Baltic J. Modern Computing, Vol. 4 (2016), No. 4, pp. 721–730
DOI: http://dx.doi.org/10.22364/bjmc.2016.4.4.09

Optimal One-shot Quantum Algorithm for EQUALITY and AND

Andris AMBAINIS, Jānis IRAIDS

Faculty of Computing, University of Latvia, Raiņa bulvāris 19, Riga, LV-1586, Latvia

ambainis@lu.lv, janis.iraids@gmail.com

Abstract. We study the computation complexity of Boolean functions in the quantum black box model. In this model our task is to compute a function $f : \{0,1\} \to \{0,1\}$ on an input $x \in \{0,1\}^n$ that can be accessed by querying the black box. Quantum algorithms are inherently probabilistic; we are interested in the lowest possible probability that the algorithm outputs incorrect answer (the error probability) for a fixed number of queries. We show that the lowest possible error probability for AND_n and $\mathrm{EQUALITY}_{n+1}$ is $\frac{1}{2} - \frac{n}{n^2+1}$.

Keywords: quantum query complexity; bounded error; total Boolean function; and; equality; single query

1 Introduction

In this paper we study the computational complexity of Boolean functions in the quantum black box model. It is a generalization of the decision tree model, where we are computing an n-bit function $f : \{0,1\}^n \to \{0,1\}$ on an input $x \in \{0,1\}^n$ that can only be accessed through a black box by querying some bit x_i of the input. In the quantum black box model the state of the computation is described by a quantum state from the Hilbert space $\mathcal{H}_Q \otimes \mathcal{H}_W \otimes \mathcal{H}_O$ where $\mathcal{H}_Q = \{|0\rangle, |1\rangle, \ldots, |n\rangle\}$ is the query subspace, $\mathcal{H}_W$ is the working memory and $\mathcal{H}_O = \{|0\rangle, |1\rangle\}$ is the output subspace. A computation using t queries consists of a sequence of unitary transformations $U_t \cdot O_x \cdot U_{t-1} \cdot O_x \cdot \ldots \cdot O_x \cdot U_0$ followed by a measurement, where the U_i's are independent of the input and $O_x = O_{Q,x} \otimes I \otimes I$ with

$$O_{Q,x} |i\rangle = \begin{cases} (-1)^{x_i} |i\rangle = \hat{x}_i |i\rangle, \text{ if } i \in [n], \\ |0\rangle, \text{ if } i = 0, \end{cases}$$

is the query transformation, where $x_i \in \{0,1\}$ or equivalently, $\hat{x}_i \in \{-1,1\}$. The final measurement is a complete projective measurement in the computational basis

and the output of the algorithm is the result of the last register, $\mathcal{H}_O$. For and $0 \leq \epsilon < \frac{1}{2}$ we denote by $Q_\epsilon(f)$ the smallest number of queries for an quantum algorithm outputting $f(x)$ with probability at least $1-\epsilon$. Usually the ϵ is omitted from $Q_\epsilon(f)$ because it changes $Q_\epsilon(f)$ by a constant factor, and $Q(f)$ is called the bounded error quantum query complexity of f. This complexity measure is widely studied as most computational problems can be expressed in the query model. The most well known examples are by Grover (1996) and Shor (1997). For the searching problem Grover's algorithm is exactly optimal as shown by Zalka (1999).

However, if one is interested in computing functions with constant number of inputs (for example, as a part of small circuit), then it may be useful to fix the number queries and minimize the probability of an incorrect answer. In this paper we will be concerned with quantum algorithms performing at most 1 query, thus we introduce $\mathcal{E}(f)$.

Definition 1. Let f be a Boolean function. Then let $\mathcal{E}(f)$ be the minimum error probability for a quantum algorithm that calculates f using just one query, i.e.,

$$\mathcal{E}(f) = \min_{\mathcal{A}:\mathcal{A} \text{ performs 1 query}} \max_x \Pr[\text{algorithm } \mathcal{A} \text{ does not output } f(x)].$$

We will be focusing on two Boolean functions defined as follows:

$$\text{EQUALITY}_n(x) = \begin{cases} 1, \text{ if } x_1 = x_2 = \ldots = x_n \\ 0, \text{ otherwise} \end{cases}$$

and

$$\text{AND}_n(x) = \begin{cases} 1, \text{ if } x_1 = x_2 = \ldots = x_n = 1 \\ 0, \text{ otherwise} \end{cases}.$$

In her doctoral thesis Miscenko-Slatenkova (2012) gave quantum algorithms showing that

$$\mathcal{E}(\text{EQUALITY}_3) \leq \frac{1}{10}; \mathcal{E}(\text{AND}_2) \leq \frac{1}{10};$$
$$\mathcal{E}(\text{EQUALITY}_4) \leq \frac{1}{4}; \mathcal{E}(\text{AND}_3) \leq \frac{1}{4};$$
$$\mathcal{E}(\text{EQUALITY}_6) \leq \frac{7}{16}; \mathcal{E}(\text{AND}_5) \leq \frac{7}{16}.$$

Our main result asserts that

Theorem 1.

$$\mathcal{E}(\text{AND}_n) = \mathcal{E}\left(\text{EQUALITY}_{n+1}\right) = \frac{1}{2} - \frac{n}{n^2+1}.$$

The proof can be summarized in a series of three inequalities:

$$\frac{1}{2} - \frac{n}{n^2+1} \leq \mathcal{E}(\text{AND}_n) \leq \mathcal{E}\left(\text{EQUALITY}_{n+1}\right) \leq \frac{1}{2} - \frac{n}{n^2+1}.$$

The first inequality can be proven using a characterization of symmetric sum-of-squares polynomials known as the Blekherman's theorem.

Theorem 4 (Blekherman). *Let $q(\hat{x})$ be the symmetrization of a polynomial $p^2(\hat{x})$ where $p(\hat{x})$ is a multilinear polynomial of degree $t \leq \frac{n}{2}$ and $\hat{x} = (x_1, \ldots, x_n)$. Then, over the Boolean hypercube $\hat{x} \in \{-1, 1\}^n$,*

$$q(\hat{x}) = \sum_{j=0}^{t} p_{t-j}(|x|) \left(\prod_{0 \leq i < j} (|x| - i)(n - |x| - i) \right)$$

where p_{t-j} is a univariate polynomial that is a sum of squares of polynomials of degree at most $t - j$ and $|x|$ denotes the number of variables $i : \hat{x}_i = -1$.

Even though it is an unpublished result, there are proofs — see Lee et al. 2016 or Section 4 in this paper for a considerably shorter proof using representation theory.

The second inequality is trivial, since

$$\mathrm{AND}_n(x_1, \ldots, x_n) = \mathrm{EQUALITY}_{n+1}(x_1, \ldots, x_n, 1),$$

and so we can use an algorithm for $\mathrm{EQUALITY}_{n+1}$ to calculate AND_n.

The third inequality can be proved by constructing a quantum algorithm for the function $\mathrm{EQUALITY}_{n+1}$. Since the algorithm is very simple we present it before the more involved proof of the first inequality.

If we compare $\mathcal{E}(f)$ with the classical analogue, let us call it $\mathcal{E}^C(f)$, Miscenko-Slatenkova (2012) has shown that $\mathcal{E}^C(\mathrm{EQUALITY}_n) = \frac{1}{2}$ and $\mathcal{E}^C(\mathrm{AND}_n) = \frac{1}{2} - \frac{1}{4n-2}$.

2 Algorithm for EQUALITY

Theorem 2.

$$\mathcal{E}\left(\mathrm{EQUALITY}_{n+1}\right) \leq \frac{1}{2} - \frac{n}{n^2+1}$$

Proof. We will prove that the following algorithm has the claimed error probability:

Algorithm 1 Algorithm for $\mathrm{EQUALITY}_{n+1}$

State space: $|1\rangle, |2\rangle, \ldots, |n+1\rangle$
Start in uniform superposition $\sum_{i=1}^{n+1} \frac{1}{\sqrt{n+1}} |i\rangle$
Query: $\sum_{i=1}^{n+1} \frac{1}{\sqrt{n+1}} |i\rangle \xrightarrow{Q} \sum_{i=1}^{n+1} \frac{(-1)^{x_i}}{\sqrt{n+1}} |i\rangle$
Perform quantum Fourier transform $F_{n+1} |i\rangle = \sum_{j=1}^{n+1} \frac{\omega^{(i-1)(j-1)}(-1)^{x_j}}{n+1} |i\rangle$,$\omega = e^{\frac{2\pi}{n+1} i}$:
$\sum_{i=1}^{n+1} \frac{(-1)^{x_i}}{\sqrt{n+1}} |i\rangle \xrightarrow{F_{n+1}} \sum_{i=1}^{n+1} \sum_{j=1}^{n+1} \frac{\omega^{(i-1)(j-1)}(-1)^{x_j}}{n+1} |i\rangle$
Perform a complete measurement
if the result is state $|1\rangle$ **then**
    With probability $\frac{1}{2} - \frac{n}{n^2+1}$ output 0; otherwise output 1
else
    Output 0

First, let us consider the case when $\text{EQUALITY}_{n+1} = 1$. In that case the state $|1\rangle$ will be measured with certainty and hence the probability to output the incorrect answer 0 is $\frac{1}{2} - \frac{n}{n^2+1}$.

If on the other hand the input is such that $\text{EQUALITY}_{n+1} = 0$, the algorithm has an opportunity to answer incorrectly only in the case it measures $|1\rangle$. Denote by $m := \sum_{i=1}^{n+1} x_i$. The probability that the algorithm answers 1 is $\left(\frac{m}{n+1}\right)^2 \cdot \left(\frac{1}{2} + \frac{n}{n^2+1}\right)$. The value of this expression is maximized when $m = \pm(n-1)$ and so the probability to answer 1 on the worst kind of input (namely the input where only one bit is different from every other bit) is

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

□

3 Lower Bound for AND

Theorem 3.

$$\mathcal{E}\left(\text{AND}_n\right) \geq \frac{1}{2} - \frac{n}{n^2+1}$$

Proof. First, we will restrict the domain of the inputs of the AND_n function to bit lists with Hamming weight of 0, $n-1$ or n. It turns out that this promise problem has the same optimal error probability. Consider any quantum algorithm computing AND_n with error probability ϵ. Following the familiar reasoning of Beals et al. (1998) we can write the probability that the algorithm outputs 1 as a sum-of-squares polynomial of degree at most 2:

$$\Pr[\text{algorithm outputs } 1] = \sum_i p_i^2(\hat{x}_1, \ldots, \hat{x}_n).$$

From Blekherman's theorem we obtain that by symmetrization there must exist a degree at most 2 univariate polynomial of the form

$$p(s) = \sum_i (a_i s + b_i)^2 + (n-s)s \sum_j c_j^2$$

such that

$$1 - \epsilon \leq p(s) \leq 1$$

when $s = |x| = n$ and

$$0 \leq p(s) \leq \epsilon$$

when $s = |x|$ and $s \in \{0, n-1\}$.

A geometric representation of the potential regions where $p(s)$ intersects $s = 0$, $s = n-1$ and $s = n$ is depicted in Figure 1. Clearly, a degree 0 polynomial p — a constant, would produce an error probability $\epsilon = \frac{1}{2}$. Consider a degree 1 polynomial — a straight line. We will apply transformations to the line that do not increase (but may

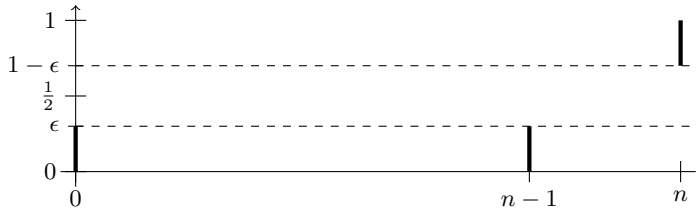

Fig. 1. Regions where $p(s)$ may intersect $s = 0$, $s = n - 1$ and $s = n$

decrease) the error probability it achieves ϵ. First, we stretch the line vertically with respect to the horizontal line $y = \frac{1}{2}$ until it passes through the origin. Then we stretch the line vertically with respect to the horizontal line $y = 0$ until it passes through both $(n-1, \epsilon)$ and $(n, 1-\epsilon)$. This line has a slope $\frac{\epsilon}{n-1} = \frac{1-\epsilon}{n}$ and so $\epsilon = \frac{1}{2} - \frac{1}{4n-2}$.

Finally, consider a degree 2 polynomial p — a parabola. If the parabola is concave, we may reason similarly as in the line case, except, the point $(n-1, \epsilon)$ must now be above the line passing through $(0, 0)$ and $(n, 1-\epsilon)$ and so the error probability is higher. If the parabola is convex, we consider further two cases.

a) If the vertex of the parabola has $s \leq 0$, then we perform the same vertical stretchings. Since the parabola now passes through $(0, 0)$ we can describe it with an equation $as^2 + bs$ where $a > 0$. Since the vertex of the parabola has $s \leq 0$, the coefficient b must be non-negative. The smallest ϵ possible for such parabolas can be described through the system

$$1 - \epsilon = \max_{a,b} an^2 + bn \quad \text{such that}$$
$$\begin{cases} an^2 + bn + a(n-1)^2 + b(n-1) = 1 \\ b \geq 0 \end{cases}$$

From the equality we can express $b = \frac{1-a(n^2+(n-1)^2)}{2n-1}$ and hence $a \leq \frac{1}{n^2+(n-1)^2}$. Plugging it all into the objective function we have that

$$1 - \epsilon \leq an^2 + \frac{n(1 - a(n^2 + (n-1)^2))}{2n-1} \leq$$
$$\leq \frac{n^2}{n^2 + (n-1)^2} \leq \frac{(n+1)^2}{2(n^2+1)} = \frac{1}{2} + \frac{n}{n^2+1}$$

b) If the vertex of the parabola has $s \geq 0$ then clearly the vertex has to be in the interval $s \in [0, n]$. Therefore we use the property from Blekherman's characterization that the polynomial $p(s)$ is non-negative in the interval $s \in [0, n]$, i.e., the term $\sum_i (a_i s + b_i)^2$ is non-negative everywhere and $(n-s)s \sum_j c_j^2$ is non-negative for $s \in [0, n]$. Now we stretch the parabola horizontally with respect to line $s = n$ until $p(0) = p(n-1)$. This will not increase ϵ and preserve the non-negativity in the interval $s \in [0, n]$. Next we stretch the parabola vertically with respect to line

$y = p(n)$ until $p\left(\frac{n-1}{2}\right) = 0$. Again, this step does not increase ϵ. Finally, we stretch vertically with respect to $y = 0$ until $p(0) = 1 - p(n)$. The last step preserved the vertex at $(\frac{n-1}{2}, 0)$ so the parabola has an equation

$$p(s) = a\left(s - \frac{n-1}{2}\right)^2.$$

But from the equation $p(0) = 1 - p(n)$ we obtain

$$a\left(\frac{n-1}{2}\right)^2 = 1 - a\left(\frac{n+1}{2}\right)^2;$$

$$a = \frac{2}{n^2+1}.$$

Consequently,

$$\epsilon \geq p(0) = \frac{2}{n^2+1}\left(\frac{n-1}{2}\right)^2 = \frac{1}{2} - \frac{n}{n^2+1}.$$

□

Interestingly, the proof only really requires the sum-of-squares characterization when $\frac{n-1}{2}$ is not an integer. The fact that the parabola $p(s)$ is non-negative at $s = \frac{n-1}{2}$ is sufficient.

4 Proof of Blekherman's Theorem

In this section we prove Blekherman's theorem.

Theorem 4 (Blekherman). *Let $q(\hat{x})$ be the symmetrization of a polynomial $p^2(\hat{x})$ where $p(\hat{x})$ is a multilinear polynomial of degree $t \leq \frac{n}{2}$ and $\hat{x} = (x_1, \ldots, x_n)$. Then, over the Boolean hypercube $\hat{x} \in \{-1, 1\}^n$,*

$$q(\hat{x}) = \sum_{j=0}^{t} p_{t-j}(|x|)\left(\prod_{0 \leq i < j}(|x| - i)(n - |x| - i)\right)$$

where p_{t-j} is a univariate polynomial that is a sum of squares of polynomials of degree at most $t - j$ and $|x|$ denotes the number of variables $i : \hat{x}_i = -1$.

Our proof utilizes concepts of representation theory. For a description of the core tools of representation theory that we require refer to the first two chapters of Serre (1977).

4.1 Group representation

Let $H_\wp$ be a Hilbert space with basis states $\hat{x}_S$ (for all $S \subseteq [n]$) corresponding to monomials $\prod_{i \in S} \hat{x}_i$. Then, the vectors in $H_\wp$ correspond to multilinear polynomials in variables $\hat{x}_i$. We consider a group representation of the symmetric group $\mathfrak{S}_n$ on $H_\wp$ with transformations U_π defined by $U_\pi \hat{x}_S = \hat{x}_{\pi(S)}$. The irreducible representations contained in $H_\wp$ are well known:

Let $S_m(\hat{x}_1, \ldots, \hat{x}_n) = \sum_{i_1,\ldots,i_m} \hat{x}_{i_1} \ldots \hat{x}_{i_m}$ be the mth elementary symmetric polynomial. We use $S_0(\hat{x}_1, \ldots, \hat{x}_n)$ to denote the constant 1.

Lemma 1. *A subspace $H \subseteq H_\wp$ is irreducible if and only if there exist b and α_m for $m = 0, 1, \ldots, n-2b$ such that H is spanned by vectors $\overrightarrow{p}_{i_1,\ldots,j_b}$ corresponding to polynomials $p_{i_1,\ldots,j_b}$ (for all choices of pairwise distinct $i_1, j_1, \ldots, i_b, j_b \in [n]$) where*

$$p_{i_1,\ldots,j_b}(\hat{x}_1, \ldots, \hat{x}_n) = (\hat{x}_{i_1} - \hat{x}_{j_1}) \ldots (\hat{x}_{i_b} - \hat{x}_{j_b}) \sum_{m=0}^{n-2b} \alpha_m S_m(\hat{x}')$$

and $\hat{x}' \in \{-1, 1\}^{n-2b}$ consists of all $\hat{x}_i$ for $i \in [n]$, $i \notin \{i_1, \ldots, j_b\}$.

See Belovs 2015 for a short proof of Lemma 1.

4.2 Decomposition of $q(\hat{x})$

Let

$$p(\hat{x}_1, \ldots, \hat{x}_n) = \sum_{S:|S| \le t} a_S \hat{x}_S.$$

We associate $p^2(\hat{x}_1, \ldots, \hat{x}_n)$ with the matrix (P_{S_1,S_2}) with rows and columns indexed by $S \subseteq [n], |S| \le t$ defined by $P_{S_1,S_2} = a_{S_1} a_{S_2}$. Let $\overrightarrow{x}$ be a column vector consisting of all $\hat{x}_S$ for $S : |S| \le t$. Then, $p^2(\hat{x}_1, \ldots, \hat{x}_n) = \overrightarrow{x}^T P \overrightarrow{x}$. This means that P is positive semidefinite.

For a permutation $\pi \in \mathfrak{S}_n$, let P^π be the matrix defined by

$$P^\pi_{S_1,S_2} = a_{\pi(S_1)} a_{\pi(S_2)}$$

and let $Q = \frac{1}{n!} \sum_{\pi \in \mathfrak{S}_n} P^\pi$ be the average of all P^π. Then, $q(\hat{x}) = \overrightarrow{x}^T Q \overrightarrow{x}$. Q is also positive semidefinite (as a linear combination of positive semidefinite matrices P^π with positive coefficients).

We decompose $Q = \sum_i \lambda_i Q_i$ with λ_i ranging over different non-zero eigenvalues and Q_i being the projectors on the respective eigenspaces. Since Q is positive semidefinite, we have $\lambda_i > 0$ for all i.

We interpret transformations U_π as permutation matrices defined by $(U_\pi)_{S,S'} = 1$ if $S = \pi(S')$ and $(U_\pi)_{S,S'} = 0$ otherwise. Then, we have

$$U_\pi Q U_\pi^\dagger = \frac{1}{n!} \sum_{\tau \in \mathfrak{S}_n} U_\pi P^\tau U_\pi^\dagger = \frac{1}{n!} \sum_{\tau \in \mathfrak{S}_n} P^{\pi\tau} = \frac{1}{n!} \sum_{\tau \in \mathfrak{S}_n} P^\tau = Q.$$

Since we also have

$$U_\pi Q U_\pi^\dagger = \sum_i \lambda_i U_\pi Q_i U_\pi^\dagger,$$

we must have $Q_i = U_\pi Q_i U_\pi^\dagger$. This means that Q_i is a projector to a subspace $H_i \subseteq H_\wp$ that is invariant under the action of $\mathfrak{S}_n$. If H_i is not irreducible, we can decompose it into a direct sum of irreducible subspaces

$$H_i = H_{i,1} \oplus H_{i,2} \oplus \ldots \oplus H_{i,m_i}.$$

Then, we have $Q_i = \sum_{j=1}^{m_i} Q_{i,j}$ where $Q_{i,j}$ is a projector to $H_{i,j}$ and $Q = \sum_{i,j} \lambda_i Q_{i,j}$. This means that we can decompose $q(\hat{x}) = \sum_{i,j} \lambda_i q_{i,j}(\hat{x})$ where $q_{i,j}(\hat{x}) = \overrightarrow{x}^T Q_{i,j} \overrightarrow{x}$ and it suffices to show the theorem for one polynomial $q_{i,j}(\hat{x})$ instead of the whole sum $q(\hat{x})$.

4.3 Projector to one subspace.

Let $H_{\wp,\ell} \subseteq H_\wp$ be an irreducible invariant subspace. We claim that the projection to the subspace $H_{\wp,\ell}$ denoted by $\Pi_{\wp,\ell}$ is of the following form:

Lemma 2.

$$\Pi_{\wp,\ell} = c\rho_{\wp,\ell} \textit{ where } \rho_{\wp,\ell} = \sum_{i_1,\ldots,j_b} \overrightarrow{p}_{i_1,\ldots,j_b} \overrightarrow{p}^T_{i_1,\ldots,j_b}$$

for some constant c.

Proof. If we restrict to the subspace $H_{\wp,\ell}$, then $\Pi_{\wp,\ell}$ is just the identity I.

On the right hand side, $\rho_{\wp,\ell}$ is mapped to itself by any U_π (since any U_π permutes the vectors $\overrightarrow{p}_{i_1,\ldots,j_b}$ in some way). Therefore, all U_π also map the eigenspaces of $\rho_{\wp,\ell}$ to themselves. This means that, if $\rho_{\wp,\ell}$ has an eigenspace $V \subset H_{\wp,\ell}$, then U_π acting on V also form a representation of $\mathfrak{S}_n$ but that would contradict $H_{\wp,\ell}$ being an irreducible representation. Therefore, the only eigenspace of $\rho_{\wp,\ell}$ is the entire $H_{\wp,\ell}$. This can only happen if $\rho_{\wp,\ell}$ is cI for some constant c. □

4.4 Final polynomial

From the previous subsection, it follows that $q_{i,j}(\hat{x})$ is a positive constant times

$$\sum_{i_1,\ldots,j_b} (\hat{x}_{i_1} - \hat{x}_{j_1})^2 \ldots (\hat{x}_{i_b} - \hat{x}_{j_b})^2 S^2(\hat{x}')$$

where $S(\hat{x}')$ is a symmetric polynomial of degree at most $t - b$. Instead of the sum, we consider the expected value of $(\hat{x}_{i_1} - \hat{x}_{j_1})^2 \ldots (\hat{x}_{i_b} - \hat{x}_{j_b})^2 S^2(\hat{x}')$ when $i_1, \ldots, j_b$ are chosen randomly. (Since the sum and the expected value differ by a constant factor, this is sufficient.)

Terms $(\hat{x}_{i_k} - \hat{x}_{j_k})^2$ are nonzero if and only if one of x_{i_k} and x_{j_k} is 1 and the other is -1. Then, for $k = 1$, we have

$$\Pr\left[\{\hat{x}_{i_1}, \hat{x}_{j_1}\} = \{-1, 1\}\right] = \frac{2s(n-s)}{n(n-1)},$$

since there are $\frac{n(n-1)}{2}$ possible sets $\{\hat{x}_{i_1}, \hat{x}_{j_1}\}$ and $s(n-s)$ of them contain one 1 and one -1. For $k > 1$,

$$\Pr\left[\{\hat{x}_{i_k}, \hat{x}_{j_k}\} = \{-1, 1\} | \{\hat{x}_{i_l}, \hat{x}_{j_l}\} = \{-1, 1\} \text{ for } l \in [k-1]\right]$$
$$= \frac{2(s-k+1)(n-s-k+1)}{(n-2k+2)(n-2k+1)},$$

since the condition $\{\hat{x}_{i_l}, \hat{x}_{j_l}\} = \{-1, 1\}$ for $l \in [k-1]$ means that, among the remaining variables, there are $s-k+1$ variables $\hat{x}_j = -1$ and $n-s-k+1$ variables $\hat{x}_j = 1$ and $n-2k+2$ variables in total (and, given that, the $k = 1$ argument applies). Thus,

$$\Pr\left[\prod_{k=1}^{b} (\hat{x}_{i_k} - \hat{x}_{j_k})^2 = 1\right] = \frac{2^b s(s-1)\dots(s-b+1)(n-s)\dots(n-s-b+1)}{n(n-1)\dots(n-2b+1)}.$$

Since S is a symmetric polynomial, we have $S(\hat{x}') = S'(s')$ where S' is a polynomial of one variable s', with s' equal to the number of variables $\hat{x}'_j = -1$. Since there are b variables $\hat{x}_j = -1$ that do not appear in $\hat{x}'$, we have $s' = s - b$. This means that S' can be rewritten as a polynomial in s (instead of s').

5 Conclusion

In this paper we have shown that

$$\mathcal{E}\left(\mathrm{AND}_n\right) = \mathcal{E}\left(\mathrm{EQUALITY}_{n+1}\right) = \frac{1}{2} - \frac{n}{n^2+1}.$$

There is a natural way to generalize $\mathcal{E}(f)$ to any fixed number of queries t. We may denote it by $\mathcal{E}_t(f)$ and have

$$\mathcal{E}_t(f) = \min_{\mathcal{A}:\mathcal{A} \text{ performs } t \text{ queries}} \max_x \Pr[\text{algorithm } \mathcal{A} \text{ does not output } f(x)].$$

From the numerical experiments of Montanaro, Jozsa, and Mitchison (2015) it seems that the connection between $\mathrm{EQUALITY}_{n+1}$ and AND_n goes much deeper.

Conjecture 1. For all positive integers t and n:

$$\mathcal{E}_t\left(\mathrm{EQUALITY}_{n+1}\right) = \mathcal{E}_t\left(\mathrm{AND}_n\right).$$

Acknowledgements

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 600700 (QALGO), ERC Advanced Grant MQC, Latvian State Research programme NexIT project No.1.

References

Beals, Robert et al. (1998). "Quantum lower bounds by polynomials". In: *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*. FOCS '98. Washington, DC, USA: IEEE Computer Society, pp. 352–. ISBN: 0-8186-9172-7. URL: http://dl.acm.org/citation.cfm?id=795664.796425.

Belovs, Aleksandrs (2015). "Quantum algorithms for learning symmetric juntas via the adversary bound". In: *Comput. Complex.* 24.2. arXiv preprint: http://arxiv.org/abs/1311.6777, pp. 255–293. ISSN: 1016-3328. DOI: 10.1007/s00037-015-0099-2. URL: http://dx.doi.org/10.1007/s00037-015-0099-2.

Grover, Lov Kumar (1996). "A fast quantum mechanical algorithm for database search". In: *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*. ACM, pp. 212–219. URL: http://dl.acm.org/citation.cfm?id=237866.

Lee, Troy et al. (2016). "On the sum-of-squares degree of symmetric quadratic functions". In: *31st Conference on Computational Complexity (CCC 2016)*. Ed. by Ran Raz. Vol. 50. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 17:1–17:31. ISBN: 978-3-95977-008-8. DOI: http://dx.doi.org/10.4230/LIPIcs.CCC.2016.17. URL: http://drops.dagstuhl.de/opus/volltexte/2016/5838.

Miscenko-Slatenkova, Taisija (2012). "Quantum query algorithms". PhD thesis. University of Latvia, Faculty of Computing.

Montanaro, Ashley, Richard Jozsa, and Graeme Mitchison (2015). "On exact quantum query complexity". In: *Algorithmica* 71.4. arXiv preprint: http://arxiv.org/abs/1111.0475, pp. 775–796. ISSN: 1432-0541. DOI: 10.1007/s00453-013-9826-8. URL: http://dx.doi.org/10.1007/s00453-013-9826-8.

Serre, Jean-Pierre (1977). *Linear representations of finite groups*. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. New York: Springer-Verlag, p. 172. ISBN: 0-387-90190-6.

Shor, Peter Williston (1997). "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". In: *SIAM Journal on Computing* 26.5, pp. 1484–1509. URL: http://epubs.siam.org/doi/abs/10.1137/S0097539795293172.

Zalka, Christof (1999). "Grover's quantum searching algorithm is optimal". In: *Phys. Rev. A* 60 (4), pp. 2746–2751. DOI: 10.1103/PhysRevA.60.2746. URL: http://link.aps.org/doi/10.1103/PhysRevA.60.2746.

Received August 29, 2016 , accepted September 19, 2016