Introducing Nega-Forrelation: Quantum Algorithms in Analyzing Nega-Hadamard and Nega-crosscorrelation Spectra

Suman Dutta and Subhamoy Maitra

Indian Statistical Institute, Kolkata
sumand.iiserb@gmail.com, subho@isical.ac.in

Abstract. Aaronson defined Forrelation (2010) as a measure of correlation between a Boolean function f and the Walsh-Hadamard transform of another function g. Very recently, we have studied different cryptographically important spectra of Boolean functions through the lens of Forrelation. In the present draft, we explore a similar kind of correlation in terms of Nega-Hadamard transform. We call it Nega-Forrelation and obtain a more efficient sampling strategy for Nega-Hadamard transform compared to the existing results. Moreover, we present an efficient sampling strategy for nega-crosscorrelation (and consequently nega-autocorrelation) spectra too, by tweaking the Nega-Forrelation technique.

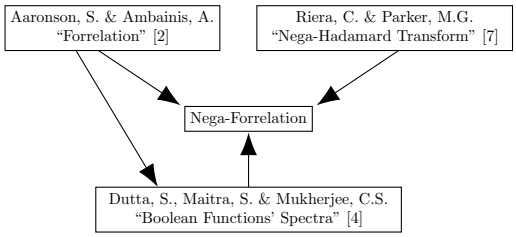
Keywords: Boolean functions · Cryptology · Forrelation · Nega-Forrelation · Nega-Hadamard transform · Quantum algorithms · Walsh-Hadamard transform

1 Introduction

The Forrelation problem, defined by Aaronson et al. [1] presents one of the central questions in the quantum black-box model that has been used to show separation between the bounded error quantum model and the randomized classical model. Forrelation estimates the amount of correlation between a Boolean function, f and the Walsh-Hadamard transform of another Boolean function, g. While the result of [2] was to show theoretical separation, it has been recently noted [4] that the algorithm can also be used for efficient sampling of different spectra of Boolean functions, for example the Walsh-Hadamard, the crosscorrelation and the autocorrelation spectra. Keeping in mind the effectiveness of Forrelation algorithm, an immediate question one may ask is whether similar formulation can be derived for the efficient sampling of the Nega-Hadamard transforms. In this regard, we define the Nega-Forrelation (denoted as η_{f_1,f_2,f_3}) which measures the correlation (suitably modified with respect to complex numbers) between a Boolean function, f_1 with the Nega-Hadamard and conjugate Nega-Hadamard transforms of f_2, f_3 respectively and present related results here.

The idea of Nega-Hadamard transform was introduced by Riera and Parker [7]. They considered some generalized bent criteria for Boolean functions which

would have flat spectrum with respect to Nega-Hadamard transform, different from the Walsh-Hadamard transform. As pointed out in [7], such a transform is motivated by local unitary transforms that play an important role in the structural analysis of pure n-qubit stabilizer quantum states. The authors provided several motivations for this transform, and in the context of cryptology, they have pointed out certain observations related to the S-Box of AES [7, Section I(C), Page 4145]. In general, like the Walsh-Hadamard and autocorrelation spectra of a Boolean function, the studies in Nega domain provide further possibilities in the analysis of Boolean functions when those are used as cryptographic primitives. This paper, in fact, connects the work done in [2], [7], and [4] and provides a deeper understanding of the state-of-the-art results in terms of Nega-Forrelation.



In this draft, we formulate the Nega-Forrelation algorithms. We also recollect the tricks and tweaks used in [4] and modify them judiciously in the Nega-Forrelation algorithms for an efficient sampling of the Nega-Hadamard spectra. For technical purposes, we will mostly follow the notations used in [4] unless otherwise mentioned and refer to that paper as a prerequisite.

The Hadamard gate, mathematically represented as $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, plays an important role in all the major quantum algorithms in the black-box (query) paradigm. Given an unknown Boolean function, f the functioning of U_f on an $n+1$ qubit state $|\mathbf{x}\rangle|-\rangle$, can be given as: $U_f|\mathbf{x}\rangle|-\rangle = f(\mathbf{x})|\mathbf{x}\rangle|-\rangle$. When applied to the all zero state, $|0^n\rangle$ the n-qubit Hadamard gate results in an equal superposition of all possible states, leading to the quantum parallelism. Now, we consider a similar kind of quantum gate, known as the Nega-Hadamard gate ([7], [5]), which is mathematically represented as $N = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix}\right)$, where $i = \sqrt{-1}$. Observe that, since the first column of H and N are essentially same, both the Nega-Hadamard (N) and the Hadamard (H) gates behave in an exact similar manner, when applied to the all zero state, $|0^n\rangle$. However, when applied to a generic n-qubit quantum state $|\psi\rangle = \sum_{\mathbf{x}\in\{0,1\}^n} \alpha_{\mathbf{x}}|\mathbf{x}\rangle$ with $\sum_{\mathbf{x}\in\{0,1\}^n} |\alpha_{\mathbf{x}}|^2 = 1$, the n-qubit Nega-Hadamard gate, ($N^{\otimes n}$) acts as follows.

$$N^{\otimes n}\left(\sum_{\mathbf{x}\in\{0,1\}^n} \alpha_{\mathbf{x}}|\mathbf{x}\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\{0,1\}^n} \alpha_{\mathbf{x}}\left(\sum_{\mathbf{y}\in\{0,1\}^n} (-1)^{\mathbf{x}\cdot\mathbf{y}}(i)^{wt(\mathbf{x})}|\mathbf{y}\rangle\right).$$

Being a complex matrix, taking conjugate of N forms in a new quantum gate, mathematically denoted as $\overline{N} = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & -i \\ 1 & i \end{smallmatrix}\right)$ and the functioning of $\overline{N}$ over the generic quantum state $|\psi\rangle$ is given as follows.

$$\overline{N}^{\otimes n}\left(\sum_{\mathbf{x}\in\{0,1\}^n} \alpha_{\mathbf{x}}|\mathbf{x}\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{\mathbf{x}\in\{0,1\}^n} \alpha_{\mathbf{x}}\left(\sum_{\mathbf{y}\in\{0,1\}^n} (-1)^{\mathbf{x}\cdot\mathbf{y}}(-i)^{wt(\mathbf{x})}|\mathbf{y}\rangle\right).$$

Note that, unlike the Forrelation algorithm, where the n-qubit Hadamard gates are used at the beginning, in between the oracles and towards the end of the circuit, in Nega-Forrelation we use different combination of H, N and $\overline{N}$ gates judiciously in order to manipulate the final state and obtain the desired results. Note that the Phase gate, $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$ can also be exploited to introduce the factor $(i)^{wt(\mathbf{x})}$ at any point of time in the algorithm. We will be using these quantum gates frequently as tricks and tweaks while designing the quantum algorithms for the Nega-Forrelation in later sections.

Boolean functions are one of most fundamental combinatorial objects that has various applications in the domain of quantum algorithms. Following [2,4], here also we define Boolean functions to be a mapping of the form $\{0,1\}^n \to \{-1,1\}$ and denote the set of all n-variable Boolean functions as $\mathcal{B}_n$. For a formal definition of a Boolean function, one may refer to [4, Definition 1].

Given oracle access of Boolean functions $f_1, f_2, f_3 \in \mathcal{B}_n$, we design the algorithms for estimating the values of (3-fold) Nega-Forrelation η_{f_1,f_2,f_3}. The first one makes 3 sequential queries and upon measurement, we obtain the all zero state with probability $|\eta_{f_1,f_2,f_3}|^2$. Note that, since Nega-Forrelation is complex valued, the probability is also given by complex square of the amplitude, η_{f_1,f_2,f_3}. The second algorithm makes 2 parallel queries to the functions, f_1, f_2, f_3 and the probability of one pre-determined qubit (driving qubit) being in the 0 states is given by $\frac{1}{2}\left(1 + \Re\left(\eta_{f_1,f_2,f_3}\right)\right)$, where $\Re(z)$ denotes the real part of the complex number z. We use both these algorithms, along with some necessary tricks and tweaks to provide efficient sampling of different Boolean functions' spectra in later sections. The organization of this draft is as follows.

Organization and Contributions. In Section 2, we define (3-fold) Nega-Forrelation and present two quantum algorithms for estimating the same. The first one requires 3 sequential queries to compute the Nega-Forrelation values whereas the second algorithm estimates the real component of the Nega-Forrelation values with the help of two parallel queries. Here, we also provide a strategy to sample the small values of the nega-Hadamard transform more efficiently compared to the Extended Deutsch-Jozsa algorithm. Section 3 presents the results related to sampling of Nega-crosscorrelation and thus the nega-autocorrelation spectra using Nega-Forrelation. First we sample the Nega-crosscorrelation value at any given point and then we present a method to sample the entire Nega-crosscorrelation spectra and the Nega-crosscorrelation spectra for a particular weight using Dicke state. We refer to [4] and the references therein for most of the definitions. Rest we explain here.

For a binary string $\boldsymbol{\omega} \in \{0,1\}^n$, the number of 1's in the bit pattern of $\boldsymbol{\omega}$ is called the *(Hamming) weight* of the string, denoted as $wt(\boldsymbol{\omega})$. We now define the Nega-Hadamard transform of a Boolean function, following the references [5,9].

Definition 1. *The Nega-Hadamard transform of a function, $f \in \mathcal{B}_n$ at any given point, $\boldsymbol{\omega} \in \{0,1\}^n$ is a complex-valued function, mathematically defined as $N_f(\boldsymbol{\omega}) = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} f(\mathbf{x}) \cdot (-1)^{\mathbf{x}\cdot\boldsymbol{\omega}} (i)^{wt(\mathbf{x})}$, where $\mathbf{x} \cdot \boldsymbol{\omega} = x_1\omega_1 \oplus x_2\omega_2 \oplus$*

$\ldots \oplus x_n\omega_n$ *is the inner product of* $\mathbf{x}$ *and* $\boldsymbol{\omega}$*, and* $wt(\mathbf{x})$ *denotes the Hamming weight of the binary string* $\mathbf{x}$ *and* $i = \sqrt{-1}$.

The multiset $\left\{N_f(\boldsymbol{\omega}) : \omega \in \{0,1\}^n\right\}$ is called the *Nega-Hadamard spectra* of the function f. For any given $f \in \mathcal{B}_n$, the constraint, $\sum_{\omega\in\{0,1\}^n} \left|N_f(\boldsymbol{\omega})\right|^2 = 2^n$ is known as the *Nega-Parseval's identity*, where $\left|N_f(\boldsymbol{\omega})\right|^2 = N_f(\boldsymbol{\omega})\overline{N_f(\boldsymbol{\omega})}$ denotes the complex square of $N_f(\boldsymbol{\omega})$. We use this result in Section 2 for an efficient sampling of Nega-Hadamard spectrum.

Given $f_1, f_2 \in \mathcal{B}_n$, the cross-correlation between f_1 and f_2 is given by the sum, $C_{f_1,f_2}(\mathbf{y}) = \sum_{\mathbf{x}\in\{0,1\}^n} f_1(\mathbf{x})f_2(\mathbf{x}\oplus\mathbf{y})$. Whereas, taking $f_1 = f_2 = f$ in the above expression gives the autocorrelation of the function, $f \in \mathcal{B}_n$, represented by $C_{f,f}(\mathbf{y}) \equiv C_f(\mathbf{y}) = \sum_{\mathbf{x}\in\{0,1\}^n} f(\mathbf{x})f(\mathbf{x}\oplus\mathbf{y})$. Now we provide the formulations of nega-crosscorrelation and nega-autocorrelation as given in [9].

Definition 2 ([9]). *The nega-crosscorrelation of two functions* $f_1, f_2 \in \mathcal{B}_n$ *at any point* $\mathbf{y} \in \{0,1\}^n$ *is defined as* $\widehat{C}_{f_1,f_2}(\mathbf{y}) = \sum_{\mathbf{x}\in\{0,1\}^n} f_1(\mathbf{x})f_2(\mathbf{x}\oplus\mathbf{y})(-1)^{x\cdot y}$. *Whenever* $f_1 = f_2 = f$*, we obtain the formulation for nega-autocorrelation for* $f \in \mathcal{B}_n$ *at a given point* $\mathbf{y} \in \{0,1\}^n$.

In Section 3, we provide efficient sampling of the nega-crosscorrelation and the nega-autocorrelation spectra using (3-fold) Nega-Forrelation.

Let us now briefly discuss the Forrelation formulation [1,2], which is one of the central results in the study of separating the computational power of the bounded error quantum and classical probabilistic models in the black-box (query) model.

Definition 3 ([1]). *Given* $f_1, f_2 \in \mathcal{B}_n$*, the (2-fold) Forrelation measures the amount of correlation between the function* f_1 *and the Walsh-Hadamard transform of the function* f_2*, which can be mathematically represented as*

$$\Phi_{f_1,f_2} = \frac{1}{2^n} \sum_{\mathbf{x_1}\in\{0,1\}^n} f_1(\mathbf{x_1})W_{f_2}(\mathbf{x_1}) = \frac{1}{2^{3n/2}} \sum_{\mathbf{x_1},\mathbf{x_2}\in\{0,1\}^n} f_1(\mathbf{x_1})(-1)^{\mathbf{x_1}\cdot\mathbf{x_2}} f_2(\mathbf{x_2}).$$

For further understanding of the Forrelation problem and its application, the readers are referred to [1,2,4] and the references therein. Following the idea of Forrelation, we now introduce the concept of (3-fold) Nega-Forrelation in the next section.

2 The (3-fold) Nega-Forrelation

Forrelation, defined by Aaronson et al. [1], captures the amount of correlation between a Boolean function, f with the normalized Walsh Spectrum of another Boolean function g. In our recent work [4], we revisited the Forrelation problem to provide efficient sampling of different cryptographically significant spectra of

Boolean functions, namely Walsh, cross-correlation and the autocorrelation spectra. Since the Forrelation problems provides a more efficient sampling strategy compared to the existing methodologies, an immediate question one might ask is that whether a similar formulation could be given in terms of Nega-Hadamard transform of a Boolean function. In this direction, here we introduce the Nega-Forrelation.

Definition 4. *Given Boolean functions $f_1, f_2, f_3 \in \mathcal{B}_n$, (3-fold) Nega-Forrelation measures the amount of correlation among the functions f_1, the Nega-Hadamard transform of f_2 and the conjugate Nega-Hadamard transform of f_3 which can be mathematically formulated as* $\eta_{f_1,f_2,f_3} = \dfrac{1}{2^n} \displaystyle\sum_{\mathbf{x}\in\{0,1\}^n} f_1(\mathbf{x}) N_{f_2}(\mathbf{x}) \overline{N}_{f_3}(\mathbf{x})$.

Observe that η_{f_1,f_2,f_3} can also be expressed as

$$\begin{aligned}
&\tfrac{1}{2^n} \textstyle\sum_{\mathbf{x_1}\in\{0,1\}^n} f_1(\mathbf{x_1}) \left(\tfrac{1}{2^{n/2}} \sum_{\mathbf{x_2}\in\{0,1\}^n} f_2(\mathbf{x_2}) (i)^{wt(\mathbf{x_2})} (-1)^{\mathbf{x_1}\cdot\mathbf{x_2}} \right) \\
&\qquad\qquad \left(\tfrac{1}{2^{n/2}} \textstyle\sum_{\mathbf{x_3}\in\{0,1\}^n} f_3(\mathbf{x_3}) (-i)^{wt(\mathbf{x_3})} (-1)^{\mathbf{x_1}\cdot\mathbf{x_3}} \right) \\
=&\tfrac{1}{2^{2n}} \sum_{\mathbf{x_1},\mathbf{x_2},\mathbf{x_3}\in\{0,1\}^n} f_2(\mathbf{x_2}) (i)^{wt(\mathbf{x_2})} (-1)^{\mathbf{x_1}\cdot\mathbf{x_2}} f_1(\mathbf{x_1}) (-1)^{\mathbf{x_1}\cdot\mathbf{x_3}} (-i)^{wt(\mathbf{x_3})} f_3(\mathbf{x_3}).
\end{aligned}$$

Remark 1. Note that in the definition of Nega-Forrelation, we consider Nega-Hadamard transform of one function and conjugate Nega-Hadamard transform of another function. This is due to the fact that Nega-Hadamard transform are complex numbers and when $f_2 = f_3 = f$, we obtain the complex-square of the Nega-Hadamard transform values for the function, f, where the combinations are decided by the function $f_1 = g$. Furthermore, for $f_2 = f_3 = f$, the Nega-Forrelation values, $\eta_{g,f,f}$ is always a real number.

This result along with the Nega-Parseval's identity provide an efficient sampling technique of Nega-Hadamard transform compared to the existing result [5]. Now we present both the 3-query and 2-query quantum algorithms for obtaining the 3-fold Nega-Forrelation values.

2.1 Quantum algorithms for (3-fold) Nega-Forrelation

We begin with the 3-query quantum algorithm. Given oracle access to $f_1, f_2, f_3 \in \mathcal{B}_n$, we obtain the 3-fold Nega-Forrelation values, η_{f_1,f_2,f_3}, beginning with the state $|0\rangle^{\otimes n} |-\rangle$ and traverse through the following sequence of steps,

$$H^{\otimes n} \to U_{f_2} \to N^{\otimes n} \to U_{f_1} \to H^{\otimes n} \to U_{f_3} \to \overline{N}^{\otimes n}$$

where all the n-qubit gates $\left(H^{\otimes n}, N^{\otimes n}, \overline{N}^{\otimes n}\right)$ are applied to the n query-qubits and the oracles are applied to all the $(n+1)$ qubits.

Ignoring the last qubit, the amplitude corresponding to $|0\rangle^{\otimes n}$ state becomes

$$\frac{1}{2^{2n}} \sum_{\mathbf{x_1},\mathbf{x_2},\mathbf{x_3}\in\{0,1\}^n} f_2(\mathbf{x_2}) (i)^{wt(\mathbf{x_2})} (-1)^{\mathbf{x_1}\cdot\mathbf{x_2}} f_1(\mathbf{x_1}) (-1)^{\mathbf{x_1}\cdot\mathbf{x_3}} (-i)^{wt(\mathbf{x_3})} f_3(\mathbf{x_3}),$$

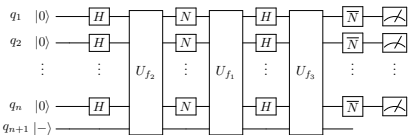


Fig. 1. The 3-query quantum circuit for estimating Nega-Forrelation, η_{f_1,f_2,f_3}.

which is equal to η_{f_1,f_2,f_3}. Since, η_{f_1,f_2,f_3} is a complex number, the probability of observing the all zero state upon measurement is given by $|\eta_{f_1,f_2,f_3}|^2$. We denote this 3-query Nega-Forrelation algorithm for η_{f_1,f_2,f_3} by $\tilde{A}_n^{3,3}(f_1, f_2, f_3)$.

Remark 2. Note that, unlike Forrelation algorithm where only the Hadamard gates were used in between the oracles, here we use the Nega-Hadamard and conjugate Nega-Hadamard gates judiciously in order to obtain the desired formulation. For any given functions $f_1, f_2, f_3 \in \mathcal{B}_n$, the circuit of $\tilde{A}_n^{3,3}$ makes 3 sequential queries and uses $2n$ many Hadamard gates, n many Nega-Hadamard gates and n many conjugate-Nega Hadamard gates.

Analogous to the idea of parallel query Forrelation algorithm [2], we now present the 2-query quantum algorithm for estimating Nega-Forrelation.

Given oracle access to $f_1, f_2, f_3 \in \mathcal{B}_n$, we begin with an $(n+2)$-qubit state, $|+\rangle |0\rangle^{\otimes n} |-\rangle$, where the first qubit is called the 'driving qubit' and the next n qubits are the query-qubits. We first apply the n-qubit Hadamard gate, $H^{\otimes n}$ to all the query qubits, and distribute the state as follows:

$$|+\rangle |0\rangle^{\otimes n} |-\rangle \xrightarrow{H^n} \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{\mathbf{x_2} \in \{0,1\}^n} |0\rangle |\mathbf{x_2}\rangle |-\rangle + \sum_{\mathbf{x_3} \in \{0,1\}^n} |1\rangle |\mathbf{x_3}\rangle |-\rangle \right).$$

Then controlled on the driving qubit being in the $|0\rangle$ state we sequentially apply $U_{f_2} \to N^{\otimes n} \to U_{f_1} \to H^{\otimes n}$ and obtain the state

$$\frac{|0\rangle}{\sqrt{2^{3n+1}}} \sum_{\mathbf{x_1},\mathbf{x_2},\mathbf{x_3} \in \{0,1\}^n} f_2(\mathbf{x_2})(i)^{wt(\mathbf{x_2})} (-1)^{\mathbf{x_1}\cdot\mathbf{x_2}} f_1(\mathbf{x_1}) (-1)^{\mathbf{x_1}\cdot\mathbf{x_3}} |\mathbf{x_3}\rangle |-\rangle .$$

Similarly, controlled on the driving qubit being in the $|1\rangle$ state, we sequentially apply: $S^{\otimes n} \to U_{f_3}$ and obtain the state $\frac{|1\rangle}{\sqrt{2^{n+1}}} \sum_{\mathbf{x_3} \in \{0,1\}^n} f_3(\mathbf{x_3})(i)^{wt(\mathbf{x_3})} |\mathbf{x_3}\rangle |-\rangle$.
After ignoring the last qubit and assuming the following notations:

$$\alpha_{\mathbf{x_3}} = \left(\frac{1}{\sqrt{2^{3n+1}}} \sum_{\mathbf{x_1},\mathbf{x_2} \in \{0,1\}^n} f_2(\mathbf{x_2})(i)^{wt(\mathbf{x_2})} (-1)^{\mathbf{x_1}\cdot\mathbf{x_2}} f_1(\mathbf{x_1}) (-1)^{\mathbf{x_1}\cdot\mathbf{x_3}} \right)$$

$$\text{and } \beta_{\mathbf{x_3}} = \frac{1}{\sqrt{2^{n+1}}} f_3(\mathbf{x_3})(i)^{wt(\mathbf{x_3})},$$

we obtain the final state, (say) $|\psi\rangle = \sum_{\mathbf{x_3} \in \{0,1\}^n} (\alpha_{\mathbf{x_3}} |0\rangle |\mathbf{x_3}\rangle + \beta_{\mathbf{x_3}} |1\rangle |\mathbf{x_3}\rangle)$. Finally, we measure the driving qubit in Hadamard basis, which is equivalent to applying a Hadamard gate, followed by the measurement in the $\{|0\rangle, |1\rangle\}$ basis. Therefore, the final state becomes

$$\frac{1}{\sqrt{2}} \left(\sum_{\mathbf{x_3} \in \{0,1\}^n} (\alpha_{\mathbf{x_3}} + \beta_{\mathbf{x_3}}) |0\rangle |\mathbf{x_3}\rangle + \sum_{\mathbf{x_3} \in \{0,1\}^n} (\alpha_{\mathbf{x_3}} - \beta_{\mathbf{x_3}}) |1\rangle |\mathbf{x_3}\rangle \right)$$

and thus the probability of obtaining $|0\rangle|\mathbf{x_3}\rangle$, where $\mathbf{x_3} \in \{0,1\}^n$, is given by

$$\frac{1}{2}\sum_{\mathbf{x_3}\in\{0,1\}^n}|\alpha_{\mathbf{x_3}}+\beta_{\mathbf{x_3}}|^2 = \frac{1}{2}\left[\sum_{\mathbf{x_3}\in\{0,1\}^n}\left(|\alpha_{\mathbf{x_3}}|^2+|\beta_{\mathbf{x_3}}|^2\right)+\Re\big(\alpha_{\mathbf{x_3}}\overline{\beta}_{\mathbf{x_3}}\big)\right]$$

where $\Re(z)$ denotes the real part of the complex number, z.

Since $\sum_{\mathbf{x_3}\in\{0,1\}^n}|\alpha_{\mathbf{x_3}}|^2+|\beta_{\mathbf{x_3}}|^2$ denotes the sum of squares of all the amplitudes for the state $|\psi\rangle$, it is equal to 1. Moreover, check that $\alpha_{\mathbf{x_3}}\overline{\beta}_{\mathbf{x_3}} = \eta_{f_1,f_2,f_3}$. *Therefore, the probability of observing* $|0\rangle$ *upon measuring the driving qubit is given by* $\frac{1}{2}\left(1+\Re\left(\eta_{f_1,f_2,f_3}\right)\right)$. We denote the 2-query Nega-Forrelation algorithm by $\tilde{A}_n^{2,3}$. Figure 2 provides a schematic diagram of the quantum circuit for $\tilde{A}_n^{2,3}(f_1,f_2,f_3)$.

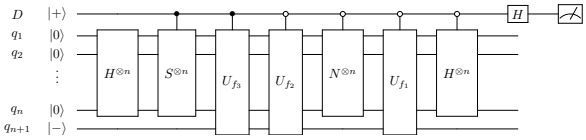


Fig. 2. The 2-query quantum circuit for Nega-Forrelation.

For n-input Boolean functions, the quantum algorithm $\tilde{A}_n^{2,3}$ makes one query to each of the functions and the number of quantum gates required in are given as follows. $2n+1$ many Hadamard gates, n many Nega-Hadamard gates and n many Phase gates. *Since Nega-Forrelation value,* η_{f_1,f_2,f_3} *can be a complex number, using the algorithm,* $\tilde{A}_n^{2,3}$ *we can only estimate the real part of* η_{f_1,f_2,f_3} *and not the complete Nega-Forrelation values.* Next we present the strategies for sampling the Nega-Hadamard transform using $\tilde{A}_n^{3,3}$ and $\tilde{A}_n^{2,3}$.

2.2 Sampling of Nega-Hadamard transform using Nega-Forrelation

Given a Boolean function $f \in \mathcal{B}_n$ and a set of points $S \subseteq \{0,1\}^n$, we now present a strategy for sampling the Nega-Hadamard transform of f using (3-fold) Nega-Forrelation. Recall that using the extended Deutsch-Jozsa algorithm, we can sample the Nega-Hadamard transform of f with probability $\frac{1}{2^n}\sum_{\mathbf{x}\in S}|N_f(\mathbf{x})|^2$. Let us denote this by p.

From the definition of Nega-Forrelation: $\eta_{g,f,f} = \frac{1}{2^n}\sum_{\mathbf{x}\in\{0,1\}^n} g(\mathbf{x})\,|N_f(\mathbf{x})|^2$. Let us define $g \in \mathcal{B}_n$ such that, $g(\mathbf{x}) = -1$ for all $\mathbf{x} \in S$ and 1 otherwise. Then the $\eta_{g,f,f}$ can be written as $\eta_{g,f,f} = \frac{1}{2^n}\left(\sum_{\mathbf{x}\notin S}|N_f(\mathbf{x})|^2 - \sum_{\mathbf{x}\in S}|N_f(\mathbf{x})|^2\right)$. From Nega-Parseval's identity, $\sum_{\mathbf{x}\in\{0,1\}^n}|N_f(\mathbf{x})|^2 = 2^n$ we obtain, $\sum_{\mathbf{x}\notin S}|N_f(\mathbf{x})|^2 = 2^n - \sum_{\mathbf{x}\in S}|N_f(\mathbf{x})|^2$. As a result, $\eta_{g,f,f}$ can now be written as

$$\frac{1}{2^n}\left(2^n - \sum_{\mathbf{x}\in S}|N_f(\mathbf{x})|^2 - \sum_{\mathbf{x}\in S}|N_f(\mathbf{x})|^2\right) = 1 - \frac{2}{2^n}\left(\sum_{\mathbf{x}\in S}|N_f(\mathbf{x})|^2\right) = 1-2p.$$

Thus $p = \frac{1-\eta_{g,f,f}}{2}$, which is same as the probability of obtaining 1 upon measuring the driving qubit from running the algorithm $\tilde{A}^{2,3}(g,f,f)$. Therefore, we have the following proposition.

Proposition 1. *The probability of obtaining* 1 *upon measuring the driving qubit from running the algorithm* $\tilde{A}^{2,3}(g,f,f)$ *where* $g(\mathbf{x}) = -1,\ \forall \mathbf{x} \in S$ *and* $g(\mathbf{x}) = 1$ *otherwise, is given by* $p = \frac{1}{2^n}\sum_{\mathbf{x}\in S} |N_f(\mathbf{x})|^2$.

Remark 3. Since $\eta_{g,f,f}$ is real, while considering the probability from algorithm $\tilde{A}^{2,3}$, we have $\Re(\eta_{g,f,f}) = \eta_{g,f,f}$. Therefore, the 2-query algorithm $\tilde{A}^{(3,2)}(g,f,f)$ makes a single query to f and another query to g, designed based on the set S, behaves exactly equivalent to the extended Deutsch-Jozsa algorithm in terms of sampling the Nega-Hadamard transform.

Now we show that $\tilde{A}^{(3,3)}(g,f,f)$ can be used for an improvement. Observe that, upon running the algorithm $\tilde{A}^{3,3}(g,f,f)$, the probability of obtaining a state with at-least one many 1 in the output bit-pattern is given by $1-\eta^2_{g,f,f}$. Using $\eta_{g,f,f} = (1-2p)$ we obtain, $1-\eta^2_{g,f,f} = 1-(1-2p)^2 = 4p-4p^2$. Therefore, we have the following theorem.

Theorem 1. *Given* $f, g \in \mathcal{B}_n$ *and a set of points* $S \subseteq \{0,1\}^n$ *such that* $g(\mathbf{x}) = -1,\ \forall \mathbf{x} \in S$ *and* $g(\mathbf{x}) = 1$ *otherwise, the* 3*-query quantum algorithm* $\tilde{A}^{3,3}(g,f,f)$ *outputs bit-pattern containing at-least one many* 1 *with probability* $4p - 4p^2$.

When $p < 0.75$, we observe that $4p - 4p^2 > p$. Therefore, the 3-query Nega-Forrelation algorithm $\tilde{A}^{3,3}(g,f,f)$ samples the small values Nega-Hadamard transform of f more efficiently as compared to the extended Deutsch-Jozsa algorithm [5]. Moreover, using the extended Deutsch-Jozsa twice (two queries to f) one can sample the Nega-Hadamard transform values with probability $1-(1-p)^2 = 2p-p^2$ which is also less compared to sampling probability obtained from $\tilde{A}^{3,3}$. We can check that the sampling probability from $\tilde{A}^{3,3}$ is also better compared to applying the extended Deutsch-Jozsa once followed by a single round of amplitude amplification. For graphical understanding, one might refer to [4, Figure 4].

3 Nega-crosscorrelation sampling algorithms using Nega-Forrelation

Here we provide an efficient sampling of the nega-crosscorrelation spectra, and consequently the nega-autocorrelation spectra, using the Nega-Forrelation algorithms, with some necessary tricks and tweaks. In this regard, we use the following observation due to [9, Lemma 4], which connects the nega-crosscorrelation of two functions, $f_1, f_2 \in \mathcal{B}_n$ with the product of Nega-Hadamard transform of the corresponding functions.

Lemma 1 ([9]). *If* $f_1, f_2 \in \mathcal{B}_n$, *then the nega-crosscorrelation equals*

$$\widehat{C}_{f_1,f_2}(\mathbf{y}) = (i)^{wt(\mathbf{y})} \sum_{\mathbf{x}\in\{0,1\}^n} N_{f_1}(\mathbf{x})\overline{N_{f_2}(\mathbf{x})}(-1)^{\mathbf{x}\cdot\mathbf{y}}.$$

For the proof of this lemma, one can refer to [8, Lemma 4]. Using this lemma, we now provide an efficient sampling of the nega-crosscorrelation spectra using the algorithms, $\tilde{A}_n^{3,3}$ and $\tilde{A}_n^{2,3}$. Efficient sampling of the nega-autocorrelation spectra follows as an immediate corollary.

Theorem 2. *Given the oracle access of the functions $f_1, f_2 \in \mathcal{B}_n$ and a point $\mathbf{y} \in \{0,1\}^n$, the algorithm $\tilde{A}_n^{3,3}$ estimates the nega-crosscorrelation value at $\mathbf{y}$ where the probability of observing $|0\rangle^{\otimes n}$ is given by $\frac{1}{2^{2n}}\left|\widehat{C}_{f_1,f_2}(\mathbf{y})\right|^2$. Further, from algorithm $\tilde{A}_n^{2,3}$, the probability of obtaining the 0 state upon measuring the driving qubit, is given by $\frac{1}{2}\left(1+\Re\left(\frac{(-i)^{wt(\mathbf{y})}\widehat{C}_{f_1,f_2}(\mathbf{y})}{2^n}\right)\right)$.*

Proof. Assuming $h(\mathbf{x}) = (-1)^{\mathbf{x}\cdot\mathbf{y}}$ is a linear function in $\mathcal{B}_n$, we can write $\widehat{C}_{f_1,f_2}(\mathbf{y})$ as $\widehat{C}_{f_1,f_2}(\mathbf{y}) = (i)^{wt(\mathbf{y})}\sum_{\mathbf{x}\in\{0,1\}^n} h(x)N_{f_1}(\mathbf{x})\overline{N_{f_2}(\mathbf{x})} = (i)^{wt(\mathbf{y})}2^n \cdot \eta_{h,f_1,f_2}$, which implies $\eta_{h,f_1,f_2} = \frac{1}{2^n}(-i)^{wt(\mathbf{y})}\widehat{C}_{f_1,f_2}(\mathbf{y})$. Rest of the proof follows directly. □

This gives us a constant query algorithm for sampling the nega-crosscorrelation value for any two functions, $f_1, f_2 \in \mathcal{B}_n$ at any given point, $y \in \{0,1\}^n$. For $f_1 = f_2 = f$, we obtain the constant query sampling of nega-autocorrelation, $\widehat{C}_f$ as an immediate corollary.

From [4, Algorithm 1], we can now design a quantum circuit where we pass superposition of states in the Nega-Forrelation circuit in place of the linear function $h(x)$ [refer to figure 3] and we observe that the amplitude of the all zero state is given by $\sum_{\mathbf{y}\in\{0,1\}^n}\alpha_{\mathbf{y}}(\mathbf{y})\,|\mathbf{y}\rangle\left(\frac{\widehat{C}_{f,g}(\mathbf{y})}{2^n}\,|0^n\rangle + \beta_{\mathbf{y}}\,|W_{\mathbf{y}}\rangle\right)$.

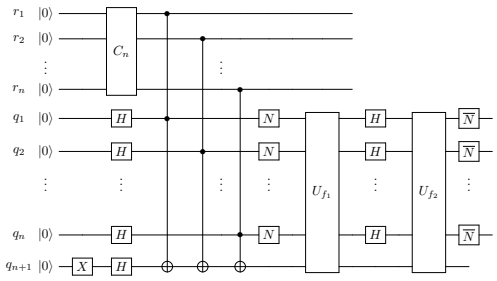


Fig. 3. Quantum circuit for sampling the complete nega-crosscorrelation spectra.

Thus, when $C_n = H^{\otimes n}$, the left most oracle becomes a superposition of all possible linear functions which helps in sampling of the entire spectra of Nega-crosscorrelation. Here the coefficient $\alpha_{\mathbf{y}}(\mathbf{y}) = \frac{1}{2^{\frac{n}{2}}}$. Therefore the corresponding probability of observing the all zero state is given by $\frac{\widehat{C}_{f,g}(\mathbf{y})^2}{2^{3n}}$.

Moreover, assuming UD_m^n prepares the Dicke state, $|D_m^n\rangle$ of weight m, replacing $C_n = UD_m^n$, we obtain the probability of observing the all zero state is $\frac{\widehat{C}_{f,g}(\mathbf{y})^2}{\binom{n}{m}2^{2n}}$, where the Hamming weight of $\mathbf{y}$ is m. This also improves the Nega-crosscorrelation sampling for small values of m, than the existing results.

We have run all the algorithms in IBMQ simulator (*'ibmq_qasm_simulator'*) and found the observations matching the theoretical results. However, the results from real quantum machines were found to be deviated due to noise. Implementation of these algorithms in a noisy quantum environment could be a future research possibility in this direction.

References

1. Aaronson, S.: BQP and the polynomial hierarchy. In Proceedings of the 42nd ACM STOC '10. Association for Computing Machinery, NY, USA, pp. 141–150, (2010).
2. Aaronson, S., Ambainis, A.: Forrelation: A Problem that Optimally Separates Quantum from Classical Computing. In Proceedings of the 47th annual ACM STOC '15. Association for Computing Machinery, NY, USA, pp. 307—316, (2015).
3. Deutsch, D., Jozsa, R.: Rapid solution of problems by quantum computation. In Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, London, vol. 439, issue 1907, pp. 553—558, (1992).
4. Dutta, S., Maitra, S., Mukherjee, C.S.: Following Forrelation – Quantum Algorithms in Exploring Boolean Functions' Spectra. (2021). Advances in Mathematics of Communications (accepted, November 2021). arXiv: `https://arxiv.org/abs/2104.12212v1`
5. Gangopadhyay, S., Maitra, S., Sinha, N., Stanica, P.: Quantum Algorithms Related to HN-Transforms of Boolean Functions. C2SI 2017. LNCS, Vol 10194. Springer, pp. 314-327, 2017.
6. Grover, L. K.: A fast Quantum Mechanical Algorithm for Database Search. In Proceedings of the 28th ACM STOC'96. Association for Computing Machinery, NY, USA, pp. 212-219, 1996.
7. Riera, C., Parker, M.G.: Generalized Bent Criteria for Boolean Functions (I). In IEEE Transactions on Information Theory, 52(9), pp. 4142-4159, Sept. (2006).
8. Stanica, P., Gangopadhyay, S., Chaturvedi, A., Gangopadhyay, A. K., Maitra, S.: Nega-Hadamard Transform, Bent and Negabent Functions. In proceedings of the 6th international conference on SETA, pp. 359–372, September, (2010)
9. Stanica, P., Gangopadhyay, S., Chaturvedi, A., Gangopadhyay, A.K., Maitra, S.: Investigations on Bent and Negabent Functions via the Nega-Hadamard Transform. In IEEE Transactions on Information Theory, 58(6), pp. 4064–4072, June (2012).