GENERALIZED BENT FUNCTIONS WITH PERFECT NONLINEAR FUNCTIONS ON ARBITRARY GROUPS

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

BY

EMRAH SERCAN YILMAZ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

SEPTEMBER 2012

Approval of the thesis:

GENERALIZED BENT FUNCTIONS WITH PERFECT NONLINEAR FUNCTIONS ON ARBITRARY GROUPS

submitted by **EMRAH SERCAN YILMAZ** in partial fulfillment of the requirements for the degree of **Master of Science 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**

Prof.Dr. Ferruh Özbudak ________________
Supervisor, **Department of Mathematics**

Assist.Prof.Dr. Zülfükar Saygı ________________
Co-supervisor, **Department of Mathematics**

Examining Committee Members:

Assoc.Prof.Dr Ali DOĞANAKSOY ________________
Department of Mathematics, METU

Prof.Dr.Ferruh ÖZBUDAK ________________
Department of Mathematics, METU

Assist.Prof.Dr Zülfükar SAYGI ________________
Department of Mathematics, TOBB

Assoc.Prof.Dr. Melek D. YÜCEL ________________
Department of Electrical and Electronics Engineering, METU

Assist.Prof.Dr Ömer KÜÇÜKSAKALLI ________________
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: EMRAH SERCAN YILMAZ

Signature :

ABSTRACT

GENERALIZED BENT FUNCTIONS WITH PERFECT NONLINEAR FUNCTIONS ON ARBITRARY GROUPS

Yılmaz, Emrah Sercan
M.S., Department of Cryptography
Supervisor : Prof.Dr. Ferruh Özbudak
Co-Supervisor : Assist.Prof.Dr. Zülfükar Saygı

September 2012, 25 pages

This thesis depends on the paper ‘Non-Boolean Almost Perfect Nonlinear Functions on Non-Abelian Groups’ by Laurent Poinsot and Alexander Pott and we have no new costructions here. We give an introduction about character theory and the paper of Poinsot and Pott, and we also compare previous definitions of bent functions with the definition of the bent function in the paper. As a conclusion, we give new theoretical definitions of bent, PN, APN ana maximum nonlinearity. Moreover, we show that bent and PN functions are not always same in the non-abelian cases.

Keywords: Bent functions, PN functions, Character Theory, Fourier transform

ÖZ

KEYFİ BİR GRUP ÜZERİNDEKİ BENT FONKSİYONLARI İLE PN FONKSİYONLARI

Yılmaz, Emrah Sercan
Yuksek Lisans, Kriptografi Bölümü
Tez Yöneticisi : Prof.Dr. Ferruh Özbudak
Ortak Tez Yöneticisi : Yrd.Doç.Dr. Zülfükar Saygı

Eylül 2011, 25 sayfa

Bu tez Laurent Poinsot ve Alexander Pott tarafından yazılan ‘Non-Boolean Almost Perfect Nonlinear Functions on Non-Abelian Groups’ adlı makaleye dayanmaktadır ve yeni bir kurgulama yoktur. Tezde karakter teorisi ve Poinsot ve Pott’un makalesi hakkında bilgi verdik ve daha önceki bent fonksiyonların tanımı ile makaledeki Bent fonksiyonlarının tanımını kıyasladık. Sonuç olarak, yeni bent, PN, APN ve ‘maksimum lineer olmama’ hakkında teorik tanımlar verdik ve ayrıca bent ve PN fonksiyonların Abel olmayan gruplar üzerinde her zaman aynı olmadığını gösterdik.

Anahtar Kelimeler: Bent fonksiyonları, PN fonksiyonları, Karakter Teorisi, Fourier transformu

1

To my family

ACKNOWLEDGMENTS

Special thanks to my brother Ömer Ali Yılmaz who were always there to motivate me whenever I needed. I also gratefully acknowledge the financial support of TÜBİTAK under Grant No. TBAG–109T344 during this thesis.

TABLE OF CONTENTS

CHAPTERS

CHAPTER 1

INTRODUCTION

Definition: [1, p.1] A *group* is a non-empty set G on which there is defined a binary operation $(g, h) \to gh$ satisfying the following properties:

1) for all g, h, k in G,

$$(gh)k = g(hk);$$

2) there exists an element e in G such that for all g in G

$$eg = ge = g;$$

3) for all g in G, there exists an element g^{-1} in G such that

$$gg^{-1} = g^{-1}g = e.$$

Examples:

$C_n =< a : a^n = 1 >$,

$D_{2n} =< a, b : a^n = b^2 = 1, b^{-1}ab = a^{-1} >$,

$Q_8 =< a, b : a^4 = 1, a^2 = b^2, b^{-1}ab = a^{-1} >$,

S_n = the symmetric group of order n,

A_n = the alternating group of order n,

GL$(n, \mathbb{C})$ = the group of invertable $n \times n$ matricies over $\mathbb{C}$.

Definition: [1, p.5] Let G and H be groups, and consider

$$G \times H = \{(g, h) : g \in G, h \in H\}.$$

Define a product operation on $G \times H$ by

$$(g, h)(g', h') = (gg', hh')$$

for all $g, g' \in G$ and all $h, h' \in H$. With this product operation, $G \times H$ is a group, called the *direct product* of G and H.

Definition: [1, p.6] A *function* from one set G to another set H is a rule which assigns a unique element in H to each element of G.

Definition: [1, p.6] If G and H are groups, then a *homomorphism* from G to H is a function $f : G \to H$ which satisfies:

$$f(g_1 g_2) = f(g_1) f(g_2)$$

for all $g_1, g_2 \in G$.

Definition: [1, p.30] A *representation* of G over $\mathbb{C}$ is a homomorphism ρ from G to $\mathrm{GL}(n, \mathbb{C})$ for some n. The degree of ρ is the integer n.

Example: [1, p.31] Let $G = D_8 =< a, b : a^4 = b^2 = 1, b^{-1}ab = a^{-1} >$. Define the matrices A and B:

$$A = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Then $A^4 = B^2 = I_2, B^{-1}AB = A^{-1}$. It follows $\rho : \begin{cases} G \to \mathrm{GL}(2, \mathbb{C}) \\ a^i b^j \to A^i B^j \end{cases}$, $(0 \le i \le 3, 0 \le j \le 1)$ is a representation over $\mathbb{C}$. The degree of ρ is 2.

Definition: [1, p.32] Let $\rho : G \to \mathrm{GL}(n, \mathbb{C})$ and $\sigma : G \to \mathrm{GL}(m, \mathbb{C})$ be representations of G over $\mathbb{C}$. We say than ρ is *equivalent* to σ if $n = m$ and there exists an invertible $n \times n$ matrix T such that for all $g \in G$,

$$\sigma(g) = T^{-1} \rho(g) T$$

Equivalence of representation is an equivalence relation.

Example: [1, p.32] Let $G = D_8$ and $A = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Let $T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$. Then $T^{-1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}$. We have

$$T^{-1}AT = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \; T^{-1}BT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and so we obtain a representation σ of D_8 for which

$$\sigma(a) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \sigma(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Definition: [1, p.39] Let V be a vector space over $\mathbb{F}$ and let G be a group. Then V is an $\mathbb{F}G$-module if a multiplication vg $(v \in V, g \in G)$ is defined, satisfying the following conditions for all $u, v \in V, \lambda \in \mathbb{F}$ and $g, h \in G$:

(1) $vg \in V$;

(2) $v(gh) = (vg)h$;

(3) $v1 = v$;

(4) $(\lambda v)g = \lambda(vg)$;

(5) $(u + v)g = ug + vg$.

Definition: [1, p.50] An $\mathbb{F}G$-module V is said to be *irreducible* if it is non-zero and it has no $\mathbb{F}G$-submodules apart from $\{0\}$ and V. If V has an $\mathbb{F}G$-submodule W with W not equal to $\{0\}$ or V, then V is *reducible*. Similarly, a representation $\rho : G \to \mathrm{GL}(n, \mathbb{F})$ is *irreducible* if the corresponding $\mathbb{F}G$-module $\mathbb{F}^n$ is irreducible; and ρ is *reducible* if $\mathbb{F}^n$ is reducible.

Define $\widehat{G}$ as the set of all equivalence classes of irreducible representation of G.

Group Algebra of G: [1, p.53]

Let G be a finite group whose elements are $g_1, ..., g_n$. We define a vector space over $\mathbb{C}$ with $g_1, ..., g_n$ as a basis, and we call this vector space $\mathbb{C}G$. Take as an element of $\mathbb{C}G$ all expressions of the form

$$\lambda_1 g_1 + ... + \lambda_n g_n \text{ (all } \lambda_i \in \mathbb{C}).$$

The rules for addition and scalar multiplication in $\mathbb{C}G$ are the natural ones; namely if

$$u = \sum_{i=1}^{n} a_i g_i \text{ and } v = \sum_{i=1}^{n} b_i g_i$$

are elements of $\mathbb{C}G$ and $\lambda \in \mathbb{C}$, then

$$u + v = \sum_{i=1}^{n} (a_i + b_i) g_i \text{ and } \lambda u = \sum_{i=1}^{n} (\lambda a_i) g_i.$$

With these rules, $\mathbb{C}G$ is a vector space over $\mathbb{C}$ of dimension n, with basis $g_1, ..., g_n$. The basis $g_1, ..., g_n$ is called the *natural basis* of $\mathbb{C}G$.

$\mathbb{C}G$ carries more structures than that of a vector space.

Define multiplication in $\mathbb{C}G$ as follows:

$$\begin{aligned}\Big(\sum_{g\in G} a_g g\Big)\Big(\sum_{h\in G} a_h h\Big) &= \sum_{g,h\in G} a_g b_h (gh)\\ &= \sum_{g\in G}\sum_{h\in G}\Big(a_h b_{h^{-1}g}\Big) g\end{aligned}$$

where all $a_g, b_g \in \mathbb{C}$.

and also define:[2, p.3]

$$\begin{aligned}\Big(\sum_{g\in G} a_g g\Big)^{(-1)} &: = \sum_{g\in G} \overline{a_g} g^{-1}\\ &= \sum_{g\in G} \overline{a_g^{-1}} g.\end{aligned}$$

Definition: [1, p.118] Suppose that V is an $\mathbb{C}G$-module with basis ß. Then the character of V is the function $\chi : G \to \mathbb{C}$ defined by:

$$\chi(g) = \mathrm{tr}[g]_{\text{ß}.}$$

The character of V does not depend on the basis ß, since if ß and ß$'$ are bases of V then

$$[g]_{\text{ß}'} = T^{-1}[g]_{\text{ß}} T$$

for some invertable matrix T. Thus for all $g \in G$

$$\mathrm{tr}[g]_{\text{ß}'} = \mathrm{tr}[g]_{\text{ß}.}$$

[1, p.119] Naturally, we define the character of a representation $\rho : G \to \mathrm{GL}(n, \mathbb{C})$ to be the character of χ of the corresponding $\mathbb{C}G$-module $\mathbb{C}^n$, namely

$$\chi(g) = \mathrm{tr}(\rho(g)) \, , \, g \in G.$$

Example: [1, p.120] Let $G = D_8 =< a, b : a^4 = b^2 = 1, b^{-1}ab = a^{-1} >$ and let $\rho : G \to \mathrm{GL}(2, \mathbb{C})$ be the representation

$$\rho(a) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \; \rho(b) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then

g	1	a	a^2	a^3	b	ab	a^2b	a^3b
$\chi(g)$	2	0	-2	0	0	0	0	0

Definition:[1, p.119] We say that χ is a *character of* G if χ is the character of some $\mathbb{C}G$-module. Further, χ is an *irreducible* character of G if χ is the character of an irreducible $\mathbb{C}G$-module; and χ is *reducible* if it is the character of a reducible $\mathbb{C}G$-module.

[1, p.152] The number of irreducible characters of a group is equal to the number of conjugacy classes of the group.

Proposition:[1, p.161] Let $\chi_1, ..., \chi_k$ be the irreducible characters of G, and let $g_1, ..., g_k$ be representatives of the conjugacy classes of G. Then the following relations hold for any $r, s \in \{1, ..., k\}$.
(1) The row orthogonality relations:

$$\sum_{i=1}^{k} \frac{\chi_r(g_i)\overline{\chi_s(g_i)}}{|C_G(g_i)|} = \delta_{rs}.$$

(2) The column orthogonality relations:

$$\sum_{i=1}^{k} \chi_i(g_r)\overline{\chi_i(g_s)} = \delta_{rs}|C_G(g_r)|.$$

CHAPTER 2

GENERALIZED BENT FUNCTIONS

Definition: [3, p.9] Let X and Y be two finite nonempty sets. A function $f : X \to Y$ said to be *balanced* if the function

$$\begin{aligned} \phi_f : Y &\longrightarrow \mathbb{N} \\ y &\longrightarrow |\{x \in X : f(x) = y\}| \end{aligned} \tag{2.1}$$

is constant and equals to $\frac{|X|}{|Y|}$.

Example: 1) Let $X = \mathbb{F}_2^n$ and $Y = \mathbb{F}_2$ and let

$$\begin{aligned} f_i : X &\longrightarrow Y \\ (x_1, ..., x_n) &\longrightarrow x_i \end{aligned}$$

is balanced for each i $\in \{1, ..., n\}$.

2) Let $X = S_3$ and $Y = C_3$ and let

$$f(x) = \begin{cases} 1 & \text{if } x \in id, (12) \\ a & \text{if } x \in (13), (23) \\ a^2 & \text{if } x \in (123), (132) \end{cases}$$

is also a balanced function.

Note That:

1) If $f : X \to Y$ is a balanced function, then $\frac{|X|}{|Y|}$ must be a positive integer; that is, order of Y must divide order of X.

2) As we see in Example 2, if order of Y divides order of X, we can define a balanced function.

Definition:[3, p.9] Let K and N be two finite groups and $f : K \to N$. The *left derivative* of f in direction $\alpha \in K$ is defined as the map

$$\begin{aligned} {d_\alpha}^{(l)} f : K &\to N \\ x &\to f(\alpha x) f(x)^{-1} \end{aligned} \tag{2.2}$$

Symmetrically, the *right derivative* of f in direction $\alpha \in K$ is the map

$$\begin{aligned} {d_\alpha}^{(r)} f : K &\to N \\ x &\to f(x)^{-1} f(\alpha x) \end{aligned} \tag{2.3}$$

[3, p.9] The left-translation actions of both K and N are each equivalent to right-translation of K and N. So we focus only on left-translation that we simply denote as $d_\alpha f$.

Example: 3) Consider Example 2, let $\alpha = (12)$, then $d_{(12)} f$ has value a^2 at (123):

$$\begin{aligned} (d_{(12)} f)(123) &= f((12)(123)) f((123))^{-1} \\ &= f((13))(a^2)^{-1} \\ &= a.a \\ &= a^2 \end{aligned} \tag{2.4}$$

Definition: [3, p.9] Let K and N be two finite groups and $f : K \to N$. The map f is said to be *perfect non-linear* if for each $\alpha \in$K*, $d_\alpha f$ is balanced; i.e, for each $(\alpha, \beta) \in$K$^* \times N$,

$$\delta_f(\alpha, \beta) := \left| \{x \in K | f(\alpha x) f(x)^{-1} = \beta\} \right| = \frac{|K|}{|N|}. \tag{2.5}$$

Note that: $f : K \to N$ is a perfect nonlinear function, then $\frac{|K|}{|N|}$ must be a positive integer; that is, order of N must divide order of K. So we can have perfect nonlinear function only if $\frac{|K|}{|N|} \in Z^+$.

Example: 4) Let $f : \mathbb{F}_3 \to \mathbb{F}_3$ be a mapping as $x \to x^2$ and consider d_α f as addition:

$$\Delta_\alpha f(x) := f(\alpha + x) - f(x) \tag{2.6}$$

Then

$$\Delta_1 f : [0,1,2] \to [1,0,2]$$
$$\Delta_2 f : [0,1,2] \to [1,2,0].$$

Since $\left|\{x \in F_3 : \Delta_\alpha f(x) = \beta\}\right| = \frac{|F_3|}{|F_3|}$ =1 for each $\alpha \in \{1,2\}$ and $\beta \in \{0,1,2,\}$, f is perfect nonlinear.

Note that: When $|K| = |N|$, these functions ara also known as *planar functions* in finite geometry, as we see in Example 4.

[2, p.2] Since perfect nonlinear functions do not exist in many cases, the following definition is meaningful: we call $f : K \to N$ an *almost perfect nonlinear function* if and only if

$$\sum_{(a,b)\in K\times N} \delta_f(a,b) \leq \sum_{(a,b)\in K\times N} \delta_g(a,b),\ \forall g : K \to N. \tag{2.7}$$

For simplicity, we define $G := K \times N$. With each function $f : K \to N$ we associate its graph

$$D_f := \{(a, f(a)) : a \in K\}. \tag{2.8}$$

D_f can be uniquely represented in C[G] as

$$D_f = \sum_{g\in G} 1_{D_f}(g)g \tag{2.9}$$

where

$$1_{D_f}(g) = \begin{cases} 1 & \text{if } g \in D_f \\ 0 & \text{if } g \notin D_f \end{cases} \tag{2.10}$$

Proposition: [2, p.3]

$$D_f D_f^{(-1)} = \sum_{(a,b)\in G} \delta_f(a,b)(a,b) \in \mathbb{Z}[G] \tag{2.11}$$

Proof: Let $h = (x, y)$ and $g = (a, b)$ be in G.

$$\begin{aligned} h, hg^{-1} \in D_f &\Longleftrightarrow f(x) = y \quad \text{and} \quad f(a^{-1}x) = b^{-1}y \\ &\Longleftrightarrow f(a(a^{-1}x))f(a^{-1}x)^{-1} = b \end{aligned}$$

Thus

$$\begin{aligned} D_f D_f^{(-1)} &= \Big(\sum_{g\in G} 1_{D_f}(g)g\Big)\Big(\sum_{h\in G} \overline{1_{D_f}(h^{-1})h}\Big) \\ &= \sum_{g\in G}\Big(\sum_{h\in G} 1_{D_f}(h)\overline{1_{D_f}(g^{-1}h)}\Big)g \\ &= \sum_{(a,b)\in G} \delta_f(a, b)(a, b) \end{aligned}$$

Theorem: [2, p.9] Let $D := \sum_{g\in G} d_g g$ be an element in the group algebra C[G]. Then the following holds:

a) (Fourier Invension)

$$d_g = \frac{1}{|G|}\sum_{\rho\in\hat{G}} \text{dim}\rho\text{tr}(\rho(D) \circ \rho(g^{-1})) \tag{2.12}$$

b) (Parseval's Equation)

$$\sum_{g\in G} |d_g|^2 = \frac{1}{|G|}\sum_{g\in\hat{G}} \text{dim}\rho||\rho(D_f)||^2 \tag{2.13}$$

where $||f||$ is the trace norm of a linear endomorphism f given by $||f|| := \sqrt{tf(f \circ f^*)}$.

Proof:

a)

$$\begin{aligned} \sum_{g\in\hat{G}} \text{dim}\rho\text{tr}(\rho(D) \circ \rho(g^{-1})) &= \sum_{g\in\hat{G}} \text{dim}\rho\text{tr}(\rho(\sum_{h\in G} d_h h \circ \rho(g^{-1}))) \\ &= \sum_{h\in G} d_h \sum_{g\in\hat{G}} \text{dim}\rho\text{tr}(\rho(hg^{-1})) \\ &= |G|d_g \end{aligned}$$

b)

$$
\begin{aligned}
DD^{(-1)} &= \left(\sum_{g\in G} d_g g\right)\left(\sum_{h\in G} {}_{h^{-1}}h\right) \\
&= \sum_{g\in G}\left(\sum_{h\in G} d_h \overline{d_{g^{-1}h}}\right)g
\end{aligned}
$$

The coefficient of identity of DD^{-1} is $\sum_{g\in G}|d_g|^2$. If we apply (a) to DD^{-1}, then

$$
\begin{aligned}
\sum_{g\in G}|d_g|^2 &= \frac{1}{|G|}\sum_{\rho\in\hat{G}}\dim\rho \operatorname{tr}(\rho(DD^{-1})\circ\rho(id^{-1})) \\
&= \frac{1}{|G|}\sum_{\rho\in\hat{G}}\dim\rho \operatorname{tr}(\rho(DD^{-1})) \\
&= \frac{1}{|G|}\sum_{\rho\in\hat{G}}\dim\rho \operatorname{tr}(\rho(D)\circ\rho(D^{-1})) \\
&= \frac{1}{|G|}\sum_{\rho\in\hat{G}}\dim\rho \|\rho(D_f)\|^2
\end{aligned}
$$

Theorem: [2, p.10] Let K and N be two finite groups. Let G be direct product $K\times N$. A function $f:\rightarrow N$ is almost perfect nonlinear if and only if

$$
\sum_{\rho\in\hat{G}}\dim\rho\|\rho(D_f)\|^4 \leq \sum_{\rho\in\hat{G}}\dim\rho\|\rho(D_g)\|^4,\ \forall g: K\rightarrow N. \tag{2.14}
$$

Proof: We have

$$
D_f D_f^{(-1)} = \sum_{(a,b)\in G}\delta_f(a,b)(a,b).
$$

Using Parseval's equation we have

$$
\begin{aligned}
\sum_{(a,b)\in G}\delta_f(a,b)^2 &= \frac{1}{|G|}\sum_{\rho\in\hat{G}}\dim\rho\|\rho(D_f D_f^{-1})\|^2 \\
&= \frac{1}{|G|}\sum_{\rho\in\hat{G}}\dim\rho\|\rho(D_f)\circ\rho(D_f)^*\|^2 \\
&= \frac{1}{|G|}\sum_{\rho\in\hat{G}}\dim\rho\|\rho(D_f)\|^4
\end{aligned}
$$

Since a function $f : K \to N$ is almost perfect nonlinear if and only if for every $g : K \to N$

$$\sum_{(a,b)\in K\times N} \delta_f(a,b)^2 \leq \sum_{(a,b)\in K\times N} \delta_g(a,b)^2, \ \forall g : K \to N.$$

Therefore, a function $f : K \to N$ is almost perfect nonlinear if and only if for every $g : K \to N$,

$$\sum_{\rho\in\hat{G}} \dim\rho \|\rho(D_f)\|^4 \leq \sum_{g\in\hat{G}} \dim\rho \|\rho(D_g)\|^4, \ \forall g : K \to N.$$

Proposition: [2, p.11] Let K and N be two finite groups with order m and n respectively, and $f :\to N$. For some $\rho \in \widehat{K\times N}$ the values of $\rho(D_f)$:

$$\rho(D_f) = \begin{cases} m & \text{if } \rho = \rho_0 \\ 0_v & \text{if } \rho = \rho_K \otimes \rho_0 \text{ and } (\rho_K, V) \text{ is non-principle on } K \end{cases} \tag{2.15}$$

Proof: Suppose $\rho = \rho_0$.

$$\begin{aligned} \rho(D_f) &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho(a,b) \\ &= \sum_{(a,b)\in G} 1_{D_f}(a,b) \\ &= |D_f| \\ &= |K| \\ &= m \end{aligned}$$

Suppose $\rho = \rho_K \otimes \rho_0$ and (ρ_K, V) is non-principle on K. Then we have

$$\begin{aligned} \rho(D_f) &= \sum_{(a,b)\in G} 1_{D_f}(a,b)\rho_K(a) \otimes \rho_0(b) \\ &= \sum_{a\in K} \rho_K(a) \otimes \rho_0(f(a)) \\ &= \sum_{a\in K} \rho_K(a) \\ &= 0 \end{aligned}$$

Theorem: [2, p.12] Let $f : K \to N$. Then

$$\max_{\rho_N \neq \rho_0} \dim\rho \|\rho(D_f)\|^2 \geq \frac{m^2(n-1)}{|\hat{K}|(|\hat{N}|-1)}. \tag{2.16}$$

Proof: By Parseval's equation applied to D_f, we have

$$\begin{aligned} \frac{1}{|G|}\sum_{\rho \in \hat{G}} \dim\rho \|\rho(D_f)\|^2 &= \sum_{(a,b)\in G} 1_{D_f}(a,b)^2 \\ &= m \end{aligned}$$

so we have

$$\sum_{\rho \in \hat{G}} \dim\rho \|\rho(D_f)\|^2 = m^2 n.$$

By proposition above we have

$$\begin{aligned} \sum_{\rho_N \neq \rho_0} \dim\rho \|\rho(D_f)\|^2 &= \sum_{\rho \in \hat{G}} \dim\rho \|\rho(D_f)\|^2 - \sum_{\rho_N = \rho_0} \dim\rho \|\rho(D_f)\|^2 \\ &= m^2 n - \dim\rho_0 \|\rho_0(D_f)\|^2 - \sum_{\rho_N = \rho_0, \rho \neq \rho_0} \dim\rho \|\rho(D_f)\|^2 \\ &= m^2 n - 1.m^2 - \sum_{\rho_N = \rho_0, \rho \neq \rho_0} (\dim\rho \times 0) \\ &= m^2(n-1) \end{aligned}$$

since number of principle representation on N is equal to $|\hat{K}|$, the number of non-principle representation is equal to $|\hat{G}| - |\hat{K}| = |\hat{K}||\hat{N}| - |\hat{K}| = |\hat{K}|(|\hat{N}|-1)$. Therefore we have

$$\max_{\rho_N \neq \rho_0} \dim\rho \|\rho(D_f)\|^2 \geq \frac{m^2(n-1)}{|\hat{K}|(|\hat{N}|-1)}.$$

The proof also shows that

$$\max_{\rho_N \neq \rho_0} \dim\rho \|\rho(D_f)\|^2 = \frac{m^2(n-1)}{|\hat{K}|(|\hat{N}|-1)}$$

$$\Updownarrow$$

$$\forall \rho_N \neq \rho_0, \|\rho(D_f)\|^2 = \frac{m^2(n-1)}{\dim\rho |\hat{K}|(|\hat{N}|-1)}.$$

[2, p.11] Parseval's equation and anology with Abelian case, suggest us to say that a function $f : K \to N$ is called maximum nonlinear if and only if the value $\sqrt{\dim\rho}||\rho(D_f)||$ is as small as possible.

Definition: Let $f : K \to N$. f is maximum nonlinear if and only if

$$\max_{\rho_N \neq \rho_0} \sqrt{\dim\rho}||\rho(D_f)|| \leq \max_{\rho_N \neq \rho_0} \sqrt{\dim\rho}||\rho(D_g)||, \forall g : K \to N.(2.17)$$

Summary: [2, p.14]

Almost perfect nonlinearity: Minimize

$$\sum_{\rho \in \hat{G}} \dim\rho||\rho(D_f)||^4$$

for functions $f : K \to N$, where $G = K \times N$.

Maximal nonlinearity: Minimize the maximum of

$$\sqrt{\dim\rho}||\rho(D_g)||$$

for all $f : K \to N$.

Bentness: Find function $f : K \to N$ such that

$$\forall \rho_N \neq \rho_0, |\rho(D_f)||^2 = \frac{m^2(n-1)}{\dim\rho|\hat{K}|(|\hat{N}|-1)}.$$

CHAPTER 3

COMPARISON WITH THE PREVIOUS DEFINITIONS OF BENT FUNCTIONS

A function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ is called a *Boolean function*. Take an integer $q \geq 2$, the imaginary unit $i = \sqrt{-1}$, and a primitive complex root of unity $\xi = e^{2\pi i}/q$ of degree q. Consider the q-ary function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$.

The Walsh-Hadamard transform of a function f is a complex-valued function from $\mathbb{Z}_q^n$ to $\mathbb{C}$ defined as follows:

$$W_f(y) = \sum_{x \in \mathbb{Z}_q^*} \xi^{<x,y>+f(x)} \tag{3.1}$$

where the inner product and addition are taken modulo q.

Denote the absolute value of a complex number z by $|z|$.

Definition:[4, p.2] (*Kumar, Schlotz and Welch,1985*) Given a positive integer q, a function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is called a q-ary bent function if $|W_f(y)| = q^{n/2}$ for every $y \in Z_q$.

Example: Let $f(x) = x^3 + 3x^2$ from $\mathbb{Z}_4$ to $\mathbb{Z}_4$. Then

$W_f(0) = \sum_{x \in \mathbb{Z}_4} i^{<x,0>+f(x)} = \sum_{x \in \mathbb{Z}_4} i^{f(x)} = 2$
$W_f(1) = \sum_{x \in \mathbb{Z}_4} i^{<x,1>+f(x)} = \sum_{x \in \mathbb{Z}_4} i^{x+f(x)} = 2i$
$W_f(2) = \sum_{x \in \mathbb{Z}_4} i^{<x,2>+f(x)} = \sum_{x \in \mathbb{Z}_4} i^{2x+f(x)} = 2$
$W_f(3) = \sum_{x \in \mathbb{Z}_4} i^{<x,3>+f(x)} = \sum_{x \in \mathbb{Z}_4} i^{3x+f(x)} = -2i$

Since $|W_f(y)| = 2 = 4^{1/2}$, for all $y \in Z_4$, f is a $4 - ary$ bent function. On the other hand, f is not a ‘generalized bent function’:

Cpnsiderin the graph of f defined by (2.8),

$$D_f = \{(0,0),(1,0),(2,0),(3,2)\}$$

Let $\rho = \rho_1 \otimes \rho_2$ where character of ρ_1 is $(1, i, -1, -i)$ and character of ρ_2 is $(1, -1, 1, -1)$. Then

$$\begin{aligned} \mathrm{tr}(\rho(D_f)) &= \mathrm{tr}[\rho((0,0),(1,0),(2,0),(3,2))] \\ &= \mathrm{tr}(\rho(0,0)) + \mathrm{tr}(\rho(1,0)) + \mathrm{tr}(\rho(2,0)) + \mathrm{tr}(\rho(3,2)) \\ &= 1.1 + i.1 + (-1).1 + (-i).1 \\ &= 1 + i - 1 - i \\ &= 0 \end{aligned}$$

Thus, $\|\rho(D_f)\| = |\rho(D_f)| = 0 \neq 4^{1/2}$. Hence f is not a 'generalized bent function'.

Now we consider q-ary functions over the finite field $\mathbb{F}_q^n$, where $q = p^l$ with prime p, positive integer l. Again take the primitive complex root of unity $\xi = e^{2\pi i/p}$ of degree p. Consider the q-ary function $f : \mathbb{F}_q^n \to \mathbb{F}_q$.
Define

$$W_{f,z}(y) = \sum_{x \in \mathbb{F}_q^n} \xi^{<<x,y>+f(x),z>} \tag{3.2}$$

with $y \in \mathbb{F}_q^n$, $z \in \mathbb{F}_q^*$

Definition: [4, p.5](*Ambrosimov, 1994*) Take $q = p^l$ with prime p, positive integer l. A function $\mathbb{F}_q^n \to \mathbb{F}_q$. is called a *bent function* if for all $z \in \mathbb{F}_q^*$ and $y \in \mathbb{F}_q^n$,

$$|W_{f,z}(y)| = q^{n/2}$$

Theorem: [4, p.6] A function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is a bent function if and only if the function $f(x + y) - f(x)$ is uniformly distributed over $\mathbb{F}_q$, with $y \in \mathbb{F}_q^*$.

Proof: [5, p.3]

$$\begin{aligned}
|W_{f,z}(y)|^2 &= W_{f,z}(y)\overline{W_{f,z}(y)} \\
&= \left(\sum_{a\in\mathbb{F}_q^n} \xi^{<<a,y>+f(a),z>}\right)\left(\overline{\sum_{b\in\mathbb{F}_q^n} \xi^{<<b,y>+f(b),z>}}\right) \\
&= \sum_{a\in\mathbb{F}_q^n} \xi^{<f(a),z>} \sum_{b\in\mathbb{F}_q^n} \xi^{-<f(b),z>+<<a-b,y>,z>} \\
&= \sum_{a\in\mathbb{F}_q^n} \xi^{<f(a),z>} \sum_{c\in\mathbb{F}_q^n} \xi^{-<f(a-c),z>+<<c,y>,z>} \\
&= \sum_{c\in\mathbb{F}_q^n} \xi^{<<c,y>,z>} \sum_{a\in\mathbb{F}_q^n} \xi^{<f(a)-f(a-c),z>}
\end{aligned}$$

Now suppose $f(x+y)-f(x)$ is uniformly distributed over $\mathbb{F}_q$, with $y\in\mathbb{F}_q$.

If $c\neq 0$, then

$$\sum_{a\in\mathbb{F}_q^n} \xi^{<f(a)-f(a-c),z>} = q^{n-1}\sum_{t\in\mathbb{F}_q} \xi^{<t,z>} = 0$$

since $z\neq 0$. Thus

$$|W_{f,z}(y)|^2 = \sum_{c\in\mathbb{F}_q^n} \xi^{<<c,y>,z>}(q^n\delta_{c,0}) = q^n$$

Hence $|W_{f,z}(y)| = q^{n/2}$ for all $z\in\mathbb{F}_q^*$ and $y\in\mathbb{F}_q^n$.

Now suppose f is bent. Define

$$\Delta_z(f,c) := \sum_{x\in\mathbb{F}_q^n} \xi^{<f(x+c)-f(x),z>}$$

Then

$$\begin{aligned}
q^n = |W_{f,z}(y)|^2 &= \sum_{c\in\mathbb{F}_q^n} \xi^{<<c,y>,z>} \sum_{a\in\mathbb{F}_q^n} \xi^{<f(a)-f(a-c),z>} \\
&= \sum_{c\in\mathbb{F}_q^n} \xi^{-<<c,y>,z>} \sum_{a\in\mathbb{F}_q^n} \xi^{<f(a)-f(a+c),z>} \\
&= \sum_{c\in\mathbb{F}_q^n} \xi^{<<c,y>,z>}\overline{\Delta_z(f,c)}
\end{aligned}$$

for all $c\in\mathbb{F}_q^n$. We need to show $\Delta_z(f,c)=0$ for all $c\in\mathbb{F}_{q^n}^*$. We have q^n equations with q^n unknowns. Ordering the elements of $\mathbb{F}_q^n$ by $\alpha_0,...,\alpha_{q^n-1}$ with $\alpha_0=0$, we have

$$\begin{pmatrix}
1 & 1 & \cdots & 1 \\
1 & \xi^{-<<\alpha_1,\alpha_1>,z>} & \cdots & \xi^{-<<\alpha_{q^n-1},\alpha_1>,z>} \\
\vdots & \vdots & \ddots & \vdots \\
1 & \xi^{-<<\alpha_1,\alpha_{q^n-1}>,z>} & \cdots & \xi^{-<<\alpha_{q^n-1},\alpha_{q^n-1}>,z>}
\end{pmatrix}
\begin{pmatrix}
\overline{\Delta_z(f,0)} \\
\overline{\Delta_z(f,\alpha_1)} \\
\vdots \\
\overline{\Delta_z(f,\alpha_{q^n-1})}
\end{pmatrix}
=
\begin{pmatrix}
q^n \\
q^n \\
\vdots \\
q^n
\end{pmatrix}$$

Let H denote the $q^n \times q^n$ matrix in above. The using the orthogonality relation of characters, we have

$$\overline{H}^T H = q^n I_n.$$

Multiplying both side with $\overline{H}^T$, we have

$$\overline{\Delta_z(f, \alpha_j)} = \sum_{i=0}^{q^n-1} \xi^{<<\alpha_j, \alpha_i>, z>}$$

for $j \in \{0, 1, ..., q^n - 1\}$. For $\alpha_j \neq 0$, since $z \neq 0$, we have

$$\sum_{i=0}^{q^n-1} \xi^{<<\alpha_j, \alpha_i>, z>} = 0$$

Thus $\Delta_z(f, \alpha_j) = 0$ for all $z \in \mathbb{F}_q^*$ is uniformly distributed over $\mathbb{F}_q$, with $y \in \mathbb{F}_q^*$.

Now let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then

$$D_f = \{(a, f(a)) : a \in \mathbb{F}_q^n\}$$

we have $q^n \times q$ irreducible representation over $\mathbb{F}_q^n \times \mathbb{F}_q$. We can propose an equivalent definition to $W_{f,z}(y)$:

$$W'_{f,z}(y) = \sum_{x \in \mathbb{F}_q^n} \xi^{\mathrm{Tr}(<x,y>+zf(x))}$$

Then we have

$$\begin{aligned} W'_{f,z}(y) &= \sum_{x \in \mathbb{F}_q^n} \xi^{\mathrm{Tr}(<x,y>+zf(x))} \\ &= \sum_{x \in \mathbb{F}_q^n} \mathrm{tr}[(\rho_y \otimes \rho_z)(x, f(x))] \\ &= \mathrm{tr}(\rho_y \otimes \rho_z)\left(\sum_{x \in \mathbb{F}_q^n} (x, f(x)) \right) \\ &= \mathrm{tr}[(\rho_y \otimes \rho_z)(D_f)] \end{aligned}$$

where ρ_y and ρ_z are corresponding representations to y and z. Hence a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is a such q-ary bent function if and only if f is '*generalized bent function*'.

For integer $q \geq 2$, take primitive complex root of unity $\xi = e^{2\pi i/p}$ of degree q. A function $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ is called *generalized Boolean function*. The Walsh-Hadamard transform of function f is complex valued function from $\mathbb{Z}_2^n$ to $\mathbb{C}$ as follows:

$$W_f(y) = \sum_{x \in \mathbb{F}_q^n} (-1)^{<x,y>} \xi^{f(x)}$$

Definition:[4, p.7] (*Schmidt,2006*) For positive integer q, a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ is called a *generalized (Boolean) bent function* if $|W_f(y)| = 2^{n/2}$ for every $y \in \mathbb{Z}_2^n$.

Example: Let $n = 2$ and $q = 4$ and $f((x_1, x_2)) = \begin{cases} 2 & \text{if } x = (1,1) \\ 0 & \text{otherwise} \end{cases}$. Then

$\mathrm{W}_f((0,0)) = \sum_{(x_1,x_2)\in\mathbb{Z}_2^2}(-1)^{<(0,0),(x_1,x_2)>} i^{f(x_1,x_2)} = \sum_{(x_1,x_2)\in\mathbb{Z}_2^2} i^{f(x_1,x_2)} = 2$
$W_f((0,1)) = \sum_{(x_1,x_2)\in\mathbb{Z}_2^2}(-1)^{<(0,1),(x_1,x_2)>} i^{f(x_1,x_2)} = \sum_{(x_1,x_2)\in\mathbb{Z}_2^2}(-1)^{x_2} i^{f(x_1,x_2)} = 2$
$W_f((1,0)) = \sum_{(x_1,x_2)\in\mathbb{Z}_2^2}(-1)^{<(1,0),(x_1,x_2)>} i^{f(x_1,x_2)} = \sum_{(x_1,x_2)\in\mathbb{Z}_2^2}(-1)^{x_1} i^{f(x_1,x_2)} = 2$
$W_f((1,1)) = \sum_{(x_1,x_2)\in\mathbb{Z}_2^2}(-1)^{<(1,1),(x_1,x_2)>} i^{f(x_1,x_2)} = \sum_{(x_1,x_2)\in\mathbb{Z}_2^2}(-1)^{x_1+x_2} i^{f(x_1,x_2)} = -2$
Thus f is generalized (Boolean) bent function. On the otherhand; f is not a 'generalized bent function', because:

$$D_f = \{((0,0),0),((0,1),0),((1,0),0),((1,1),2)\}$$

Let $\rho = \rho_1 \otimes \rho_2$ where character of ρ_1 is $(1,-1,1,-1)$ and character of ρ_2 is $(1,-1,1,-1)$. Then

$$\mathrm{tr}(\rho(D_f)) = 0$$

Thus $\|\rho(D_f)\| = |\rho(D_f)| = 0 \neq 4^{1/2}$. Hence f is not a 'generalized bent function'.

Take a finite group $(K,+)$ of order n, the maximal order of whose elements equal to q. Denote the group of degree q roots of unity by

$$U_q = \{e^{2\pi ik/q} : k = 0,1,...,q-1\}$$

and the group homomorphism $\chi : K \to U_q$, by $\hat{K}$, which is the character group of K.
The Fourier transform of a complex valued function $f : K \to \mathbb{C}$ as

$$\hat{f}(y) = \sum_{x\in K} f(x)\overline{\chi_y(x)}$$

where χ_y is the corresponding character of y.

Definition: [4, p.8] (*Logachev,Sal'nikov, and Yashchenko, 1997*) Take a finite abelian group K of order n. A function as $f : K \to S_1(\mathbb{C})$ is called a *bent function* if $|\hat{f}(y)|^2 = n$ for every $y \in K$.

Theorem: [4, p.9] A function $f : K \to S_1(\mathbb{C})$ is a bent function if and only if $\overline{f(x)}f(x+y)$ is balanced for every $y \in K\backslash\{0\}$.

Proof: Suppose $\overline{f(x)}f(x+y)$ is balanced for every $y \in K\backslash\{0\}$.

$$\begin{aligned}
|\hat{f}(y)|^2 &= \sum_{a\in K} f(a)\overline{\chi_y(a)}\left(\overline{\sum_{b\in K} f(b)\overline{\chi_y(b)}}\right)\\
&= \sum_{a\in K} f(a)\sum_{b\in K}\overline{f(b)}\chi_y(b-a)\\
&= \sum_{a\in K} f(a)\sum_{c\in K}\overline{f(c+a)}\chi_y(c)\\
&= \sum_{c\in K}\chi_y(c)\overline{\sum_{c\in K}\overline{f(a)}f(c+a)}\\
&= \chi_y(0)\overline{\sum_{a\in K}\overline{f(a)}f(a)}\\
&= \sum_{a\in K} 1\\
&= n
\end{aligned}$$

Now suppose f is bent.

$$\begin{aligned}
n = |\hat{f}(y)|^2 &= \sum_{c\in K}\chi_y(c)\overline{\sum_{c\in K}\overline{f(a)}f(c+a)}\\
&= \sum_{c\in K}\chi_y(c)\overline{\Delta_f(c)}
\end{aligned}$$

for all $y \in K$ where $\Delta_f(c) = \sum_{c\in K}\overline{f(a)}f(c+a)$. Ordering elements of K as $k_0, ..., k_{n-1}$ with $k_0 = 0$, we have

$$\begin{pmatrix} 1 & 1 & \cdots & 1\\ 1 & \chi_1(k_1) & \cdots & \chi_1(k_{n-1})\\ \vdots & \vdots & \ddots & \vdots\\ 1 & \chi_{k_{n-1}}(k_1) & \cdots & \chi_{k_{n-1}}(k_{n-1}) \end{pmatrix}\begin{pmatrix} \overline{\Delta_f(0)}\\ \overline{\Delta_f(k_1)}\\ \vdots\\ \overline{\Delta_f(k_{n-1})} \end{pmatrix} = \begin{pmatrix} n\\ n\\ \vdots\\ n \end{pmatrix}$$

Let H denote the $n\times n$ matrix in above. The using the orthogonality relation of characters, we have

$$\overline{H}^T H = q^n I_n.$$

Multiplying both side with $\overline{H}^T$, we have

$$\overline{\Delta_f(k_j)} = \sum_{i=0}^{q^n-1}\overline{\chi_{k_j}(k_j)}$$

for $j \in \{0, ..., n-1\}$. For $k_j \neq 0$

$$\sum_{i=0}^{q^n-1}\overline{\chi_{k_j}(k_j)} = \sum_{i=0}^{q^n-1}\chi_{k_j}(-k_j) = 0$$

Thus $\Delta_f(k_j) = 0$ for all $k_j \neq 0$. Hence $\sum_{x \in K} \overline{f(x)} f(x+y) = 0$ for all $y \in K \backslash \{0\}$; that is, $\overline{f(x)} f(x+y)$ is balanced for every $y \in K \backslash \{0\}$.

Take another group N, and take a function $f : K \to N$. The Fourier transform of the characters of f for $z \in N$ to function

$$\hat{f_z}(y) = \sum_{x \in K} \eta_z(f(x)) \overline{\chi_y(x)}$$

$y \in K$ where η_z is corresponding character of $z \in N$.

Definition: (*Solodovnikov,2002*) [4, p.10]A function $f : K \to N$ is called *bent function* if $|\hat{f_z}(y)|^2 = n$ for every $z \in N \backslash \{0\}$ and $y \in K$.

Theorem: [4, p.10]A function $f : K \to N$ is bent function if and only if $f(x+y) - f(x)$ is uniformly distributed.

Proof:

$$\begin{aligned} |\hat{f_z}(y)|^2 &= \left(\sum_{a \in K} \eta_z(f(a)) \overline{\chi_y(a)} \right) \left(\overline{\sum_{b \in K} \eta_z(f(b)) \overline{\chi_y(b)}} \right) \\ &= \sum_{a \in K} \eta_z(f(a)) \sum_{b \in K} \overline{\eta_z(f(b))} \chi_y(b-a) \\ &= \sum_{a \in K} \eta_z(f(a)) \sum_{c \in K} \overline{\eta_z(f(a+c))} \chi_y(c) \\ &= \sum_{c \in K} \chi_y(c) \sum_{a \in K} \eta_z(f(a) - f(a+c)) \end{aligned}$$

Suppose $f(x+y) - f(x)$ is uniformly distributed on N for all $y \in K \backslash \{0\}$

$$|\hat{f_z}(y)|^2 = \chi_y(0) \sum_{a \in K} \eta_z(f(a) - f(a)) = n$$

Thus f is bent.

Now suppose f is bent. Say

$$\Delta_z(f, c) = \sum_{a \in K} \eta_z(f(a+c) - f(a))$$

Then

$$n = |\hat{f_z}(y)|^2 = \sum_{c \in K} \chi_y(c) \overline{\Delta_z(f, c)}$$

for $c \in K$. We need to show $\Delta_z(f, c) = 0$ for all $c \in K \backslash \{0\}$. We have n equations with n

unknows. Ordering elements of K as $k_0, ..., k_{n-1}$ with $k_0 = 0$, we have

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \chi_1(k_1) & \cdots & \chi_1(k_{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \chi_{k_{n-1}}(k_1) & \cdots & \chi_{k_{n-1}}(k_{n-1}) \end{pmatrix} \begin{pmatrix} \overline{\Delta_z(f,0)} \\ \overline{\Delta_z(f,k_1)} \\ \vdots \\ \overline{\Delta_z(f,k_{n-1})} \end{pmatrix} = \begin{pmatrix} n \\ n \\ \vdots \\ n \end{pmatrix}$$

Let H denote the $n \times n$ matrix in above. The using the orthogonality relation of characters, we have

$$\overline{H}^T H = q^n I_n.$$

Multiplying both side with $\overline{H}^T$, we have

$$\overline{\Delta_z(f,k_j)} = \sum_{i=0}^{q^n-1} \overline{\chi_{k_j}(k_j)} = 0$$

for all $y \in K \backslash \{0\}$. Hence $f(x+y) - f(x) = 0$ is balanced for every $y \in K \backslash \{0\}$.

In this case, let $f : K \to N$ be a map with K and N abelian groups. Then

$$D_f = \{(a, f(a)) : a \in K\}$$

We have $|K|.|N|$ irreducible representation over $K \times N$. Now

$$\begin{aligned} \hat{f}_z(y) &= \sum_{a \in K} \eta_z(f(a)) \overline{\chi_y(a)} \\ &= \sum_{a \in K} \chi_{y^{-1}}(a) \eta_z(f(a)) \\ &= \sum_{a \in K} (\chi_{y^{-1}} \otimes \eta_z)(a, f(a)) \\ &= (\chi_{y^{-1}} \otimes \eta_z)(D_f) \end{aligned}$$

for every $z \in N \backslash \{0\}$ and $y \in K$.Thus this type bent function is also '*generalized bent function*'. Futhermore, prev,ous theorem shos us:

Theorem: A function $f : K \to N$ is a '*generalized bent function*' if and only if f is perfect nonlinear.

Example: [2, p.15] Let $K = S_3$ and $N = C_3$ and

$$f : [id, (12), (13), (23), (123), (132)] \to [0, 0, 0, 0, 1, 1]$$

is a '*generalized bent function*', but not perfect nonlinear.

In abelian case we showed that a function is a '*generalized bent function*' if and only if it is perfect nonlinear. Now we will show the connection of bent and perfect nonlinear in some non-abelian cases:

Proposition: [1, p.168] Assume that $N \lhd G$ and $\tilde{\chi}$ be a character of G/N. Define $\chi : G \to \mathbb{C}$ by

$$\chi(g) = \tilde{\chi}(Ng) \ (g \in G)$$

Then χ is a character of G and χ and $\tilde{\chi}$ has the same degree.

Proof: Let $\tilde{\rho} : G/N \to \mathrm{GL}(n, \mathbb{C})$ be a representation of G/N with character $\tilde{\chi}$. The function $\rho : G \to \mathrm{GL}(n, \mathbb{C})$ which is given by the composition

$$g \to Ng \to \tilde{\rho}(Ng)$$

$g \in G$, is a homomorphism G to $\mathrm{GL}(n, \mathbb{C})$. Thus ρ is a representation of G. The character $\chi(g)$ if ρ satisfies

$$\chi(g) = \mathrm{tr}(\rho(g)) = \mathrm{tr}(\tilde{\rho}(Ng)) = \tilde{\chi}(Ng)$$

for all $g \in G$. Moreover, $\chi(1) = \tilde{\chi}(N)$, so χ and $\tilde{\chi}$ have the same degree.

Definition: [1, p.173] For a group G, let G' be the subgroup of G which is generated by all elements of the form $(g, h \in G)$

$$g^{-1}h^{-1}gh$$

Then G' is called the *derived subgroup* of G. Define $[g, h] := g^{-1}h^{-1}gh$. Then

$$G' = \{[g, h] : g, h \in G\}$$

Proposition: [1, p.174]

1) $G' \lhd G$

2)G/G' is abelian.

Proof:

1) Since $e \in G'$, G' is nonempty. For all $a, b, x \in G$ we have

$$x^{-1}(ab^{-1})x = (x^{-1}ax)(x^{-1}b^{-1}x)$$

By using this equality, G' consists of products of the elements of the form $[g, h]$ and their inverses. Since we have also

$$\begin{aligned} x^{-1}[g,h]x &= x^{-1}g^{-1}h^{-1}ghx \\ &= (x^{-1}gx)^{-1}(x^{-1}hx)^{-1}(x^{-1}gx)(x^{-1}hx) \\ &= [x^{-1}gx, x^{-1}hx] \end{aligned}$$

for all $a, b, x \in G$. Therefore $G' \lhd G$.

2)Let $g, h \in G$. $ghg^{-1}h^{-1} \in G'$ implies $gh \in Nhg$, which implies $Ngh = Nhg$. Since $G' \lhd G$, $(G'g)(G'h) = G'gh = G'hg = (G'h)(G'g)$. Hence G/G' is abelian.

Proposition: [1, p.173] If χ is a linear character of G, then $G' \leq Ker\chi$.

Proof: Let χ be a linear character of G. Then χ is a homomorphism from G to the multiplicative group of non-zero complex numbers. Therefore, for all $g, h \in G$,

$$\chi(g^{-1}h^{-1}gh) = \chi(g)^{-1}\chi(h)^{-1}\chi(g)\chi(h) = 1$$

Hence $G' \leq Ker\chi$.

Proposition: [1, p.173] The linear characters of G are precisely the lifts to G of the irreducible characters of G/G'. In particular, the number of distinct linear characters of G is equal to $|G/G'|$, and so divides $|G|$.

Proof: Let $m = |G/G'|$. Since G/G' is abelian, it has exactly m irreducible characters, all of degree 1. So their lifts are also have degree 1. By using 'Irreducible characters of G/N (N-normal) correspond to irreducible characters of G which have N in their kernel', [1, p.169] these are the all irreducible linear characters of G.

Proposition: [2, p.13] Let $f : K \to N$ be a perfect nonlinear function. Then $||\rho(D_f)||^2 = mdim\rho$.

Proof: Let $f : K \to N$ be a perfect nonlinear function. Then

$$\begin{aligned} D_fD_f^{-1} &= \sum_{(a,b)\in G} \delta_f(a,b)(a,b) \\ &= m(id,id) + \frac{m}{n}\left(\sum_{(a,b)\in G}(a,b) - \sum_{b\in N} b \right) \\ &= m(id,id) + \frac{m}{n}(0-0) \\ &= m(id,id) \end{aligned}$$

Then we have

$$\begin{aligned}||\rho(D_f)||^2 &= \text{tr}[\rho(D_f)\circ\rho(D_f)^*]\\ &= \text{tr}[\rho(D_f D_f^{-1})]\\ &= mdim\rho\end{aligned}$$

Theorem: [2, p.13] Let $f : K \to N$ be a function. Assume at least one of K and N is non-abelian and not equal to its derived subgroup. Then f cannot be both perfect nonlinear and bent.

Proof: Assume $f : K \to N$ be a perfect nonlinear function, then $||\rho(D_f)||^2 = mdim\rho$. Assume also f is bent, then $||\rho(D_f)||^2 = \frac{m^2(n-1)}{dim\rho|\hat{K}|(|\hat{N}|-1)}$. Thus in order to be f both perfect nonlinear and bent, we must have

$$m(n-1) = (dim\rho)^2|\hat{K}|(|\hat{N}|-1)$$

This equality holds if and only if $dim\rho$ is the same for every $\rho \in \widehat{G}$ such than $\rho_N \neq \rho_0$.

Case I: Suppose that N is non-abelian and not equal to its derived subgroup. Since N is non-abelian, it has at least one representation of dimension $d' > 1$, call it $\rho_N^{(1)}$. Since number of irreducible linear representation is $|N/N'|$ and since $N \neq N'$, there is also at least one non-principle irreducible linear character of N, call it $\rho_N^{(2)}$. Take any representation ρ_K of K of degree d. Then we have

$$dim(\rho_K \otimes \rho_N^{(1)}) = d'd > d = dim(\rho_K \otimes \rho_N^{(2)})$$

Case II: Suppose that K is non-abelian and not equal to its derived subgroup and N is abelian. K has at least one representation of dimension $d > 1$, call it $\rho_K^{(1)}$.Since number of irreducible linear representation is $|K/K'|$ and since $K \neq K'$, there is also at least one non-principle irreducible linear character of K, call it $\rho_K^{(2)}$. Since $N \neq$id, take any non-principle representation ρ_N of N. Then we have

$$dim(\rho_K^{(1)} \otimes \rho_N) = d > 1 = dim(\rho_K^{(2)} \otimes \rho_N).$$

REFERENCES

[1] Gordon James and Martin Liebeck, *Representations and Charecters of Groups*, Second Edition

[2] Laurent Poinsot and Alexander Pott, *Non-Boolean Almost Perfect Nonlinear Functions on Non-Abelian Groups*, International Journal of Foundations of Computer Science 22, 6 (2011) 1351-1367

[3] Laurent Poinsot, *Non Abelian Bent Functions*, arXiv:1012.4079v1

[4] Natalia Tokareva, *Generalizations of Bent Functions. A Survey*, Russian Journal Discrete Analysis and Operation Research, N 1. V. 17. 2010. P. 34-64.

[5] Robert S. Coulter and Rex W. Matthews, *Bent Polynomials over Finite Fields*, BULL. AUSTRAL. MATH. SOC. VOL. 56 (1997) [429-437]