbb{R}$. First, we give the definition of the *Kronecker product* which is also called *tensor product* or *direct product*. This product and the matrix are named after L. Kronecker, but Henderson, Pukelsheim and Searle presented that the first occurrence of such matrices was given by J. G. Zehfuss in 1858, see [68] and [144] respectively.

Definition 2.4. ([144]) Let $A = (a_{ij})$ be an $m \times n$ and $B = (b_{ij})$ be an $p \times q$ matrix over any field. Then the Kronecker product $A \otimes B := aijB$ of A and B is the $mp \times nq$ matrix given as follows:

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}$$

where $a_{ij}B$ denotes the $p \times q$ matrix obtained by multiplying each entry of B with a_{ij}.

In 1867, J. J. Sylvester in his paper [136], using the Kronecker product, recursively constructed the following matrices H_n of order 2^n over $\mathbb{R}$.

$$\mathsf{H}_0 = [1], \mathsf{H}_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

and

$$\mathsf{H}_n = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \mathsf{H}_{n-1} = \begin{bmatrix} \mathsf{H}_{n-1} & \mathsf{H}_{n-1} \\ \mathsf{H}_{n-1} & -\mathsf{H}_{n-1} \end{bmatrix}.$$

J. Hadamard, in his pioneering paper [56], studied the maximal determinant bound of the matrices whose entries are lying in the unit circle (i.e. complex numbers satisfying $|m_{ij}| \leq 1$) and proved the following inequality.

Theorem 2.11. *[56] Let M be a $n \times n$ matrix with complex entries satisfying $|m_{i,j}| \leq 1$. Then*

$$|det(M)| \leq n^{n/2}.$$

Following the inequality given in the above theorem, the matrices attaining the maximal determinant bound are called *Hadamard matrices* and can be defined as follows.

Definition 2.5. [56] An $n \times n$ matrix H with all entries 1 or -1 over $\mathbb{R}$ is called Hadamard matrix if the following holds.

$$HH^t = nI_n \ ,$$

or equivalently,

$$|det(H)| = n^{n/2} \ .$$

J. Hadamard constructed some examples, but more importantly he proved that H_n matrices of order 2^n constructed by Sylvester attains the maximal determinant bound. Therefore, H_n matrices of order 2^n matrices are called *Sylvester Hadamard matrices*. Hadamard also presented the necessary bound for the existence of Hadamard matrices, however sufficiency is still an open problem.

Conjecture 2.12 (Hadamard's Conjecture)**.** [110] There exists a Hadamard matrix of order $4n$ for all $n \in \mathbb{N}$.

Paley, who is first to state the above conjecture, using quadratic residues in finite fields gave a direct constructions of another family of Hadamard matrices [110]. Williamson, who is being first to use the term "Hadamard matrices" developed a number theoretic approach to construct another type of Hadamard matrices [141]. An enormous literature for both construction and applications of the Hadamard matrices now exists, see [1, 59, 69].

The constructions of Hadamard matrices lead to necessity of an equivalence relation in order to classify the Hadamard matrix families. In his seminal paper [57], Hall defined an equivalence relation between Hadamard matrices:

Definition 2.6. [57] Two Hadamard matrices of order n, H and H' are equivalent if H can be obtained from H' by any finite succession of the following operations:

- permuting rows;
- permuting columns;
- changing the sign of a row, i.e. multiplying a row by -1; or
- changing the sign of a column, i.e. multiplying a column by -1.

Indeed, permuting with or without sign change of the rows of the Hadamard matrix can be regarded as matrix multiplication PH of H with a monomial matrix $P \in \mathscr{S}_n^{\pm}$. Similarly, permuting with or without sign change of the columns of the Hadamard matrix can be regarded as matrix multiplication HQ of H with a monomial matrix $Q \in \mathscr{S}_n^{\pm}$ where $\mathscr{S}_n^{\pm}$ is the group of ± 1 monomial matrices of order n as defined and proved in Definition & Proposition 2.9.

Let us denote the set of all Hadamard matrices of order n by $\mathscr{H}_n$ for a moment. Then, we can define a map φ of the group $\mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm}$ on $\mathscr{H}_n$ as follows:

$$\begin{aligned} \varphi : (\mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm}) \times \mathscr{H}_n &\to \mathscr{H}_n \\ : ((P,Q),H) &\mapsto \varphi((P,Q),H) \\ \varphi((P,Q),H) &:= PHQ^{-1} \ , \end{aligned} \tag{2.2}$$

for all $H \in \mathscr{H}_n$ and for some $P,Q \in \mathscr{S}_n^{\pm}$.

Note that the map defined above does not hold for all $(P,Q) \in \mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm}$. Let us consider the subset G of $\mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm}$ such that

$$G := \{(P,Q) \in \mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm} \mid \varphi((P,Q),H) \in \mathscr{H}_n, \text{ for all } H \in \mathscr{H}_n\}, \tag{2.3}$$

where φ is as defined in (2.2).

Claim 2.13. *Let φ and G be as defined in (2.2) and (2.3), respectively. Then G is a subgroup of $\mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm}$.*

Proof. Trivially, $(\mathsf{I}_n, \mathsf{I}_n)$ is the identity element of the group $\mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm}$, constructed by the direct product of $\mathscr{S}_n^{\pm}$ with itself, and $\varphi((\mathsf{I}_n, \mathsf{I}_n), H) := \mathsf{I}_n H \mathsf{I}_n^{-1} = H$ for all $H \in \mathscr{H}_n$. Thus, G is non-empty. The closedness of G under the operation $\cdot$ as defined in (2.1) follows from definition of G. Hence, the statement now follows. □

Thus, now we can prove that φ actually defines an action of G on $\mathscr{H}_n$.

Lemma 2.14. *Let φ and G be as defined in (2.2) and (2.3), respectively. $\varphi : G \times \mathscr{H}_n \to \mathscr{H}_n$ is a (left) action of G on $\mathscr{H}_n$.*

Proof. For (I_n, I_n), the identity element of G we have $\varphi((I_n, I_n), H) := I_n H I_n^{-1} = H$ for all $H \in \mathscr{H}_n$. Let $(P_1, Q_1), (P_2, Q_2) \in G$, we have $(P_1, Q_1) \cdot (P_2, Q_2) = (P_1 \cdot P_2, Q_1 \cdot Q_2)$. Then,

$$\begin{aligned}((P_1, Q_1), ((P_2, Q_2), H)) &= ((P_1, Q_1), (P_2 H Q_2^{-1})) \\ &= P_1 (P_2 H Q_2^{-1}) Q_1^{-1} \\ &= (P_1 \cdot P_2) H (Q_2^{-1} \cdot Q_1^{-1}) \\ &= (P_1 \cdot P_2) H (Q_1 \cdot Q_2)^{-1} \\ &= (P_1 \cdot P_2) H (Q_1 \cdot Q_2)^{-1} \\ &= ((P_1 \cdot P_2, Q_1 \cdot Q_2), H) \\ &= (((P_1, Q_1) \cdot (P_2, Q_2)), H)\end{aligned}$$

Thus, the assertion follows. □

With abusing the notation, we will still denote G by $\mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm}$ and in what follows $\mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm}$ will be composed of elements for which (2.3) holds.

The equivalence relation given in Definition 2.6 can be associated to the action given in (2.2) and hence can be formalized as follows.

Definition 2.7. [57] Two Hadamard matrices H and H' of order n are said to be equivalent if there exists some monomial pair $(P, Q) \in \mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm}$ satisfying

$$H = P H' Q^{-1} \tag{2.4}$$

where the permutation and sign changes for the rows (resp. columns) is determined by P (resp. Q).

The orbits of the action of $\mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm}$ on $\mathscr{H}_n$ are then the *equivalence classes* under the relation (2.4). Furthermore, recall that the stabilizer of Hadamard matrix H of order n is the subgroup $(\mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm})_H$ satisfying

$$(\mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm})_H := \{(P, Q) \in \mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm} \mid H = P H Q^{-1}\} \ .$$

For a given Hadamard matrix H of order n, Hall calls the elements of $(\mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm})_H$ as the *automorphisms* of H and defines $(\mathscr{S}_n^{\pm} \times \mathscr{S}_n^{\pm})_H$ as the *automorphism group* of H, see [57]. Hereafter we will follow the same notion and denote the automorphism group of an Hadamard matrix H by $\mathsf{Aut}(H)$. A vast study on the equivalences and automorphism group now exists, for instance see [58, 76, 89, 73].

We conclude this section by we recalling and proving that $\mathsf{Aut}(\mathsf{H}_n)$ forms a group since our concern is limited to the Sylvester Hadamard matrices.

Definition & Proposition 2.15. [57] The direct product $\mathscr{S}_{2^n}^{\pm} \times \mathscr{S}_{2^n}^{\pm}$ acts on the set of Sylvester Hadamard matrices as $(P, Q)\mathsf{H}_n := P \mathsf{H}_n Q^{-1}$, where $P \in \mathscr{S}_{2^n}^{\pm}$ corresponding to signed row operations and $Q \in \mathscr{S}_{2^n}^{\pm}$ corresponding to signed column operations. Then for each Sylvester Hadamard matrix H_n, the stabiliser of H_n which is the subgroup of

$\mathscr{S}_{2^n}^{\pm} \times \mathscr{S}_{2^n}^{\pm}$ that fixes H_n is said to be the automorphism group of H_n and denoted by $\mathsf{Aut}(\mathsf{H}_n)$, i.e.,

$$\mathsf{Aut}(\mathsf{H}_n) = \{(P,Q) \in \mathscr{S}_{2^n}^{\pm} \times \mathscr{S}_{2^n}^{\pm} \mid P\mathsf{H}_n Q^{-1} = \mathsf{H}_n\}.$$

$\mathsf{Aut}(\mathsf{H}_n)$ forms a group under the operation $\cdot$ given by

$$(P_1,Q_1)\cdot(P_2,Q_2) := (P_1 \cdot P_2, Q_1 \cdot Q_2).$$

Proof. Follows directly from from Lemma 2.14. □

Here, either P or Q determines the other as follows:

$$P = \mathsf{H}_n Q \mathsf{H}_n^{-1} \quad .$$

2.4 Boolean Functions

A *Boolean function* f of n variables is a mapping from the n-dimensional $\mathbb{F}_2$–vector space to $\mathbb{F}_2$, i.e. $f : \{0,1\}^n \mapsto \{0,1\}$. The set of all Boolean functions of n variables is denoted by $\mathscr{F}_n$. There are different ways to represent Boolean functions, each of which give cryptographically valuable information. Unless otherwise stated explicitly, from now on a function will be a Boolean function.

2.4.1 Representations of Boolean functions

2.4.1.1 Truth Table

Usually, a Boolean function f is given by its *truth table* that is the ordered tuple of its values for all possible 2^n elements of $\mathbb{F}_2^n$. Such a tuple, denoted by T_f,

$$\mathsf{T}_f = (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$$

assumes lexicographic ordering of the $\mathbb{F}_2^n$ in a canonical way.

As an example, the 3 variable function given by the truth table $\mathsf{T}_f = (1,1,0,1,0,0,1,0)$ explained in Table 2.1.

In fact, the truth table of a n variable function can also be seen as an vector of length 2^n with elements belonging to $\mathbb{F}_2$. Since there exists only two possible values for each of 2^n different inputs, one can easily conclude that $\#(\mathscr{F}_n) = 2^{2^n}$. Each element of 2^n dimensional vector space, $\mathbb{F}_2^n$, can be also used to represent a unique Boolean function of n variable. Hence, considering the truth table representation, one can mention a one-to-one correspondence between $\mathscr{F}_n$ and $\mathbb{F}_2^{2^n}$. Due to the this one-to-one correspondence, naturally we can define *support*, *Hamming weight* and *Hamming distance* of a function as follows.

Table 2.1: 3 variable function truth table example

i	$\alpha_i = (a_1, a_2, a_3)$	$f(\alpha_i)$
0	$(0,0,0)$	1
1	$(0,0,1)$	1
2	$(0,1,0)$	0
3	$(0,1,1)$	1
4	$(1,0,0)$	0
5	$(1,0,1)$	0
6	$(1,1,0)$	1
7	$(1,1,1)$	0

Definition 2.8. The support $\mathsf{sup}(f)$ of a function $f \in \mathscr{F}_n$ is the set of input arguments which has nonzero values in the truth table, i.e.

$$\mathsf{sup}(f) = \{\alpha \in \mathbb{F}_2^n \mid f(\alpha) = 1\} \ . \tag{2.5}$$

Definition 2.9. [60] The Hamming weight $\mathsf{w}(f)$ of $f \in \mathscr{F}_n$ is the number of its nonzero values, so

$$\mathsf{w}(f) = \#(\mathsf{sup}(f)) \ . \tag{2.6}$$

Definition 2.10. [60] The Hamming distance $\mathsf{d}(f,g)$ between f and g on $\mathscr{F}_n$ is the number of values in which they differ, hence

$$\mathsf{d}(f,g) = \mathsf{w}(f \oplus g) = \sum_{\alpha \in \mathbb{F}_2^n} f(\alpha) \oplus g(\alpha) \ , \tag{2.7}$$

where the last equation is "par abus de notation" by identifying $1 \in \mathbb{F}_2$ with $1 \in \mathbb{R}$.

In practical cryptosystems, one of the dominant design criterion is *balancedness*, which can be stated as follows.

Definition 2.11. A Boolean function $f \in \mathscr{F}_n$ is said to be balanced if $\mathsf{w}(f) = 2^{n-1}$.

We denote the set of all balanced functions by $\mathscr{E}_n$. The number of all balanced functions is $\binom{2^n}{2^{n-1}}$.

2.4.1.2 Signed Sequence

In some cases, instead of representing the truth table of a function by $\{0,1\}$, it would be more useful to represent by $\{1,-1\}$. Before going further, we will recall the underlying fact that enables us to go forth and back between the $\{0,1\}$-additive group and the $\{1,-1\}$multiplicative group.

Definition 2.12. Let $(\mathbb{F}_2,+)$ denote the additive group of $\mathbb{F}_2$. An *additive character* of $(\mathbb{F}_2,+)$ is a homomorphism $\chi : (\mathbb{F}_2,+) \to \mathbb{C}^*$ from $(\mathbb{F}_2,+)$ to the multiplicative group of the field of complex numbers $\mathbb{C}^*$.

Table 2.2: 3 variable function sequence example

i	$\alpha_i = (a_1, a_2, a_3)$	$f(\alpha_i)$	$\chi_f(\alpha_i)$
0	$(0,0,0)$	1	-1
1	$(0,0,1)$	1	-1
2	$(0,1,0)$	0	1
3	$(0,1,1)$	1	-1
4	$(1,0,0)$	0	1
5	$(1,0,1)$	0	1
6	$(1,1,0)$	1	-1
7	$(1,1,1)$	0	1

Since $(\mathbb{F}_2, +)$ is a finite group of order 2, all of the characters of $(\mathbb{F}_2, +)$ takes values from the set $\{z \in \mathbb{C} \mid z^2 = 1\}$ of the 2^{nd} (square) roots of unity in $\mathbb{C}$. Indeed, there exist only two additive characters of $(\mathbb{F}_2, +)$ which can be defined as:

- The trivial group homomorphism $\chi_0(a) := (1)^a$, i.e. $\chi_0 : a \mapsto 1$,
- the only non-trivial group homomorphism $\chi(a) := (-1)^a$, i.e. $\chi : a \mapsto (-1)^a$.

Now, we can define the *sign function* or *character form*

$$\chi_f(.) := \chi \cdot f : \mathbb{F}_2^n \to \mathbb{R}^* \subseteq \mathbb{C}^*$$

of a function $f \in \mathscr{F}_n$ as

$$\chi_f : \alpha \mapsto (-1)^{f\alpha)} \quad . \tag{2.8}$$

For two functions $f, g \in \mathscr{F}_n$ the following holds.

$$\begin{aligned} \chi_{f \oplus g}(\alpha) &= (-1)^{f(\alpha)}(-1)^{g(\alpha)} = \chi_f \chi_g \\ 2\chi_{fg} &= 1 + \chi_f + \chi_g - \chi_f \chi_g \end{aligned} \tag{2.9}$$

Then the truth table of the sign function of a function $f \in \mathscr{F}_n$, denoted by ζ_f,

$$\begin{aligned} \zeta_f &= (\chi_f(\alpha_0), \chi_f(\alpha_1), \ldots, \chi_f(\alpha_{2^n-1})) \\ &= ((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})}) \end{aligned} \tag{2.10}$$

is called the *sequence* or *polarity truth table* of f.

Continuing with the previous example, the 3 variable function given by the sequence $\zeta_f = (-1,-1,1,-1,1,1,-1,1)$ explained in Table 2.2.

The Hamming distance can also be computed by using the sequences of the functions as follows.

Lemma 2.16. *[123] Let $f,g \in \mathscr{F}_n$ be any functions. Then we have*

$$\mathsf{d}(f,g) = 2^{n-1} - \frac{1}{2}\left\langle \zeta_f, \zeta_g \right\rangle \tag{2.11}$$

where $\left\langle \zeta_f, \zeta_g \right\rangle$ denotes the standart inner product over $\mathbb{R}$.

Proof. Observe that

$$\begin{aligned}\left\langle \zeta_f, \zeta_g \right\rangle &= (2^n - \#(\mathsf{sup}(f \oplus g))) - \#(\mathsf{sup}(f \oplus g)) \\ &= 2^n - 2\#(\mathsf{sup}(f \oplus g)).\end{aligned}$$

Since $\mathsf{d}(f,g) = \#(\mathsf{sup}(f \oplus g))$, we get

$$2\mathsf{d}(f,g) = 2^n - \left\langle \zeta_f, \zeta_g \right\rangle \quad .$$

Now the assertion follows. □

2.4.1.3 Algebraic Normal Form

Let us denote the multi-variate polynomial ring over $\mathbb{F}_2$ by $\mathbb{F}_2[x_1, x_2, \ldots, x_n]$ with $x := (x_1, x_2, \ldots, x_n)$ being n–tuple of indeterminates. It is easy to construct a surjective homomorphism

$$\mathbb{F}_2[x_1, x_2, \ldots, x_n] \to \mathscr{F}_n \quad .$$

Since for any $a \in \mathbb{F}_2$ we have $a^2 = a$, all the polynomials

$$x_1^2 \oplus x_1, x_2^2 \oplus x_2, \ldots, x_n^2 \oplus x_n$$

and also the ideal they generate

$$(x_1^2 \oplus x_1, x_2^2 \oplus x_2, \ldots, x_n^2 \oplus x_n)$$

all lie in the kernel of the above homomorphism.

Then, the induced homomorphism

$$\mathbb{F}_2[x_1, x_2, \ldots, x_n]/(x_1^2 \oplus x_1, x_2^2 \oplus x_2, \ldots, x_n^2 \oplus x_n) \to \mathscr{F}_n$$

is also be surjective.

Each polynomial in $\mathbb{F}_2[x_1, x_2, \ldots, x_n]/(x_1^2 \oplus x_1, x_2^2 \oplus x_2, \ldots, x_n^2 \oplus x_n)$ can be written as a linear combination of the monomials of degree less than 1 in each x_i, $i = 1, 2, \ldots, n$.

Since, there exists 2^n monomials, i.e. $x^I := x_{i_1} x_{i_2} \cdots x_{i_r}$ for any subsets

$$I := \{i_1, i_2, \ldots, i_r\} \subseteq \{1, 2, \ldots, n\},$$

this induced homomorphism

$$\mathbb{F}_2[x_1, x_2, \ldots, x_n]/(x_1^2 \oplus x_1, x_2^2 \oplus x_2, \ldots, x_n^2 \oplus x_n) \to \mathscr{F}_n$$

is in fact an isomorphism. Hence,

Proposition 2.17. *[145] Every n variable Boolean function f can be uniquely written as a multi-variate polynomial defined in $\mathbb{F}_2[x_1,x_2,\ldots,x_n]/(x_1^2\oplus x_1,x_2^2\oplus x_2,\ldots,x_n^2\oplus x_n)$, that is,*

$$\begin{aligned} f(x_1,x_2,\ldots,x_n) &= \bigoplus_{I\subseteq\{1,2,\ldots,n\}} c_I x^I \\ &= \bigoplus_{I\subseteq\{1,2,\ldots,n\}} c_I \prod_{i\in I} x_i \\ &= \bigoplus_{\alpha=(a_1,a_2,\ldots,a_n)\in\mathbb{F}_2^n} c_\alpha x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \end{aligned}$$

where c_i's belonging to $\mathbb{F}_2$.

In the cryptographic literature, representing Boolean function with algebraic normal formal mostly credited to Jansen [74]. In switching theory and coding theory studies cites to work of Reed [115] and Muller [105] and refer as *Reed-Muller expansion* or *positivy polarty Reed–Muller form* of Boolean functions. However above all, in [119] and [112, p. 223], it is mentioned that algebraic normal form was actually first introduced and used by Zhegalkin [145].

Explicitly, algebraic normal form of a function f can be written as follows,

$$\begin{aligned} f(x_1,x_2,\ldots,x_n) =& c_0\oplus c_1x_1\oplus\cdots\oplus c_nx_n \\ & \oplus c_{12}x_1x_2\oplus\cdots c_{n-1n}x_{n-1}x_n \\ & \vdots \\ & \oplus c_{12\cdots n}x_1x_2\cdots x_n \end{aligned} \tag{2.12}$$

or, in a short form, A_f , by considering the coefficients with regarding the lexicographical ordering, i.e

$$\mathsf{A}_f = (c_0,c_n,c_{n-1},c_{n-1n},c_{n-2},c_{n-2n},c_{n-2n-1},c_{n-2n-1n},c_{n-3},\ldots,c_{12\ldots n}).$$

Considering the previous example, the 3 variable function given by its algebraic normal form $f(x_1,x_2,\ldots,x_n) = 1\oplus x_1\oplus x_2\oplus x_2x_3$, explained in Table 2.3.

Definition 2.13. Let f be an n variable Boolean function, then *algebraic normal transform* or *Reed-Muller transform* is a linear transformation with respect to $\mathbf{F}_2$ addition which is defined as

$$[\mathsf{A}_f] = \mathsf{A}_n\cdot[\mathsf{T}_f]$$

where A_n defined over $\mathbb{F}_2$ satisfies the following.

$$\mathsf{A}_0=[1],\ \mathsf{A}_n=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}\otimes\mathsf{A}_{n-1}=\begin{bmatrix}\mathsf{A}_{n-1} & 0\\ \mathsf{A}_{n-1} & \mathsf{A}_{n-1}\end{bmatrix}.$$

It can be easily proved that $\mathsf{A}_n^2 = I_{2^n}$ which leads that this transformation is in fact an involution:

$$[\mathsf{T}_f] = \mathsf{A}_n\cdot[\mathsf{A}_f].$$

Table 2.3: 3 variable function algebraic normal form example

i	$I \subseteq \{1,2,3\}$	monomial	$\alpha \in \mathbb{F}_2^n$	$[\mathsf{T}_f]$	$[\zeta_f]$	$[\mathsf{A}_f]$
0	$\emptyset$	1	$(0,0,0)$	1	-1	1
1	$\{3\}$	x_3	$(0,0,1)$	1	-1	0
2	$\{2\}$	x_2	$(0,1,0)$	0	1	1
3	$\{2,3\}$	x_2x_3	$(0,1,1)$	1	-1	1
4	$\{1\}$	x_1	$(1,0,0)$	0	1	1
5	$\{1,3\}$	x_1x_3	$(1,0,1)$	0	1	0
6	$\{1,2\}$	x_1x_2	$(1,1,0)$	1	-1	0
7	$\{1,2,3\}$	$x_1x_2x_3$	$(1,1,1)$	0	1	0

Definition 2.14. The degree of the algebraic normal form of a function f is called the *algebraic degree* or *degree* of f and is denoted by $\deg(f)$.

The degree of a Boolean function is also defined as *nonlinear order* of Boolean functions due to its importance in stream ciphers cryptanalysis, see [81, 132, 102, 109].

Obviously, we have $\deg(f) \leq n$. In particular, the functions having $\deg(f) \leq 1$ are considered to be *weak* are called the *affine functions*:

A function $\ell \in \mathscr{F}_n$ satisfying

$$\ell(\alpha \oplus \beta) = \ell(\alpha) \oplus \ell(\beta)$$

for all $\alpha, \beta \in \mathbb{F}_2^n$ is called *linear function* that is of the form

$$\ell(x) = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n \text{ for some } a_i \in \mathbb{F}_2 \ .$$

Indeed, by letting $\alpha = (a_1, a_2, \ldots, a_n)$ and $x = (x_1, x_2, \ldots, x_n)$, every linear function can be written as a standard inner product with a fixed vector as

$$\ell_\alpha(x) := \langle x, \alpha \rangle = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n \ . \tag{2.13}$$

We will use ℓ_α or ℓ_ω to denote any linear function, and ℓ_{α_i} or ℓ_i to denote the linear function $\ell_{\alpha_i}(x) = \langle x, \alpha_i \rangle$. Furthermore, We denote the set of all linear functions by $\mathscr{L}_n$ and we have $\#(\mathscr{L}_n) = 2^n$.

In a similar way, a function $\ell \in \mathscr{F}_n$ satisfying

$$\ell(\alpha \oplus \beta) = \ell(\alpha) \oplus \ell(\beta) \oplus \ell(\alpha_0)$$

for all $\alpha, \beta \in \mathbb{F}_2^n$ is called *affine function* that can be written as

$$\ell_{\alpha,a}(x) := \langle x, \alpha \rangle \oplus a = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n \oplus a \ . \tag{2.14}$$

We denote the set of all affine functions by $\mathscr{A}_n$ and additionally we $\#(\mathscr{A}_n) = 2^{n+1}$.

Indeed, we the sequence of the linear functions constructs the Sylvester Hadamard matrices as follows.

Lemma 2.18. *[123] The rows and columns of the Sylvester Hadamard matrix H_n are the sequence of the linear functions respectively regarding the lexicographic order, that is*

$$H_n = \left[\zeta_{\ell_0}\ \zeta_{\ell_1}\ \cdots\ \zeta_{\ell_{2^n-1}}\right] \tag{2.15}$$

or, equivalently

$$H_n = \begin{bmatrix} \zeta_{\ell_0} \\ \zeta_{\ell_1} \\ \vdots \\ \zeta_{\ell_{2^n-1}} \end{bmatrix} \tag{2.16}$$

Aside from the given above, it is also possible to use following function representations;

– *Univariate polynomial*:
By fixing bases $(\beta_1, \beta_2, \ldots, \beta_n)$ for the field $\mathbb{F}_{2^n}$, one can construct an group isomorphism between the vector space $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$, with representing an element of $x \in \mathbb{F}_2^n$ as $x_1\beta_1 + x_2\beta_2 + \cdots + x_n\beta_n \in \mathbb{F}_{2^n}$. Then, since $\mathbb{F}_2$ is the base field of $\mathbb{F}_{2^n}$ it is also possible to represent a Boolean function as a *univariate polynomial* in $\mathbb{F}_{2^n}[x]$ of degree at most $2^n - 1$:

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

where $\kappa_i \in \mathbb{F}_{2^n}$, [24, 15].

– *Absolute trace function*:
The *absolute trace function* from $\mathbb{F}_{2^n}$ to the base field $\mathbb{F}_2$,

$$tr(x) = x + x^2 + x^{2^2} + \cdots x^{2^{n-1}}.$$

Any Boolean function can be also represented, but not uniquely, as follows,

$$tr(\sum_{i=0}^{2^n-1} \kappa_i x^i).$$

where $\kappa_i \in \mathbb{F}_{2^n}$, [24, p. 265–268].

– *Numerical Normal Form (NNF)*:
Instead of the quotient ring $\mathbb{F}_2[x_1, x_2, \ldots, x_n]/(x_1^2 \oplus x_1, x_2^2 \oplus x_2, \ldots, x_n^2 \oplus x_n)$ as in ANF case, by considering the $\mathbb{R}[x_1, x_2, \ldots, x_n]/(x_1^2 - x_1, x_2^2 - x_2, \ldots, x_n^2 - x_n)$ or $\mathbb{Z}[x_1, x_2, \ldots, x_n]/(x_1^2 - x_1, x_2^2 - x_2, \ldots, x_n^2 - x_n)$, it is also possible to represent a Boolean function over reals or integers, such representation is called *numerical normal form (NNF)*, see [27].

– *Cayley Map*:
Bernasconi and Codenotti proposed another unique representation of Boolean functions, that associates the function with mimicked Cayley graph, [29]. Any n variable function f can be given by the Cayley graph $G_f = G(\mathbb{F}_2^n, \mathsf{sup}(f))$, $\mathbb{F}_2^n$ being its vertex set and $\{(\alpha,\beta) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid \alpha \oplus \beta \in \mathsf{sup}(f)\}$ being its edge set [7].

– *Karnaugh map*:
In 1953, Karnaugh introduced the *Karnaugh map* where instead of an 2^n ordered tuple, output values are written onto the cells of an two-dimensional grid whose cells are indexed in Gray code [77].

2.4.2 Walsh Transform

Recall that, based on the non-trivial additive character of $(\mathbb{F}_2, +)$, the character form of each linear functions is given by

$$\chi_{\ell_\omega}(\alpha) := (-1)^{\langle \alpha, \omega \rangle}$$

for all $\omega \in \mathbb{F}_2^n$. These are also called *Fourier kernel or basis function*, see [90]. Further we have the following proposition.

Proposition 2.19. *[90, 88] The set (also known as the* character group of $\mathbb{F}_2^n$*)*

$$\{\chi_{\ell_\omega} \mid \ell_\omega \in \mathscr{L}_2^n\} := \{(-1)^{\langle x, \omega \rangle} \mid \omega \in \mathbb{F}_2^n\}$$

forms an orthogonal basis for space of all complex-valued functions defined from $\mathbb{F}_2^n$ *into* $\mathbb{C}^*$.

Proposition 2.19 actually tells us that using the non-trivial additive character χ, one can construct a group homomorphism from $\mathbb{F}_2^n$ to the direct product of n replicas of the multiplicative subgroup $\{\pm 1\}$ of $\mathbb{C}^*$. From which, now we can define a special case of the *discrete Fourier transform* as follows.

Definition 2.15. [137, 78] The Walsh transform W_f of a function $f : \mathbb{F}_2^n \to \mathbb{R} \leq \mathbb{C}$ is defined as

$$\mathsf{W}_f(\omega) := \sum_{x \in \mathbb{F}_2^n} \chi_f \chi_{\ell_\omega} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, \omega \rangle} \tag{2.17}$$

and the inverse Walsh transform is

$$\chi_f(x) := 2^{-n} \sum_{\omega \in \mathbb{F}_2^n} \mathsf{W}_f(\omega) \chi_{\ell_x} = 2^{-n} \sum_{\omega \in \mathbb{F}_2^n} \mathsf{W}_f(\omega) (-1)^{\langle \omega, x \rangle} \quad . \tag{2.18}$$

Naming convention for the above transformations has not been settled yet and *Walsh transform, Walsh Hadamard transform, discrete Fourier transform, abstract Fourier*

transform are also used[2]. Sometimes, instead of the character form, by embedding $\mathbb{F}_2$ into $\mathbb{R}$ and abusing the notation, the function itself is used as follows:

$$\mathsf{F}_f(\omega) := \sum_{x\in\mathbb{F}_2^n} f(x)\chi_{\ell_\omega} = \sum_{x\in\mathbb{F}_2^n} f(x)(-1)^{\langle x,\omega\rangle}$$

and the inverse Walsh transform is

$$f(x) := 2^{-n} \sum_{\omega\in\mathbb{F}_2^n} \mathsf{F}_f(\omega)\chi_{\ell_x} = 2^{-n} \sum_{\omega\in\mathbb{F}_2^n} \mathsf{F}_f(\omega)(-1)^{\langle \omega,x\rangle} \ ,$$

see [143, 50]. Nevertheless for both cases, it is easy to relate each other as given [50, Lemma 1]:

$$\mathsf{W}_f(\omega) = -2\mathsf{F}_f(\omega) + 2^n\delta(\omega) \tag{2.19}$$

or equivalently

$$\mathsf{F}_f(\omega) = 2^{n-1}\delta(\omega) - \frac{1}{2}\mathsf{W}_f(\omega) \ , \tag{2.20}$$

where $\delta(\omega)$ is *Kronecker delta function* defined as

$$\delta(\omega) = \begin{cases} 1 & \text{for } \omega = 0 \\ 0 & \text{otherwise.} \end{cases} \tag{2.21}$$

The lexicographically ordered 2^n tuple

$$\mathsf{W}_f = (\mathsf{W}_f(\alpha_0), \mathsf{W}_f(\alpha_1), \ldots, \mathsf{W}_f(\alpha_{2^n-1}))$$

is comprised of the Walsh transform values of a function f is called *Walsh spectrum* of f. Moreover, when we write the Walsh spectrum explicitly, we get

$$\begin{aligned} \mathsf{W}_f &= (\chi_f(\alpha_0), \chi_f(\alpha_1), \ldots, \chi_f(\alpha_{2^n-1}))[\zeta_{\ell_{\alpha_0}}\ \zeta_{\ell_{\alpha_1}}\ \ldots\ \zeta_{\ell_{\alpha_{2^n-1}}}] \\ &= \zeta_f[\zeta_{\ell_{\alpha_0}}\ \zeta_{\ell_{\alpha_1}}\ \ldots\ \zeta_{\ell_{\alpha_{2^n-1}}}] \end{aligned}$$

and taking the result of Lemma 2.18 into account,

$$\mathsf{W}_f = \zeta_f \mathsf{H}_n, \tag{2.22}$$

and for inverse Walsh transform

$$\zeta_f = 2^{-n}\mathsf{W}_f\mathsf{H}_n \ . \tag{2.23}$$

Continuing with the previous example, the 3 variable function given by its Walsh spectrum $\mathsf{W}_f = (0,0,0,0,-4,4,-4,-4)$, explained in Table 2.4.

The naive method for computing the Walsh transform would require 2^{2n} complexity. However, the pioneering work of Cooley and Tukey lead to an efficient algorithm called *fast Fourier transform* see [31]. Later Brown presented a recursive *fast Walsh transform* [19]. Both of these algorithms reduce the complexity to $n2^n$.

[2] Following the [24], we use "Walsh transform" for the transform of the character form and "discrete Fourier transform" for the transform of the function itself.

Table 2.4: 3 variable function Walsh spectrum example

i	$I \subseteq \{1,2,3\}$	monomial	$\alpha \in \mathbb{F}_2^n$	$[\mathsf{T}_f]$	$[\zeta_f]$	$[\mathsf{A}_f]$	$[\mathsf{W}_f]$
0	$\emptyset$	1	$(0,0,0)$	1	-1	1	0
1	$\{3\}$	x_3	$(0,0,1)$	1	-1	0	0
2	$\{2\}$	x_2	$(0,1,0)$	0	1	1	0
3	$\{2,3\}$	x_2x_3	$(0,1,1)$	1	-1	1	0
4	$\{1\}$	x_1	$(1,0,0)$	0	1	1	-4
5	$\{1,3\}$	x_1x_3	$(1,0,1)$	0	1	0	4
6	$\{1,2\}$	x_1x_2	$(1,1,0)$	1	-1	0	-4
7	$\{1,2,3\}$	$x_1x_2x_3$	$(1,1,1)$	0	1	0	-4

2.4.3 Cryptographic Properties

Let $f \in \mathscr{F}_n$ in the following definitions and propositions.

We have already defined the balancedness property of Boolean functions, which is one of basic and most wanted property in practical crypto schemes.

Proposition 2.20. *f is balanced, i.e. $f \in \mathscr{E}_n$, if and only if $\mathsf{W}_f(\alpha_0) = 0$.*

Proof.

$$\begin{aligned}\mathsf{W}_f(\alpha_0) &= \sum_{x\in\mathbb{F}_n} (-1)^{f(x)\oplus\langle x,\alpha_0\rangle} \\ &= \sum_{x\in\mathbb{F}_n} (-1)^{f(x)} \\ &= 2^n - 2\#(\mathsf{sup}(f))\end{aligned}$$

by definition f is balanced if $\#(\mathsf{sup}(f)) = 2^{n-1}$.

Hence the assertion now follows. □

In order to resist correlation attacks and linear cryptanalysis, f should possess higher nonlinearity. Nonlinearity of a function is defined as follows.

Definition & Proposition 2.21. [111, 102] The *nonlinearity* N_f of a function f is its distance to the nearest affine function and it can be expressed by the Walsh transform of f as follows:

$$\begin{aligned}\mathsf{N}_f &:= \min_{\ell_{\alpha,a}\in\mathscr{A}_n} \mathsf{d}(f,\ell_{\alpha,a}) \\ &:= 2^{n-1} - \frac{1}{2}\max_{\omega\in\mathbb{F}_2^n} \left|\mathsf{W}_f(\omega)\right| \quad .\end{aligned} \tag{2.24}$$

where $\left|\mathsf{W}_f(\omega)\right|$ is the absolute value of $\mathsf{W}_f(\omega)$.

Proof. First note that

$$\zeta_{\ell_{\alpha,1}} = -\zeta_{\ell_{\alpha,0}} = -\zeta_{\ell_\alpha} \ .$$

By Lemma 2.16, Lemma 2.18 and Equation 2.22, we have

$$\begin{aligned} \mathsf{d}(f, \ell_\alpha) &= 2^{n-1} - \frac{1}{2} \left\langle \zeta_f, \zeta_{\ell_\alpha} \right\rangle \\ &= 2^{n-1} - \frac{1}{2} \mathsf{W}_f(\alpha) \end{aligned}$$

Combining these two relations leads to the assertion. □

Meier and Staffelbach [102] were the first to recognize that the set of functions with maximum nonlinearity was identical to the set of bent functions.

Definition 2.16. [118] A Boolean function f is called bent function if all the Walsh coefficients of W_f are $\pm 2^{n/2}$.

Rothaus further proved that bent functions only exist for even number of variables and the degree of their algebraic normal form is always bounded above by $n/2$. When exists, we will denote the set comprised of bent functions by $\mathscr{B}_n$.

Since, in this study we mainly focus on nonlinearity and Hamming weight criteria, we will not include the other design criteria. However, for any further reading please refer to

- [132] for *correlation immunity* and *resiliency*,
- [140] for *strict avalanche criterion*,
- [114] for *propagation criterion*,
- [111] for *nonlinearity*,
- [101] for *algebraic immunity*,
- [24] for other criteria,

CHAPTER 3

NONLINEARITY PRESERVING PERMUTATIONS

In this chapter, we first define the representation for the bijective mappings group, more formally $\mathscr{S}_{2^{2^n}}$, and its action on $\mathscr{F}_n$. We then analyze the nonlinearity preserving ones among these mappings.

Any mapping $\psi : \mathbb{F}_2^{2^n} \to \mathbb{F}_2^{2^n}$ can be written as

$$\psi : (x) \mapsto (\psi_1(x), \psi_2(x), \psi_3(x) \ldots, \psi_{2^n}(x)),$$

more explicitly as,

$$\psi : (x_1, x_2, x_3, \ldots, x_{2^n}) \mapsto (\psi_1(x_1, x_2, \ldots, x_{2^n}), \ldots, \psi_{2^n}(x_1, x_2, \ldots, x_{2^n})),$$

or,

$$\psi : [x] \mapsto \begin{bmatrix} \psi_1(x_1, x_2, \ldots, x_{2^n})) \\ \psi_2(x_1, x_2, \ldots, x_{2^n})) \\ \vdots \\ \psi_{2^n}(x_1, x_2, \ldots, x_{2^n})) \end{bmatrix}, \tag{3.1}$$

where each $\psi_i : \mathbb{F}_2^{2^n} \to \mathbb{F}_2$ is a 2^n variable Boolean function called *coordinate function* of ψ. Hence based on (2.12), each ψ_i's can be represented by its algebraic normal form uniquely;

$$\psi_i(x_1, x_2, \cdots, x_{2^n}) = c_0^{(i)} \oplus c_1^{(i)} x_1 \oplus \ldots \oplus c_{12\cdots 2^n}^{(i)} x_1 x_2 \cdots x_{2^n} \ . \tag{3.2}$$

Then, by porting (3.2) into (3.1), we get

$$\psi : [x] \mapsto \begin{bmatrix} c_0^{(1)} \oplus & c_1^{(1)} x_1 \oplus & \ldots \oplus & c_{12\cdots 2^n}^{(1)} x_1 x_2 \cdots x_{2^n} \\ c_0^{(2)} \oplus & c_1^{(2)} x_1 \oplus & \ldots \oplus & c_{12\cdots 2^n}^{(2)} x_1 x_2 \cdots x_{2^n} \\ & & \vdots & \\ c_0^{(2^n)} \oplus & c_1^{(2^n)} x_1 \oplus & \ldots \oplus & c_{12\cdots 2^n}^{(2^n)} x_1 x_2 \cdots x_{2^n} \end{bmatrix} . \tag{3.3}$$

By decomposing into an explicit form, we can re-write 3.3 as

$$\psi : [x] \mapsto \Bigg(\underbrace{\begin{bmatrix} c_0^{(1)} \\ c_0^{(2)} \\ \vdots \\ c_0^{(2^n)} \end{bmatrix}}_{[\lambda_0]} \oplus \underbrace{\begin{bmatrix} c_1^{(1)} \\ c_1^{(2)} \\ \vdots \\ c_1^{(2^n)} \end{bmatrix}}_{[\lambda_1]} x_1 \oplus \cdots \oplus \underbrace{\begin{bmatrix} c_{2^n}^{(1)} \\ c_{2^n}^{(2)} \\ \vdots \\ c_{2^n}^{(2^n)} \end{bmatrix}}_{[\lambda_{2^n}]} x_{2^n} \oplus \underbrace{\begin{bmatrix} c_{12}^{(1)} \\ c_{12}^{(2)} \\ \vdots \\ c_{12}^{(2^n)} \end{bmatrix}}_{[\lambda_{12}]} x_1 x_2 \oplus$$

$$\underbrace{\begin{bmatrix} c_{13}^{(1)} \\ c_{13}^{(2)} \\ \vdots \\ c_{13}^{(2^n)} \end{bmatrix}}_{[\lambda_{13}]} x_1 x_3 \oplus \cdots \oplus \underbrace{\begin{bmatrix} c_{123}^{(1)} \\ c_{123}^{(2)} \\ \vdots \\ c_{123}^{(2^n)} \end{bmatrix}}_{[\lambda_{123}]} x_1 x_2 x_3 \oplus \cdots \oplus \underbrace{\begin{bmatrix} c_{12\cdots 2^n}^{(1)} \\ c_{12\cdots 2^n}^{(2)} \\ \vdots \\ c_{12\cdots 2^n}^{(2^n)} \end{bmatrix}}_{[\lambda_{12\cdots 2^n}]} x_1 x_2 \cdots x_{2^n} \Bigg) ,$$

and now, equivalently we have

$$\begin{aligned} \psi : [x] \mapsto & \lambda_0 \oplus M[x] \oplus [\lambda_{12}] x_1 x_2 \oplus \cdots \oplus [\lambda_{(2^n-1)2^n}] x_{2^n-1} x_{2^n} \\ & \oplus [\lambda_{123}] x_1 x_2 x_3 \oplus \cdots \oplus [\lambda_{(2^n-2)(2^n-1)2^n}] x_{2^n-2} x_{2^n-1} x_{2^n} \\ & \vdots \\ & \oplus [\lambda_{12\cdots 2^n}] x_1 x_2 \cdots x_{2^n} \end{aligned} \tag{3.4}$$

where

- $x = (x_1, x_2, \ldots, x_{2^n}) \in \mathbb{F}_2^{2^n}$ hence each $x_i \in \mathbb{F}_2$,
- $\lambda_j \in \mathbb{F}_2^{2^n}$ with each $c_j^i \in \mathbb{F}_2$,
- M is the $2^n \times 2^n$ matrix whose column form is $M = [[\lambda_1]\ [\lambda_2]\ \ldots\ [\lambda_{2^n}]]$.

Let the notations be as above and for a moment denote the set of all bijective mappings defined from $\mathbb{F}_2^{2^n}$ onto itself by G. In fact, G has exactly $2^{2^n}!$ elements and it is easy to verify that G associated with the composition of mappings operation satisfies the group axioms. That is,

Fact 3.1. *G forms a group with the group law being composition of mappings and the identity element 1_G of G is the identity mapping under which each element of $\mathbb{F}_2^{2^n}$ is mapped to itself.*

Based on Definition 2.1, we can define an action of G on $\mathbb{F}_2^{2^n}$ which leads to a homomorphism from G into the symmetric group of $\mathbb{F}_2^{2^n}$ such that $\psi \mapsto \pi_\psi$ where $\psi \in G$ and $\pi_\psi \in Sym(\mathbb{F}_2^{2^n})$. Then,

Claim 3.2. *G is isomorphic to $\mathscr{S}_{2^{2^n}}$.*

Proof. Immediately follows from Theorem 2.3 and $\#(\mathscr{S}_{2^{2^n}}) = \#(G) = 2^{2^n}!$ □

Hereafter, we will use $\mathscr{S}_{2^{2^n}}$ instead of G to denote the bijective mappings acting on $\mathbb{F}_2^{2^n}$.

The number of n variable Boolean functions is 2^{2^n}, i.e. $\#(\mathscr{F}_n) = 2^{2^n}$. Each of these functions has unique $\{0,1\}$ valued 2^n ordered tuple called the truth table. Hence, it is possible to regard the truth tables of n variable functions as elements of the 2^n dimensional $\mathbb{F}_2$–vector space $\mathbb{F}_n^{2^n}$. This process in fact gives us a one-to-one correspondence between $\mathscr{F}_n$ and $\mathbb{F}_n^{2^n}$. In what follows, we will regard $\mathscr{F}_n$ as $\mathbb{F}_n^{2^n}$ and mostly consider the truth tables of the functions. Therefore, the aforementioned definitions and notions in this chapters also holds for any f in $\mathscr{F}_n$ and (3.4) can be re-written as follow.

$$\begin{aligned}\psi : [\mathsf{T}_f] \mapsto & \lambda_0 \oplus M[\mathsf{T}_f] \oplus [\lambda_{12}] f(\alpha_0) f(\alpha_1) \oplus \cdots \oplus [\lambda_{(2^n-1)2^n}] f(\alpha_{2^n-2}) f(\alpha_{2^n-1}) \oplus \\ & [\lambda_{123}] f(\alpha_0) f(\alpha_1) f(\alpha_3) \oplus \cdots \oplus [\lambda_{(2^n-2)(2^n-1)2^n}] f(\alpha_{2^n-3}) f(\alpha_{2^n-2}) f(\alpha_{2^n-1}) \\ & \vdots \\ & \oplus [\lambda_{12\cdots 2^n}] f(\alpha_0) f(\alpha_1) \cdots f(\alpha_{2^n})\end{aligned} \tag{3.5}$$

where

- $\mathsf{T}_f = (f(\alpha_0) f(\alpha_1) \cdots f(\alpha_{2^n})) \in \mathbb{F}_2^{2^n}$ hence each $f(\alpha_i) \in \mathbb{F}_2$,
- $\lambda_j := \mathsf{T}_{h_j} \in \mathbb{F}_2^{2^n}$ for some $h_j \in \mathscr{F}_n$,
- M is the $2^n \times 2^n$ matrix whose column form is $M = [[\lambda_1]\ [\lambda_2]\ \ldots\ [\lambda_{2^n}]]$.

The action of $\mathscr{S}_{2^{2^n}}$ on $\mathscr{F}_n$ is a map from $\mathscr{S}_{2^{2^n}} \times \mathscr{F}_n \to \mathscr{F}_n$ such that $(\psi, f) \mapsto \psi f$. We will use interchangeably ψf, ψ_f or $\psi(f)$ to denote the image of (ψ, f).

We now focus on some of the subgroups (also called permutation groups) of $\mathscr{S}_{2^{2^n}}$. The subgroups of $\mathscr{S}_{2^{2^n}}$, that are studied or considered in this thesis, are illustrated in Figure 3.1 as a lattice of subgroups. Note that Figure 3.1 does not present a comprehensive list of subgroups of $\mathscr{S}_{2^{2^n}}$. For instance, see [135] for the subgroups of $\mathscr{S}_{2^n}$.

Let $f \in \mathscr{F}_n$, we have the following definitions for the subgroups of $\mathscr{S}_{2^{2^n}}$ that will be considered in our study.

- The identity mapping 1_G that maps each element to itself.
- *Translations of input variables ($\mathscr{T}_n$)*:
  ψ belongs to $\mathscr{T}_n$ if for all $f \in \mathscr{F}_n$, it can be given in the form $\psi : f(x) \mapsto f(x \oplus \alpha)$ for some $\alpha \in \mathbb{F}_2^n$. In deed, regarding (3.5), it can be written as
  $$\psi : [\mathsf{T}_f] \mapsto P_\alpha [\mathsf{T}_f] \tag{3.6}$$
  where the permutation matrix $P_\alpha \in \mathscr{S}_{2^n}$ of order 2^n corresponds to the translation $\upsilon_\alpha \in \mathscr{T}_n$.

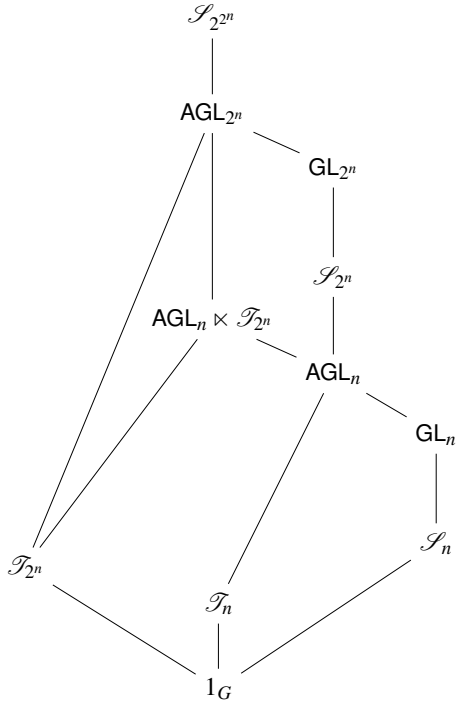


Figure 3.1: Lattice of subgroups of $\mathscr{S}_{2^{2^n}}$ (not a complete list)

– *Permuting the input coordinates ($\mathscr{S}_n$)*:
$\psi \in \mathscr{S}_n$ if for all $f \in \mathscr{F}_n$ it is of the form $\psi : f(x) \mapsto f(\pi(x))$ for some $\pi \in \mathscr{S}_n$ of order n such that $\pi(x) = (\pi(x_1), \pi(x_2), \pi(x_3), \ldots, \pi(x_n))$ for $x = (x_1, x_2, x_3, \ldots, x_n) \in \mathbb{F}_2^n$. Similarly, regarding (3.5), we can see ψ as

$$\psi : [\mathsf{T}_f] \mapsto P_\pi[\mathsf{T}_f] \tag{3.7}$$

where the permutation matrix $P_\pi \in \mathscr{S}_{2^n}$ of order 2^n corresponds to the $\pi \in \mathscr{S}_n$.

– *Linear transformations of input variables (GL_n)*:
Bijective mapping $\psi \in \mathsf{GL}_n$ if for all $f \in \mathscr{F}_n$ it satisfies $\psi : f(x) \mapsto f(xA)$ for some $A \in \mathsf{GL}_n$. Such a ψ can also be regarded as

$$\psi : [\mathsf{T}_f] \mapsto P_A[\mathsf{T}_f] \tag{3.8}$$

where the permutation matrix $P_A \in \mathscr{S}_{2^n}$ of order 2^n corresponds to the $A \in \mathsf{GL}_n$.

– *Affine transformations of input variables (AGL_n)*:
ψ lies in AGL_n, provided that for all $f \in \mathscr{F}_n$ it is of the form $\psi : f(x) \mapsto f(xA \oplus \alpha)$ for some $A \in \mathsf{GL}_n$ and $\alpha \in \mathbb{F}_2^n$. Based on (3.5), it can be given as

$$\psi : [\mathsf{T}_f] \mapsto P_{A,\alpha}[\mathsf{T}_f] \tag{3.9}$$

where the permutation matrix $P_{A,\alpha} \in \mathscr{S}_{2^n}$ of order 2^n corresponds to the $A \in \mathsf{GL}_n$ and $\alpha \in \mathbb{F}_2^n$.

– *Bijections on input variables ($\mathscr{S}_{2^n}$)*:
Comprised of all the bijective mapping of the form

$$\psi : [\mathsf{T}_f] \mapsto P[\mathsf{T}_f] \tag{3.10}$$

for some permutation matrix $P \in \mathscr{S}_{2^n}$ of order 2^n.

– *Translations of truth tables ($\mathscr{T}_{2^n}$)*:
ψ belongs to $\mathscr{T}_{2^n}$ if for all $f \in \mathscr{F}_n$ it is of the form

$$\psi : [\mathsf{T}_f] \mapsto [\mathsf{T}_f] \oplus [\mathsf{T}_g] \tag{3.11}$$

for some $g \in \mathscr{F}_n$.

– *Linear transformations of truth tables (GL_{2^n})*:
ψ lies in GL_{2^n} if for all $f \in \mathscr{F}_n$ it can be written in the form

$$\psi : [\mathsf{T}_f] \mapsto M[\mathsf{T}_f] \tag{3.12}$$

for some $m \in \mathsf{GL}_{2^n}$ of order 2^n.

– *Affine equivalency mappings ($\mathsf{AGL}_n \ltimes \mathscr{T}_{2^n}$)*[1]:
ψ belongs to $\mathsf{AGL}_n \ltimes \mathscr{T}_{2^n}$ if for all all $f \in \mathscr{F}_n$ it is of the form

$$\psi : f(x) \mapsto f(xA \oplus \alpha) \oplus g(x)$$

for some $A \in \mathsf{GL}_n$ and $g \in \mathscr{F}_n$. In deed, regarding (3.5), ψ can be written also as

$$\psi : [\mathsf{T}_f] \mapsto P_{A,\alpha}[\mathsf{T}_f] \oplus [\mathsf{T}_g] \tag{3.13}$$

where the permutation matrix $P_{A,\alpha} \in \mathscr{S}_{2^n}$ of order 2^n corresponds to $A \in \mathsf{GL}_n$ and $\alpha \in \mathbb{F}_2^n$, and T_g is the truth table of the function $g \in \mathscr{F}_n$.

– *Affine transformations of truth tables AGL_{2^n})*:
AGL_{2^n} is comprised of the bijective mappings of the form

$$\psi : [\mathsf{T}_f] \mapsto M[\mathsf{T}_f] \oplus [\mathsf{T}_g] \tag{3.14}$$

for some $M \in \mathsf{GL}_{2^n}$ and $g \in \mathscr{F}_n$.

– *Non-affine transformations of truth tables ($\mathscr{S}_{2^{2^n}} - \mathsf{AGL}_{2^n}$)*:
Bijective mappings that does not lie in AGL_{2^n}, that is regarding (3.5), the ones having at least one non-zero λ_j for $j \in \{12, 13, \ldots, 12\cdots 2^n\}$.

In this chapter, since our main concern is to classify nonlinearity preserving mappings we skip the proofs, which can be easily achieved by elementary group theory techniques, for showing that the above sets are actually subgroups of $\mathscr{S}_{2^{2^n}}$.

Let $\psi \in \mathscr{S}_{2^{2^n}}$, then we say that ψ preserves nonlinearity if $\mathsf{N}_f = \mathsf{N}_{\psi f}$ for all $f \in \mathscr{F}_n$. In fact, we have the following proposition for keeping nonlinearity invariant.

[1] In fact, affine equivalency mapping synonym is generally used for the group $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ that will be defined in the following section. Here we are just abusing the naming convention for a moment.

Proposition 3.3. *ψ preserves nonlinearity if and only if the absolute maximum of the Walsh spectra of f remains invariant, that is*

$$\max_{\omega\in\mathbb{F}_2^n} \left|W_f(\omega)\right| = \max_{\omega\in\mathbb{F}_2^n} \left|W_{\psi f}(\omega)\right| \text{ for all } f \in \mathscr{F}_n.$$

Proof. Recall from (2.24) that

$$\mathsf{N}_f = 2^{n-1} - \frac{1}{2}\max_{\omega\in\mathbb{F}_2^n} \left|\mathsf{W}_f(\omega)\right| \ ,$$

hence the statement follows. □

We denote the set of all nonlinearity preserving bijective maps acting on the n-variables Boolean functions by

$$\mathscr{P}_n(\mathsf{N}) = \{\psi \in \mathscr{S}_{2^{2^n}} \mid \mathsf{N}_f = \mathsf{N}_{\psi f} \text{ for all } f \in \mathscr{F}_n\} \ .$$

Proposition 3.4. *$\mathscr{P}_n(\mathsf{N})$ is a subgroup of $\mathscr{S}_{2^{2^n}}$.*

Proof. It is clear that identity mapping of $\mathscr{S}_{2^{2^n}}$ lies in $\mathscr{P}_n(\mathsf{N})$. We take any $\psi, \theta \in \mathscr{P}_n(\mathsf{N})$. We have $\mathsf{N}_f = \mathsf{N}_{\psi f}$ and $\mathsf{N}_f = \mathsf{N}_{\theta f}$ for all $f \in \mathscr{F}_n$. Then, it follows by Definition & Proposition 2.21 that $\mathsf{N}_f = \mathsf{N}_{\theta(\psi f)} = \mathsf{N}_{(\theta\psi)f}$. □

3.1 Bijections on Input Variables ($\mathscr{S}_{2^n}$)

In the cryptographic literature, Meier and Staffelbach were first to analyze the behavior of the nonlinearity, degree and linear structure criteria under the action of $\mathscr{S}_{2^n}$ on $\mathscr{F}_n$ [102]. Among the bijections on input variables, they proved that the nonlinearity, degree and linear structure values are preserved only under the action of AGL_n for all n variable functions. For the sake of completeness, here we include their result related to nonlinearity.

Theorem 3.5. *[102] Let $\psi \in \mathscr{S}_{2^n}$, then $\psi \in \mathscr{P}_n(\mathsf{N})$ if and only if $\psi \in \mathsf{AGL}_n$.*

The theorem above includes that the bijective mappings belonging to the subgroups $\mathscr{S}_n$, $\mathscr{T}_n$ and GL_n are all nonlinearity preserving and hence are all lie in $\mathscr{P}_n(\mathsf{N})$. In deed, regarding (3.5) we can equivalently state Theorem **??** as the following corollary.

Corollary 3.6. *Let $\psi \in \mathscr{S}_{2^n}$ such that $\psi : [T_f] \mapsto P[T_f]$ for a permutation matrix $P \in \mathscr{S}_{2^n}$ of order 2^n. Then $\psi \in \mathscr{P}_n(\mathsf{N})$ if and only if there exists a monomial matrix $Q \in \mathscr{S}_{2^n}^{\pm}$ such that $(P,Q) \in \mathsf{Aut}(H_n)$.*

Proof. Assume that $\psi \in \mathscr{P}_n(\mathsf{N})$, then Theorem **??** restricts ψ into AGL_n which means that $\psi : f(x) \mapsto f(xA \oplus \alpha)$ for some $A \in \mathsf{GL}_n$ and $\alpha \in \mathbb{F}_2^n$ for all $f \in \mathscr{F}_n$. Then by writing down the Walsh transform of the function ψf, for all $\omega \in \mathbb{F}_2^n$, we get

$$
\begin{aligned}
\mathsf{W}_{\psi f}(\omega) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(xA\oplus\alpha)\oplus\langle x,\omega\rangle} \\
&= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\langle (x\oplus\alpha)A^{-1},\omega\rangle} \\
&= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\langle x,\omega(A^{-1})^t\rangle\oplus\langle\alpha,\omega(A^{-1})^t\rangle} \\
&= (-1)^{\langle\omega,\alpha A^{-1}\rangle} \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\langle x,\omega(A^{-1})^t\rangle} \\
&= (-1)^{\langle\omega,\alpha A^{-1}\rangle} \mathsf{W}_f(\omega(A^{-1})^t) \ ,
\end{aligned}
$$

By letting $Q' \in \mathscr{S}_{2^n}$ represent the permutation on W_f and $D \in \mathscr{D}_n$ satisfying $D = diag(\zeta_{\ell_{\alpha A^{-1}}})$, we can construct a monomial matrix $Q \in \mathscr{S}_{2^n}^{\pm}$ such that $Q = Q'D$ and

$$
\mathsf{W}_{\psi f} = \zeta_f P \mathsf{H}_n = \mathsf{W}_f Q = \zeta_f \mathsf{H}_n Q \ .
$$

Then we get $P\mathsf{H}_n = \mathsf{H}_n Q$ which means $(P,Q) \in \mathsf{Aut}(\mathsf{H}_n)$.

Conversely, suppose that there exists a $Q \in \mathscr{S}_{2^n}^{\pm}$ such that $(P,Q) \in \mathsf{Aut}(\mathsf{H}_n)$. Then, for all $f \in \mathscr{F}_n$, we have

$$
\mathsf{W}_{\psi f} = \zeta_f P \mathsf{H}_n = \zeta_f \mathsf{H}_n Q = \mathsf{W}_f Q \ ,
$$

that is the absolute Walsh spectra maximum remains unchanged. Thus with Proposition 3.3 we conclude that $\psi \in \mathscr{P}_n(\mathsf{N})$ which also completes the proof. □

In fact, Q is strictly determined by P such that $Q = \mathsf{H}_n^{-1} P \mathsf{H}_n$.

3.2 Affine Equivalency Mappings ($\mathsf{AGL}_n \ltimes \mathscr{A}_n$)

First, note that;

Claim 3.7. *Let $\psi \in \mathsf{AGL}_n \ltimes \mathscr{T}_{2^n}$ such that*

$$
\psi : f(x) \mapsto f(xA \oplus \alpha) \oplus g(x) \ .
$$

If $\psi \in \mathscr{P}_n(\mathsf{N})$ then $g \in \mathscr{A}_n$.

Proof. By definition, $\psi \in \mathscr{P}_n(\mathsf{N})$ means that $\mathsf{N}_f = \mathsf{N}_{\psi f}$ for all functions $f \in \mathscr{F}_n$. Then particularly for the function $\ell_{\alpha_0} \in \mathscr{L}_n$, we have $\psi : \ell_{\alpha_0} \mapsto g$ and $\mathsf{N}_{\ell_{\alpha_0}} = \mathsf{N}_g$. Therefore, we conclude that $g \in \mathscr{A}_n$. □

Thus, in the pursue of the nonlinearity preserving mappings, we can restrict ourselves to the set $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ within $\mathsf{AGL}_n \ltimes \mathscr{T}_{2^n}$.

Definition 3.1. [96] Let

$$\mathsf{AGL}_n \ltimes \mathscr{A}_n := \{(\tau, \ell_{\beta,a}) |\ \tau \in \mathsf{AGL}_n, \ell_{\beta,a} \in \mathscr{A}_n\},$$

or, more explicitly;

$$\mathsf{AGL}_n \ltimes \mathscr{A}_n := \{(A, \alpha, \beta, a) \mid A \in \mathsf{GL}_n, \alpha, \beta \in \mathbb{F}_2^n, a \in \mathbb{F}_2\},$$

where τ and $\ell_{\beta,a}$ are given by the mappings $\tau : x \mapsto xA \oplus \alpha$ and $\ell_{\beta,a} : x \mapsto \langle x, \beta \rangle \oplus a$.

Indeed, $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ forms also a subgroup. To the best of our knowledge, although $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ forms a group, its proof is not given explicitly in the literature. For the sake of completeness, we give an elementary proof that $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ forms a group.

Proposition 3.8. *$\mathsf{AGL}_n \ltimes \mathscr{A}_n$ forms a group under the operation and its inverse given by*

$$(\tau, \ell_{\beta,a})(\tau', \ell_{\beta',a'}) := (\tau\tau',\ \tau(\ell_{\beta',a'}) + \ell_{\beta,a}),$$
$$(\tau, \ell_{\beta,a})^{-1} := (\tau^{-1}, \tau^{-1}(\ell_{\beta,a}))$$

for all $\tau, \tau' \in \mathsf{AGL}_n$ and $\ell_{\beta,a}, \ell_{\beta',a'} \in \mathscr{A}_n$, respectively. This operation and its inverse can also be given by

$$(A, \alpha, \beta, a) \circ (A', \alpha', \beta', a') := (A'A, \alpha'A \oplus \alpha, \beta'A^t \oplus \beta, \langle \alpha, \beta' \rangle \oplus a' \oplus a),$$
$$(A, \alpha, \beta, a)^{-1} := (A^{-1}, \alpha A^{-1}, \beta (A^{-1})^t, \langle \alpha, \beta (A^{-1})^t \rangle \oplus a)$$

for all $A, A' \in \mathsf{GL}_n$, $\alpha, \alpha', \beta, \beta' \in \mathbb{F}_2^n$, $a, a' \in \mathbb{F}_2$, respectively.

Proof. $(A = \mathsf{I}_n, \alpha = \alpha_0, \beta = \alpha_0, a = 0)$ is the identity element of $\mathsf{AGL}_n \ltimes \mathscr{A}_n$. Closedness and existence of inverse elements follows immediately from the same properties of the underlying groups of components. Associativity follows also from the associativity of the underlying operations for each component. □

We have an immediate action of the group $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ on $\mathscr{F}_n$ defined as

$$(A, \alpha, \beta, a) f := f(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a.$$

Definition 3.2. Two Boolean functions f and g are said to be *affine equivalent* if and only if for some $(A, \alpha, \beta, a) \in \mathsf{AGL}_n \ltimes \mathscr{A}_n$ the following holds

$$f(x) = (A, \alpha, \beta, a) g = g(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a.$$

We call the elements of $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ *affine equivalency mappings* and if f and g are affine equivalent functions we denote them by $f \sim g$.

In the following proposition, Preneel proved that the action of an affine equivalency mappings results in a signed permutation on the Walsh spectra of the function and consequently preserves its nonlinearity.

Proposition 3.9. *[112] Let $f,g \in \mathscr{F}_n$ be $f \sim g$ with $f(x) = g(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a$ for some $A \in \mathsf{GL}_n$, $\alpha, \beta \in \mathbb{F}_2^n$, $a \in \mathbb{F}_2$. Then for the Walsh transforms of f and g the following relation holds:*

$$W_f(\omega) = (-1)^{\langle \alpha, (\omega \oplus \beta)(A^{-1})^t \rangle \oplus a} \; W_g((\omega \oplus \beta)(A^{-1})^t).$$

Therefore, affine equivalency mappings keep nonlinearity invariant, i.e.

$$(\mathsf{AGL}_n \ltimes \mathscr{A}_n) \subset \mathscr{P}_n(\mathsf{N}) \quad .$$

Furthermore, they also preserve the degree of a function and frequency distribution of absolute Walsh spectrum values [112], for a detailed list please refer to [15, Section 5.1, p. 81].

In the sequel, we will derive an isomorphism, but first we are going to prove a $1-1$ correspondence between $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ and $\mathsf{Aut}(\mathsf{H}_n)$.

Theorem 3.10. *Let the notations be as above and $f,g \in \mathscr{F}_n$. Then the following assertions are equivalent:*

(i) There exists a unique $(A, \alpha, \beta, a) \in \mathsf{AGL}_n \ltimes \mathscr{A}_n$ such that $(A, \alpha, \beta, a)g = f$.

(ii) There exists a unique $(P,Q) \in \mathsf{Aut}(H_n)$ such that $\zeta_f = \zeta_g P$.

(iii) There exists a unique $(P,Q) \in \mathsf{Aut}(H_n)$ such that $W_f = W_g Q$.

Proof. $((i) \Rightarrow (ii))$ Let $f \sim g$. Since we have $f(x) = g(xA \oplus \alpha) \oplus \langle x, \beta \rangle \oplus a$, it is not difficult to see that

$$\zeta_f = \zeta_g P' D$$

where $D = diag(\zeta_{\ell_{\beta,a}}) \in \mathscr{D}_{2^n}$ and $P' \in \mathscr{S}_{2^n}$ is the permutation matrix corresponding to $xA \oplus \alpha \in \mathsf{AGL}_n$.

Then, letting $P = P'D \in \mathscr{S}_{2^n}^{\pm}$ a signed permutation, we obtain $\zeta_f = \zeta_g P$. Uniqueness of the pair (P,Q) follows immediately by the definition of $\mathscr{S}_{2^n}^{\pm}$.

$((ii) \Rightarrow (iii))$ We have $\zeta_f = \zeta_g P$. Then we obtain easily

$$\mathsf{W}_f = \zeta_f \mathsf{H}_n = \zeta_g P \mathsf{H}_n = \zeta_g \mathsf{H}_n Q = \mathsf{W}_g Q.$$

$((iii) \Rightarrow (i))$ Writing $P = P'D$ for $P \in \mathscr{S}_{2^n}^{\pm}$ with $P' \in \mathscr{S}_{2^n}$ and $D \in \mathscr{D}_{2^n}$, it follows that

$$\mathsf{W}_f = \zeta_f \mathsf{H}_n = \mathsf{W}_g Q = \zeta_g \mathsf{H}_n Q = \zeta_g P \mathsf{H}_n \quad .$$

Hence, we get

$$\zeta_f = \zeta_g P = \zeta_g P' D \quad .$$

By rewriting this equation in the additive case and using the truth tables of the functions f and g, we derive

$$\mathsf{T}_f = \mathsf{T}_g P' \oplus \mathsf{T}_\ell \quad ,$$

where T_ℓ is the corresponding truth table to the diagonal of the matrix D. Interpreting this truth table based equation to the algebraic normal forms of the functions

$$f(x) = g(\tau(x)) \oplus \ell(x)$$

is obtained, where $\tau \in \mathscr{S}_{2^n}$ is a permutation of $\mathbb{F}_2^n$ and $\ell \in \mathscr{F}_n$. From Lemma 9.2.3 of [39, p. 102], we conclude that $\tau \in \mathsf{AGL}_n$ and $\ell \in \mathscr{A}_n$ and the result follows. □

We are now ready to prove that we have not only a $1-1$ correspondence but also an isomorphy between $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ and $\mathsf{Aut}(\mathsf{H}_n)$.

Theorem 3.11. *The authomorphism group of $2^n \times 2^n$ Sylvester Hadamard matrix is isomorphic to the group of affine equivalence relations acting on n variable Boolean functions, that is* $\mathsf{Aut}(H_n) \cong \mathsf{AGL}_n \ltimes \mathscr{A}_n$.

Proof. Bijection between $\mathsf{Aut}(\mathsf{H}_n)$ and $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ follows immediately from uniqueness properties of Theorem 3.10.

Consider the map

$$\phi : \mathsf{AGL}_n \ltimes \mathscr{A}_n \to \mathscr{S}_{2^n}^{\pm}$$

that sends each $(\tau, \ell_{\beta,a})$ to $P = P'D$ where $P' \in \mathscr{S}_{2^n}$ is the permutation matrix representing τ and $D \in \mathscr{D}_{2^n}$ is the diagonal matrix having the signed sequence of $\ell_{\beta,a}$ as its diagonal. It can be easily seen that this map is well-defined.

Further, we define the map

$$\vartheta : \mathsf{AGL}_n \ltimes \mathscr{A}_n \to \mathsf{Aut}(\mathsf{H}_n)$$

with $\vartheta : (\tau, \ell_{\beta,a}) \mapsto (P, \mathsf{H}_n^{-1} P \mathsf{H}_n)$. Since ϕ is a well-defined map and by Lemma 2.14, we see that the map ϑ is also well-defined. It certainly is a surjection by the implication $(iii) \Rightarrow (i)$ of Theorem 3.10. Therefore, we have an explicit version of the bijection given in Theorem 3.10.

Let $\vartheta((\tau, \ell_{\beta,a})) = (P_1, \mathsf{H}_n^{-1} P_1 \mathsf{H}_n)$ and $\vartheta((\tau', \ell_{\beta',a'})) = (P_2, \mathsf{H}_n^{-1} P_2 \mathsf{H}_n)$. Then we obtain

$$(P_1, \mathsf{H}_n^{-1} P_1 \mathsf{H}_n) \star (P_2, \mathsf{H}_n^{-1} P_2 \mathsf{H}_n) = (P_1 \cdot P_2, \mathsf{H}_n^{-1} (P_1 \cdot P_2) \mathsf{H}_n).$$

By Definition 3.1, we let (A, α, β, a) and $(A', \alpha', \beta', a')$ be the representations corresponding to $(\tau, \ell_{\beta,a})$ and $(\tau', \ell_{\beta',a'})$, respectively. Let $P_1 = P_1' D_1$ and $P_2 = P_2' D_2$ with $P_1', P_2' \in \mathscr{S}_{2^n}$ and $D_1, D_2 \in \mathscr{D}_{2^n}$.

We have the property that $\phi((\tau, \ell_{\beta,a})(\tau', \ell_{\beta',a'}))$ corresponds to a matrix P. Note that by Definition & Proposition 2.9, P can be written as $P = P'D$, where $P' = P_1' P_2'$ is the matrix representing the composition of the permutations determined by $\tau\tau' : x \mapsto xA'A \oplus \alpha' A \oplus \alpha$ and $D = D_1 P_1' D_2 (P_1')^{-1}$ is the diagonal matrix having the signed sequence of $\tau(\ell_{\beta',a'}) + \ell_{\beta,a} : x \mapsto \langle x, \beta' A^t \oplus \beta \rangle \oplus \langle \alpha, \beta' \rangle \oplus a' \oplus a)$ as its diagonals. This

implies that we have

$$\begin{aligned}\vartheta((\tau,\ell_{\beta,a})\circ(\tau',\ell_{\beta',a'})) &= (P,\mathsf{H}_n^{-1}P\mathsf{H}_n)\\ &= (P'D,\mathsf{H}_n^{-1}P'D\mathsf{H}_n)\\ &= (P_1'P_2'D_1P_1'D_2(P_1')^{-1},\mathsf{H}_n^{-1}P_1'P_2'D_1P_1'D_2(P_1')^{-1}\mathsf{H}_n)\\ &= (P_1\cdot P_2,\mathsf{H}_n^{-1}(P_1\cdot P_2)\mathsf{H}_n)\\ &= (P_1,\mathsf{H}_n^{-1}P_1\mathsf{H}_n)\star(P_2,\mathsf{H}_n^{-1}P_2\mathsf{H}_n)\\ &= \vartheta((\tau,\ell_{\beta,a}))\star\vartheta((\tau',\ell_{\beta',a'}))\end{aligned}$$

Therefore, it follows $\mathsf{Aut}(\mathsf{H}_n)\cong\mathsf{AGL}_n\ltimes\mathscr{A}_n$. □

Remark 3.1. There exists another isomorphic group to $\mathsf{Aut}(\mathsf{H}_n)$, see Theorem 9.2.4 of [39, p.103] for details.

The cardinality of $\mathsf{Aut}(\mathsf{H}_n)$ can easily be calculated using simple counting arguments and by Theorem 3.10.

Corollary 3.12. $\#(\mathsf{Aut}(H_n))=\#(\mathsf{AGL}_n\ltimes\mathscr{A}_n)=2^{2n+1}\prod_{i=0}^{n-1}(2^n-2^i)$.

Indeed, based on Theorem 3.10 it is not difficult to prove the following corollary.

Corollary 3.13. *Let $f,g\in\mathscr{F}_n$ with $f\sim g$, i.e. there exists $(A,\alpha,\beta,a)\in\mathsf{AGL}_n\ltimes\mathscr{A}_n$ such that $(A,\alpha,\beta,a)g=f$. The corresponding monomial matrix pair $(P,Q)\in\mathsf{Aut}(H_n)$ satisfies the following properties:*

- *$P\in S_{2^n}$ if and only if $\beta=\alpha_0$ and $a=0$. Moreover, $Q\in S_{2^n}$ if and only if $\alpha=\alpha_0$.*
- *$P,Q\in D_{2^n}$ if and only if $A=I_n$ and $\alpha=\alpha_0$.*

Under the action of $\mathsf{AGL}_n\ltimes\mathscr{A}_n$, the orbits partition $\mathscr{F}_n$ into *equivalence classes*. These equivalence classes contains functions having the same degree, nonlinearity and frequency distribution of absolute Walsh spectrum values.

Characterizing these equivalence classes dates back to Ninomiya's thesis [108]. For $n\leq 4$, Ninomiya completely answered the counting problem (enumeration of equivalence classes) and recognition problem (to which equivalence class given function belong),see [87]. In the sequel, Lechner, who named these mappings as *restricted affine mappings (RAG)*, in his thesis pursue the problems and shown that there exists 48 equivalence classes for $n=5$ and presented class representative for 46 of 48 equivalence classes [85]. Berlekamp and Welch, later characterized all of equivalence classes for $n=5$ and in a while later, Maiorana given that for $n=6$, there exist 150357 equivalence classes and presented class representatives for each of them [96].

3.3 Affine Bijective Mappings (AGL_{2^n})

The group of affine equivalency mappings is obviously contained in AGL_{2^n}. In this section we will analyze the group AGL_{2^n}, but first we need to prove the following proposition that characterizes the nonlinearity preserving mappings in GL_{2^n} which is also another subgroup of AGL_{2^n}.

Proposition 3.14. *Let $n \geq 3$ and $\psi \in GL_{2^n}$ be such that for all $f \in \mathscr{F}_n$,*

$$\psi : [T_f] \mapsto M[T_f]$$

where $M = [[\lambda_1]\ [\lambda_2]\ \ldots\ [\lambda_{2^n}]] \in GL_n$ is a fixed invertible matrix of order 2^n. Then the following statements are equivalent.

(i) $\psi \in \mathscr{P}_n(N)$.

(ii) $M = [[\lambda_1]\ [\lambda_2]\ \ldots\ [\lambda_{2^n}]] \in GL_n$ *satisfies the following assertions.*

- *The functions g_j such that $\lambda_j := T_{g_j}$ have $N_{g_j} = 1$ for all $1 \leq j \leq 2^n$,*
- *The functions h_{jk} such that $\lambda_j \oplus \lambda_k := T_{h_{jk}}$ have $N_{h_{jk}} = 2$ for all distinct $1 \leq j,k \leq 2^n$ pair.*

(iii) $M = P_{A,\alpha} \oplus B$, *where $P_{A,\alpha} \in \mathscr{S}_{2^n}$ corresponds to a matrix representation of an element in AGL_n and $B = [\varepsilon_1\ \varepsilon_2\ \ldots\ \varepsilon_{2^n}]$ with $\varepsilon_j \in \mathscr{A}_n$, $1 \leq j \leq 2^n$.*

Proof. $((i) \Rightarrow (ii))$ Assume $\psi \in \mathscr{P}_n(\mathsf{N})$. Then we have $\mathsf{N}_f = \mathsf{N}_{\psi f}$ for all $f \in \mathscr{F}_n$. So in particular consider the functions e_j, $1 \leq j \leq 2^n$, having $\mathsf{w}(e_j) = 1$ that is $\mathsf{T}_{e_j} = (0,0,0,\ldots,0,1,0,\ldots,0)$. Then for each e_j, we have

$$\psi(\mathsf{T}_{e_j}) = \lambda_j.$$

Since $\mathsf{N}_{e_j} = 1$, we conclude that the functions g_j such that $\lambda_j := \mathsf{T}_{g_j}$ have $\mathsf{N}_{g_j} = 1$ for all $1 \leq j \leq 2^n$.

Similarly, consider the functions of e_{jk}, $1 \leq j,k \leq 2^n$ with $j \neq k$, having $\mathsf{w}(e_{ij}) = 2$. Then for each e_{jk}, we have

$$\psi(\mathsf{T}_{e_{jk}}) = \lambda_j \oplus \lambda_k.$$

For $n \geq 3$, each function e_{jk} has $\mathsf{N}_{e_{jk}} = 2$ which proves the second expression.

$((ii) \Rightarrow (iii))$ Suppose that $M = [[\lambda_1]\ [\lambda_2]\ \ldots\ [\lambda_{2^n}]] \in \mathsf{GL}_n$ satisfies the following expressions.

- The functions g_j such that $\lambda_j := \mathsf{T}_{g_j}$ have $\mathsf{N}_{g_j} = 1$ for all $1 \leq j \leq 2^n$,
- The functions h_{jk} such that $\lambda_j \oplus \lambda_k := \mathsf{T}_{h_{jk}}$ have $\mathsf{N}_{h_{jk}} = 2$ for all distinct $1 \leq j,k \leq 2^n$ pair.

Note that for $n \geq 2$, the functions with nonlinearity value 1 have the Hamming distance of 1 to their closest affine function. Thus, each λ_j can be decomposed as follows.

$$\lambda_j = \mathsf{T}_{g_j} = \mathsf{T}_{e_{l_j}} \oplus \mathsf{T}_{\ell_j}$$

where $\mathsf{w}(e_{l_j}) = 1$ and $\ell_j \in \mathscr{A}_n$ is the closest affine function to g. Here, due to the second constraint, we further have that for any distinct pair of λ_j and λ_k we have $e_{l_j} \neq e_{l_k}$. When we re-write the column based representation according to this decomposition, we get the following.

$$\begin{aligned} M &= [[\lambda_1]\ [\lambda_2]\ \ldots\ [\lambda_{2^n}]] \\ &= [[\mathsf{T}_{e_{l_1}} \oplus \mathsf{T}_{\ell_1}]\ [\mathsf{T}_{e_{l_2}} \oplus \mathsf{T}_{\ell_2}]\ \ldots\ [\mathsf{T}_{e_{l_{2^n}}} \oplus \mathsf{T}_{\ell_{2^n}}]] \\ &= \underbrace{[[\mathsf{T}_{e_{l_1}}]\ [\mathsf{T}_{e_{l_2}}]\ \ldots\ [\mathsf{T}_{e_{l_{2^n}}}]]}_{P} \oplus \underbrace{[[\mathsf{T}_{\ell_1}]\ [\mathsf{T}_{\ell_2}]\ \ldots\ [\mathsf{T}_{\ell_{2^n}}]]}_{B} \\ &= P \oplus B \end{aligned}$$

Since each e_{l_j} are different, we can conclude that P is a permutation matrix and thus $P \in \mathscr{S}_{2^n}$. Moreover, in order to preserve nonlinearity, from (3.9) and Theorem 3.5, we conlcude that $P = P_{A,\alpha}$ for some $A \in \mathsf{GL}_n$ and $\alpha \in \mathbb{F}_2^n$ and the matrix B have affine functions as its columns. Thus we prove the assertion

$$M = P_{A,\alpha} \oplus B\,.$$

$((iii) \Rightarrow (i))$ Let $M = P_{A,\alpha} \oplus B$, where $P_{A,\alpha} \in \mathscr{S}_{2^n}$ corresponds to a matrix representation of an element in AGL_n and $B = [\varepsilon_1\ \varepsilon_2\ \ldots\ \varepsilon_{2^n}]$ with $\varepsilon_j \in \mathscr{A}_n$, $1 \leq j \leq 2^n$. Then for all $f \in \mathscr{F}_n$ we have,

$$\begin{aligned} \psi(f) &= M[\mathsf{T}_f] \\ &= (P_{A,\alpha} \oplus B)[\mathsf{T}_f] \\ &= P_{A,\alpha}[\mathsf{T}_f] \oplus \underbrace{B[\mathsf{T}_f]}_{\in \mathscr{A}_n}, \end{aligned}$$

which reduces to

$$\psi : f(x) \mapsto f(xA \oplus \alpha) \oplus \ell_{\beta,a}\,,$$

where $\ell_{\beta,a} \in \mathscr{A}_n$ is determined by the acted function's support. Now, from Proposition 3.3 and Proposition 3.9, the statement follows, that is $\psi \in \mathscr{P}_n(\mathsf{N})$. □

Now, we are ready to classify elements of AGL_{2^n} regarding the nonlinearity preservability by giving the necessary and sufficient conditions.

Theorem 3.15. *Let $\psi \in \mathsf{AGL}_{2^n}$ be an affine bijective transformation so that for all $f \in \mathscr{F}_n$,*

$$\psi : [T_f] \mapsto M[T_f] \oplus [T_g]$$

where $g \in \mathscr{F}_n$ and $M \in \mathsf{GL}_{2^n}$ are fixed.

$\psi \in \mathscr{P}_n(\mathsf{N})$ if and only if

– $M = P_{A,\alpha} \oplus B$, *where* $P_{A,\alpha} \in \mathscr{S}_{2^n}$ *corresponds to a matrix representation of an element in* AGL_n *and* $B = [\varepsilon_1\ \varepsilon_2\ \ldots\ \varepsilon_{2^n}]$ *with* $\varepsilon_j \in \mathscr{A}_n$, $1 \leq j \leq 2^n$,

– $g \in \mathscr{A}_n$.

Proof. Due to the function $\ell_{\alpha_0} \in \mathscr{L}_n$, the necessity and sufficiency of $g \in \mathscr{A}_n$ is assured. Then rest follows immediately from Proposition 3.14. □

Naturally the above theorem includes the previous proposition. Moreover it also proves the existence of nonlinearity preserving bijective mappings other than the ones included in affine equivalency mappings $\mathsf{AGL}_n \ltimes \mathscr{A}_n$. On the other hand, as proved in the following claim, for a fixed function the mappings derived in Theorem 3.15 and affine equivalency mappings $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ provide the same orbit.

Claim 3.16. *For a given function* $f \in \mathscr{F}_n$, *the nonlinearity preserving bijective mappings belonging to* $\mathsf{AGL}_{2^n} - (\mathsf{AGL}_n \ltimes \mathscr{A}_n)$ *and the affine equivalency mappings* ($\mathsf{AGL}_n \ltimes \mathscr{A}_n$) *produce the same orbits.*

Proof. By Definition 2.2, we have the following orbits of f under the related sets

$$\begin{aligned}(\mathsf{AGL}_n \ltimes \mathscr{A}_n)_f &= \{\vartheta f \mid \vartheta \in \mathsf{AGL}_n \ltimes \mathscr{A}_n\} \\ (\mathsf{AGL}_{2^n} - (\mathsf{AGL}_n \ltimes \mathscr{A}_n))_f &= \{\psi f \mid \psi \in G\}\ .\end{aligned}$$

Now, let $\psi \in \mathsf{AGL}_{2^n} - (\mathsf{AGL}_n \ltimes \mathscr{A}_n)$ be a nonlinearity preserving bijective mapping. Then, by Theorem 3.15, for fixed function f,

$$\begin{aligned}\psi(f) &= (P_{A,\alpha} \oplus B)[\mathsf{T}_f] \oplus [\mathsf{T}_g] \\ &= P_{A,\alpha}[\mathsf{T}_f] \oplus \underbrace{\bigoplus_{\alpha_i \in \mathsf{sup(f)}} \varepsilon_i}_{=B[\mathsf{T}_f]} \oplus [\mathsf{T}_g] \\ &= P_{A,\alpha}[\mathsf{T}_f] \oplus \underbrace{\bigoplus_{\alpha_i \in \mathsf{sup(f)}} \varepsilon_i \oplus [\mathsf{T}_g]}_{\in \mathscr{A}_n}\end{aligned}$$

which reduces to

$$\psi : P_{A,\alpha}[\mathsf{T}_f] \oplus [\mathsf{T}_{\ell_{\beta,a}}]$$

for some $\ell_{\beta,a} \in \mathscr{A}_n$ which is strictly determined by $\mathsf{sup}(f)$.

Hence, the assertion now follows. □

3.4 Non-affine Bijective Mappings ($\mathscr{S}_{2^{2^n}} - \mathsf{AGL}_{2^n}$)

Recall that we write a bijective mapping in $\mathscr{S}_{2^{2^n}}$ as given in (3.5):

$$\begin{aligned}\psi : [\mathsf{T}_f] \mapsto & \lambda_0 \oplus M[\mathsf{T}_f] \oplus [\lambda_{12}] f(\alpha_0) f(\alpha_1) \oplus \cdots \oplus [\lambda_{(2^n-1)2^n}] f(\alpha_{2^n-2}) f(\alpha_{2^n-1}) \oplus \\ & [\lambda_{123}] f(\alpha_0) f(\alpha_1) f(\alpha_3) \oplus \cdots \oplus [\lambda_{(2^n-2)(2^n-1)2^n}] f(\alpha_{2^n-3}) f(\alpha_{2^n-2}) f(\alpha_{2^n-1}) \\ & \vdots \\ & \oplus [\lambda_{12\cdots 2^n}] f(\alpha_0) f(\alpha_1) \cdots f(\alpha_{2^n})\end{aligned}$$

where

- $\mathsf{T}_f = (f(\alpha_0) f(\alpha_1) \cdots f(\alpha_{2^n})) \in \mathbb{F}_2^{2^n}$ hence each $f(\alpha_i) \in \mathbb{F}_2$,
- $\lambda_j := \mathsf{T}_{h_j} \in \mathbb{F}_2^{2^n}$ for some $h_j \in \mathscr{F}_n$,
- M is the $2^n \times 2^n$ matrix whose column form is $M = [[\lambda_1]\ [\lambda_2]\ \ldots\ [\lambda_{2^n}]]$.

Bijective mappings that do not lie in AGL_{2^n}, that is the ones having at least one non-zero λ_j for $j \in \{12, 13, \ldots, 12\cdots 2^n\}$ in the above representation are named *non-affine bijective mappings*.

We now give a sufficient condition for non-affine bijective mappings to keep nonlinearity invariant.

Proposition 3.17. *Let $\psi \in S_{2^{2^n}} - \mathsf{AGL}_{2^n}$ be a non-affine mapping that satisfies the following conditions, with respect to (3.5),*

1. *$\lambda_0 \in \mathscr{A}_n$,*
2. *The matrix $M = P_{A,\alpha} \oplus B$, where $P_{A,\alpha} \in \mathscr{S}_{2^n}$ corresponds to a matrix representation of an element in AGL_n and $B = [\varepsilon_1\ \varepsilon_2\ \ldots\ \varepsilon_{2^n}]$ with $\varepsilon_j \in \mathscr{A}_n$, $1 \le j \le 2^n$,*
3. *$\lambda_j \in \mathscr{A}_n$ for all $j \in \{12, 13, \ldots, 12\cdots 2^n\}$ where at least one of them is non-zero, i.e. $\lambda_j \neq \ell_{\alpha_0}$.*

Then, $\psi \in \mathscr{P}_n(N)$.

Proof. For each function f, we get

$$\begin{aligned}\psi(f) &= \lambda_0 \oplus (P_{A,\alpha} \oplus B)[\mathsf{T}_f] \oplus \lambda_{12} f(\alpha_0) f(\alpha_1) \oplus \cdots \oplus \lambda_{12\cdots 2^n} f(\alpha_0) f(\alpha_1) \cdots f(\alpha_{2^n-1}) \\ &= P_{A,\alpha}[\mathsf{T}_f] \oplus \underbrace{B[\mathsf{T}_f]}_{\in \mathscr{A}_n} \oplus \lambda_0 \oplus \lambda_{12} f(\alpha_0) f(\alpha_1) \oplus \cdots \oplus \lambda_{12\cdots 2^n} f(\alpha_0) f(\alpha_1) \cdots f(\alpha_{2^n-1}) \\ &= P_{A,\alpha}[\mathsf{T}_f] \oplus \underbrace{B[\mathsf{T}_f] \oplus \lambda_0 \oplus \lambda_{12} f(\alpha_0) f(\alpha_1) \oplus \cdots \oplus \lambda_{12\cdots 2^n} f(\alpha_0) f(\alpha_1) \cdots f(\alpha_{2^n-1})}_{= \mathsf{T}_{\ell_{\beta,b}} \in \mathscr{A}_n}\end{aligned}$$

reduces to the mapping $\mathsf{T}_f \mapsto P_{A,\alpha}[\mathsf{T}_f] \oplus \mathsf{T}_{\ell_{\beta,b}}$, for some affine function $\mathsf{T}_{\ell_{\beta,b}}$ due to the given conditions. Therefore now, from the Theorem 3.15, the assertion follows. □

Hence, we prove the existence of nonlinearity preserving non-affine bijective mappings by explicitly constructing a family of bijective mappings. On the other hand, these non-affine nonlinearity preserving bijective mappings still produces the same orbit as $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ for a fixed function. That is;

Claim 3.18. *Let the notations be as above. Let further $\psi \in \mathscr{S}_{2^{2^n}}$ be a non-affine mapping satisfying*

1. $\lambda_0 \in \mathscr{A}_n$,
2. *The matrix $M = P_{A,\alpha} \oplus B$, where $P_{A,\alpha} \in \mathscr{S}_{2^n}$ corresponds to a matrix representation of an element in AGL_n and $B = [\varepsilon_1\ \varepsilon_2\ \ldots\ \varepsilon_{2^n}]$ with $\varepsilon_j \in \mathscr{A}_n$, $1 \leq j \leq 2^n$,*
3. *$\lambda_j \in \mathscr{A}_n$ for all $j \in \{12, 13, \ldots, 12\cdots 2^n\}$ where at least one of $\lambda_j \neq \ell_{\alpha_0}$.*

Then for a fixed function $f \in \mathscr{F}_n$, ψ behaves as an element of $\mathsf{AGL}_n \ltimes \mathscr{A}_n$.

Proof. As shown in the proof of Proposition 3.17, ψ reduces to the mapping $\mathsf{T}_f \mapsto P_{A,\alpha}[\mathsf{T}_f] \oplus \mathsf{T}_{\ell_{\beta,b}}$, for some affine function. In deed, $\mathsf{T}_{\ell_{\beta,b}}$ is strictly determined by summation of ε_i and λ_j based on $\mathsf{sup}(f)$. For a moment, let's denote the set of bijective mappings satisfying the given conditions by G. Then, for any fixed function f, we have the orbit of f

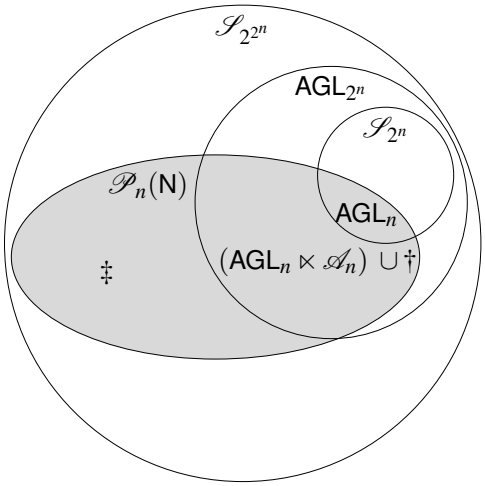
$$G_f := \{\psi f \mid \psi \in G\} = (\mathsf{AGL}_n \ltimes \mathscr{A}_n)_f := \{\vartheta f \mid \vartheta \in \mathsf{AGL}_n \ltimes \mathscr{A}_n\} \ .$$

Thus, the statement now follows. □

Up to now, we have constructed some nonlinearity preserving bijective mappings explicitly. These explicitly known nonlinearity preserving mappings are illustrated in Figure 3.2. Furthermore, for a given function, we have shown that all of these explicitly constructed nonlinearity preserving bijective mappings produce the same orbit with the affine equivalency mappings. Thus, by using the action of these mappings, searching for new Boolean functions would not give new results.

In order to analyze these mappings further, we performed a computer based search for $n = 2$ we scanned $\mathscr{S}_{16}$ exhaustively. Based on this search, we derive that $\mathscr{P}_2(\mathsf{N})$ comprised of the mappings given in Proposition 3.17. Detailed results are given in Appendix B comprehensively.

For $n \geq 3$, even with computer assistance scanning the group $\mathscr{S}_{2^{2^n}}$ exhaustively is computationally impossible for the time being, for instance for $n = 3$, there exists $\#(\mathscr{S}_{256}) \approx 10^{503}$ bijective mappings. Therefore we need to change the perspective to gather new results.



$\dagger : \mathscr{P}_n(\mathsf{N}) \cap (\mathsf{AGL}_{2^n} - (\mathsf{AGL}_n \ltimes \mathscr{A}_n))$, see Theorem 3.15

$\ddagger$: see Proposition 3.17

Figure 3.2: Explicitly known nonlinearity preserving families.

At this point our problem is "is there any other bijective mapping that preserve nonlinearity?". To find an answer for this question, let's consider the problem in a different way and take a closer look on the nonlinearity preserving mappings.

First, assume that we partition the Boolean functions set $\mathscr{F}_n$ into nonlinearity classes. That is,

$$\begin{aligned}
\mathsf{N}_0 &:= \{f \in \mathscr{A}_n\},\\
\mathsf{N}_1 &:= \{f \in \mathscr{F}_n \mid \mathsf{N}_f = 1\},\\
\mathsf{N}_2 &:= \{f \in \mathscr{F}_n \mid \mathsf{N}_f = 2\},\\
&\vdots\\
\mathsf{N}_{2^{n-1}-2^{\frac{n}{2}-1}} &:= \{f \in \mathscr{B}_n\}, \qquad \text{only exists when } n \text{ is even.}
\end{aligned}$$

satisfying

$$\mathscr{F}_n = \bigcup_{0 \le i \le 2^{n-1}-2^{\frac{n}{2}-1}} \mathsf{N}_i \ .$$

Clearly, $\mathsf{N}_i \cap \mathsf{N}_j = \varnothing$ for $i \neq j$, hence this is indeed a well-defined partition of $\mathscr{F}_n$.

Now, let $\psi \in \mathscr{P}_n$. Then as a definition ψ maps each and every partition to itself, that is,

$$\psi : \mathsf{N}_i \mapsto \mathsf{N}_i.$$

In fact, this is necessary and sufficient for bijective mapping $\psi \in \mathscr{S}_{2^{2^n}}$ to be nonlinearity preserving and this is formally stated in the following fact.

Fact 3.19. Suppose $\mathscr{F}_n$ be partitioned into nonlinearity classes N_i such that

$$\mathscr{F}_n = \bigcup_{0 \le i \le 2^{n-1}-2^{\frac{n}{2}-1}} \mathsf{N}_i \ . \tag{3.15}$$

Then $\psi \in \mathscr{P}_n(\mathsf{N})$ if and if only for all $0 \le i \le 2^{n-1}-2^{\frac{n}{2}-1}$, ψ maps nonlinearity classes onto themselves, that is

$$\psi : \mathsf{N}_i \mapsto \mathsf{N}_i.$$

Based on the fact given above, whenever we know the cardinalities of each nonlinearity classes, we can enumerate the nonlinearity preserving bijective mappings.

Proposition 3.20. *Suppose $\mathscr{F}_n$ be partitioned into nonlinearity classes N_i such that*

$$\mathscr{F}_n = \bigcup_{0 \le i \le 2^{n-1}-2^{\frac{n}{2}-1}} \mathsf{N}_i \ . \tag{3.16}$$

Then,

$$\#(\mathscr{P}_n(\mathsf{N})) = \prod_{0 \le i \le 2^{n-1}-2^{\frac{n}{2}-1}} \#(\mathsf{Sym}(\mathsf{N}_i)) \ . \tag{3.17}$$

Proof. Immediately follows from Fact 3.19. □

In fact, Wu has proven the enumeration of Boolean functions with nonlinearity $\le 2^{n-2}$ [142]. Here we will include his result to give a loose lower bound for the cardinality of the nonlinearity preserving bijective mappings for any $n \in \mathbb{N}$, namely $\#\mathscr{P}_n(\mathsf{N})$.

Theorem 3.21. *[142] Let, $t \le 2^{n-2}$ with $n,t \in \mathbb{N}$. Then, for $t < 2^{n-2}$ the number of Boolean functions with nonlinearity t is*

$$\#(\mathsf{N}_t) = 2^{n+1}\binom{2^n}{t},$$

and for $t = 2^{n-2}$ the number of functions with nonlinearity 2^{n-2} is

$$\#(\mathsf{N}_{2^{n-2}}) = 2^{n+1}\left(\binom{2^n}{2^{n-2}} - (2^n-1)\binom{2^{n-1}}{2^{n-2}} + \binom{2^n-1}{2}\right) \ .$$

Then by Proposition 3.20 and Theorem 3.21, we have an immediate and a very loose lower bound for $\#\mathscr{P}_n(\mathsf{N})$ as follows.

Corollary 3.22.

$$\#\mathscr{P}_n(\mathsf{N}) \ggg \left(\prod_{0 \le t < 2^{n-2}} \left(2^{n+1}\tbinom{2^n}{t}\right)!\right)\left(\left(2^{n+1}\left(\tbinom{2^n}{2^{n-2}} - (2^n-1)\tbinom{2^{n-1}}{2^{n-2}} + \tbinom{2^n-1}{2}\right)\right)!\right) \ .$$

Meanwhile, this lower bound sufficiently indicates the existence of non-affine nonlinear bijective mappings. In other words, the corollary above proves that

$$\mathscr{P}_n(\mathsf{N}) \cap (\mathscr{S}_{2^{2^n}} - \mathsf{AGL}_{2^n}) \neq \varnothing \ .$$

For $n \leq 6$, we know the nonlinearity distributions which are given Appendix A, Table A.1. Therefore, based on Proposition 3.20, for $n \leq 6$, the cardinality of $\mathscr{P}_n(\mathsf{N})$ can be computed. We present the cardinality of $\mathscr{P}_n(\mathsf{N})$ for $n \leq 6$ in Table 3.1, where the computation is based on the nonlinearity distribution given in Appendix A.

Table 3.1: Enumeration of $\mathscr{P}_n(\mathsf{N})$ for $n \leq 6$

n	$\#(\mathscr{P}_n(\mathsf{N}))$	$\#(\mathscr{S}_{2^{2^n}}) = 2^{2^n}!$
2	$8! \times 8! \approx 10^{11}$	$2^{2^2}! \approx 10^{13}$
3	$16! \times 128! \times 112! \approx 10^{413}$	$2^{2^3}! \approx 10^{506}$
4	$32! \times 512! \times \cdots \times 896! \approx 10^{249727}$	$2^{2^4}! \approx 10^{287194}$
5	$64! \times \cdots \times 27387136! \approx 10^{3,66x10^{10}}$	$2^{2^5}! \approx 10^{3.95x10^{10}}$
6	$128! \times \cdots \times 5425430528! \approx 10^{3.32x10^{20}}$	$2^{2^6}! \approx 10^{3,47x10^{20}}$

We know that for $n = 2$ there exists $\approx 10^{11}$ nonlinearity preserving bijective mappings. In fact we also validate this with an exhaustive computer search and prove that all of these bijective mappings belong to the set defined in Proposition 3.17.

For $n \geq 3$, let's try to count the nonlinearity preserving bijective mappings that lies in the set defined in Proposition 3.17. We have

- $\#(\mathscr{A}_3) = 2^4$ choices for λ_0,
- $\leq 2^{64}$ choices for the matrix M,
- $\#(\mathscr{A}_3) = 2^4$ choices for each λ_j such that $j \in \{12, 13, \ldots, 12 \cdots 2^n\}$.

Hence for $n = 3$, Proposition 3.17 defines at most $2^{64} \times 16^{248} = 2^{1056}$ nonlinearity preserving mappings. Surprisingly, from Table 3.1 we see that Proposition 3.17 does not give all of the nonlinearity preserving bijective mappings.

In a similar way, for $n = 4$ we can conclude that Proposition 3.17 does not define all of the nonlinearity preserving bijective mappings. Therefore, we can now prove the existence of new non-affine mappings that are not belonging to the class of Proposition 3.17, using the basic counting techniques and nonlinearity distributions.

Theorem 3.23. *For $n \geq 3$ there exist nonlinearity preserving non-affine mappings not lying in the class of Proposition 3.17.*

Proof. The number of the nonlinearity preserving mappings defined in Proposition 3.17 is strictly less than

$$2^{2^{2n}} 2^{(n+1)(2^{2^n} - 2^n)} = 2^{2^{2n} + (n+1)(2^{2^n} - 2^n)} \ .$$

For $3 \leq n \leq 6$, using Table 3.1 we can easily verify that

$$2^{2^{2n}+(n+1)(2^{2^n}-2^n)} < \#(\mathscr{P}_n(\mathsf{N})) \ .$$

For $n \geq 7$ the ratio of $\#(\mathscr{A}_n)$ to $\#(\mathscr{F}_n)$ will decrease as n increases. Thus, for $n \geq 3$, mappings coming from Proposition 3.17 do constitute just a proper subset of $\mathscr{P}_n(\mathsf{N})$. □

Even if these new mappings have not been described with their algebraic normal form, we present some examples for $n = 3, 4, 6$ in Appendix C to illustrate the situation.

In deed, in a generic way, one can easily construct new nonlinearity preserving mappings in the following way. Consider two different affine equivalency classes of the same nonlinearity values, for instance regard the classes given in [6, 96, 52, 15]. Taking into account of the bijectivity property of the transformation, map the one of affine equivalency class members to the other class. Basically, while mapping the rest to themselves, select at least two functions belonging to the different affine equivalency classes and then map each to the other to produce a bijective nonlinearity preserving mapping. By Proposition 3.17, it is certain that the transformations created as above won't belong to the explicitly known non-affine bijective nonlinearity preserving mapping. Moreover these transformations will not produce the same orbit structure as affine equivalency mappings.

Open Problem 3.24. Is it possible to construct explicitly the nonlinearity preserving bijective mappings that lie in the definition given in Proposition 3.17?

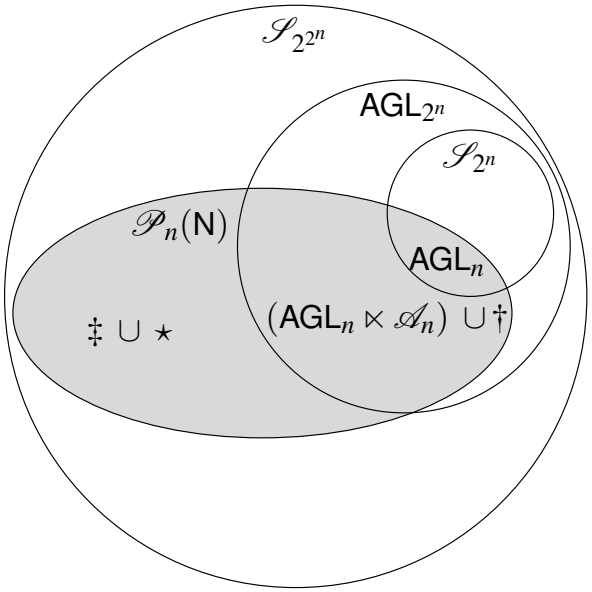
Beside the partial solutions and results given above, the enumeration and the classification problem for $\mathscr{P}_n(\mathsf{N})$ is still an open problem. The current state of the classification of nonlinearity preserving mappings is illustrated in Figure 3.3.

We believe beside the theoretical curiosity, these mappings if a generic construction would be achieved, might have led to a new practical tool for search and construction of new function families.

3.5 Automorphism Group of Nonlinearity Classes

There are some proposals in the literature stating that the automorphism group of the bent functions set $\mathscr{B}_n$ is just the group $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ [138, 28].

Definitely, each element of $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ gives us an automorphism in the sense of stabilizing the bentness property of the functions. However, there are other transformations mapping $\mathscr{B}_n$ to itself which are not lying in the group $\mathsf{AGL}_n \ltimes \mathscr{A}_n$. This observation suggests that the definition of automorphism group of bent functions should be reformulated. For example, for $n = 4$, there are $|\mathscr{P}_4(\mathsf{N})| \approx 2^{829564}$ bijective mappings preserving nonlinearity. However, only $896! \approx 2^{7500}$ of them constitute different permutations on $\mathscr{B}_4$, while $|\mathsf{AGL}_4 \ltimes \mathscr{A}_4| \approx 2^{23}$. Thus, $\mathsf{AGL}_4 \ltimes \mathscr{A}_4$ must only be a proper subset of the whole automorphism group (stabilizer) of bent functions set $\mathscr{B}_n$.



$\dagger : \mathscr{P}_n(\mathsf{N}) \cap (\mathsf{AGL}_{2^n} - (\mathsf{AGL}_n \ltimes \mathscr{A}_n))$, see Theorem 3.15

$\ddagger$: see Proposition 3.17

$\star$: see Theorem 3.23

Figure 3.3: Current state of nonlinearity preserving bijective transformations.

This new treatment of automorphisms suggests that main cryptographical design concerns for the automorphism groups in the common literature should be criticized. For example in [138], it is shown that $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ preserves nonlinearity by preserving the distance between the function to its closest affine function. However, it is an unnecessarily strong condition for cryptographic purposes because preserving the distance of any function to the affine function class is ample. More generally, determination of the automorphism group of nonlinearity classes should be studied as a subgroup of $\mathscr{S}_{2^{2^n}}$ since $\mathsf{AGL}_n \ltimes \mathscr{A}_n \leq \mathscr{P}_n(\mathsf{N})$.

In fact, the procedure followed for $\mathscr{B}_n$ is naturally applicable to all nonlinearity partitions N_t of $\mathscr{F}_n$. Therefore, the concept should be given explicitly at the beginning. One of the explicit way would be first to define the action of considered permutation group, and then under the action this group, gathering the mappings that stabilize the particular set of functions would be more convenient.

CHAPTER 4

HAMMING WEIGHT PRESERVING PERMUTATIONS

In the previous chapter, we studied the nonlinearity preserving bijective mappings and presented some results. Such an analysis can be pursued for the other design criteria as well.

For any design criterion C, we can define the set $\mathscr{P}_n(\mathsf{C})$ of bijective mappings which leaves the criterion C invariant, that is

$$\mathscr{P}_n(\mathsf{C}) = \{\psi \in \mathscr{S}_{2^{2^n}} \mid \mathsf{C}_f = \mathsf{C}_{\psi f} \text{ for all } f \in \mathscr{F}_n\}. \tag{4.1}$$

In fact, for any criterion C, $\mathscr{P}_n(\mathsf{C})$ forms a subgroup of $\mathscr{S}_{2^{2^n}}$, i.e.

Proposition 4.1. *$\mathscr{P}_n(C)$ is a subgroup of $\mathscr{S}_{2^{2^n}}$.*

Proof. Trivially, the identity mapping of $\mathscr{S}_{2^{2^n}}$ lies in $\mathscr{P}_n(\mathsf{C})$, thus it is not empty. Take any $\psi, \theta \in \mathscr{P}_n(\mathsf{C})$. Then, we have $\mathsf{C}_f = \mathsf{C}_{\psi f}$ and $\mathsf{C}_f = \mathsf{C}_{\theta f}$ for all $f \in \mathscr{F}_n$ and $\mathsf{C}_f = \mathsf{C}_{\theta(\psi f)} = \mathsf{C}_{(\theta\psi)f}$. Thus the assertion follows. □

In the rest of this chapter, we are going to study the mappings that preserve the Hamming weight of the functions.

At first sight, it may seem that the concepts of nonlinearity preserving and Hamming weight preserving are in a way equivalent. Thus, here at the very beginning we will make some clarifications and show the differences.

The necessary and sufficient condition for a nonlinearity preserving mapping is to conserve the minimum distance to the affine functions set, namely $\mathscr{A}_n$. More formally for each function $f \in \mathscr{F}_n$ we have

$$\psi \in \mathscr{P}_n(\mathsf{N}) \iff \min \mathsf{d}(f, \mathscr{A}_n) = \min \mathsf{d}(\psi f, \mathscr{A}_n), \tag{4.2}$$

where $\min \mathsf{d}(f, \mathscr{A}_n) = \mathsf{N}_f = \min\limits_{\ell_{\alpha,a} \in \mathscr{A}_n} \mathsf{d}(f, \ell_{\alpha,a})$.

On the other hand, the necessary and sufficient condition for a Hamming weight preserving mapping is to keep the distance to the linear function ℓ_{α_0} (i.e. the function

having only zeros in its truth table) unchanged. In other words, for each function $f \in \mathscr{F}_n$ we have

$$\psi \in \mathscr{P}_n(\mathsf{w}) \iff \mathsf{d}(f, \ell_{\alpha_0}) = \mathsf{d}(\psi f, \ell_{\alpha_0}). \tag{4.3}$$

As it can be seen explicitly from the two statement given above, the enumeration and classification problems for Hamming weight preserving mappings and nonlinearity preserving mappings are not the same.

Now, let's formally state the Hamming weight preserving bijective mappings $\mathscr{P}_n(\mathsf{w})$ subgroup as follows;

$$\mathscr{P}_n(\mathsf{w}) = \{\psi \in \mathscr{S}_{2^{2^n}} \mid \mathsf{w}(f) = \mathsf{w}(\psi f) \text{ for all } f \in \mathscr{F}_n\}.$$

We have an immediate proposition that states the necessary and sufficient condition for a mapping to leave Hamming weight invariant.

Proposition 4.2. *ψ preserves Hamming weight if and only if the Walsh spectrum value of f at $\omega = \alpha_0$ remains unchanged, that is*

$$W_f(\alpha_0) = W_{\psi f}(\alpha_0) \quad \textit{for all } f \in \mathscr{F}_n.$$

Proof. Recall that

$$\begin{aligned} \mathsf{W}_f(\alpha_0) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) \oplus \langle x, \alpha_0 \rangle} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} \quad (\text{Since } \langle x, \alpha_0 \rangle = 0 \text{ for all } x \in \mathbb{F}_{2^n}) \\ &= 2^n - 2\#(\mathsf{sup}(f)) \end{aligned}$$

Now the assertion follows. □

As we did for nonlinearity criterion, we can also construct a well-defined partitioning for the Boolean functions set $\mathscr{F}_n$ into Hamming weight classes, i.e.,

$$\begin{aligned} \mathsf{w}_0 &:= \{\ell_{\alpha_0}\}, \\ \mathsf{w}_1 &:= \{f \in \mathscr{F}_n \mid \mathsf{w}(f) = 1\}, \\ \mathsf{w}_2 &:= \{f \in \mathscr{F}_n \mid \mathsf{w}(f) = 2\}, \\ \mathsf{w}_3 &:= \{f \in \mathscr{F}_n \mid \mathsf{w}(f) = 3\}, \\ &\vdots \\ \mathsf{w}_{2^{n-1}} &:= \{f \in \mathscr{E}_n\}, \quad \text{(i.e. balanced functions.)} \\ &\vdots \\ \mathsf{w}_{2^n} &:= \{\ell_{\alpha_{2^n-1}}\}, \end{aligned}$$

with

$$\mathscr{F}_n = \bigcup_{0 \le i \le 2^n} \mathsf{w}_i.$$

Clearly, $\mathsf{w}_i \cap \mathsf{w}_j = \varnothing$ for $i \neq j$, hence this is indeed a well-defined partition of $\mathscr{F}_n$. Furthermore, for all $0 \le i \le 2^n$, since we have to choose i coordinates out of 2^n for constructing a function of weight i, we can easily derive the cardinality of each w_i. That is, for each $0 \le i \le 2^n$, we have

$$\#(\mathsf{w}_i) = \tbinom{2^n}{i}. \tag{4.4}$$

Based on the cardinalities of Hamming weight classes, we easily enumerate the Hamming weight preserving bijective mappings.

Theorem 4.3. *Let $\mathscr{F}_n$ be partitioned into Hamming weight classes w_i such that*

$$\mathscr{F}_n = \bigcup_{0 \le i \le 2^n} \mathsf{w}_i \ .$$

Then,

$$\#(\mathscr{P}_n(\mathsf{w})) = \prod_{0 \le i \le 2^n} \tbinom{2^n}{i}! \ . \tag{4.5}$$

Proof. Note that we have,

$$\#(\mathscr{P}_n(\mathsf{w})) = \prod_{0 \le i \le 2^n} \#(\mathsf{Sym}(\mathsf{w}_i)).$$

Then, by using (4.4) we derive the statement. □

In fact, following the notions above, we can also enumerate the bijective mappings that preserve balancedness property of the balanced functions but not necessarily the Hamming weight for all the other functions. For such mappings the sufficient condition is to map $\mathscr{E}_n$ onto itself. Therefore we have the following corollary.

Corollary 4.4. *For $n \in \mathbb{N}$, there are*

$$\tbinom{2^n}{2^{n-1}}! \, (2^{2^n} - \tbinom{2^n}{2^{n-1}})!$$

bijective mappings in $\mathscr{S}_{2^{2^n}}$ that necessarily keep balancedness property invariant.

Proof. For $n \in \mathbb{N}$, we know that $\#(\mathsf{w}_{2^{n-1}}) = \#(\mathscr{E}_n) = \tbinom{2^n}{2^{n-1}}$. For any $\psi \in \mathscr{S}_{2^{2^n}}$ the only constraint then will be

$$\psi : \mathscr{E}_n \mapsto \mathscr{E}_n.$$

Regarding the bijective property ψ should map the remaining elements to each other. Thus the statement now follows. □

So far, we have completely solve the enumeration problem for the Hamming weight preserving bijective mappings. Next we will focus on the question: Is it possible to construct these Hamming weight preserving mappings explicitly.

4.1 Affine Bijective Mappings (AGL_{2^n})

Theorem 4.5. *[86]*

$$\mathscr{S}_{2^n} \subset \mathscr{P}_n(\mathsf{w}).$$

Proof. Recall from (3.10) that any mapping $\psi \in \mathscr{S}_{2^n}$ is of the form:

$$\psi : [\mathsf{T}_f] \mapsto P[\mathsf{T}_f]$$

for a fixed permutation matrix $P \in \mathscr{S}_{2^n}$ of order 2^n. Hence, each $\psi \in \mathscr{S}_{2^n}$ will only permute position of image values in the truth table but also keep the each value unchanged. Thus, we conclude that

$$\mathscr{S}_{2^n} \subset \mathscr{P}_n(\mathsf{w}).$$

□

The theorem above includes that the bijective mappings belonging to the subgroups $\mathscr{S}_n$, $\mathscr{T}_n$ and GL_n and AGL_n are all weight preserving and hence are all included in $\mathscr{P}_n(\mathsf{w})$.

In fact, using a proper subgroup of $\mathscr{S}_{2^n}$, a further partitioning of the Hamming weight classes, i.e. w_i's, is also possible. To the best of our knowledge, chronologically, following the Slepian [134] and Harrison [65], Lechner formally studied the orbits of GL_n and AGL_n, see [86]. Under the action of GL_n, Lechner presented the equivalence classes of n variable Boolean functions of weight m, for $0 \leq m \leq 19$ and $1 \leq n \leq 9$.

Claim 4.6. *Let $\psi \in \mathsf{AGL}_n \ltimes \mathscr{T}_{2^n}$ such that*

$$\psi : f(x) \mapsto f(xA \oplus \alpha) \oplus g(x) \quad .$$

Then $\psi \in \mathscr{P}_n(\mathsf{w})$ if and only if $g = \ell_{\alpha_0} \in \mathscr{L}_n$.

Proof. Necessary and sufficiency condition for g follows particularly from the all-zero function, i.e. $\mathsf{w}(\ell_{\alpha_0}) = \mathsf{w}(g)$, and by Theorem 4.5 we derive the assertion. □

Hence, we have

$$\mathscr{P}_n(\mathsf{w}) \cap (\mathsf{AGL}_n \ltimes \mathscr{T}_{2^n}) = \mathsf{AGL}_n \subset \mathscr{S}_{2^n}.$$

Claim 4.7. *Let $\psi \in \mathsf{GL}_{2^n}$ be a linear bijective transformation, such that for all $f \in \mathscr{F}_n$,*

$$\psi : [T_f] \mapsto M[T_f]$$

where $M \in \mathsf{GL}_{2^n}$ is fixed.

$\psi \in \mathscr{P}_n(\mathsf{w})$ if and only if $M \in \mathscr{S}_{2^n}$ is a permutation matrix of order 2^n.

Proof. If $M \in \mathscr{S}_{2^n}$, the statement trivially holds by Theorem 4.5.

Let M be written in column based form as $M = [[\lambda_1]\ [\lambda_2]\ \ldots\ [\lambda_{2^n}]]$. Suppose, $\psi \in \mathscr{P}_n(\mathsf{w})$, which means that it keeps Hamming weight invariant for all functions in $\mathscr{F}_n$. Without loss of generality, consider the functions e_i with Hamming weight 1 and e_{ij} with weight 2.

For e_i, $1 \leq i \leq 2^n$ with $\mathsf{w}(e_i) = 1$, we have

$$\psi(\mathsf{T}_{e_i}) = \lambda_i.$$

Since $\mathsf{w}(e_i) = 1$, we conclude that the functions g_i such that $\lambda_j := \mathsf{T}_{g_i}$ satisfy $\mathsf{w}(g_i) = 1$ for all $1 \leq i \leq 2^n$.

Similarly, for the functions of e_{ij} with $\mathsf{w}(e_{ij}) = 2$ for all $1 \leq i, j \leq 2^n$ with $i \neq j$, we have

$$\psi(\mathsf{T}_{e_{ij}}) = \lambda_i \oplus \lambda_j,$$

and hence $\lambda_i \neq \lambda_j$ for $i \neq j$. By combining these results, we prove that $M \in \mathscr{S}_{2^n}$, which concludes the proof. □

Thus, we again have

$$\mathscr{P}_n(\mathsf{w}) \cap \mathsf{GL}_{2^n} = \mathscr{S}_{2^n}.$$

Claim 4.8. *Let $\psi \in \mathsf{AGL}_{2^n}$ be an affine bijective transformation so that for all $f \in \mathscr{F}_n$,*

$$\psi : [T_f] \mapsto M[T_f] \oplus [T_g]$$

where $g \in \mathscr{F}_n$ and $M \in \mathsf{GL}_{2^n}$ are fixed.

$\psi \in \mathscr{P}_n(\mathsf{w})$ if and only if $g = \ell_{\alpha_0}$ and $M \in \mathscr{S}_{2^n}$ is a permutation matrix of order 2^n.

Proof. Similarly, necessary and sufficiency condition for the function g follows particularly from the all-zero function, i.e. $\mathsf{w}(\ell_{\alpha_0}) = \mathsf{w}(g)$, and by Claim 4.7 the statement follows.

□

Therefore, we still get

$$\mathscr{P}_n(\mathsf{w}) \cap \mathsf{AGL}_{2^n} = \mathscr{S}_{2^n}.$$

4.2 Non-affine Bijective Mappings ($\mathscr{S}_{2^{2^n}} - \mathsf{AGL}_{2^n}$)

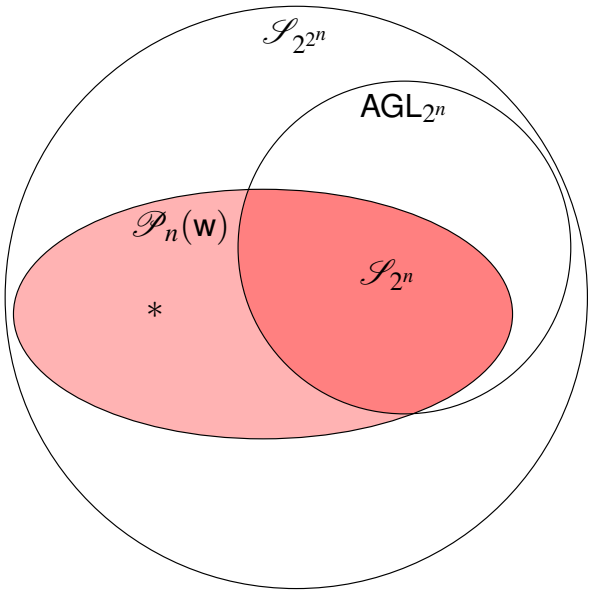
In the previous section, we demonstrated and proved that

$$\mathscr{P}_n(\mathsf{w}) \cap \mathsf{AGL}_{2^n} = \mathscr{S}_{2^n}.$$

On the other hand, by Theorem 4.3 we know that

$$\#(\mathscr{P}_n(\mathsf{w})) = \prod_{0 \leq i \leq 2^n} \binom{2^n}{i}! \ .$$

Therefore, with a direct comparison of the cardinalities of both $\mathscr{P}_n(\mathsf{w})$ and $\mathscr{S}_{2^n}$, one can easily conclude the existence of non-affine Hamming weight preserving mappings.



$*$: see Proposition 4.9

Figure 4.1: Current state of Hamming weight preserving bijective transformations.

Proposition 4.9. *Let $n \in \mathbb{N}$ be such that $n \geq 2$. There exist non-affine mappings, i.e. lying in the set $\mathscr{S}_{2^{2^n}} - \mathsf{AGL}_{2^n}$, that leave Hamming weight invariant for all functions in $\mathscr{F}_n$.*

Proof. Trivially follows from the fact

$$\#(\mathscr{P}_n(\mathsf{w})) = \prod_{0 \leq i \leq 2^n} \binom{2^n}{i}! > (2^n)! = \#(\mathscr{S}_{2^n}) \ .$$

□

Unfortunately, we could not manage to explicitly construct those non-affine Hamming weight preserving bijective mappings. As proved in Proposition 4.9 and illustrated in Figure 4.1, we know the existence.

Open Problem 4.10. Is it possible to construct explicitly the Hamming weight preserving bijective mappings that belong to the set $\mathscr{S}_{2^{2^n}} - \mathsf{AGL}_{2^n}$ (as existence proved Proposition 4.9)?

Despite the fact that, the Hamming weight classes, w_i's, are known, the study on the Hamming weight preserving mappings may still lead some practical tools for cryptographic tools. For example, consider the balanced functions. When some generic non-affine Hamming weight preserving mapping families are known, applying these mapping to the balanced functions might lead to other balanced functions with higher criterion values.

CHAPTER 5

CONCLUSION

5.1 Future Work

We have presented two open questions. One for non-affine nonlinearity preserving bijective mappings and the other for non-affine Hamming weight preserving bijective mappings, see Open Problem 3.24 and 4.10, respectively. These problems may seem vey involving but on the other hand they may lead to a very useful tool for practical cryptography.

Another completely unresolved issue is the definition of the automorphism of nonlinearity classes. We have pointed out some in a way contradicting notions but a deeper analysis would be useful.

Last but not the least, same procedures might be easily pursued for the other design criteria. It is conceptually obvious that following the same way would give similar results for almost all of the other design criteria.

5.2 Summary

We have extended the family of bijective mappings to the maximal group, namely $\mathscr{S}_{2^{2^n}}$. We studied the action of these bijective mapping on the set of all n variable Boolean functions. We tried to answer the enumeration and classification problem for nonlinearity and Hamming weight preserving bijective mappings, independently. Unfortunately, we have only supplied partial results in both cases. But on the other hand, we have presented a different perspective for the bijective mappings acting on Boolean functions.

We first stated the representation of the bijective mappings based on the coordinate functions algebraic normal form. Following this representation, we listed the our focal subgroups. Then we analyze the action of these bijective mappings regarding these subgroups. Our aim was to enumerate and classify these bijective mappings with respect to preserving a cryptographic design criterion. After the necessary definitions and notions, we mainly studied the nonlinearity preserving bijective mappings. Then we applied the procedures that we constructed on nonlinearity preservability to another

cryptographic design criterion, namely the Hamming weight.

At the bottom-line, from a theoretical viewpoint, we have shown the existence of new families of bijective mappings that leaves nonlinearity (respectively, Hamming weight) invariant. This is the fundamental result of this study. Even if we have not studied these mappings for the other design criteria such as correlation immunity, propagation criterion, algebraic immunity, one can foresee that similar results might be also gathered.

We believe that that these mappings evolve into a practical tool in cryptography. However, for the moment we have not manage to construct such a tool yet. Studying the elements $\mathscr{S}_{2^n}$ and classifying them with respect to nonlinearity preserving property is still an open problem. Due to the huge cardinality of the mappings, pursuing this research may seem to be highly involved. Despite this fact, it may lead to a deeper insight to the nonlinear functions or nonlinearity classes and additionally it may become a practical tool for constructions of new Boolean functions.

We are concluding the thesis with the summary of our results as follows.

5.2.1 Nonlinearity Preserving Bijective Mappings

Our first focal point was to try to enumerate and classify the nonlinearity preserving bijective mappings. On the one hand, we categorically and explicitly constructed new nonlinearity preserving mapping families both in the affine subgroup (i.e. in AGL_{2^n}) and in the non-affine set (namely in $\mathscr{S}_{2^n} - \mathsf{AGL}_{2^n}$). More precisely, we can summarize our results on stabilizing nonlinearity property as follows.

- We have given the necessary and sufficient conditions for a linear mapping which belongs to the subgroup GL_{2^n}.
- Next, we have presented necessary and sufficient conditions of nonlinearity preserving affine mapping, i.e AGL_{2^n}. Meanwhile we also proved the existence of nonlinearity preserving mappings in $\mathsf{AGL}_{2^n} - (\mathsf{AGL}_n \ltimes \mathscr{A}_n)$.
- Furthermore, we have demonstrated and explicitly constructed an isomorphism between the group of affine equivalency mappings $\mathsf{AGL}_n \ltimes \mathscr{A}_n$ and the automorphism group of the Sylvester Hadamard matrices $\mathsf{Aut}(\mathsf{H}_n)$. Immediately following this result we have given the exact cardinality of $\mathsf{Aut}(\mathsf{H}_n)$.
- In addition, we have given sufficient conditions for non-affine nonlinearity preserving bijective mappings that belong to the set $\mathscr{S}_{2^n} - \mathsf{AGL}_{2^n}$. Thus we have constructed a family of non-affine nonlinearity preserving bijective mappings explicitly. But, later we have shown that all of these explicitly constructed nonlinearity preserving bijective mappings produce the same orbit structure as the affine equivalency mappings.
- Finally, we have given the exact number of nonlinearity preserving bijective mappings for $n \leq 6$. Then, based on these cardinalities, we proved the existence of new non-affine nonlinearity preserving mappings, without construct-

ing explicitly. We demonstrated some illustrative examples for these non-affine mappings.

Formerly, it was proposed that automorphism group of bent functions is $\mathsf{AGL}_n \ltimes \mathscr{A}_n$. In this work, it is shown that there are new transformations keeping nonlinearity invariant. Therefore, such propositions should be reexamined by means of considering a larger set than $\mathsf{AGL}_n \ltimes \mathscr{A}_n$. For future studies, it would be interesting to further investigate nonlinearity preserving mappings in order to construct those mappings with explicit methods.

5.2.2 Hamming Weight Preserving Bijective Mappings

Following the nonlinearity criterion, we also studied the enumeration and classification of Hamming weight preserving bijective mappings under the action of the maximal group $\mathscr{S}_{2^{2^n}}$.

- First we completely solve the enumeration problem of Hamming weight preserving bijective mappings, and for any $n \in \mathbb{N}$ presented the exact number of the Hamming weight preserving bijective mappings.
- Afterwards, we studied the classification problem and give partial results related to this problem. We restated that Hamming weight is preserved under the action of $\mathscr{S}_{2^n}$.
- Next, we prove that among the affine bijective mappings only the elements of $\mathscr{S}_{2^n}$ preserve the Hamming weight.
- Finally, again based on the enumeration of the Hamming weight preserving bijective mappings we proved the existence of Hamming weight preserving non-affine bijective mappings.

REFERENCES

[1] S. S. Agaian, *Hadamard Matrices and Their Applications*, volume 1168 of *Lecture Notes in Mathematics*, Springer-Verlag, 1985.

[2] J. L. Alperin and R. B. Bell, *Groups and Representations*, volume 162 of *Graduate texts in Mathematics*, Springer, 1995.

[3] E. Artin, *Geometric Algebra*, Interscience Publishers, 1957.

[4] K. G. Beauchamp, *Applications of Walsh and Related Functions, with an introduction to sequency theory*, Microelectronics and signal processing, Academic Press, London, Orlando, 1984.

[5] T. Berger and P. Charpin, The automorphism group of Generalized Reed-Muller codes, Discrete Mathematics, 117(1–3), pp. 1 – 17, 1993.

[6] E. Berlekamp and L. Welch, Weight Distributions of the Cosets of the $(32, 6)$ Reed-Muller Code, Information Theory, IEEE Transactions on, 18(1), pp. 203–207, Jan 1972.

[7] A. Bernasconi and B. Codenotti, Spectral Analysis of Boolean Functions as a Graph Eigenvalue Problem, Computers, IEEE Transactions on, 48(3), pp. 345–351, Mar 1999.

[8] E. Biham and O. Dunkelman, *Techniques for Cryptanalysis of Block Ciphers*, Information Security and Cryptography, Springer, 2014.

[9] E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology, 4(1), pp. 3–72, 1991.

[10] E. Biham and A. Shamir, *Differential Cryptanalysis of Data Encryption Standard*, Springer-Verlag, 1993.

[11] E. Biham and A. Shamir, Differential Cryptanalysis of the Full 16-round DES, in E. Brickell, editor, *Advances in Cryptology — CRYPTO' 92*, volume 740 of *Lecture Notes in Computer Science*, pp. 487–496, Springer Berlin Heidelberg, 1993.

[12] G. Boole, *The Mathematical Analysis of Logic: Being an Essay Towards a Calculus of Deductive Reasoning*, B. Blackwell, 1847.

[13] G. Boole, *An Investigation of the Laws of Thought: on which are founded the mathematical theories of logic and probabilities*, volume 2, Walton and Maberly, 1854.

[14] Y. Borissov, A. Braeken, S. Nikova, and B. Preneel, On the Covering Radius of Second Order Binary Reed-Muller Code in the Set of Resilient Boolean Functions, in K. Paterson, editor, *Cryptography and Coding*, volume 2898 of *Lecture Notes in Computer Science*, pp. 82–92, Springer Berlin Heidelberg, 2003.

[15] A. Braeken, *Cryptographic Properties of Boolean Functions and S-Boxes*, Ph.D. thesis, Katholieke Universiteit Leuven, Leuven, Belgium, 2006.

[16] A. Braeken, Y. Borissov, S. Nikova, and B. Preneel, Classification of Boolean Functions of 6 Variables or Less with Respect to Some Cryptographic Properties, in L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, editors, *Automata, Languages and Programming*, volume 3580 of *Lecture Notes in Computer Science*, pp. 324–334, Springer Berlin Heidelberg, 2005.

[17] A. Braeken, S. Nikova, and Y. Borissov, Classification of Cubic Boolean Functions in 7 variables, in *Proceedings of 26th Symposium on Information Theory in the Benelux*, pp. 285–292, Brussels, Belgium, May 2005.

[18] L. Breveglieri, A. Cherubini, and M. Macchetti, On the Generalized Linear Equivalence of Functions Over Finite Fields, in P. Lee, editor, *Advances in Cryptology - ASIACRYPT 2004*, volume 3329 of *Lecture Notes in Computer Science*, pp. 79–91, Springer Berlin Heidelberg, 2004.

[19] R. D. Brown, A Recursive Algorithm for Sequency-Ordered Fast Walsh Transforms, Computers, IEEE Transactions on, C-26(8), pp. 819–822, August 1977.

[20] L. Budaghyan and C. Carlet, CCZ-equivalence and Boolean functions, Cryptology ePrint Archive, Report 2009/063, 2009.

[21] P. J. Cameron, *Permutation Groups*, volume 45, Cambridge University Press, 1999.

[22] G. Cantor, Beiträge zur begründung der transfiniten mengenlehre I, Mathematische Annalen, 46, pp. 481–512, 1895.

[23] G. Cantor, Beiträge zur begründung der transfiniten mengenlehre II, Mathematische Annalen, 49, pp. 207–246, 1897.

[24] C. Carlet, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, chapter Boolean Functions for Cryptography and Error Correcting Codes, pp. 257–397, Cambridge University Press, New York, NY, USA, 1st edition, 2010.

[25] C. Carlet, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, chapter Vectorial Boolean Functions for Cryptography, pp. 398–469, Cambridge University Press, New York, NY, USA, 1st edition, 2010.

[26] C. Carlet, P. Charpin, and V. Zinoviev, Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems, Design Codes and Cryptography, 15, pp. 125–156, November 1998.

[27] C. Carlet and P. Guillot, A New Representation of Boolean Functions, in M. Fossorier, H. Imai, S. Lin, and A. Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1719 of *Lecture Notes in Computer Science*, pp. 94–103, Springer Berlin Heidelberg, 1999.

[28] C. Carlet and S. Mesnager, On Dillon's Class H of Bent Functions, Niho Bent Functions and O-Polynomials, Cryptology ePrint Archive, Report 2010/567, 2010.

[29] A. Cayley, Desiderata and Suggestions: No. 2. The Theory of Groups: Graphical Representation, American Journal of Mathematics, 1(2), pp. 174–176, 1878.

[30] D. Chaum and J.-H. Evertse, Cryptanalysis of DES with a Reduced Number of Rounds, in H. C. Williams, editor, *Advances in Cryptology — CRYPTO '85 Proceedings*, volume 218 of *Lecture Notes in Computer Science*, pp. 192–211, Springer Berlin Heidelberg, 1986.

[31] J. W. Cooley and J. W. Tukey, An Algorithm for the Machine Calculation of Complex Fourier Series, Math. comput, 19(90), pp. 297–301, 1965.

[32] D. Coppersmith, H. Krawczyk, and Y. Mansour, The shrinking generator, in D. Stinson, editor, *Advances in Cryptology – CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pp. 22–39, Springer Berlin Heidelberg, 1994.

[33] N. T. Courtois and W. Meier, Algebraic attacks on stream ciphers with linear feedback, in E. Biham, editor, *Advances in Cryptology — EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pp. 345–359, Springer Berlin Heidelberg, 2003.

[34] Y. Crama and P. L. Hammer, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, volume 134 of *Encyclopedia of Mathematics and Its Applications*, Cambridge University Press, 2010.

[35] Y. Crama and P. L. Hammer, *Boolean functions: theory, algorithms, and applications*, volume 142 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, 2011.

[36] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*, volume 55 of *North Holland Mathematical Library*, Elsevier, 1998.

[37] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*, Academic Press, 2009.

[38] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Information Security and Cryptography, Springer-Verlag, 2002.

[39] W. De Launey and D. L. Flannery, *Algebraic Design Theory*, volume 175, American Mathematical Society, 2011.

[40] J. Denev and V. Tonchev, On the Number of Equivalence Classes of Boolean Functions under a Transformation Group (Corresp.), Information Theory, IEEE Transactions on, 26(5), pp. 625–626, Sep 1980.

[41] W. Diffie and M. Hellman, New directions in cryptography, Information Theory, IEEE Transactions on, 22(6), pp. 644–654, Nov 1976.

[42] J. F. Dillon, A Survey of Bent Functions, The NSA Technical Journal, Spacial Issue, pp. 191–215, 1972.

[43] J. F. Dillon, *Elementary Hadamard difference sets*, Ph.D. thesis, University of Maryland, College Park, MD, USA, 1974.

[44] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, in B. Preneel, editor, *Fast Software Encryption*, volume 1008 of *Lecture Notes in Computer Science*, pp. 61–74, Springer Berlin Heidelberg, 1995.

[45] X. dong Hou, Some Results on the Covering Radii of Reed-Muller codes, Information Theory, IEEE Transactions on, 39(2), pp. 366–378, Mar 1993.

[46] X. dong Hou, $GL(m,2)$ acting on $R(r,m)/R(r-1,m)$, Discrete Mathematics, 149(1-3), pp. 99 – 122, 1996.

[47] J.-H. Evertse, Linear Structures in Blockciphers, in D. Chaum and W. L. Price, editors, *Advances in Cryptology — EUROCRYPT' 87*, volume 304 of *Lecture Notes in Computer Science*, pp. 249–266, Springer Berlin Heidelberg, 1988.

[48] H. Feistel, Cryptography and Computer Privacy, Scientific American, 228(5), pp. 15–23, May 1973.

[49] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography engineering: design principles and practical applications*, John Wiley & Sons, first edition, 2010.

[50] R. Forré, The Strict Avalanche Criterion: Spectral Properties of Boolean Functions and an Extended Definition, in S. Goldwasser, editor, *Advances in Cryptology — CRYPTO' 88*, volume 403 of *Lecture Notes in Computer Science*, pp. 450–468, Springer New York, 1990.

[51] J. Fuller, E. Dawson, and W. Millan, Evolutionary Generation of Bent Functions for Cryptography, in *Proceedings of Congress Evolutionary Computation CEC '03*, volume 3, pp. 1655–1661, 2003.

[52] J. E. Fuller, *Analysis of affine equivalent Boolean functions for cryptography*, Ph.D. thesis, Queensland University of Technology, Queensland, Australia, 2003.

[53] J. Golić, Cryptanalysis of Alleged A5 Stream Cipher, in W. Fumy, editor, *Advances in Cryptology – EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pp. 239–255, Springer Berlin Heidelberg, 1997.

[54] S. W. Golomb, *Shift Register Sequences*, Holden-Day Series in Information Systems, Holden-Day, 1967.

[55] C. Günther, Alternating step generators controlled by De Bruijn sequences, in D. Chaum and W. L. Price, editors, *Advances in Cryptology – EUROCRYPT '87*, volume 304 of *Lecture Notes in Computer Science*, pp. 5–14, Springer Berlin Heidelberg, 1988.

[56] J. Hadamard, Résolution d'une question relative aux déterminants, Bull. Sciences Math., 2(17), pp. 240–246, 1893.

[57] M. Hall, Jr., Note on the Mathieu group $\mathscr{M}_{12}$, Archiv der Mathematik, 13, pp. 334–340, 1962.

[58] M. Hall, Jr., Group properties of Hadamard matrices, Journal of Australian Mathematical Society Series A, 21(2), pp. 247–256, 1976.

[59] M. Hall, Jr., *Combinatorial Theory*, volume 71 of *Wiley Classics Library*, John Wiley and Sons, second edition, 1998.

[60] R. W. Hamming, Error Detecting and Error Correcting Codes, Bell System Technical Journal, 29(2), pp. 147–160, 1950.

[61] M. A. Harrison, *Combinatorial Problems in Boolean Algebras and Applications to the Theory of Switching*, Ph.D. thesis, University of Michigan, Michigan, United States, June 1963.

[62] M. A. Harrison, The number of classes of invertible Boolean functions, Journal of the ACM (JACM), 10(1), pp. 25–28, 1963.

[63] M. A. Harrison, The number of equivalence classes of Boolean functions under groups containing negation functions under groups containing negation, Electronic Computers, IEEE Transactions on, (5), pp. 559–561, 1963.

[64] M. A. Harrison, The number of transitivity sets of Boolean functions, Journal of the Society for Industrial & Applied Mathematics, 11(3), pp. 806–828, 1963.

[65] M. A. Harrison, On the classification of Boolean functions by the general linear and affine groups, Journal of the Society for Industrial & Applied Mathematics, 12(2), pp. 285–299, 1964.

[66] M. A. Harrison, *Introduction to Switching and Automata Theory*, McGraw-Hill Book Company, New York, NY, USA, 1965.

[67] M. A. Harrison, On asymptotic estimates in switching and automata theory, Journal of the ACM (JACM), 13(1), pp. 151–157, 1966.

[68] H. Henderson, F. Pukelsheim, and S. Searle, On the history of the kronecker product, Linear and Multilinear Algebra, 14, pp. 113–120, 1983.

[69] K. J. Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, Princeton, New Jersey, 2007.

[70] X.-d. Hou, Classification of cosets of the Reed Muller code $R(m-3,m)$, Discrete Mathematics, 128(1–3), pp. 203–224, 1994.

[71] X.-d. Hou, $AGL(m,2)$ Acting on $R(r,m)/R(s,m)$, Journal of Algebra, 171(3), pp. 921 – 938, 1995.

[72] I. M. Isaacs, *Finite Group Theory*, volume 92 of *Graduate Studies in Mathematics*, American Mathematical Society, 2008.

[73] N. Ito, Hadamard matrices with "doubly transitive" automorphism groups, Archiv der Mathematik, 35(1), pp. 100–111, 1980.

[74] C. J. A. Jansen, *Investigations on nonlinear streamcipher systems: construction and evaluation methods*, Ph.D. thesis, Technical University of Delft, Delft, Netherlands, 1989.

[75] J. B. Kam and G. I. Davida, Structured Design of Substitution-Permutation Encryption Networks, IEEE Transactions on Computers, 28(10), pp. 747–753, 1979.

[76] W. M. Kantor, Automorphism Groups of Hadamard Matrices, Journal of Combinatorial Theory, 6(3), pp. 279–281, 1969.

[77] M. Karnaugh, The map method for synthesis of combinational logic circuits, American Institute of Electrical Engineers, Part I: Communication and Electronics, Transactions of the, 72(5), pp. 593–599, 1953.

[78] M. G. Karpovsky, *Finite Orthogonal Series in the Desgins of Digital Devices*, John Wiley & Sons, New York, 1976.

[79] S. Kavut and M. D. Yücel, 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class, Information and Computation, 208(4), pp. 341 – 350, 2010.

[80] A. Kerckhoffs, La cryptographie militaire, Journal des sciences militaires, IX, pp. 5–38 & 161–191, jan 1883.

[81] E. L. Key, An analysis of the structure and complexity of nonlinear binary sequence generators, Information Theory, IEEE Transactions on, 22(6), pp. 732–736, Nov 1976.

[82] A. Klein, *Stream Ciphers*, Springer, 2013.

[83] L. R. Knudsen and M. Robshaw, *The Block Cipher Companion*, Information Security and Cryptography, Springer, 2011.

[84] P. Langevin and G. Leander, Counting all bent functions in dimension eight 99270589265934370305785861242880, Designs, Codes and Cryptography, Dec 2010.

[85] R. J. Lechner, *Affine Equivalence of Switching Functions*, Ph.D. thesis, Harvard University, Cambridge, Massachusetts, 1963.

[86] R. J. Lechner, A Correspondence Between Equivalence Classes of Switching Functions and Group Codes, Electronic Computers, IEEE Transactions on, EC-16(5), pp. 621–624, Oct 1967.

[87] R. J. Lechner, A Transform Approach to Logic Design, Computers, IEEE Transactions on, C-19(7), pp. 627–640, July 1970.

[88] R. J. Lechner, *Harmonic Analysis of Switching Functions*, chapter V, Electrical Science, A Series of Monographs and Texts, Academic Press, 1971.

[89] J. S. Leon, An Algorithm for Computing the Automorphism Group of a Hadamard Matrix, Journal of Combinatorial Theory, Ser. A, 27(3), pp. 289–306, 1979.

[90] D. E. Littlewood, *The Theory of Group Characters and Matrix Representations of Group*, Oxford University Press, London, 1950.

[91] L. H. Loomis, *An Introduction to Abstract Hamonic Analysis*, D. Van Nostrand Company, Princeton, New Jersey, 1953.

[92] C. S. Lorens, Invertible Boolean Functions, Electronic Computers, IEEE Transactions on, EC-13(5), pp. 529–541, Oct 1964.

[93] M. Macchetti, Addendum to "On the Generalized Linear Equivalence of Functions over Finite Fields", Cryptology ePrint Archive, Report 2004/347, 2004.

[94] M. Macchetti, M. Caironi, L. Breveglieri, and A. Cherubini, A Complete Formulation of Generalized Affine Equivalence, in M. Coppo, E. Lodi, and G. Pinna, editors, *Theoretical Computer Science*, volume 3701 of *Lecture Notes in Computer Science*, pp. 338–347, Springer Berlin / Heidelberg, 2005.

[95] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-holland Publishing Company, Amsterdam, 2nd edition, 1978.

[96] J. A. Maiorana, A Classification of the Cosets of the Reed-Muller Code $R(1,6)$, Mathematics of Computation, 57(195), pp. 403–414, July 1991.

[97] S. Maitra, Boolean functions on odd number of variables having nonlinearity greater than the bent concatenation bound, in B. Preneel and O. A. Logachev, editors, *NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (NATO ASI Zvenigorod, 2007)*, NATO Science for Peace and Security Series, pp. 173–182, IOS Press books, 2008.

[98] M. Matsui, The first experimental cryptanalysis of the data encryption standard, in Y. G. Desmedt, editor, *Advances in Cryptology – CRYPTO '94*, volume 839 of *Lecture Notes in Computer Science*, pp. 1–11, Springer Berlin Heidelberg, 1994.

[99] M. Matsui, Linear Cryptanalysis Method for DES Cipher, in T. Helleseth, editor, *Advances in Cryptlogy – EUROCRYPT 93*, volume 765 of *Lecture Notes in Computer Science*, pp. 386–397, Springer Berlin / Heidelberg, 1994.

[100] R. L. McFarland, A family of difference sets in non-cyclic groups, Journal of Combinatorial Theory, Series A, 15(1), pp. 1 – 10, 1973.

[101] W. Meier, E. Pasalic, and C. Carlet, Algebraic attacks and decomposition of boolean functions, in C. Cachin and J. L. Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pp. 474–491, Springer Berlin Heidelberg, 2004.

[102] W. Meier and O. Staffelbach, Nonlinearity Criteria for Cryptographic Functions, in J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology — EUROCRYPT '89*, volume 434 of *Lecture Notes in Computer Science*, pp. 549–562, Springer Berlin Heidelberg, 1990.

[103] W. Meier and O. Staffelbach, The self-shrinking generator, in A. De Santis, editor, *Advances in Cryptology – EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pp. 205–214, Springer Berlin Heidelberg, 1995.

[104] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, Discrete Mathematics and Its Applications, CRC press, first edition, 1996.

[105] D. E. Muller, Application of Boolean algebra to switching circuit design and error detection, IRE Trans. on Electronic Computers, 3, pp. 6–12, 1954.

[106] National Institute of Standards and Technology, FIPS 46-3: Data Encryption Standard (DES), Federal Information Processing Standards Publication Series, January 1977.

[107] National Institute of Standards and Technology, FIPS 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication Series, 2001.

[108] I. Ninomiya, *A study of the structures of Boolean functions and its application to the synthesis of switching circuits*, Ph.D. thesis, Nagoya University, Nagoya, Japan, 1958.

[109] L. O'Connor and A. Klapper, Algebraic nonlinearity and its applications to cryptography, Journal of Cryptology, 7(4), pp. 213–227, 1994.

[110] R. E. A. C. Paley, On orthogonal matrices, Journal of Mathematics and Physics, 12, pp. 311–320, 1933.

[111] J. Pieprzyk and G. Finkelstein, Towards effective nonlinear cryptosystem design, Computers and Digital Techniques, IEE Proceedings E, 135(6), pp. 325–335, 1988.

[112] B. Preneel, *Analysis and Design of Cryptographic Hash Functions*, Ph.D. thesis, Katholieke Universiteit Leuven, Leuven, Belgium, January 1993.

[113] B. Preneel and O. A. Logachev, *Boolean Functions in Cryptology and Information Security*, volume 18 of *NATO Science for Peace and Security Series - D: Information and Communication Security*, IOS Press, 2008.

[114] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, Propagation Characteristics of Boolean Functions, in I. B. Damgård, editor, *Advances in Cryptology – EUROCRYPT '90*, volume 473 of *Lecture Notes in Computer Science*, pp. 161–173, Springer Berlin / Heidelberg, 1991.

[115] I. S. Reed, A class of multiple-error-correcting codes and the decoding scheme, IRE Trans. on Inf. Theory, 3, pp. 6–12, 1954.

[116] R. L. Rivest, The RC4 Encryption Algorithm, 1987, rSA Data Security Inc.

[117] M. Robshaw and O. Billet, *New Stream Ciphers Designs: The eSTREAM Finalists*, volume 4986 of *Lecture Notes in Computer Science*, Springer, 2008.

[118] O. S. Rothaus, On "bent" functions, Journal of Combinatorial Theory, Series A, 20(3), pp. 300 – 305, 1976.

[119] T. Sasao, *Switching Theory for Logic Synthesis*, Kluwer Academic Publishers, Norwell, MA, USA, 1st edition, 1999.

[120] T. Sasao and J. T. Butler, *Progress in Applications of Boolean Functions*, volume 26 of *Synthesis Lectures on Digital Circuits and Systems*, Morgan & Claypool, 2010.

[121] B. Schneier, *Applied Cryptography*, John Wiley & Sons, second edition, 1996.

[122] J. Seberry, X. Zhang, and Y. Zheng, Nonlinearity and Propagation Characteristics of Balanced Boolean Functions, Information and Computation, 119(1), pp. 1 – 13, 1995.

[123] J. Seberry, X.-M. Zhang, and Y. Zheng, Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics, in D. R. Stinson, editor, *Advances in Cryptology — CRYPTO' 93*, volume 773 of *Lecture Notes in Computer Science*, pp. 49–60, Springer Berlin Heidelberg, 1994.

[124] İ. Sertkaya, *Nonlinearity Preserving Post-Transformations*, Master's thesis, Middle East Technical University, Ankara, Turkey, June 2004.

[125] İ. Sertkaya and A. Doğanaksoy, Some examples of new nonlinearity preserving bijective mappings, submitted to the 7^{th} International Conference on Information Security and Cryptology (ISCTurkey 2014).

[126] İ. Sertkaya and A. Doğanaksoy, On Nonlinearity Preserving Bijective Transformations, in *Proceedings of the National Cryptology Symposium II*, pp. 27–36, Ankara, Turkey, December 2006.

[127] İ. Sertkaya and A. Doğanaksoy, Some Results on Nonlinearity Preserving Bijective Transformations, in *Proceedings of BFCA'07 Conference*, pp. 27–42, Paris, France, May 2007.

[128] İ. Sertkaya and A. Doğanaksoy, On the Affine Equivalence and Nonlinearity Preserving Bijective Mappings, Cryptology ePrint Archive, Report 2010/655, 2010.

[129] İ. Sertkaya, A. Doğanaksoy, O. Uzunkol, and M. S. Kiraz, Affine Equivalency and Nonlinearity Preserving Bijective Mappings over $\mathbb{F}_2$, submitted to the International Workshop on the Arithmetic of Finite Fields (WAIFI 2014).

[130] C. E. Shannon, *A Symbolic Analysis of Relay and Switching Circuits*, Master's thesis, Massachusetts Institute of Technology, 1937.

[131] C. E. Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, 28, pp. 656–715, 1949.

[132] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications (Corresp.), IEEE Transactions on Information Theory, 30(5), pp. 776–780, 1984.

[133] D. Slepian, On the number of symmetry types of Boolean functions of n variables, Canadian Journal of Mathematics, 5, pp. 185–193, 1953.

[134] D. Slepian, Some Further Theory of Group Codes, Bell System Technical Journal, 39, pp. 1219–1252, 1960.

[135] I. Strazdins, Universal Affine Classification of Boolean Functions, Acta Applicandae Mathematica, 46(2), pp. 147–167, 1997.

[136] J. J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colors, with applications to Newton's rule, ornamental tile-work, and the theory of numbers, Philosophical Magazine, 34, pp. 461–475, 1867.

[137] R. C. Titsworth, *Correlation Properties of Cyclic Sequences*, Ph.D. thesis, California Institute of Technology, Pasadena, California, 1962.

[138] N. Tokareva, Automorphism group of the set of all bent functions, Cryptology ePrint Archive, Report 2010/255, 2010.

[139] G. S. Vernam, Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications, American Institute of Electrical Engineers, Transactions of the, XLV, pp. 295–301, Jan 1926.

[140] A. Webster and S. Tavares, On the Design of S-Boxes, in H. Williams, editor, *Advances in Cryptology – CRYPTO 85*, volume 218 of *Lecture Notes in Computer Science*, pp. 523–534, Springer Berlin / Heidelberg, 1986.

[141] J. Williamson, Hadamard's determinant theorem and the sum of four squares, Duke Mathematical Journal, 11(1), pp. 65–81, 03 1944.

[142] C. Wu, On Distribution of Boolean functions with Nonlinearity $\leq 2^{n-2}$, Australasian Journal of Combinatorics, 17, pp. 51–59, 1998.

[143] G.-Z. Xiao and J. L. Massey, A spectral characterization of correlation-immune combining functions, Information Theory, IEEE Transactions on, 34(3), pp. 569–571, May 1988.

[144] J. G. Zehfuss, Ueber eine gewisse determinante, Zeitschrift für Mathematik und Physik, 3, pp. 298–301, 1858.

[145] I. I. Zhegalkin, On the Technique of Calculating Propositions in Symbolic Logic, Matematicheskii Sbornik, 43, pp. 9–28, 1927.

APPENDIX A

Nonlinearity Distributions for $n \leq 6$

Table A.1: Nonlinearity distributions for $n \leq 6$

N_f	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$
0	8	16	32	64	128
1	8	128	512	2048	8192
2	-	112	3840	31744	258048
3	-	-	17920	317440	5332992
4	-	-	28000	2301440	81328128
5	-	-	14336	12888064	975937536
6	-	-	896	57996288	9596719104
7	-	-	-	215414784	79515672576
8	-	-	-	647666880	566549167104
9	-	-	-	1362452480	3525194817536
10	-	-	-	1412100096	19388571496448
11	-	-	-	556408832	95180260073472
12	-	-	-	27387136	420379481991168
13	-	-	-	-	1681517927964672
14	-	-	-	-	6125529594728448
15	-	-	-	-	20418431982428160
16	-	-	-	-	62526600834171264
17	-	-	-	-	176395152249028608
18	-	-	-	-	458313050588725248
19	-	-	-	-	1087405010755682304
20	-	-	-	-	2291582136636334080
21	-	-	-	-	4011570131804454912
22	-	-	-	-	5097726702198767616
23	-	-	-	-	3821934098435833856
24	-	-	-	-	1305039828998603264
25	-	-	-	-	103868560519987200
26	-	-	-	-	1617838297055232
27	-	-	-	-	347227553792
28	-	-	-	-	5425430528

APPENDIX B

Complete Classification of $\mathscr{P}_2(\mathsf{N})$

For $n = 2$, regarding the nonlinearity values, $\mathscr{F}_2$ is partitioned into two subsets as follows;

$$\mathsf{N}_0 = \{f \in \mathscr{F}_n \mid \mathsf{N}_f = 0\}$$

and

$$\mathsf{N}_1 = \{f \in \mathscr{F}_n \mid \mathsf{N}_f = 1\}.$$

Thus, any $\psi \in \mathscr{P}_2(\mathsf{N})$ must satisfy

$$\psi : \mathsf{N}_0 \mapsto \mathsf{N}_0 \text{ and } \psi : \mathsf{N}_1 \mapsto \mathsf{N}_1 \ .$$

Therefore, the number of the nonlinearity preserving bijective mappings acting on the functions with 2-variables is equal to

$$8! \times 8! = 40320 \times 40320 = 1625702400 \approx 2^{30}.$$

That is to say, $|\mathscr{P}_2(\mathsf{N})| \approx 2^{30}$.

We experimented a computer search on $\mathscr{S}_{2^{2^2}}$ comprised of $16! \approx 2^{44}$ elements. As a result, we scanned all the nonlinearity preserving bijective mappings and classified them with respect to their algebraic structure. The results are presented in the Table B.1.

At this point, additionally we have seen that:

Fact B.1. For $n = 2$, according to the form given in (3.5), all the non-affine nonlinearity preserving bijective mappings are of the form presented in Proposition 3.17, i.e. $\psi \in \mathscr{S}_{2^{2^2}} - \mathsf{AGL}_{2^2}$ is nonlinearity preserving if and only if it satisfies the following constraints:

Table B.1: Classification of $\mathscr{P}_2(N)$

Type	#Maps
$\mathsf{AGL}_2 \ltimes \mathscr{A}_2$	192
$\mathsf{GL}_4 - \mathsf{AGL}_2$	1320
$\mathsf{AGL}_4 - (\mathsf{GL}_4 \cup (\mathsf{AGL}_2 \ltimes \mathscr{A}_2))$	9240
$\mathscr{S}_{16} - \mathsf{AGL}_4$	1625691648

1. $\lambda_0 \in \mathscr{A}_2$,
2. The matrix $M = P_{A,\alpha} \oplus B$, where $P_{A,\alpha} \in \mathscr{S}_{2^2}$ corresponds to a matrix representation of an element in AGL_2 and $B = [\varepsilon_1\ \varepsilon_2\ \ldots\ \varepsilon_{2^2}]$ with $\varepsilon_j \in \mathscr{A}_2$, $1 \leq j \leq 2^2$,
3. $\lambda_j \in \mathscr{A}_2$ for all $j \in \left\{12, 13, \ldots, 12\cdots 2^2\right\}$ where at least one of them is non-zero, i.e. $\lambda_j \neq \ell_{\alpha_0}$.

Furthermore, regarding the form (3.5), the nonlinearity preserving bjective maps are analyzed with respect to their matrices $M = [[\lambda_1]\ [\lambda_2]\ \ldots\ [\lambda_{2^n}]]$, the results are presented in Table B.2. Please, note that the matrix classes are not inclusive, that is for example, idendity matrix is not counted in neither permutation nor invertible matrices.

Table B.2: Matrix M Classification of $\mathscr{P}_2(N)$

Type of the Matrix M	#Maps	Notes
Zero	0	-
Idendity	967680	$= 1 \times 967680$
Permutation	22256640	$= 23 \times 967680$
Invertible	1277337600	$= 1320 \times 967680$
Singular	325140480	$= 336 \times 967680$

Remark B.1. Notes on the Table B.2:

- Unexpectedly, there are 336 different singular (not-invertible) matrices that still contribute to nonlinearity preserving non-affine bijective maps.
- The only invertible matrices that contribute to nonlinearity preserving bijective maps are the one that are seen in nonlinearity preserving linear bijective maps.

Each of the following nonlinearity preserving non-affine bijective maps that possess singular matrix.

Example B.1. Let $\psi \in \mathscr{S}_{2^{2^2}}$ be defined as follows.

$$\begin{aligned}\psi(x_0,x_1,x_2,x_3) = (&\psi_0(x_0,x_1,x_2,x_3), \psi_1(x_0,x_1,x_2,x_3),\\ &\psi_2(x_0,x_1,x_2,x_2), \psi_3(x_0,x_1,x_2,x_3)),\end{aligned}$$

where the truth table of each $\psi_0, \psi_1, \psi_2, \psi_3$ from $\mathscr{F}_4$ is as follows:

$$\begin{aligned}T_{\psi_0} &= (0,1,0,1,0,1,0,0,1,1,1,0,1,0,1,1),\\ T_{\psi_1} &= (0,0,1,1,0,0,1,0,1,1,0,1,1,0,0,1),\\ T_{\psi_2} &= (0,0,0,0,1,1,1,0,1,0,0,0,0,1,1,1),\\ T_{\psi_3} &= (0,0,0,0,0,0,0,1,0,1,1,1,1,1,1,1).\end{aligned}$$

Then, the ANF of each $\psi_0, \psi_1, \psi_2, \psi_3$ will be:

$$\begin{aligned}
\mathsf{A}_{\psi_0} &= (0,1,0,0,0,0,0,1,1,1,1,1,1,1,1,0),\\
\mathsf{A}_{\psi_1} &= (0,0,1,0,0,0,0,1,1,1,1,1,1,1,1,0),\\
\mathsf{A}_{\psi_2} &= (0,0,0,0,1,0,0,1,1,1,1,1,1,1,1,0),\\
\mathsf{A}_{\psi_3} &= (0,0,0,0,0,0,0,1,0,1,1,1,1,1,1,0).
\end{aligned}$$

Hence we have,

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

Trivially, the matrix M is not invertible. However, ψ is invertible and moreover it is bijective, non-affine and nonlinearity preserving mapping.

APPENDIX C

Examples of New Nonlinearity Preserving Mappings for $n = 3, 4, 6$

Due to the space constraints the algebraic normal form of the nonlinearity preserving transformations are not given explicitly for $n \geq 4$. However, since any transformation is an element of $\mathscr{S}_{2^n}$, it is possible to represent the permutations as a product of disjoint cycles. Within these cycles, the functions will be given by their truth table in hexadecimal value without the "`0x`" prefix.

Example C.1. Let $\psi \in S_{2^{2^3}}$ be,

$$\begin{aligned}\psi : [\mathsf{T}_f] \mapsto & [\lambda_0] \oplus M[\mathsf{T}_f] \oplus [\lambda_{123457}] f(\alpha_0) f(\alpha_1) f(\alpha_2) f(\alpha_3) f(\alpha_4) f(\alpha_6) \oplus \\ & [\lambda_{1234578}] f(\alpha_0) f(\alpha_1) f(\alpha_2) f(\alpha_3) f(\alpha_4) f(\alpha_6) f(\alpha_7) \oplus \\ & [\lambda_{123456}] f(\alpha_0) f(\alpha_1) f(\alpha_2) f(\alpha_3) f(\alpha_4) f(\alpha_5) \oplus \\ & [\lambda_{1234568}] f(\alpha_0) f(\alpha_1) f(\alpha_2) f(\alpha_3) f(\alpha_4) f(\alpha_5) f(\alpha_7)\end{aligned}$$

where $\lambda_0 = [00001111]$, $\lambda_{123457} = \lambda_{1234578} = \lambda_{123456} = \lambda_{1234568} = [00010100]$ and M is the matrix;

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Trivially, ψ is not an affine mapping. In particular, it does not satisfy the conditions of Proposition 3.17 since $(0,0,0,1,0,1,0,0)$ is not a truth table of an affine function. Moreover, it can be easily checked that this map is invertible and preserves nonlinearity for all functions.

Example C.2. Let $\psi \in S_{2^{2^3}}$ be the mapping, whose explicit permutation representation is

$$\begin{aligned}\pi_\psi =&(00,0f,55,3c,5a,66,33)(01,0e,54,3d,5b,67,32)(02,\\
&0b,45,3e,5e,76,31,04,1f,57,38,4a,64,37,10,0d,51,\\
&2c,58,62,23)(03,0a,44,3f,5f,77,30,05,1e,56,39,4b,\\
&65,36,11,0c,50,2d,59,63,22)(06,1b,47,3a,4e,74,\\
&35,14,1d,53,28,48,60,27,12,09,41,2e,5c,72,21)\\
&(07,1a,46,3b,4f,75,34,15,1c,52,29,49,61,26,13,\\
&08,40,2f,5d,73,20)(16,19,43,2a,4c,70,25)(17,18,\\
&42,2b,4d,71,24)(6a,6c,78)(6b,6d,79)(6e,7c,7a)\\
&(6f,7d,7b)(82,84,90)(83,85,91)(86,94,92)(87,95,\\
&93)(88,cf,fa,e4,b8,c5,b1,8b,ca,eb,e2,ac,d7,b7,9f,\\
&d8,ed,f6,be,d1,a3,8d,de,f9,e1,a9,c6,b4,9a,c9,ee,\\
&f3,af,d2,a6,9c,dd,fc,f5,bb,c0,a0)(89,ce,fb,e0,a8,\\
&c7,b5,9b,c8,ef,f2,ae,d3,a7,9d,dc,fd,f4,ba,c1,a1)\\
&(8a,cb,ea,e3,ad,d6,b6,9e,d9,ec,f7,bf,d0,a2,8c,\\
&df,f8,e5,b9,c4,b0)(8e,db,e8,e7,bd,d4,b2)(8f,da,\\
&e9,e6,bc,d5,b3)(98,cd,fe,f1,ab,c2,a4)(99,cc,ff,\\
&f0,aa,c3,a5)\ .\end{aligned}$$

It can be easily seen that ψ has algebraic form as follows.

$$\begin{aligned}\psi : [T_f] \mapsto &[\lambda_0] \oplus M[T_f] \oplus \\
&[\lambda_{123458}] f(\alpha_0) f(\alpha_1) f(\alpha_2) f(\alpha_3) f(\alpha_4) f(\alpha_7) \oplus \\
&[\lambda_{123457}] f(\alpha_0) f(\alpha_1) f(\alpha_2) f(\alpha_3) f(\alpha_4) f(\alpha_6) \oplus \\
&[\lambda_{1234568}] f(\alpha_0) f(\alpha_1) f(\alpha_2) f(\alpha_3) f(\alpha_4) f(\alpha_5) f(\alpha_7) \oplus \\
&[\lambda_{1234567}] f(\alpha_0) f(\alpha_1) f(\alpha_2) f(\alpha_3) f(\alpha_4) f(\alpha_5) f(\alpha_6)\end{aligned}$$

where $\lambda_0 = (0,0,0,0,1,1,1,1)$, $\lambda_{123458} = \lambda_{123457} = \lambda_{1234568} = \lambda_{1234567} = (0,0,0,0,0,1,0,1)$ and the M is the matrix;

$$\begin{bmatrix}1&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&1&0&0\\1&0&1&0&1&0&0&0\\1&0&0&0&1&0&1&0\\1&0&0&1&1&0&0&0\\1&0&0&0&1&0&0&1\end{bmatrix}$$

Trivially, ψ is not an affine mapping, indeed it does not satisfies the conditions given in Proposition 3.17, since $(0,0,0,0,0,1,0,1)$ is not truth table of an affine function. Moreover, it can be easily checked that this map is invertible and preserves nonlinearity for all functions.

Example C.3. Assume $\psi \in \mathscr{S}_{2^{2^4}}$ be a permutation of $\mathbb{F}_2^{2^4}$ with cycle representation,

$$\begin{aligned}\pi_\psi =&(0000,6699,\mathsf{f0f0},\mathsf{a9e2},9999,9696,\mathsf{5aa5},\mathsf{3cc3})(0081,\mathsf{00bd},\mathsf{01f7})\\ &(0107,\mathsf{0c3f},\mathsf{f0ff},\mathsf{0a41},\mathsf{5fcc},\mathsf{bf1f},\mathsf{2e8b},0251,\mathsf{30cf},\mathsf{13d3})(0471,\mathsf{fee4},\\ &0495,\mathsf{242f},\mathsf{6c7f})(\mathsf{065c},\mathsf{8d28},\mathsf{0a9c},4478,\mathsf{1d7b},\mathsf{2eed},\mathsf{de74})(\mathsf{09b1},2882,\\ &\mathsf{60e8},1284,\mathsf{e44e})(\mathsf{12ed},1441,1482,1428)(1414,1698,\mathsf{16c2})(\mathsf{5a58},7996,\mathsf{5a5b})\ .\end{aligned}$$

It can be easily verified that ψ keeps nonlinearity values invariant for all $f \in \mathscr{F}_n$, that is $\psi \in \mathscr{P}_4(\mathsf{N})$. When the algebraic normal form of ψ is written explicitly, it will be seen that some non-affine terms are not the truth table of an affine function. Thus ψ is not of the form given in Proposition 3.17.

Example C.4. Assume $\psi \in \mathscr{S}_{2^{2^4}}$ be a permutation of $\mathbb{F}_2^{2^4}$ with cycle representation,

$$\begin{aligned}\pi_\psi =&(\mathsf{0002},\mathsf{3ec3},\mathsf{fffe},\mathsf{33ce},\mathsf{7fff},\mathsf{2ff0})(\mathsf{001b},\mathsf{33aa},\mathsf{e48d},\mathsf{f681},\\ &\mathsf{6a77},\mathsf{97f7},\mathsf{050a},\mathsf{027c},\mathsf{665a},1370,\mathsf{fff0})(\mathsf{059c},\mathsf{a63f},\\ &\mathsf{e1ee},\mathsf{36af},\mathsf{72be},\mathsf{fca9})\end{aligned}$$

It can be easily verified that ψ keeps nonlinearity values invariant for all $f \in \mathscr{F}_n$, that is $\psi \in \mathscr{P}_4(\mathsf{N})$. When the algebraic normal form of ψ is written explicitly, it will be seen that some non-affine terms are not the truth table of an affine function. Thus ψ is not of the form given in Proposition 3.17.

Example C.5. Let $\psi \in \mathscr{S}_{2^{2^6}}$ be the permutation such that its disjoint cycle representation is

$$\pi_\psi =(\mathsf{9556566a3ffcfcc0},\mathsf{0ddfcbb3a4456dd9})$$

Trivially, ψ maps all functions to itself except the ones in the disjoint cycles, i.e. it keeps nonlinearity invariant for those functions. The cycle has bent functions whose nonlinearity values are 28. Thus, $\psi \in \mathscr{P}_6(\mathsf{N})$.

However, the bent function $\mathsf{9556566a3ffcfcc0}$ has algebraic degree 2 while its image under ψ, $\mathsf{0ddfcbb3a4456dd9}$, has algebraic degree 3. ψ can not be of the form as given in Proposition 3.17 since in that case it should have also keep the algebraic degree invariant.

Example C.6. Let $\psi \in \mathscr{S}_{2^{2^6}}$ be the permutation such that its disjoint cycle representation is

$$\begin{aligned}\pi_\psi =&(\mathsf{0217177f68818115},\mathsf{051307ff58900943})\\ &(\mathsf{c003033f6aa9a995},\mathsf{c113077f6889a115},\mathsf{c113077f984a9215})\end{aligned}$$

Trivially, ψ maps all functions to itself except the ones in the disjoint cycles, i.e. it keeps nonlinearity invariant for those functions. The first cycle has functions whose

nonlinearity values are 26 whereas the second has 28. Thus, $\psi \in \mathscr{P}_6(\mathsf{N})$. However, the bent function c003033f6aa9a995 has algebraic degree 2 while its image under ψ, c113077f6889a115 has algebraic degree 3. ψ can not be of the form as given in Proposition 3.17 since in that case it should have also keep the algebraic degree invariant.

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Sertkaya, İsa
Nationality: Turkish
Date and Place of Birth: 1979, Konya
Marital Status: Married
E-mail: isa.sertkaya@tubitak.gov.tr
Phone: +90 262 6481743
Fax: +90 262 6481100

EDUCATION

Degree	Institution	Year of Graduation
M.S.	Department of Cryptography, METU	2004
B.S.	Department of Mathematics, METU	2002
High School	ISDFL	1997

PROFESSIONAL EXPERIENCE

Year	Place	Enrollment
2002–	TÜBİTAK BİLGEM UEKAE	Chief Researcher

PUBLICATIONS

İ. Sertkaya and A. Doğanaksoy, "**On Nonlinearity Preserving Bijective Transformations**," in *Proceedings of the National Cryptology Symposium II*, Ankara, Turkey, 2006, pp. 27–36.

İ. Sertkaya and A. Doğanaksoy, "**Some Results on Nonlinearity Preserving Bijective Transformations**," in *Proceedings of BFCA'07 Conference*, Paris, France, 2007, pp. 27–42.

İ. Sertkaya and A. Doğanaksoy, "**On the Affine Equivalence and Nonlinearity Preserving Bijective Mappings**," *Cryptology ePrint Archive, Report 2010/655*, 2010.

İ. Sertkaya, A. Doğanaksoy, O. Uzunkol, and M. S. Kiraz, "**Affine Equivalency and Nonlinearity Preserving Bijective Mappings over $\mathbb{F}_2$**," *accepted to the International Workshop on the Arithmetic of Finite Fields (WAIFI 2014)*.

İ. Sertkaya and A. Doğanaksoy, "**Some Examples of New Nonlinearity Preserving Bijective Mappings**," *accepted to the 7^{th} International Conference on Information Security and Cryptology (ISCTurkey 2014)*.

İ. Sertkaya and A. Doğanaksoy, "**Enumeration of Hamming Weight Preserving Bijective mappings acting Boolean Functions**," *forthcoming*.