Quantum Algorithms Related to *HN*-Transforms of Boolean Functions

Sugata Gangopadhyay[1(✉)], Subhamoy Maitra[2], Nishant Sinha[1], and Pantelimon Stănică[3]

[1] Department of Computer Science and Engineering, Indian Institute of Technology Roorkee, Roorkee 247667, India
gsugata@gmail.com, nishantsinha.iitr@gmail.com
[2] Applied Statistics Unit, Indian Statistical Institute, 203, B.T. Road, Kolkata 700108, India
subho@isical.ac.in
[3] Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216, USA
pstanica@nps.edu

Abstract. *HN*-transforms, which have been proposed as generalizations of Hadamard transforms, are constructed by tensoring Hadamard and nega-Hadamard kernels in any order. We show that all the 2^n possible *HN*-spectra of a Boolean function in n variables, each containing 2^n elements (i.e., in total 2^{2n} values in transformed domain) can be computed in $O(2^{2n})$ time (more specific with little less than 2^{2n+1} arithmetic operations). We propose a generalization of Deutsch-Jozsa algorithm, by employing *HN*-transforms, which can be used to distinguish different classes of Boolean functions over and above what is possible by the traditional Deutsch-Jozsa algorithm.

Keywords: Boolean function · *HN*-transform , Deutsch-Jozsa algorithm

1 Introduction

Hadamard spectrum (or, Walsh-Hadamard spectrum) is possibly the most important tool in analyzing a Boolean function. This explains how a given Boolean function is correlated with each linear function and thus provides nonlinearity as a summary data. High nonlinearity is an important property for the Boolean functions used in cryptographic primitives for resisting linear cryptanalysis [14] as well as correlation and fast correlation attacks [15,22]. Consider Boolean functions on n-variables. For n even, the functions with provably maximum nonlinearity $2^{n-1}-2^{\frac{n}{2}-1}$ exist [6] and such functions are called bent, though

S. Maitra is supported by the project "Cryptography & Cryptanalysis: How far can we bridge the gap between Classical and Quantum Paradigm", awarded by the Scientific Research Council of the Department of Atomic Energy (DAE-SRC), the Board of Research in Nuclear Sciences (BRNS).

S. El Hajji et al. (Eds.): C2SI 2017, LNCS 10194, pp. 314–327, 2017.
DOI: 10.1007/978-3-319-55589-8_21

the complete characterization of such functions is not yet known for $n > 8$. For n odd, consider the truth table of an n-variable function f constructed by the concatenation of the truth tables of two $(n-1)$-variable bent functions g and h, i.e., $f(x_0, x_1, \ldots, x_{n-1}) = x_0 g(x_1, \ldots, x_{n-1}) \oplus (x_0 \oplus 1) h(x_1, \ldots, x_{n-1})$ for all $(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$. One can then easily check that the nonlinearity of f is $2^{n-1} - 2^{\frac{n-1}{2}}$. This is famously known as the bent concatenation bound, which had been conjectured [10] to be the maximum attainable nonlinearity until disproved [18] in 1983. The maximum nonlinearity problem is directly related to coding theory also, since it corresponds to the covering radius of the first order Reed-Muller codes of block length 2^n.

There are several efficient methods in constructing Boolean functions with reasonably good cryptographic properties. However, commercial symmetric (stream or block) ciphers generally do not exploit Boolean functions on large number of variables. Instead, the trend is to use Boolean functions or S-Boxes on small number of variables (say 4 to 8) and then to introduce several rounds to obtain high confusion and diffusion. One can certainly regard the complete algorithm as a Boolean function on the key and IV bits, however, since we generally use between 80 to 256-bit key or IV, these Boolean functions are in reality very complicated to analyze. It is generally impossible to write the complete Truth Table (TT) or Algebraic Normal Form (ANF) of such functions. At the same time, it is well known that for randomly chosen Boolean functions the Hadamard spectrum values are concentrated around a low value [12] (i.e., their nonlinearities are high). However, it is not only the properties of the Boolean function as a whole that need to be studied. One may consider some sub-functions of the said Boolean function or the coefficient of certain monomials that may provide substantially high values of the Hadamard spectrum (i.e., low values of nonlinearity). Such a situation is needed for differential [11] or cube attacks [1,7] on heuristically designed stream ciphers. Thus identifying such high Hadamard spectrum values for a Boolean function (or its sub-functions) on large number of variables is an important question from cryptanalytic perspective. Apart from classical algorithms, quantum algorithms are also considered for approximating large spectrum values (and their positions). It has been observed [13] that in the quantum domain Deutsch-Josza algorithm [5] can create a superposition of states whose amplitudes are precisely the corresponding spectrum values.

The theory of linear approximations, which is based on Hadamard transform of the functions, has been generalized by Danielsen and Parker [3,4] as well as Riera and Parker [19,20], by introducing nega-Hadamard transforms leading to a class of generalized transforms, referred to as *HN*-transforms, combining Hadamard and nega-Hadamard kernels. It has been observed [19,20] that the quantum error correcting codes with optimal distance appear to have most flat spectra with respect to such transforms. In the context of *HN*-spectra, several results and constructions of Boolean functions and cryptographically strong S-Boxes had been studied in [4,8,16,17,19,21,24]. Surprisingly, while the *HN*-transform has been used for several purposes, its algorithmic issues have never been studied in detail. While it is natural that similar kind of ideas as for the

traditional Hadamard transform might be applicable, there are specific details that need to be worked out. The algorithmic issues also provide several generalized techniques and characterizations related to Boolean functions.

In Sect. 3, we show that all the *HN*-spectra of an n-variable function can be simultaneously computed in time $O(2^{2n})$ as opposed to the naive estimate $O(n2^{2n})$ and we therefore design the corresponding algorithm. Note that the computation of the Hadamard (or Walsh-Hadamard transform) of a Boolean function on n-variables require $O(n2^n)$ time, by using the Fast Discrete Fourier Transform algorithm. As we will explain later, there are 2^n different *HN*-spectra, each containing 2^n elements. One of them is the well known Walsh spectrum. Similar to the algorithm of Hadamard spectrum, we may re-use the algorithm for each of the *HN* spectrum and that would require $O(2^n \cdot n2^n)$ time. However, while analyzing the algorithm for obtaining all the 2^n spectra, we note that the structure of the transforms are of such a nice pattern that this can be executed in $O(2^{2n})$ time, to be more specific, in exactly $2^{2n+1} - 2^{n+1}$ addition or subtraction operations. This is indeed a tight bound as 2^{2n} transformed values can be computed using $2^{2n+1} - 2^{n+1}$ arithmetic operations. Note that each transformed value, which depends on all the 2^n values of the Boolean function, can be obtained at an average cost of only 2 operations.

Next we consider quantum algorithms with respect to the *HN*-spectra. Suppose that we have an oracle access to a Boolean function f in n variables which is either constant or balanced. A classical algorithm will require $2^{n-1}+1$ queries to determine whether f is constant or balanced. It is well known that Deutsch-Jozsa algorithm [5] solves this problem in a single query. In Sect. 4, we generalize the Deutsch-Jozsa algorithm by using *HN*-transforms and characterize larger classes of Boolean functions that can be distinguished by exploiting these transforms. We identify certain classes of quadratic symmetric functions that are related to these separations.

2 Preliminaries

Let $\mathbb{F}_2$ be the finite field with two elements and $\mathbb{Z}$ be the ring of integers. For any $n \in \mathbb{Z}^+$ (the set of positive integers), let $[n] = \{1, \ldots, n\}$. The Cartesian product of n copies of $\mathbb{F}_2$ is $\mathbb{F}_2^n = \{\mathbf{x} = (x_n, \ldots, x_1) : x_i \in \mathbb{F}_2, i \in [n]\}$ which is an n-dimensional vector space over $\mathbb{F}_2$ with respect to element-wise addition denoted by $\oplus$, scalar multiplication defined by $a\mathbf{x} = (ax_n, \ldots, ax_1)$, for all $a \in \mathbb{F}_2$ and $\mathbf{x} \in \mathbb{F}_2^n$. We define the inner product by $\mathbf{u} \cdot \mathbf{x} = \bigoplus_{i\in[n]} u_i x_i$ and intersection by $\mathbf{u} * \mathbf{x} = (u_n x_n, \ldots, u_1 x_1)$, for all $\mathbf{u} = (u_n, \ldots, u_1), \mathbf{x} = (x_n, \ldots, x_1) \in \mathbb{F}_2^n$. For any $\mathbf{v} = (v_n, \ldots, v_1) \in \mathbb{F}_2^n$, we can associate a unique integer $j = \sum_{i\in[n]} v_i 2^{i-1}$. When order is needed, we shall write $\mathbf{v} = \mathbf{u}_j$. The (Hamming) weight of a vector $\mathbf{v} \in \mathbb{F}_2^n$ is the integer sum $wt(\mathbf{v}) = \sum_{i\in[n]} v_i$. The (Hamming) distance between two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^n$ is $d(\mathbf{u}, \mathbf{v}) = wt(\mathbf{u} \oplus \mathbf{v})$.

Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a Boolean function in n variables, whose set will be denoted by $\mathcal{B}_n$. The character form of $f \in \mathcal{B}_n$, $\chi_f(\mathbf{x}) =$

$(-1)^{f(\mathbf{x})}$, for all $\mathbf{x} \in \mathbb{F}_2^n$. Let M^T denote the transpose of a matrix M. We associate the column vectors (i.e., $2^n \times 1$ matrices) $\mathbf{f} = (f(\mathbf{u}_0), \ldots, f(\mathbf{u}_{2^n-1}))^T$ and $\chi_{\mathbf{f}} = (\chi_f(\mathbf{u}_0), \ldots, \chi_f(\mathbf{u}_{2^n-1}))^T$ to $f \in \mathcal{B}_n$. The vector $\mathbf{f}^T \in \mathbb{F}_2^{2^n}$ is said to be the truth table of f. The weight of a Boolean function f is $wt(f) = wt(\mathbf{f}^T)$. The Hamming distance between two Boolean functions $f, g \in \mathcal{B}_n$ is $d(f,g) = wt(\mathbf{f}^T \oplus \mathbf{g}^T)$. The algebraic normal form of $f \in \mathcal{B}_n$ is $f(\mathbf{x}) = \bigoplus_{\mathbf{a} \in \mathbb{F}_2^n} \mu_{\mathbf{a}} \prod_{i \in [n]} x_i^{a_i}$, where $\mu_{\mathbf{a}} \in \mathbb{F}_2$, for all $\mathbf{a} = (a_n, \ldots, a_1) \in \mathbb{F}_2^n$. The algebraic degree of f, $\deg(f) = \max_{\mathbf{a} \in \mathbb{F}_2^n} \{wt(\mathbf{a}) : \mu_{\mathbf{a}} \neq 0\}$. The Boolean functions of the form $f(\mathbf{x}) = \bigoplus_{i \in [n]} a_i x_i \oplus a_0 = \mathbf{a} \cdot \mathbf{x} \oplus a_0$, where $a_i \in \mathbb{F}_2$ for all $i \in [n] \cup \{0\}$, are said to be affine functions. Affine functions are said to be linear if $\mu_0 = 0$. The set of affine functions and linear functions are denoted by $\mathcal{A}_n$ and $\mathcal{L}_n$, respectively.

2.1 *HN*-Transforms as a Generalization of Hadamard Transform

Recall that the tensor (sometimes, called Kronecker) product $A \otimes B$, where $A = (a_{ij})_{ij}, B = (b_{k\ell})_{k\ell}$ are $m \times n$, respectively, $p \times q$ matrices, is defined by

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

The Hadamard and nega-Hadamard kernels $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $N = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & \imath \\ 1 & -\imath \end{bmatrix}$, respectively, are unitary transformations over $\mathbb{C}^{\otimes 2} = \mathbb{C} \otimes \mathbb{C}$, where $\mathbb{C}$ is the field of complex numbers. The set of all tensor products

$$\{H, N\}^n = \left\{ \bigotimes_{i=n}^{1} K_i = K_n \otimes \cdots \otimes K_1 : K_i \in \{H, N\}, i \in [n] \right\}$$

is a subset (its cardinality is 2^n) of the set of all unitary transformations overs $(\mathbb{C}^2)^{\otimes n}$.

Definition 1. *Let $f \in \mathcal{B}_n$. Suppose $\mathbf{c} = (c_n, \ldots, c_1) \in \mathbb{F}_2^n$ and $\mathcal{K}^{\mathbf{c}} \in \{H, N\}^n$ is such that $\mathcal{K}^{\mathbf{c}} = K_n \otimes \cdots \otimes K_1 = \bigotimes_{i=n}^{1} K_i$ where $K_i = \begin{cases} H \text{ if } c_i = 0, \\ N \text{ if } c_i = 1 \end{cases}$. For $0 \leq j \leq 2^n - 1$, we define,*

$$\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}_j) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u}_j \cdot \mathbf{x}} \imath^{wt(\mathbf{c} * \mathbf{x})}, \tag{1}$$

which is referred to as the HN-transform of f at $\mathbf{u}_j$ with respect to $\mathcal{K}^{\mathbf{c}}$ (cf. [8]). *The whole spectrum is denoted by $\mathcal{K}^{\mathbf{c}}\chi_{\mathbf{f}}$ and is referred as the HN-spectrum of f with respect to $\mathcal{K}^{\mathbf{c}}$.*

For easy writing, let us denote $\mathbf{u}_0$ by $\mathbf{0}$ and $\mathbf{u}_{2^n-1}$ by $\mathbf{1}$. Then, $\mathcal{K}_f^{\mathbf{0}}(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}}$ and $\mathcal{K}_f^{\mathbf{1}}(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} \imath^{wt(\mathbf{x})}$ are said to be the Hadamard and nega-Hadamard transforms of f at $\mathbf{u}$ and denoted by $\mathcal{H}_f(\mathbf{u})$ and $\mathcal{N}_f(\mathbf{u})$, respectively. For a detailed theory of Hadamard transform in the context of cryptographic Boolean functions we refer to [2,9,19,20,24].

3 The Complexity of Computing *HN*-Spectra

Given any function $f \in \mathcal{B}_n$ we can apply transformations from $\{H, N\}^n$ to obtain 2^n *HN*-spectra. Time complexity of computing each *HN*-spectrum is the same as the time complexity of computing the Hadamard spectrum of f, which is $O(n2^n)$, using the fast Hadamard transform algorithm. Thus, naively computing all *HN*-spectra will require $O(n2^{2n})$ time if we calculate each of them separately. In the following theorem we prove that this complexity can be improved.

Theorem 1. *The time complexity of computing HN-spectra of $f \in \mathcal{B}_n$ is $O(2^{2n})$.*

Proof. For $f \in \mathcal{B}_n$ there exist two functions $f_1, f_2 \in \mathcal{B}_{n-1}$ such that $f(\mathbf{x}, y) = (y \oplus 1)f_1(\mathbf{x}) \oplus yf_2(\mathbf{x})$, for all $\mathbf{x} \in \mathbb{F}_2^{n-1}$ and $y \in \mathbb{F}_2$. Then $2^{-\frac{n}{2}}\mathcal{K}_f^{(c_n,\mathbf{c})}(v, \mathbf{u}) =$

$$\sum_{\mathbf{x}\in\mathbb{F}_2^{n-1}} (-1)^{\mathbf{u}\cdot\mathbf{x}\oplus f_1(\mathbf{x})} i^{wt(\mathbf{c}*\mathbf{x})} + (-1)^v i^{wt(c_n)} \sum_{\mathbf{x}\in\mathbb{F}_2^{n-1}} (-1)^{\mathbf{u}\cdot\mathbf{x}\oplus f_2(\mathbf{x})} i^{wt(\mathbf{c}*\mathbf{x})}, \tag{2}$$

for all $(v, \mathbf{u}), (c_n, \mathbf{c}) \in \mathbb{F}_2 \times \mathbb{F}_2^{n-1}$. We denote by $T(n)$ the time complexity to compute all *HN*-spectra of any Boolean function in n variables. We show our result by finding a recurrence satisfied by $T(n)$. The computation of $2^{-\frac{n}{2}}\mathcal{K}_{f_1}^{\mathbf{c}}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^{n-1}}(-1)^{\mathbf{u}\cdot\mathbf{x}\oplus f_1(\mathbf{x})} i^{wt(\mathbf{c}*\mathbf{x})}$, $2^{-\frac{n}{2}}\mathcal{K}_{f_2}^{\mathbf{c}}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^{n-1}}(-1)^{\mathbf{u}\cdot\mathbf{x}\oplus f_2(\mathbf{x})} i^{wt(\mathbf{c}*\mathbf{x})}$, for all $\mathbf{u}, \mathbf{c} \in \mathbb{F}_2^{n-1}$, will therefore take $2T(n-1)$ time. For each $\mathbf{c} \in \mathbb{F}_2^{n-1}$, the computation of $2^{-\frac{n}{2}}\mathcal{K}_f^{(c_n,\mathbf{c})}(v, \mathbf{u})$ where $c_n \in \mathbb{F}_2$ and $(v, \mathbf{u}) \in \mathbb{F}_2 \times \mathbb{F}_2^{n-1}$ requires $4 \cdot 2^{n-1} = 2^{n+1}$ additions. If we vary $\mathbf{c}$ over $\mathbb{F}_2^{n-1}$ the total number of additions to compute all *HN*-spectra is $2^{n-1} \cdot 2^{n+1} = 2^{2n}$. Thus, we have the following first order recurrence relation:

$$T(n) = 2T(n-1) + 2^{2n},$$

which by iteration renders

$$T(n) = 2^{n-1}T(1) + 2^{2n}\sum_{i=0}^{n-2}\frac{1}{2^i} = 2^{n-1}T(1) + 2^{2n+1} - 2^{n+2} = O(2^{2n}),$$

and the theorem is shown. □

3.1 Fast *HN*-Transform Algorithm

Based on the above observations we design Algorithm 1 to efficiently compute *HN*-spectra of a Boolean function $f \in \mathcal{B}_n$. In Fig. 1 we demonstrate the steps of Algorithm 1 when $f \in \mathcal{B}_3$. It is clear from Fig. 1 that the total number of additions and subtractions required is $T(3) = 8 \times 2 + 8 \times 4 + 8 \times 8 = 2^3(2 + 2^2 + 2^3) = 2^4(2^3 - 1) = 2^{2(3)+1} - 2^{3+1} = 112$. In general $T(n) = 2^n(2 + 2^2 + \cdots + 2^{n-1} + 2^n) = 2^{2n+1} - 2^{n+1} = O(2^{2n})$, as discussed before.

Input: A Boolean function $f \in \mathcal{B}_n$, available in the form of the 2^n length array $\chi_{\mathbf{f}} = (\chi_f(\mathbf{u_0}), \ldots, \chi_f(\mathbf{u}_{2^n-1}))$
Output: All 2^n *HN*-spectra of f, each containing 2^n elements

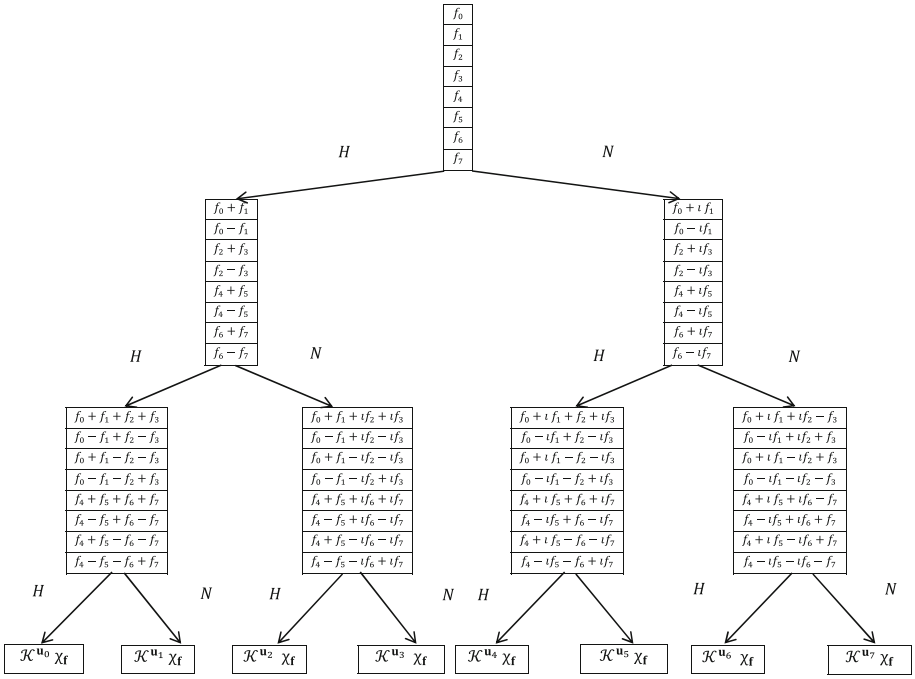
Initialize a $2^n \times 2^n$ matrix h whose columns and rows are numbered from 0 to $2^n - 1$. The entry in the ith column and jth row is denoted by $h_{i,j}$.
$(h_{0,0}, h_{0,1}, \ldots, h_{0,2^n-1}) \leftarrow (\chi_f(\mathbf{u}_0), \chi_f(\mathbf{u}_1), \ldots, \chi_f(\mathbf{u}_{2^n-1}))$
for $j = 0$ **to** $n - 1$ **do**
  for $\ell = 2^{j+1} - 1$ **downto** 0 **do**
    if $\ell \equiv 0 \pmod 2$ **then**
      $k = 0$
      while $k < 2^n$ **do**
        for $i = k$ **to** $k + 2^j - 1$ **do**
          $tmp \leftarrow f_{\lfloor \frac{\ell}{2} \rfloor, i}$
          $f_{\ell,i} \leftarrow tmp + f_{\lfloor \frac{\ell}{2} \rfloor, i+2^j}$
          $f_{\ell,i+2^j} \leftarrow tmp - f_{\lfloor \frac{\ell}{2} \rfloor, i+2^j}$
        od
        $k \leftarrow k + 2^{j+1}$
      od
    fi
    if $\ell \equiv 1 \pmod 2$ **then**
      $k = 0$
      while $k < 2^n$ **do**
        for $i = k$ **to** $k + 2^j - 1$ **do**
          $tmp \leftarrow f_{\lfloor \frac{\ell}{2} \rfloor, i}$
          $f_{\ell,i} \leftarrow tmp + \imath f_{\lfloor \frac{\ell}{2} \rfloor, i+2^j}$
          $f_{\ell,i+2^j} \leftarrow tmp - \imath f_{\lfloor \frac{\ell}{2} \rfloor, i+2^j}$
        od
        $k \leftarrow k + 2^{j+1}$
      od
    fi
  od
od

Algorithm 1. Fast *HN*-transform algorithm.

3.2 *HN*-Transform and Quadratic Symmetric Functions on a Subspace Depending on c

In this section we describe the connection between *HN*-spectra and quadratic approximations of a Boolean function as discussed in Gangopadhyay, Pasalic and Stănică [8].

Consider any vector $\mathbf{c} \in \mathbb{F}_2^n$. The $(n-1)$-dimensional subspace orthogonal to $\mathbf{c}$ is $\mathbf{c}^\perp = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{c} \cdot \mathbf{x} = 0\}$. Let $\ell_\mathbf{c} \in \mathcal{L}_n$ be defined by $\ell_\mathbf{c}(\mathbf{x}) = \mathbf{c} \cdot \mathbf{x}$, for all $\mathbf{x} \in \mathbb{F}_2^n$. Let $s \in \mathcal{B}_n$ be the symmetric quadratic bent function defined by



$\chi_{\mathbf{f}} = (f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7)^T$. The vector $\mathbf{u}_j = (u_{j2}, u_{j1}, u_{j0})$ corresponds to the binary representation of $0 \le j \le 7$.
$\mathcal{K}^{\mathbf{u}_j}\chi_{\mathbf{f}} = K_2 \otimes K_1 \otimes K_0\, \chi_{\mathbf{f}}$ where $K_i = H$, if $u_{ji} = 0$ and $K_i = N$, if $u_{ji} = 1$, for all $0 \le i \le 2$. The normalizing factors of $\frac{1}{\sqrt{2}}$ and $\frac{1}{2}$ for the first and second levels, respectively, are not shown.

Fig. 1. Fast *HN*-transform algorithm for a function in $\mathcal{B}_n$.

$s(\mathbf{x}) = \bigoplus_{i<j} x_i x_j$, for all $\mathbf{x} \in \mathbb{F}_2^n$. For each $\mathbf{c} \in \mathbb{F}_2^n$ we define $s_{\mathbf{c}} \in \mathcal{B}_n$ by $s_{\mathbf{c}}(\mathbf{x}) = s(\mathbf{c} * \mathbf{x})$, for all $\mathbf{x}, \mathbf{c} \in \mathbb{F}_2^n$. We can think of $s_{\mathbf{c}}$'s as quadratic symmetric functions on the variables x_i's for which $c_i = 1$. Since (*cf.* [20,24]) $wt(\mathbf{c}*\mathbf{x}) \equiv 2s_{\mathbf{c}}(\mathbf{x}) + \mathbf{c}\cdot\mathbf{x} \pmod 4$, we obtain from (1)

$$2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbf{c}^{\perp}} (-1)^{f(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}} + \iota \sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^{\perp}} (-1)^{f(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}}. \tag{3}$$

Suppose that $f \in \mathcal{B}_n$ such that

$$\left|\sum_{\mathbf{x}\in\mathbf{c}^{\perp}} (-1)^{f(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}}\right| = (-1)^{\epsilon_1(\mathbf{u},\mathbf{c})} \sum_{\mathbf{x}\in\mathbf{c}^{\perp}} (-1)^{f(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}} \text{ and}$$

$$\left|\sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^{\perp}} (-1)^{f(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}}\right| = (-1)^{\epsilon_2(\mathbf{u},\mathbf{c})} \sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^{\perp}} (-1)^{f(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}},$$

where $\epsilon_1(\mathbf{u},\mathbf{c}), \epsilon_2(\mathbf{u},\mathbf{c}) \in \mathbb{F}_2$ and $\mathbf{c},\mathbf{u} \in \mathbb{F}_2^n$. Then

$$\begin{aligned}
&\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})\oplus\epsilon_1(\mathbf{u},\mathbf{c})\oplus(\epsilon_1(\mathbf{u},\mathbf{c})\oplus\epsilon_2(\mathbf{u},\mathbf{c}))\mathbf{c}\cdot\mathbf{x}\oplus\mathbf{u}\cdot\mathbf{x}} \\
&= \left|\sum_{\mathbf{x}\in\mathbf{c}^\perp} (-1)^{f(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\right| + \left|\sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^\perp} (-1)^{f(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\right| \qquad (4) \\
&= |\Re(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))| + |\Im(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))|.
\end{aligned}$$

The Hamming distance between f and $s_{\mathbf{c}} \oplus \epsilon_1(\mathbf{u},\mathbf{c}) \oplus (\epsilon_1(\mathbf{u},\mathbf{c}) \oplus \epsilon_2(\mathbf{u},\mathbf{c}))\ell_{\mathbf{c}} \oplus \ell_{\mathbf{u}}$ is

$$2^{n-1} - \frac{1}{2}\left(|\Re(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))| + |\Im(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))|\right).$$

Given any Boolean function $f \in \mathcal{B}_n$, for all $\mathbf{c} \in \mathbb{F}_2^n$ we can obtain the spectra

$$\left[|\Re(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))| + |\Im(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))| : \mathbf{u} \in \mathbb{F}_2^n\right]. \qquad (5)$$

by computing the *HN*-spectra. We then find

$$\max_{\mathbf{c}\in\mathbb{F}_2^n}\max_{\mathbf{u}\in\mathbb{F}_2^n}\left[|\Re(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))| + |\Im(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))| : \mathbf{u} \in \mathbb{F}_2^n\right]. \qquad (6)$$

Suppose that the maximum value (6) is attained at $\mathbf{u}', \mathbf{c}' \in \mathbb{F}_2^n$. Then by using the *HN*-spectra the best possible quadratic approximation of f that we obtain is $s_{\mathbf{c}'} \oplus \epsilon_1(\mathbf{u}',\mathbf{c}') \oplus (\epsilon_1(\mathbf{u}',\mathbf{c}') \oplus \epsilon_2(\mathbf{u}',\mathbf{c}'))\ell_{\mathbf{c}'} \oplus \ell_{\mathbf{u}'}$.

Example 1. The 7-variable, 2-resilient functions with nonlinearity 56 are considered to be cryptographically strong functions and in [23, Table 4], all such rotation symmetric functions are listed. We have computed the spectra defined in (5), namely, $\left[|\Re(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))| + |\Im(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))| : \mathbf{u} \in \mathbb{F}_2^n\right]$ for all $\mathbf{c} \in \mathbb{F}_2^n$. Since these functions have nonlinearity the $\max_{\mathbf{u}\in\mathbb{F}_2^n} |2^{\frac{n}{2}}\mathcal{H}_f(\mathbf{u})| = 16$ for each function f in the list. Considering the *HN*-spectra for these functions we observe that for the first 12 functions $\max_{\mathbf{c}\in\mathbb{F}_2^n}\max_{\mathbf{u}\in\mathbb{F}_2^n}\left(|\Re(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))| + |\Im(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))| : \mathbf{u} \in \mathbb{F}_2^n\right) = 72$, and for the remaining functions

$$\max_{\mathbf{c}\in\mathbb{F}_2^n}\max_{\mathbf{u}\in\mathbb{F}_2^n}\left(|\Re(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))| + |\Im(2^{\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{u}))| : \mathbf{u} \in \mathbb{F}_2^n\right) = 40.$$

This provides an example of how the *HN*-transforms enable us to obtain quadratic approximations efficiently and it is very clear that the second set of functions will have less correlation to the quadratic functions than the first ones.

Example 2. Parker [16] has computed the maximum of the square of the moduli of the 2^n times the *HN*-transformation values for several S-boxes including the AES S-box. This is related to peak-to-average ration (PAR) of the corresponding functions. In this example we consider the PRESENT S-box which is a permutation on $\mathbb{F}_2^4$. Let $\{f_i : i = 1,\ldots,15\}$ be its 15 non-zero component functions. For each $\mathbf{c} \in \mathbb{F}_2^4$ we compute

$$\max\{2^n|\mathcal{K}_f^{\mathbf{c}}(\mathbf{u})|^2 : \mathbf{u} \in \mathbb{F}_2^4\}.$$

Table 1. *HN*-spectra analysis of PRESENT S-box.

	$\mathbf{c}_0$	$\mathbf{c}_1$	$\mathbf{c}_2$	$\mathbf{c}_3$	$\mathbf{c}_4$	$\mathbf{c}_5$	$\mathbf{c}_6$	$\mathbf{c}_7$	$\mathbf{c}_8$	$\mathbf{c}_9$	$\mathbf{c}_{10}$	$\mathbf{c}_{11}$	$\mathbf{c}_{12}$	$\mathbf{c}_{13}$	$\mathbf{c}_{14}$	$\mathbf{c}_{15}$
f_1	64	32	64	32	64	32	128	64	32	16	32	16	32	16	64	32
f_2	64	32	40	40	40	40	32	32	40	40	32	32	32	32	40	40
f_3	64	32	40	40	40	40	32	32	32	64	40	72	40	72	32	64
f_4	64	32	40	40	40	40	32	32	40	40	32	32	32	32	40	40
f_5	64	64	40	72	40	72	32	64	40	72	32	64	32	64	40	72
f_6	64	32	40	40	40	40	32	32	32	32	40	40	40	40	32	32
f_7	64	64	40	72	40	72	32	64	40	72	32	64	32	64	40	72
f_8	64	32	32	32	32	64	32	32	40	40	40	40	40	72	40	40
f_9	64	32	32	16	32	16	64	32	32	16	64	32	64	32	128	64
f_{10}	64	32	32	64	32	32	32	32	40	40	40	72	40	40	40	40
f_{11}	64	32	32	32	32	64	32	32	40	40	40	40	40	72	40	40
f_{12}	64	32	32	16	32	16	64	32	64	32	32	16	32	16	32	16
f_{13}	64	32	32	64	32	32	32	32	40	40	40	72	40	40	40	40
f_{14}	64	32	40	40	40	40	32	32	32	32	40	40	40	40	32	32
f_{15}	64	32	40	40	40	40	32	32	32	64	40	72	40	72	32	64

Whether this provides us the best possible distribution of the *HN*-transformation values among all the permutations on $\mathbb{F}_2^4$ is an open question. In Table 1 we tabulate the values of $\max\{2^n|\mathcal{K}_f^{\mathbf{c}}(\mathbf{u})|^2 : \mathbf{u} \in \mathbb{F}_2^4\}$ for each $\mathbf{c} \in \mathbb{F}_2^4$. For convenience we write $\mathbf{c}_j = (c_3, c_2, c_1, c_0)$ whenever $j = 2^3c_3+2^2c_2+2c_1+1c_0$. If F is the vector Boolean function corresponding to the PRESENT S-box then define $f_i = \mathbf{c}_i \cdot F$ for all $i = 0, 1, \ldots, 15$.

4 Extended Deutsch-Jozsa Algorithm

The extended Deutsch-Jozsa algorithm is pictorially represented in Fig. 2 and described in Algorithm 2. If we consider the specific case $H^{\otimes n}$ in place of $\mathcal{K}^{\mathbf{c}}$, then we obtain the traditional Deutsch-Jozsa algorithm [5]. Given $f \in \mathcal{B}_n$ either constant or balanced, if the corresponding quantum bit oracle implementation $\mathcal{U}_f$ is available, Deutsch-Jozsa [5] provided a quantum algorithm that decides in a constant number of queries which one it is. One can simply describe Deutsch-Jozsa algorithm in terms of Hadamard spectrum values and it can be observed that

$$\sum_{\mathbf{z}\in\mathbb{F}_2^n}\sum_{\mathbf{x}\in\mathbb{F}_2^n}\frac{(-1)^{\mathbf{x}\cdot\mathbf{z}\oplus f(\mathbf{x})}}{2^n}|\mathbf{z}\rangle = \sum_{\mathbf{z}\in\mathbb{F}_2^n} 2^{-\frac{n}{2}}\mathcal{H}_f(\mathbf{z})|\mathbf{z}\rangle,$$

i.e., the associated probability for the state $|\mathbf{z}\rangle$ is $2^{-\frac{n}{2}}\mathcal{H}_f(\mathbf{z})$. In this regard, we have the following technical result (see [13] for details).

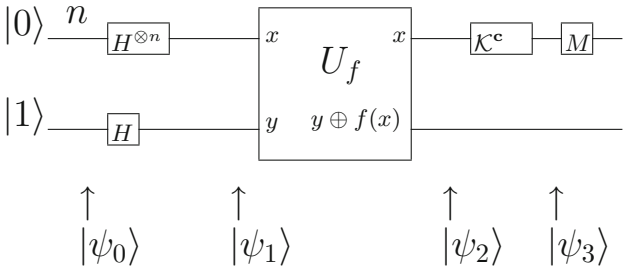


Fig. 2. Quantum circuit to implement extended Deutsch-Jozsa algorithm

Input: A Boolean function $f \in \mathcal{B}_n$, available in the form of the unitary transformation $\mathcal{U}_f$

Output: n-bit pattern

1 Take an $(n+1)$ qubit state $|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$;

2 Apply Hadamard Transform $H^{\otimes(n+1)}$ on $|\psi_0\rangle$ to get $|\psi_1\rangle = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \frac{|\mathbf{x}\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$**3**; Apply $\mathcal{U}_f$ on $|\psi_1\rangle$ to get $|\psi_2\rangle = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \frac{(-1)^{f(\mathbf{x})}|\mathbf{x}\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$**4**; Apply *HN*-Transform on the first n qubits of $|\psi_2\rangle$ to obtain

$$|\psi_3\rangle = \sum_{\mathbf{z}\in\mathbb{F}_2^n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \frac{(-1)^{\mathbf{x}\cdot\mathbf{z}\oplus f(\mathbf{x})} i^{wt(\mathbf{c}*\mathbf{x})}|\mathbf{z}\rangle}{2^n} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right];$$

5 Measurement at M: measure the first n qubits of $|\psi_3\rangle$ in computational basis;

6 After measurement, the state $\mathbf{v}$ such that $wt(\mathbf{v}) = 0$ or $\mathbf{v} = \mathbf{c}$ implies that the function is in $S_{\mathbf{c}}$, else it is in $T_{\mathbf{c}}$.

Algorithm 2. Extended Deutsch-Jozsa algorithm.

Proposition 1. *Given $f \in \mathcal{B}_n$, $\mathcal{D}_f|0\rangle^{\otimes n}$ produces a superposition of all states $\mathbf{z} \in \mathbb{F}_2^n$ with the amplitude $2^{-\frac{n}{2}}\mathcal{H}_f(\mathbf{z})$ corresponding to each state $|\mathbf{z}\rangle$.*

In what follows, we trace the states through this circuit in the general case. The input state is $|\psi_0\rangle = |\mathbf{0}\rangle^{\otimes n}|1\rangle$. After applying $H^{\otimes(n+1)}$ and $\mathcal{U}_f$ successively we obtain as before

$$|\psi_1\rangle = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \frac{|\mathbf{x}\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \text{ and } |\psi_2\rangle = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \frac{(-1)^{f(\mathbf{x})}|\mathbf{x}\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right],$$

respectively. Finally we apply the *HN*-transform $\mathcal{K}^{\mathbf{c}}$ on the first n qubits of $|\psi_2\rangle$ to obtain

$$\begin{aligned}|\psi_3\rangle &= \sum_{\mathbf{z}\in\mathbb{F}_2^n}\sum_{\mathbf{x}\in\mathbb{F}_2^n}\frac{(-1)^{\mathbf{x}\cdot\mathbf{z}\oplus f(\mathbf{x})}\imath^{wt(\mathbf{c}*\mathbf{x})}|\mathbf{z}\rangle}{2^n}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\\ &= \sum_{\mathbf{z}\in\mathbb{F}_2^n}2^{-\frac{n}{2}}\mathcal{K}_f^{\mathbf{c}}(\mathbf{z})|\mathbf{z}\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right].\end{aligned} \tag{7}$$

Consider the sets $S_{\mathbf{c}} = \{s_{\mathbf{c}}(\mathbf{x}), 1\oplus s_{\mathbf{c}}(\mathbf{x}), s_{\mathbf{c}}(\mathbf{x})\oplus \ell_{\mathbf{c}}(x), 1\oplus s_{\mathbf{c}}(\mathbf{x})\oplus \ell_{\mathbf{c}}(\mathbf{x})\}$ and

$$T_{\mathbf{c}} = \left\{ g\in\mathcal{B}_n : \sum_{\mathbf{x}\in\mathbf{c}^\perp=0}(-1)^{g(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})} = \sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^\perp}(-1)^{g(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})} = 0\right\}.$$

Theorem 2. *Suppose that $f\in\mathcal{B}_n$ is chosen from the set $S_{\mathbf{c}}\cup T_{\mathbf{c}}$ where*

$$S_{\mathbf{c}} = \{s_{\mathbf{c}}(\mathbf{x}), 1\oplus s_{\mathbf{c}}(\mathbf{x}), s_{\mathbf{c}}(\mathbf{x})\oplus \ell_{\mathbf{c}}(x), 1\oplus s_{\mathbf{c}}(\mathbf{x})\oplus \ell_{\mathbf{c}}(\mathbf{x})\} \text{ and}$$

$$T_{\mathbf{c}} = \left\{ g\in\mathcal{B}_n : \sum_{\mathbf{x}\in\mathbf{c}^\perp}(-1)^{g(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})} = \sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^\perp}(-1)^{g(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})} = 0,\right\},$$

for any $\mathbf{c}\in\mathbb{F}_2^n$. Applying the extended Deutsch–Jozsa algorithm on f, as above, and measure the first n qubits of $|\psi_3\rangle$ as obtained in (7), if we observe n-bit string $\mathbf{v}$ such that $wt(\mathbf{v})=0$ or $\mathbf{v}=\mathbf{c}$, then the function is in $S_{\mathbf{c}}$, otherwise the function is in $T_{\mathbf{c}}$.

Proof. Using Eq. (3) $|\psi_3\rangle$ is equal to

$$\sum_{\mathbf{z}\in\mathbb{F}_2^n}\frac{\sum_{\mathbf{x}\in\mathbf{c}^\perp}(-1)^{\mathbf{x}\cdot\mathbf{z}\oplus s_{\mathbf{c}}(\mathbf{x})\oplus f(\mathbf{x})} + \imath\sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^\perp}(-1)^{\mathbf{x}\cdot\mathbf{z}\oplus s_{\mathbf{c}}(\mathbf{x})\oplus f(\mathbf{x})}|\mathbf{z}\rangle}{2^n}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right].$$

If $f\in S_{\mathbf{c}}$, then $f(\mathbf{x}) = s_{\mathbf{c}}(\mathbf{x})\oplus a_1\ell_{\mathbf{c}}(\mathbf{x})\oplus a_2$, where $(a_1,a_2)\in\mathbb{F}_2\times\mathbb{F}_2$. Putting $\mathbf{z}=\mathbf{0}$

$$\begin{aligned}&\sum_{\mathbf{x}\in\mathbf{c}^\perp}(-1)^{s_{\mathbf{c}}(\mathbf{x})\oplus f(\mathbf{x})} + \imath\sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^\perp}(-1)^{s_{\mathbf{c}}(\mathbf{x})\oplus f(\mathbf{x})}\\ &= \sum_{\mathbf{x}\in\mathbf{c}^\perp}(-1)^{a_1\ell_{\mathbf{c}}(\mathbf{x})\oplus a_2} + \imath\sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^\perp}(-1)^{a_1\ell_{\mathbf{c}}(\mathbf{x})\oplus a_2}\\ &= \sum_{\mathbf{x}\in\mathbf{c}^\perp}(-1)^{a_2} + \imath(-1)^{a_1}\sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^\perp}(-1)^{a_2} = (-1)^{a_2}2^{n-1}(1+(-1)^{a_1}).\end{aligned}$$

Putting $\mathbf{z}=\mathbf{c}$, $\sum_{\mathbf{x}\in\mathbf{c}^\perp}(-1)^{\mathbf{x}\cdot\mathbf{c}\oplus s_{\mathbf{c}}(\mathbf{x})\oplus f(\mathbf{x})} + \imath\sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^\perp}(-1)^{\mathbf{x}\cdot\mathbf{c}\oplus s_{\mathbf{c}}(\mathbf{x})\oplus f(\mathbf{x})}$

$$\begin{aligned}&= \sum_{\mathbf{x}\in\mathbf{c}^\perp}(-1)^{a_1\ell_{\mathbf{c}}(\mathbf{x})\oplus a_2} + \imath\sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^\perp}(-1)^{1\oplus a_1\ell_{\mathbf{c}}(\mathbf{x})\oplus a_2}\\ &= \sum_{\mathbf{x}\in\mathbf{c}^\perp}(-1)^{a_2} + \imath(-1)^{a_1\oplus 1}\sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^\perp}(-1)^{a_2} = (-1)^{a_2}2^{n-1}(1+(-1)^{a_1\oplus 1}).\end{aligned}$$

Thus, if $f \in S_{\mathbf{c}}$, then after measuring the first n qubits of $|\psi_3\rangle$ we will observe the $|\mathbf{0}\rangle$ or the $|\mathbf{c}\rangle$ state each with probability $\frac{1}{2}$. The probability is zero that any other state is observed.

On the other hand, if $f \in T_{\mathbf{c}}$ then

$$\sum_{\mathbf{x}\in\mathbf{c}^{\perp}} (-1)^{f(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})} = \sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^{\perp}} (-1)^{f(\mathbf{x})\oplus s_{\mathbf{c}}(\mathbf{x})} = 0.$$

The probability amplitudes of the first n qubits of $|\psi_3\rangle$ for the states $|\mathbf{0}\rangle$ and $|\mathbf{c}\rangle$ are

$$\sum_{\mathbf{x}\in\mathbf{c}^{\perp}} (-1)^{s_{\mathbf{c}}(\mathbf{x})\oplus f(\mathbf{x})} + \imath \sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^{\perp}} (-1)^{s_{\mathbf{c}}(\mathbf{x})\oplus f(\mathbf{x})} = 0 + \imath 0 \text{ and}$$

$$\sum_{\mathbf{x}\in\mathbf{c}^{\perp}} (-1)^{\mathbf{x}\cdot\mathbf{c}\oplus s_{\mathbf{c}}(\mathbf{x})\oplus f(\mathbf{x})} + \imath \sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^{\perp}} (-1)^{\mathbf{x}\cdot\mathbf{c}\oplus s_{\mathbf{c}}(\mathbf{x})\oplus f(\mathbf{x})}$$
$$= \sum_{\mathbf{x}\in\mathbf{c}^{\perp}} (-1)^{s_{\mathbf{c}}(\mathbf{x})\oplus f(\mathbf{x})} - \imath \sum_{\mathbf{x}\in\mathbb{F}_2^n\setminus\mathbf{c}^{\perp}} (-1)^{s_{\mathbf{c}}(\mathbf{x})\oplus f(\mathbf{x})} = 0 + \imath 0,$$

respectively. Therefore, the observation of either the state $|\psi_3\rangle$ or the state $|\psi_3\rangle$ implies $f \in S_{\mathbf{c}}$, otherwise $f \in T_{\mathbf{c}}$. □

Form this theorem we obtain Algorithm 2 which can distinguish Boolean functions from a larger set than the set of constant and balanced functions. It is to be noted that, if $wt(\mathbf{c}) = 0$, then we obtain the traditional Deutsch-Jozsa algorithm with all H gates.

5 Conclusion

In this paper, we have studied algorithms related to the *HN*-transform which is a generalization of the well known (Walsh-)Hadamard transform. First we presented an $O(2^{2n})$ algorithm to obtain all the values in the *HN*-spectra. Then we show that the Deutsch-Jozsa algorithm can be generalized considering the *HN*-transform. These results have application in cryptology, coding theory and related areas. While results related to *HN*-spectra have been investigated for more than a decade, a disciplined study of the related computing algorithms had not been attempted earlier, and that is the main goal of this paper.

References

1. Aumasson, J.-P., Dinur, I., Meier, W., Shamir, A.: Cube testers and key recovery attacks on reduced-round MD6 and trivium. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 1–22. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03317-9_1
2. Cusick, T.W., Stănică, P.: Cryptographic Boolean Functions and Applications, 2nd edn. Academic Press, San Diego (2017). 1st edn. (2009)

3. Danielsen, L.E., Parker, M.G.: Spectral orbits and peak-to-average power ratio of boolean functions with respect to the I, H, N^n transform. In: Helleseth, T., Sarwate, D., Song, H.-Y., Yang, K. (eds.) SETA 2004. LNCS, vol. 3486, pp. 373–388. Springer, Heidelberg (2005). doi:10.1007/11423461_28
4. Danielsen, L.E.: On connections between graphs, codes, quantum states, and Boolean functions. Ph.D. thesis, Department of Informatics, The Selmer Center, University of Bergen, Norway (2008)
5. Deutsch, D., Jozsa, R.: Rapid solution of problems by quantum computation. Proc. Roy. Soc. Lond. **A439**, 553–558 (1992)
6. Dillon, J.F.: Elementary Hadamard difference sets. Ph.D. thesis, University of Maryland (1974)
7. Dinur, I., Shamir, A.: Cube attacks on tweakable black box polynomials. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 278–299. Springer, Heidelberg (2009). doi:10.1007/978-3-642-01001-9_16. See also: Cube Attacks on Tweakable Black Box Polynomials. http://eprint.iacr.org/2008/385.pdf
8. Gangopadhyay, S., Pasalic, E., Stănică, P.: A note on generalized bent criteria for boolean functions. IEEE Trans. Inf. Theor. **59**(5), 3233–3236 (2013)
9. Gangopadhyay, S., Gangopadhyay, A.K., Pollatos, S., Stănică, P.: Cryptographic Boolean functions with biased inputs. Crypt. Commun. Discrete Struct. Seq. **9**, 301–314 (2017). doi:10.1007/s12095-015-0174-1
10. Helleseth, T., Kløve, T., Mvkkeltveit, J.: On the covering radius of binary codes. IEEE Trans. Inf. Theor. **24**(5), 627–628 (1978)
11. Knudsen, L.R.: Truncated and higher order differentials. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 196–211. Springer, Heidelberg (1995). doi:10.1007/3-540-60590-8_16
12. Litsyn, S., Shpunt, A.: On the distribution of Boolean function nonlinearity. SIAM J. Discrete Math. **23**(1), 79–95 (2008)
13. Maitra, S., Mukhopadhyay, P.: Deutsch-Jozsa algorithm revisited in the domain of cryptographically significant boolean functions. Int. J. Quantum Inf. **3**(2), 359–370 (2005)
14. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994). doi:10.1007/3-540-48285-7_33
15. Meier, W., Staffelbach, O.: Fast correlation attacks on stream ciphers. In: Barstow, D., Brauer, W., Brinch Hansen, P., Gries, D., Luckham, D., Moler, C., Pnueli, A., Seegmüller, G., Stoer, J., Wirth, N., Günther, C.G. (eds.) EUROCRYPT 1988. LNCS, vol. 330, pp. 301–314. Springer, Heidelberg (1988). doi:10.1007/3-540-45961-8_28
16. Parker, M.G.: Generalised S-box nonlinearity. NESSIE Public Document, 11.02.03: NES/DOC/UIB/WP5/020/A
17. Parker, M.G., Pott, A.: On boolean functions which are bent and negabent. In: Golomb, S.W., Gong, G., Helleseth, T., Song, H.-Y. (eds.) SSC 2007. LNCS, vol. 4893, pp. 9–23. Springer, Heidelberg (2007). doi:10.1007/978-3-540-77404-4_2
18. Patterson, N.J., Wiedemann, D.H.: The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. IEEE Trans. Inf. Theor. **29**(3), 354–356 (1983). See also correction: IEEE Trans. Inf. Theor. **36**(2), 443 (1990)
19. Riera, C.: Spectral properties of Boolean functions, graphs and graph states. Ph.D. thesis, University of Bergen (2005)
20. Riera, C., Parker, M.G.: Generalized bent criteria for Boolean functions. IEEE Trans. Inf. Theor. **52**(9), 4142–4159 (2006)

21. Schmidt, K.-U., Parker, M.G., Pott, A.: Negabent functions in the Maiorana–McFarland class. In: Golomb, S.W., Parker, M.G., Pott, A., Winterhof, A. (eds.) SETA 2008. LNCS, vol. 5203, pp. 390–402. Springer, Heidelberg (2008). doi:10.1007/978-3-540-85912-3_34
22. Siegenthaler, T.: Decrypting a class of stream ciphers using ciphertext only. IEEE Trans. Comput. **34**(1), 81–85 (1985)
23. Stănică, P., Maitra, S.: Rotation symmetric Boolean functions - count and cryptographic properties. Disc. Appl. Math. **156**, 1567–1580 (2008)
24. Stănică, P., Gangopadhyay, S., Chaturvedi, A., Kar-Gangopadhyay, A., Maitra, S.: Investigations on bent and negabent functions via the nega-Hadamard transform. IEEE Trans. Inf. Theor. **58**(6), 4065–4072 (2012)