Cryptographic Boolean functions with biased inputs

Sugata Gangopadhyay[1], Aditi Kar Gangopadhyay[2],
Spyridon Pollatos[3], Pantelimon Stănică[3]

[1]Department of Computer Science and Engineering
Indian Institute of Technology Roorkee, INDIA
gsugata@gmail.com
[2]Department of Mathematics
Indian Institute of Technology Roorkee, INDIA
ganguli.aditi@gmail.com
[3] Department of Applied Mathematics
Naval Postgraduate School, Monterey, CA 93943–5216, USA
pstanica@nps.edu

July 31, 2015

Abstract

While performing cryptanalysis, it is of interest to approximate a Boolean function in n variables $f : \mathbb{F}_2^n \to \mathbb{F}_2$ by affine functions. Usually, it is assumed that all the input vectors to a Boolean function are equiprobable while mounting affine approximation attack or fast correlation attacks. In this paper we consider a more general case when each component of the input vector to f is independent and identically distributed Bernoulli variates with the parameter p. Since our scope is within the area of cryptography, we initiate an analysis of cryptographic Boolean functions under the previous considerations and derive expression of the analogue of Walsh–Hadamard transform and nonlinearity in the case under consideration. We observe that if we allow p to take up complex values then a framework involving quantum Boolean functions can be introduced, which provides a connection between Walsh-Hadamard transform, nega-Hadamard transform and Boolean functions with biased inputs.

Keywords: Boolean functions, quantum Boolean functions, bias, Walsh–Hadamard transform, nega-Hadamard transform.

1 Introduction

Let $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ be the sets of integers, real numbers, and complex numbers respectively. Additions over $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ are all denoted by '+' and multiplications are denoted by juxtaposing the two elements to be multiplied. Any complex number can be written as $z = a + \imath b$ where $\imath^2 = -1$ and the absolute value of z is $|z| = \sqrt{a^2 + b^2}$, this includes the case when $b = 0$ that is z is essentially a real number. The real part a of z is denoted by $\Re(z)$ and the imaginary part b is denoted by $\Im(z)$. If S is a set then $|S|$ denotes the cardinality of S. The set of positive integers x such that $1 \leq x \leq n$ is denoted by $[n]$. Let $0 \leq p < 1$ and $\mathbb{V}_n(p) = \{\mathbf{x} = (x_1, \ldots, x_n) : x_i \in \mathbb{F}_2, \text{ for all } i \in [n]\}$ ($\mathbb{F}_2$ is the two-element field) be the n-dimensional Hamming space with the probability measure μ_p defined by

$$\mu_p(\mathbf{x}) = p^{\mathrm{wt}(\mathbf{x})}(1-p)^{n-\mathrm{wt}(\mathbf{x})}, \tag{1}$$

for all $\mathbf{x} \in \mathbb{V}_n(p)$, where $\mathrm{wt}(\mathbf{x}) = \sum_{i\in[n]} x_i$ is the weight of $\mathbf{x}$. The binary operation addition modulo 2 is defined on $\mathbb{F}_2$ which induces a componentwise addition on $\mathbb{V}_n(p)$, both of them denoted by '$\oplus$'. The multiplication over $\mathbb{F}_2$ is denoted by juxtaposing the two elements to be multiplied, and is also known as multiplication modulo 2. When we need not emphasize the probability measure on $\mathbb{V}_n(p)$ we shall use the more standard notation $\mathbb{F}_2^n$ for that vector space. For any $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, define the inner product as $\mathbf{x} \cdot \mathbf{y} = \sum_{i\in[n]} x_i y_i$. Another operation which is often useful is the intersection, which is defined as $\mathbf{x} * \mathbf{y} = (x_1y_1, \ldots, x_ny_n)$, for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$. Moreover, we have

$$\mathrm{wt}(\mathbf{x}) + \mathrm{wt}(\mathbf{y}) - 2\mathrm{wt}(\mathbf{x} * \mathbf{y}) = \mathrm{wt}(\mathbf{x} \oplus \mathbf{y}).$$

Let $\mathfrak{B}_n(p)$ denote the set of all functions from $\mathbb{V}_n(p)$ to $\mathbb{F}_2$. We refer to these functions as *μ_p-Boolean functions.* The algebraic normal form (ANF) of $f \in \mathfrak{B}_n(p)$ is

$$f(\mathbf{x}) = \bigoplus_{\mathbf{a}=(a_1,\ldots,a_n)} c_{\mathbf{a}} \prod_{i\in[n]} x_i^{a_i} \tag{2}$$

where $c_{\mathbf{a}} \in \mathbb{F}_2$ for all $\mathbf{a} \in \mathbb{F}_2^n$.

In this paper we start a systematic study of this generalization for cryptographic Boolean functions first by considering their distances from affine functions and thereby introducing μ_p-Walsh–Hadamard transform at $\mathbf{u} \in \mathbb{V}_n(p)$

$$W^{(p)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}$$

where $\rho = \frac{p}{1-p}$. We observe that if we substitute $p = \frac{1+\imath}{2}$, then $W^{(p)}(\mathbf{u})$ is the nega-Hadamard transform

$$W^{(p)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \imath^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}$$

which is considered by Parker [10], Riera et al. [13], Parker et al. [11], Schmidt et al. [15], Stănică et al. [16]. We introduce a quantum Boolean function framework to explain the complex values of the constant ρ. Parker [10] has left the development of cryptanalytic techniques by using the generalized spectra of Boolean functions as a future research problem. The connection between the affine approximations of μ_p-Boolean functions, μ_p-Walsh-Hadamard spectra and nega-Hadamard spectra in this paper might prove to be a step towards that problem.

Boolean functions with biased inputs, which we refer to as μ_p-Boolean functions, is a common generalization of Boolean functions which stems from the theory of random graphs developed by Erdős and Rényi [2]. The graph properties in a random graph expressed as such Boolean functions are used by Friedgut and Kalai [3]. Fourier Entropy-Influence conjecture is also formulated in the biased framework by Keller, Mossel and Schlank [4], O'Donnell and Tan [9]. For a detailed discussion on the Fourier analysis of μ_p-Boolean functions we refer to [8]. Using our notations, the Fourier expansion of $f \in \mathfrak{B}_n(p)$ used in [4, 8] can be written as

$$(-1)^{f(\mathbf{x})} = \sum_{\mathbf{u}\in\mathbb{F}_2^n} \widehat{f}(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{x}}(\sqrt{\rho})^{\mathrm{wt}(\mathbf{x})}\rho^{\mathrm{wt}(\mathbf{u}*\mathbf{x})} \tag{3}$$

where the Fourier coefficient

$$\widehat{f}(\mathbf{u}) = (1-p)^n \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}(\sqrt{\rho})^{\mathrm{wt}(\mathbf{x})}\rho^{\mathrm{wt}(\mathbf{u}*\mathbf{x})}. \tag{4}$$

The above expansion is with respect to an orthonormal basis and is a part of the standard theory of μ_p-Boolean functions. However this expansion does not lead to the interconnection between Walsh–Hadamard and nega-Hadamard transform which is immediate from our approach. The interest shown in the recent past by researchers on nega-Hadamard transform along with its generalizations, and the possibility of their cryptographic significance, motivates our present investigation.

2 The distance in $\mathfrak{B}_n(p)$ and μ_p-Walsh–Hadamard transform

We note that in the cryptographic or the coding theoretic context we consider approximations of Boolean functions by the affine functions when the inputs are equiprobable. The set of all such functions is denoted by $\mathfrak{B}_n\left(\frac{1}{2}\right)$, in short $\mathfrak{B}_n$. The distance $d_p(f,g)$ between f and g, referred to as μ_p-distance, is defined as 2^n times the probability that their outputs differ when the input is from $\mathbb{V}_n(p)$. This distance is the same as the Hamming distance if $p=\frac{1}{2}$. Precisely, if $S_{f\neq g}=\{\mathbf{x}\in\mathbb{F}_2^n : f(\mathbf{x})\neq g(\mathbf{x})\}$, then (we set $\rho := \frac{p}{1-p}$)

$$\begin{aligned}
d_p(f,g) &= 2^n \sum_{\mathbf{x}\in S_{f\neq g}} p^{\mathrm{wt}(\mathbf{x})}(1-p)^{n-\mathrm{wt}(\mathbf{x})}\\
&= 2^n(1-p)^n \sum_{\mathbf{x}\in S_{f\neq g}} \rho^{\mathrm{wt}(\mathbf{x})}\\
&= 2^{n-2}(1-p)^n \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}((-1)^{f(\mathbf{x})}-(-1)^{g(\mathbf{x})})^2\\
&= 2^{n-2}(1-p)^n \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(2-2(-1)^{f(\mathbf{x})\oplus g(\mathbf{x})})\\
&= 2^{n-1}(1-p)^n \left(\sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})} - \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus g(\mathbf{x})}\right)\\
&= 2^{n-1}(1-p)^n \left(\sum_{k=0}^{n}\binom{n}{k}\rho^k - \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus g(\mathbf{x})}\right)\\
&= 2^{n-1}(1-p)^n \left((\rho+1)^n - \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus g(\mathbf{x})}\right)\\
&= 2^{n-1} - \frac{2^n(1-p)^n}{2} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus g(\mathbf{x})}.
\end{aligned}$$

For each $\mathbf{u}\in\mathbb{F}_2^n$, $b\in\mathbb{F}_2$, we define the corresponding affine function $\ell_{\mathbf{u},b}$ by $\ell_{\mathbf{u},b}(\mathbf{x})=\mathbf{u}\cdot\mathbf{x}\oplus b$, for all $\mathbf{x}\in\mathbb{F}_2^n$. Then

$$d_p(f,\ell_{\mathbf{u},b}) = 2^{n-1} - (-1)^b\frac{2^n(1-p)^n}{2}\sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}. \tag{5}$$

Comparing (5) to the case of $p = \frac{1}{2}$ we observe that we can define an analogue of the Walsh–Hadamard transform, which we shall refer to as the Walsh–Hadamard transform of f with respect to the probability measure μ_p or the μ_p-*Walsh–Hadamard transform* of f at $\mathbf{u} \in \mathbb{V}_n(p)$

$$W_f^{(p)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \tag{6}$$

where $\rho = \frac{p}{1-p} \in \mathbb{C}$. From (6) we have

$$\begin{aligned}\sum_{\mathbf{u}\in\mathbb{F}_2^n} W_f^{(p)}(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{v}} &= \sum_{\mathbf{u}\in\mathbb{F}_2^n}\sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}(-1)^{\mathbf{u}\cdot\mathbf{v}}\\ &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})} \sum_{\mathbf{u}\in\mathbb{F}_2^n}(-1)^{\mathbf{u}\cdot(\mathbf{v}\oplus\mathbf{x})}\\ &= 2^n\rho^{\mathrm{wt}(\mathbf{v})}(-1)^{f(\mathbf{v})},\end{aligned}$$

and so, the inverse of the μ_p-Walsh–Hadamard transform is

$$(-1)^{f(\mathbf{x})} = 2^{-n}\rho^{-\mathrm{wt}(\mathbf{x})} \sum_{\mathbf{u}\in\mathbb{F}_2^n} W_f^{(p)}(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{x}}. \tag{7}$$

It is observed that if $\rho = \imath$, then

$$W_f^{(p)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \imath^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}},$$

forcing $p = \frac{1+\imath}{2}$. Since p is defined to be the probability that $x_i = 1$ where $i \in [n]$, it must satisfy $0 \le p \le 1$, ρ cannot take complex values in the context of (classical) Boolean functions discussed above. However by lifting the classical Boolean functions to the set of quantum Boolean functions in the next section we observe that some naturally occurring sums are μ_p-Walsh–Hadamard transforms where p can admit complex values. This leads us to obtain Walsh–Hadamard transform and nega-Hadamard transform as a special cases of μ_p-Walsh–Hadamard transform.

3 Quantum Boolean function framework

In this section we provide a framework in which it is natural to consider the parameter ρ as a complex number rather than a real number. At the outset we briefly introduce some notations related to quantum Boolean functions discussed in details by Montanaro and Osborne [6, 7]. Corresponding to each vector $\mathbf{x} \in \mathbb{F}_2^n$ we associate a quantum state $|\mathbf{x}\rangle$. Consider a linear combination of these states

$$|\varphi\rangle = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \beta_{\mathbf{x}}|\mathbf{x}\rangle \tag{8}$$

where $\beta_{\mathbf{x}} \in \mathbb{C}$, for all $\mathbf{x} \in \mathbb{F}_2^n$, and $\sum_{\mathbf{x}\in\mathbb{F}_2^n} |\beta_{\mathbf{x}}|^2 = 1$. This is referred to as an n-qubit. The set $\{|\mathbf{x}\rangle : \mathbf{x} \in \mathbb{F}_2^n\}$ is said to be the computational basis. When we measure the n-qubit $|\varphi\rangle$ we get exactly one state of the computational basis, say $|\mathbf{x}\rangle$, as the result with the probability $|\beta_{\mathbf{x}}|^2$. It is possible to consider an n-qubit as an element of $(\mathbb{C}^2)^{\otimes n}$. Let $\mathbb{I}$ be the identity operator on $(\mathbb{C}^2)^{\otimes n}$. Quantum Boolean functions are defined by Montanaro and Osborne [6] as follows.

Definition 1. *A unitary operator U on $(\mathbb{C}^2)^{\otimes n}$ whose square is identity, that is $U^2 = \mathbb{I}$, is said to be a quantum Boolean function.*

The phase oracle implementation (cf. [6]) of a classical Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ on quantum computers is

$$F : |\mathbf{x}\rangle \mapsto (-1)^{f(\mathbf{x})}|\mathbf{x}\rangle, \text{ for all } \mathbf{x} \in \mathbb{F}_2^n. \tag{9}$$

We will denote the classical Boolean functions by lower case letters and their quantum versions by the corresponding upper case letters. Using this convention the operator corresponding to the affine function $\ell_{\mathbf{u},b}$ is denoted by $L_{\mathbf{u},b}$. Let us consider a single qubit state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{10}$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. Let $q = |\alpha|^2$ and $p = |\beta|^2$. Tensoring $|\psi\rangle$ with itself n times we prepare the n-qubit state

$$|\varphi\rangle = (|\psi\rangle)^{\otimes n} = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \gamma_{\mathbf{x}}|\mathbf{x}\rangle \tag{11}$$

where $\gamma_{\mathbf{x}} = \alpha^{n-\mathrm{wt}(\mathbf{x})}\beta^{\mathrm{wt}(\mathbf{x})}$, for all $\mathbf{x} \in \mathbb{F}_2^n$. For all $\mathbf{x} \in \mathbb{F}_2^n$, $|\gamma_{\mathbf{x}}|^2 = p^{\mathrm{wt}(\mathbf{x})}q^{n-\mathrm{wt}(\mathbf{x})}$. Suppose we apply F and $L_{\mathbf{u},b}$ to $|\psi\rangle$. Then the resulting state is

$$\begin{aligned}(F \circ L_{\mathbf{u},b})(|\varphi\rangle) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \gamma_{\mathbf{x}}(-1)^{f(\mathbf{x})\oplus\ell_{\mathbf{u},b}(\mathbf{x})}|\mathbf{x}\rangle \\ &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \gamma_{\mathbf{x}}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}\oplus b}|\mathbf{x}\rangle.\end{aligned} \tag{12}$$

The square of L^2 distance between the states $|\varphi\rangle$ and $(F \circ L_{\mathbf{u},b})(|\varphi\rangle)$ is

$$\begin{aligned}\Delta_2(|\varphi\rangle, (F \circ L_{\mathbf{u},b})(|\varphi\rangle))^2 &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} |\gamma_{\mathbf{x}}|^2 |1-(-1)^{f(\mathbf{x})\oplus\ell_{\mathbf{u},b}(\mathbf{x})}|^2 \\ &= 4 \sum_{\mathbf{x}\in S_{f\neq\ell_{\mathbf{u},b}}} p^{\mathrm{wt}(\mathbf{x})} q^{n-\mathrm{wt}(\mathbf{x})} \\ &= 2^{2-n} d_p(f, \ell_{\mathbf{u},b}) \\ &= 2 - 2(-1)^b (1-p)^n \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\end{aligned}$$

where $\rho = \frac{p}{1-p}$ as before. Thus we see that Δ_2 depends on $W_f^{(p)}(\mathbf{u})$ which is the usual Walsh–Hadamard transform at $\mathbf{u}$ if $\alpha = \frac{1}{2} - \imath\frac{1}{2}$ and $\beta = \frac{1}{2} + \imath\frac{1}{2}$.

If we consider the two states $|\varphi\rangle$ and $(F \circ L_{\mathbf{u},b})(|\varphi\rangle)$ as vectors with complex components and consider the sum of all the components of their difference $|\varphi\rangle - (F \circ L_{\mathbf{u},b})(|\varphi\rangle)$ we obtain

$$\begin{aligned}\delta(|\varphi\rangle, (F \circ L_{\mathbf{u},b})(|\varphi\rangle)) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \gamma_{\mathbf{x}} (1-(-1)^{f(\mathbf{x})\oplus\ell_{\mathbf{u},b}(\mathbf{x})}) \\ &= 2 \sum_{\mathbf{x}\in S_{f\neq\ell_{\mathbf{u},b}}} \beta^{\mathrm{wt}(\mathbf{x})} \alpha^{n-\mathrm{wt}(\mathbf{x})} \\ &= 2^{2-n} d_\beta(f, \ell_{\mathbf{u},b}) \\ &= 1 - (-1)^b (1-p)^n \sum_{\mathbf{x}\in\mathbb{F}_2^n} \sigma^{\mathrm{wt}(\mathbf{x})} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\end{aligned}$$

where $\sigma = \frac{\beta}{1-\beta}$. Thus, we observe that $\delta(|\varphi\rangle, (F \circ L_{\mathbf{u},b})(|\varphi\rangle))$ depends on $W_f^{(\beta)}(\mathbf{u})$. If $\alpha = \frac{1}{2} - \imath\frac{1}{2}$ and $\beta = \frac{1}{2} + \imath\frac{1}{2}$, then

$$W_f^{(\beta)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \imath^{\mathrm{wt}(\mathbf{x})} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}},$$

which is the nega-Hadamard transform of f at $\mathbf{u}$.

From the above discussion it is clear that the transformation of the type $W_f^{(p)}(\mathbf{u})$ where p is a complex number can be associated to the effect of the actions of F and $L_{\mathbf{u},b}$ on an appropriately prepared quantum state. It is observed that for special choices of p namely $p = \frac{1}{2}$ and $p = \frac{1+\imath}{2}$ we obtain, respectively, Walsh–Hadamard and nega-Hadamard transforms on the Boolean function f. Thus, in order to investigate a general framework where the inputs are not equiprobable it is natural to study μ_p-Walsh–Hadamard transform where $p \in \mathbb{C}$ and $p \neq 1$.

4 Properties of the μ_p-Walsh–Hadamard transform

In this section we explore some basic properties of μ_p-Walsh–Hadamard transform. Using (5) we can also define the *μ_p-weight* of a function to be

$$\begin{aligned}\mathrm{wt}^{(p)}(f) = d_p(f, \mathbf{0}) &= 2^{n-1} - \frac{2^n(1-p)^n}{2} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})} \\ &= 2^{n-1}\left(1 - (1-p)^n W_f^{(p)}(\mathbf{0})\right).\end{aligned}$$

We will use the following identity throughout the paper (we always use the convention that anything raised to the power 0 is 1).

Lemma 2. *Let $p \in \mathbb{C}$ and $\mathbf{u} \in \mathbb{V}_n(p)$, then*

$$\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}} \rho^{\mathrm{wt}(\mathbf{x})} = (1+\rho)^{n-\mathrm{wt}(\mathbf{u})}(1-\rho)^{\mathrm{wt}(\mathbf{u})} = \frac{(1-2p)^{\mathrm{wt}(\mathbf{u})}}{(1-p)^n}.$$

Proof. We have

$$\begin{aligned}\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}} \rho^{\mathrm{wt}(\mathbf{x})} &= \prod_{k=1}^{n} \left(1 + \rho(-1)^{u_k}\right) \\ &= (1+\rho)^{n-\mathrm{wt}(\mathbf{u})}(1-\rho)^{\mathrm{wt}(\mathbf{u})} \\ &= (1+\rho)^n \left(\frac{1-\rho}{1+\rho}\right)^{\mathrm{wt}(\mathbf{u})} \\ &= \frac{(1-2p)^{\mathrm{wt}(\mathbf{u})}}{(1-p)^n},\end{aligned}$$

since $1+\rho = \frac{1}{1-p}$ and $\frac{1-\rho}{1+\rho} = 1-2p$. □

Corollary 3. *The μ_p-weight of an affine function $\ell_{\mathbf{u},b}$ is*

$$\mathrm{wt}^{(p)}(\ell_{\mathbf{u},b}) = 2^{n-1}\left(1 - (-1)^b(1-2p)^{\mathrm{wt}(\mathbf{u})}\right).$$

The next lemma is immediate.

Lemma 4. *If $W_f^{(p)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}$, then $W_f^{(p)}(\mathbf{u}\oplus\mathbf{1}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-\rho)^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}$.*

We prove next a theorem similar to [16, Theorem 3] in the nega context.

Theorem 5. *The following are true:*

(*i*) *Plancherel identity:*

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n} \left|W_f^{(p)}(\mathbf{u})\right|^2 = 2^n(|\rho|^2+1)^n. \tag{13}$$

(*ii*) *For* $\mathbf{u}\in\mathbb{V}_n(p)$, $b\in\mathbb{F}_2$, *then* $W_{\ell_{\mathbf{u},b}}^{(p)}(\mathbf{v}) = (-1)^b\dfrac{(1-2p)^{\mathrm{wt}(\mathbf{u}\oplus\mathbf{v})}}{(1-p)^n}$.

(*iii*) *If* $f\in\mathfrak{B}_n(p), \mathbf{u}\in\mathbb{V}_n(p)$, $b\in\mathbb{F}_2$, *then* $W_{f\oplus\ell_{\mathbf{u},b}}^{(p)}(\mathbf{v}) = (-1)^b W_f^{(p)}(\mathbf{u}\oplus\mathbf{v})$.

(*iv*) *If* $h(\mathbf{x}) = f(\mathbf{x})\oplus g(\mathbf{x})$, *then*

$$2^n W_h^{(p)}(\mathbf{u}) = \sum_{\mathbf{v}\in\mathbb{F}_2^n} W_f^{(p)}(\mathbf{v})W_g(\mathbf{u}\oplus\mathbf{v}) = \sum_{\mathbf{v}\in\mathbb{F}_2^n} W_g^{(p)}(\mathbf{v})W_f(\mathbf{u}\oplus\mathbf{v}).$$

(*v*) *If* $h(\mathbf{x},\mathbf{y}) = f(\mathbf{x})\oplus g(\mathbf{y})$, *then* $W_h^{(p)}(\mathbf{u},\mathbf{v}) = W_f^{(p)}(\mathbf{u})W_g^{(p)}(\mathbf{v})$.

(*vi*) *If* $h(\mathbf{x},\mathbf{y}) = f(\mathbf{x})\cdot g(\mathbf{y})$, $\mathbf{x}\in\mathbb{F}_2^n, \mathbf{y}\in\mathbb{V}_k(p)$, *then*

$$\begin{aligned} W_h^{(p)}(\mathbf{u},\mathbf{v}) &= W_f^{(p)}(\mathbf{u})S_{g1}(\mathbf{v}) + \frac{(1-2p)^{\mathrm{wt}(\mathbf{u})}}{(1-p)^n}S_{g0}(\mathbf{v}) \\ &= W_g^{(p)}(\mathbf{v})S_{f1}(\mathbf{u}) + \frac{(1-2p)^{\mathrm{wt}(\mathbf{v})}}{(1-p)^k}S_{f0}(\mathbf{u}), \end{aligned}$$

where $S_{g1}(\mathbf{v}) = \sum_{\substack{\mathbf{y}\in\mathbb{V}_k(p)\\ g(\mathbf{y})=1}} (-1)^{\mathbf{y}\cdot\mathbf{v}}\,\rho^{\mathrm{wt}(\mathbf{y})}$, $S_{g0}(\mathbf{v}) = \sum_{\substack{\mathbf{y}\in\mathbb{V}_k(p)\\ g(\mathbf{y})=0}} (-1)^{\mathbf{y}\cdot\mathbf{v}}\,\rho^{\mathrm{wt}(\mathbf{y})}$, *and so,* $S_{g0}(\mathbf{v}) + S_{g1}(\mathbf{v}) = \frac{(1-2p)^{\mathrm{wt}(\mathbf{v})}}{(1-p)^n}$. *If* $k=1$ *and* $g(y)=y$, *then*

$$\begin{aligned} W_{yf(\mathbf{x})}(\mathbf{u},v) &= (-1)^v\,\rho\,W_f^{(p)}(\mathbf{u}) + \frac{(1-2p)^{\mathrm{wt}(\mathbf{u})}}{(1-p)^n} \\ W_{(y\oplus1)f(\mathbf{x})}(\mathbf{u},v) &= W_f^{(p)}(\mathbf{u}) + (-1)^v\,\frac{p(1-2p)^{\mathrm{wt}(\mathbf{u})}}{(1-p)^{n+1}}. \end{aligned}$$

(*vii*) *If* $h(\mathbf{x}) = f(\mathbf{x}A\oplus\mathbf{a})$, *for* $A\in O_n(\mathbb{F}_2)$ *(orthogonal group), then*

$$W_h^{(p)}(\mathbf{u}) = (-1)^{\mathbf{u}\cdot(\mathbf{a}A^{-1})}\sum_{\mathbf{z}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{z})\oplus\mathbf{z}\cdot\mathbf{u}A^{-1}}\rho^{\mathrm{wt}(\mathbf{z}\oplus\mathbf{a})},$$

$$W_h^{(p)}(\mathbf{u}) = (-1)^{\mathbf{u}\cdot(\mathbf{a}A^{-1})}\,W_f^{(p)}(\mathbf{u}A^{-1}),\ \textit{if}\ \mathbf{a}=\mathbf{0}.$$

Proof. First, we note that

$$\begin{aligned}
&\sum_{\mathbf{u}\in\mathbb{F}_2^n} \left|W_f^{(p)}(\mathbf{u})\right|^2 \\
&= \sum_{\mathbf{u}\in\mathbb{F}_2^n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \sum_{\mathbf{y}\in\mathbb{F}_2^n} \bar{\rho}^{\mathrm{wt}(\mathbf{y})}(-1)^{f(\mathbf{y})\oplus\mathbf{u}\cdot\mathbf{y}} \\
&= \sum_{\mathbb{F}_2^n} \sum_{\mathbf{x}\in\mathbb{V}_n(p)} \sum_{\mathbf{y}\in\mathbb{V}_n(p)} \rho^{\mathrm{wt}(\mathbf{x})}\bar{\rho}^{\mathrm{wt}(\mathbf{y})}(-1)^{f(\mathbf{x})\oplus f(\mathbf{y})\oplus\mathbf{u}\cdot\mathbf{x}\oplus\mathbf{u}\cdot\mathbf{y}} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \sum_{\mathbf{y}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}\bar{\rho}^{\mathrm{wt}(\mathbf{y})}(-1)^{f(\mathbf{x})\oplus f(\mathbf{y})} \sum_{\mathbf{u}\in\mathbb{V}_n(p)} (-1)^{\mathbf{u}\cdot(\mathbf{x}\oplus\mathbf{y})} \\
&= 2^n \sum_{\mathbf{x}\in\mathbb{F}_2^n} |\rho|^{2\mathrm{wt}(\mathbf{x})} = 2^n \sum_{k=0}^{n} \binom{n}{k} |\rho|^{2k} = 2^n(|\rho|^2+1)^n,
\end{aligned}$$

which shows Plancherel identity (i).
To show (ii),

$$\begin{aligned}
W_{\ell_{\mathbf{u},b}}^{(p)}(\mathbf{v}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}\oplus\, b\oplus\mathbf{v}\cdot\mathbf{x}} \\
&= (-1)^b \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{(\mathbf{u}\oplus\mathbf{v})\cdot\mathbf{x}} \\
&= (-1)^b \frac{(1-2p)^{\mathrm{wt}(\mathbf{u}\oplus\mathbf{v})}}{(1-p)^n}.
\end{aligned}$$

Next, to show (iii),

$$\begin{aligned}
W_{f\oplus\ell_{\mathbf{u},b}}^{(p)}(\mathbf{v}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}\oplus\, b\oplus\mathbf{v}\cdot\mathbf{x}} \\
&= (-1)^b \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})}(-1)^{f(\mathbf{x})\oplus(\mathbf{u}\oplus\mathbf{v})\cdot\mathbf{x}} \\
&= (-1)^b W_f^{(p)}(\mathbf{u}\oplus\mathbf{v}).
\end{aligned}$$

To prove (iv) start with

$$\begin{aligned}
W_f^{(p)}(\mathbf{v}) &= \sum_{\mathbf{y}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{y})}(-1)^{f(\mathbf{y})\oplus\mathbf{y}\cdot\mathbf{v}}, \\
W_g(\mathbf{u}\oplus\mathbf{v}) &= \sum_{\mathbf{z}\in\mathbb{F}_2^n} (-1)^{g(\mathbf{z})\oplus\mathbf{z}\cdot(\mathbf{u}\oplus\mathbf{v})},
\end{aligned}$$

and since (see [1, p. 8])

$$\sum_{\mathbf{v}} (-1)^{\mathbf{v}\cdot\mathbf{w}} = \begin{cases} 2^n & \text{if } \mathbf{w} = \mathbf{0} \\ 0 & \text{if } \mathbf{w} \neq \mathbf{0}, \end{cases}$$

we obtain

$$\begin{aligned} \sum_{\mathbf{v}\in\mathbb{F}_2^n} W_f^{(p)}(\mathbf{v}) W_g(\mathbf{u}\oplus\mathbf{v}) &= \sum_{\substack{\mathbf{v},\mathbf{y},\mathbf{z} \\ \text{in } \mathbb{F}_2^n}} (-1)^{f(\mathbf{y})\oplus g(\mathbf{z})\oplus \mathbf{v}\cdot(\mathbf{y}\oplus\mathbf{z})\oplus\mathbf{u}\cdot\mathbf{z}} \rho^{wt(\mathbf{y})} \\ &= \sum_{\substack{\mathbf{y},\mathbf{z} \\ \text{in } \mathbb{F}_2^n}} (-1)^{f(\mathbf{y})\oplus g(\mathbf{z})\oplus\mathbf{u}\cdot\mathbf{z}} \rho^{wt(\mathbf{y})} \sum_{\mathbf{v}} (-1)^{\mathbf{v}\cdot(\mathbf{y}\oplus\mathbf{z})} \\ &= \sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{y})\oplus g(\mathbf{y})\oplus\mathbf{u}\cdot\mathbf{y}} \rho^{wt(\mathbf{y})} \\ &= 2^n W_{f\oplus g}^{(p)}(\mathbf{u}). \end{aligned}$$

The second claim of (iv) is similar. To prove (v) we write

$$\begin{aligned} W_f^{(p)}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})} (-1)^{f(\mathbf{x})\oplus\mathbf{x}\cdot\mathbf{u}}, \\ W_g^{(p)}(\mathbf{v}) &= \sum_{\mathbf{y}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{y})} (-1)^{g(\mathbf{y})\oplus\mathbf{y}\cdot\mathbf{v}}, \end{aligned}$$

and multiplying these expressions, we obtain

$$\begin{aligned} W_f^{(p)}(\mathbf{u}) W_g^{(p)}(\mathbf{v}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{x})} (-1)^{f(\mathbf{x})\oplus\mathbf{x}\cdot\mathbf{u}} \sum_{\mathbf{y}\in\mathbb{F}_2^n} \rho^{\mathrm{wt}(\mathbf{y})} (-1)^{g(\mathbf{y})\oplus\mathbf{y}\cdot\mathbf{v}} \\ &= \sum_{\substack{\mathbf{x},\mathbf{y} \\ \text{in } \mathbb{F}_2^n}} \rho^{\mathrm{wt}(\mathbf{x})} \rho^{\mathrm{wt}(\mathbf{y})} (-1)^{f(\mathbf{x})\oplus\mathbf{x}\cdot\mathbf{u}} (-1)^{g(\mathbf{y})\oplus\mathbf{y}\cdot\mathbf{v}} \\ &= \sum_{\substack{\mathbf{x},\mathbf{y} \\ \text{in } \mathbb{F}_2^n}} \rho^{\mathrm{wt}(\mathbf{x})+\mathrm{wt}(\mathbf{y})} (-1)^{f(\mathbf{x})\oplus g(\mathbf{y})\oplus\mathbf{x}\cdot\mathbf{u}\oplus\mathbf{y}\cdot\mathbf{v}} \\ &= \sum_{(\mathbf{x},\mathbf{y})\in\mathbb{F}_2^{2n}} \rho^{\mathrm{wt}(\mathbf{x},\mathbf{y})} (-1)^{h(\mathbf{x},\mathbf{y})\oplus(\mathbf{x},\mathbf{y})\cdot(\mathbf{u},\mathbf{v})} \\ &= W_h^{(p)}(\mathbf{u},\mathbf{v}). \end{aligned}$$

To prove (vi) we write

$$\begin{aligned}
W_h^{(p)}(\mathbf{u},\mathbf{v}) &= \sum_{(\mathbf{x},\mathbf{y})\in\mathbb{F}_2^{n+k}} (-1)^{h(\mathbf{x},\mathbf{y})\oplus(\mathbf{x},\mathbf{y})\cdot(\mathbf{u},\mathbf{v})} \rho^{\mathrm{wt}(\mathbf{x},\mathbf{y})}\\
&= \sum_{(\mathbf{x},\mathbf{y})\in\mathbb{F}_2^{n+k}} (-1)^{f(\mathbf{x})g(\mathbf{y})\oplus\mathbf{x}\cdot\mathbf{u}\oplus\mathbf{y}\cdot\mathbf{v}}\, \rho^{\mathrm{wt}(\mathbf{x})+\mathrm{wt}(\mathbf{y})}\\
&= \sum_{\substack{\mathbf{y}\in\mathbb{F}_2^k\\ g(\mathbf{y})=1}} (-1)^{\mathbf{y}\cdot\mathbf{v}}\, \rho^{\mathrm{wt}(\mathbf{y})} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x})\oplus\mathbf{x}\cdot\mathbf{u}}\, \rho^{\mathrm{wt}(\mathbf{x})}\\
&\qquad + \sum_{\substack{\mathbf{y}\in\mathbb{F}_2^k\\ g(\mathbf{y})=0}} (-1)^{\mathbf{y}\cdot\mathbf{v}}\, \rho^{\mathrm{wt}(\mathbf{y})} \sum_{\mathbf{x}} (-1)^{\mathbf{x}\cdot\mathbf{u}}\, \rho^{\mathrm{wt}(\mathbf{x})}\\
&= W_f^{(p)}(\mathbf{u}) \sum_{\substack{\mathbf{y}\in\mathbb{F}_2^k\\ g(\mathbf{y})=1}} (-1)^{\mathbf{y}\cdot\mathbf{v}}\, \rho^{\mathrm{wt}(\mathbf{y})}\\
&\qquad + \frac{(1-2p)^{\mathrm{wt}(\mathbf{u})}}{(1-p)^n} \sum_{\substack{\mathbf{y}\in\mathbb{F}_2^k\\ g(\mathbf{y})=0}} (-1)^{\mathbf{y}\cdot\mathbf{v}}\, \rho^{\mathrm{wt}(\mathbf{y})},
\end{aligned}$$

from which we obtain the first identity (the second is obtained by switching the roles of f and g). Moreover, if $k=1$, and $g(y)=y$, then $S_{g0}(v)=1, S_{g1}(v)=(-1)^v\,\rho$, and if $g(y)=y\oplus 1$, then $A_{g1}(v)=1, A_{g0}(v)=(-1)^v\,\rho$, and so

$$\begin{aligned}
W_{yf(\mathbf{x})}^{(p)}(\mathbf{u},v) &= (-1)^v\,\rho\, W_f^{(p)}(\mathbf{u}) + \frac{(1-2p)^{\mathrm{wt}(\mathbf{u})}}{(1-p)^n}\\
W_{(y\oplus 1)f(\mathbf{x})}^{(p)}(\mathbf{u},v) &= W_f^{(p)}(\mathbf{u}) + (-1)^v\,\rho\frac{(1-2p)^{\mathrm{wt}(\mathbf{u})}}{(1-p)^n}.
\end{aligned}$$

We now show (vii). If $h(\mathbf{x})=f(\mathbf{x}A\oplus\mathbf{a})$, then

$$W_h^{(p)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{h(\mathbf{x})\oplus\mathbf{x}\cdot\mathbf{u}} \rho^{\mathrm{wt}(\mathbf{x})} = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x}A\oplus\mathbf{a})\oplus\mathbf{x}\cdot\mathbf{u}} \rho^{\mathrm{wt}(\mathbf{x})}.$$

When $\mathbf{x}$ runs over $\mathbb{F}_2^n$, so does $\mathbf{z}=\mathbf{x}A\oplus\mathbf{a}$ (since A is invertible). Further, $\mathbf{z}A^{-1}=\mathbf{x}AA^{-1}\oplus\mathbf{a}A^{-1}$, so $\mathbf{z}A^{-1}\oplus\mathbf{a}A^{-1}=\mathbf{x}$. Moreover, when A is orthogonal, that is, $A^TA = I_n$ (A^T is the transpose of A), then

$$\begin{aligned}
\mathrm{wt}(\mathbf{z}A^{-1} \oplus \mathbf{a}A^{-1}) &= (\mathbf{z}A^T \oplus \mathbf{a}A^T) \cdot (\mathbf{z}A^T \oplus \mathbf{a}A^T)^T \\
&= (\mathbf{z}A^T \oplus \mathbf{a}A^T) \cdot (A\mathbf{z}^T \oplus A\mathbf{a}^T) \\
&= (\mathbf{z} \oplus \mathbf{a})A^TA(\mathbf{z}^T \oplus \mathbf{a}^T) \\
&= (\mathbf{z} \oplus \mathbf{a})(\mathbf{z} \oplus \mathbf{a})^T \\
&= \mathrm{wt}(\mathbf{z} \oplus \mathbf{a}).
\end{aligned}$$

Further,

$$\begin{aligned}
W_h^{(p)}(\mathbf{u}) &= \sum_{\mathbf{z}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{z})\oplus\mathbf{u}\cdot(\mathbf{z}A^{-1}\oplus\mathbf{a}A^{-1})} \rho^{\mathrm{wt}(\mathbf{z}A^{-1}\oplus\mathbf{a}A^{-1})} \\
&= \sum_{\mathbf{z}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{z})\oplus\mathbf{u}\cdot(\mathbf{z}A^{-1})\oplus\mathbf{u}\cdot(\mathbf{a}A^{-1})} \rho^{\mathrm{wt}(\mathbf{z}\oplus\mathbf{a})} \\
&= (-1)^{\mathbf{u}\cdot(\mathbf{a}A^{-1})} \sum_{\mathbf{z}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{z})\oplus\mathbf{z}\cdot\mathbf{u}A^{-1}} \rho^{\mathrm{wt}(\mathbf{z}\oplus\mathbf{a})},
\end{aligned}$$

where we used the fact that $\mathbf{u} \cdot (\mathbf{z}A^{-1}) = \mathbf{z} \cdot (\mathbf{u}A^{-1})$. If $\mathbf{a} = \mathbf{0}$, then

$$W_h^{(p)}(\mathbf{u}) = (-1)^{\mathbf{u}\cdot(\mathbf{a}A^{-1})}\, W_f^{(p)}(\mathbf{u}A^{-1}).$$

□

Remark 6. *If we substitute $p = \frac{1}{2}$, that is $\rho = 1$, the identity* (13) *reduces to the Parseval identity*

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n} \left(W_f^{(1/2)}(\mathbf{u})\right)^2 = 2^{2n}. \tag{14}$$

5 μ_p-nonlinearity and μ_p-bent Boolean functions

In this section we introduce a notion of nonlinearity of μ_p-Boolean functions where $p \in \mathbb{C}$ and refer to it by μ_p-nonlinearity. We show that μ_p-nonlinearity is essentially the same as the (classical) nonlinearity when p is real. From (5) we have

$$d_p(f, \ell_{\mathbf{u},b}) = 2^{n-1}\left(1 - (-1)^b(1-p)^n W_f^{(p)}(\mathbf{u})\right).$$

The square of the absolute value

$$\begin{aligned}\frac{|d_p(f,\ell_{\mathbf{u},b})|^2}{2^{2(n-1)}} &= \left(1-(-1)^b(1-p)^nW_f^{(p)}(\mathbf{u})\right)\overline{\left(1-(-1)^b(1-p)^nW_f^{(p)}(\mathbf{u})\right)}\\ &= \left(1-(-1)^b(1-p)^nW_f^{(p)}(\mathbf{u})\right)\left(1-(-1)^b\overline{(1-p)^nW_f^{(p)}(\mathbf{u})}\right)\\ &= 1-2(-1)^b\Re((1-p)^nW_f^{(p)}(\mathbf{u}))+|(1-p)^nW_f^{(p)}(\mathbf{u})|^2.\end{aligned}$$

We define the p-distance between f and $\ell_{\mathbf{u},b}$ by

$$dist_p(f,\ell_{\mathbf{u},b}) = 2^{n-1}\sqrt{1-2(-1)^b\Re((1-p)^nW_f^{(p)}(\mathbf{u}))+|(1-p)^nW_f^{(p)}(\mathbf{u})|^2}.$$

From the above computation, we see that if $p\in\mathbb{R}$, then $d_p(f,\ell_{\mathbf{u},b}) = dist_p(f,\ell_{\mathbf{u},b})$. If $1\neq p\in\mathbb{C}$, in general $d_p(f,\ell_{\mathbf{u},b})$ may not be a real number but $dist_p(f,\ell_{\mathbf{u},b})$ is always a real number and therefore a meaningful measure of distance from affine functions. Further, we define the μ_p-nonlinearity as follows.

Definition 7. *Suppose $f\in\mathfrak{B}_n(p)$ where $1\neq p\in\mathbb{C}$. Then the μ_p-nonlinearity of f is defined as*

$$nl_p(f) = 2^{n-1}\min_{\mathbf{u}\in\mathbb{F}_2^n}\sqrt{1-2|\Re((1-p)^nW_f^{(p)}(\mathbf{u}))|+|(1-p)^nW_f^{(p)}(\mathbf{u})|^2}.$$

We define μ_p-bent functions as follows, deriving its motivation from the Plancherel identity (13).

Definition 8. *Suppose $f\in\mathfrak{B}_n(p)$ where $1\neq p\in\mathbb{C}$. Then f is said to be μ_p-bent if*

$$|W_f^{(p)}(\mathbf{u})|^2 = (|\rho|^2+1)^n,\ \textit{for all } \mathbf{u}\in\mathbb{F}_2^n.$$

It is known that μ_p-bent functions with exist for $p=\frac{1}{2}$ (thus, $\rho=1$) and $p=\frac{1+\imath}{2}$ (thus, $\rho=\imath$) and are called *bent*, respectively, *negabent* Boolean functions. Whether such functions exist for other values of p is a question whose answer is contained in our next result. Since ρ is complex, then we write $\rho=a\zeta$, where $|\rho|=a$ and ζ is on the unit circle, that is, $\zeta=e^{\imath\theta}$, for some $0\le\theta<2\pi$.

Theorem 9. *Suppose $n\in\mathbb{Z}$, $p\in\mathbb{C}-\{1\}$ such that $\rho=\frac{p}{1-p}=\imath\, a$, where $a\in\mathbb{R}$. Then $\ell_{\mathbf{v},b}$ is μ_p-bent for all $\mathbf{v}\in\mathbb{F}_2^n$ and $b\in\mathbb{F}_2$.*

Proof. The μ_p-Walsh–Hadamard transform of $\ell_{\mathbf{v},b}$ at $\mathbf{u} \in \mathbb{F}_2^n$ is

$$\begin{aligned} W_{\ell_{\mathbf{v},b}}^{(p)}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{(\mathbf{v}\oplus\mathbf{u})\cdot\mathbf{x}\oplus b} \rho^{\mathrm{wt}(\mathbf{x})} \\ &= (-1)^b \prod_{i=1}^{n} \left(1+\rho(-1)^{u_i\oplus v_i}\right) \\ &= (-1)^b \prod_{i=1}^{n} \left(1+\imath a(-1)^{u_i\oplus v_i}\right) \\ &= (-1)^b (1+a^2)^{\frac{n}{2}} \prod_{i=1}^{n} \frac{\left(1+\imath a(-1)^{u_i\oplus v_i}\right)}{\sqrt{1+a^2}}. \end{aligned} \tag{15}$$

Therefore, $\left|W_{\ell_{\mathbf{v},b}}^{(p)}(\mathbf{u})\right| = (1+a^2)^{\frac{n}{2}}$, for all $\mathbf{u} \in \mathbb{F}_2^n$. This proves that $\ell_{\mathbf{v},b}$ is μ_p-bent for all $\mathbf{v} \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2$. □

Challenge. *We therefore challenge the research community to construct other classes of μ_p-bent functions, or other cryptographically significant functions or show that under certain conditions on ρ they do not exist.*

Acknowledgment: The authors thank Dr. Aalok Misra of the Department of Physics, Indian Institute of Technology Roorkee for extremely helpful discussions on quantum mechanics.

References

[1] T. W. Cusick and P. Stănică, Cryptographic Boolean functions and applications, Elsevier–Academic Press, 2009.

[2] P. Erdős and A. Rényi, *On the evolution of random graphs*, Publ. Math. Inst. Hungar. Acad. Sci. 5 (1960), 17–61.

[3] E. Friedgut and Gil Kalai, *Every monotone graph property has a sharp threshold*, Proc. AMS 124(10) (1996), 2293–3002.

[4] N. Keller, E. Mossel and T. Schlank, *A note on the entropy/influence conjecture*, Discrete Math. 312(22) (2012), 3364–3372.

[5] Y. Lu and Y. Desmedt, *Bias analysis of a certain problem with applications to E0 and Shannon ciper*, ICISC 2010, LNCS 6829, 2011, pp. 16–28.

[6] A. Montanaro and T. J. Osborne, *Quantum Boolean functions*, Chicago J. Theor. Comput. Sci. Article 1, pages 1–45, (2010). http://cjtcs.cs.uchicago.edu/, http://arxiv.org/abs/0810.2435v5.

[7] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[8] R. O'Donnell, Analysis of Boolean functions, Cambridge University Press, 2014.

[9] R. O'Donnell and L-Y. Tan, *A composition theorem for the Fourier entropy-influence conjecture*, ICALP (1) 2013, 780–791. (Available at: arXiv:1304.1347v1 [cs.CC] 4 Apr 2013).

[10] M. G. Parker, *Generalised S-box nonlinearity*, NESSIE Public Document, 11.02.03: NES/DOC/UIB/WP5/020/A.

[11] M. G. Parker, A. Pott, *On Boolean functions which are bent and negabent*, in Proc. Int. Conf. Sequences, Subsequences, Consequences, 2007, LNCS 4893, pp. 9–23.

[12] C. Riera, Spectral Properties of Boolean functions, Graphs and Graph States, Ph. D. thesis, University of Bergen, 2005.

[13] C. Riera, M. G. Parker, *Generalized bent criteria for Boolean functions*, IEEE Trans. Inf. Theory 52:9 (2006), 4142–4159.

[14] O. S. Rothaus, *On bent functions*, J. Combin. Theory, Ser. A 20 (1976), 300–305.

[15] K. U. Schmidt, M. G. Parker, A. Pott, *Negabent functions in the Maiorana–McFarland class*, In: S.W. Golomb, M.G. Parker, A. Pott, A. Winterhof (eds.), SETA 2008, LNCS 5203 (2008), Springer, Heidelberg, 390–402.

[16] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay, S. Maitra, *Investigations on bent and negabent functions via the nega–Hadamard transform*, IEEE Trans. Inf. Theory 58:6 (2012), 4064–4072.