A Quantum Algorithm for Testing Junta Variables and Learning Boolean Functions via Entanglement Measure

Khaled El-Wazan *, Ahmed Younes †, and S. B. Doma ‡

1Department of Mathematics and Computer Science, Faculty of Science, Alexandria University, Egypt
2School of Computer Science, University of Birmingham, Birmingham, B15 2TT, United Kingdom

Abstract
Given a black-box representing an unknown Boolean function $f$ of $n$ variables, in this paper we propose a fast quantum algorithm to test whether or not a certain variable in the function $f$ is a junta variable. The proposed algorithm creates entanglement between the variable under test and an auxiliary qubit, where the entanglement is measured using concurrence measure to decide if the variable is junta. The paper shows applications to the proposed algorithm in learning and categorization of Boolean functions.

Keywords: Quantum algorithm; Junta variables; Property testing; Boolean function learning; Entanglement

1 Introduction
Quantum computers [1 2 3] are powerful probabilistic computational devices which harness quantum phenomena like entanglement and superposition, to create problem solving paradigms more powerful than that of classical counterpart [4]. For instance, L. Grover introduced an optimal quantum search algorithm [5 6] to search for an item among list of unstructured items in quadratic speed-up compared to classical search algorithms. Boyer et al. later generalized Grover search algorithm [7] to search for multiple items in a list of unstructured items, also in quadratic speed-up. P. Shor presented a quantum algorithm [8] to find the prime factors of integer numbers in polynomial time.

* khaled.elwazan@alex-sci.edu.eg
† ayounes@alexu.edu.eg
‡ sbdoma@yahoo.com
Einstein et al. were the first to characterize entanglement [9], and it was later discovered the potentials of such strange correlation as a useful resource for computations and information processing [10], with crucial utilization in many applications, for instance quantum search algorithm [11, 12] with reliable behavior, satellite-based quantum key distribution [13, 14], and quantum internet [15]. For those reasons, the need to create entanglement drives many experimental research groups to reach that goal, and recently there has been significant advances [16, 17, 18]. Still in many applications that utilize entanglement, it is necessary useful to detect such correlation and quantify it theoretically and experimentally. Many entanglement detection methods for bipartite and multipartite systems have been proposed [19, 20, 21, 22], based on popular entanglement measures [23], for instance, entanglement of formation, distance measurement and concurrence.

During the last two decades, the computation industry has been facing a real challenge due to the increasing amount of data [24] that needs to be handled and processed for certain purposes, and the increasing demand of the market to introduce faster computation devices that can cope up with the increasing amount of data as convenient as possible. One of the purposes for processing such data is the requirement to decide whether a given data has a certain property or not. But considering the enormous size of data, a classical algorithm testing all entries in that data for containing a certain property might not be practical or even feasible. One of the novel methods in property testing algorithms is quantum testing of classical properties, in which a quantum algorithm is utilized by harnessing quantum phenomena to introduce quantum speed-ups compared to classical property testing algorithms. The unique nature of quantum tester algorithms allows global extraction of properties and information about the input and the nature of the data itself by querying all the possible entries at the same time.

One of the important classical properties that gained attention lately in the last decade [25] is junta property testing. Let $f$ be a function that maps a binary vector to either 0 or 1, i.e. $f : \{0, 1\}^n \rightarrow \{0, 1\}$, a junta variable $x_i$ is an input variable to the function $f$ which the function does not depend on to perform such mapping. The junta property is considered an important typical problem, for instance, in machine learning techniques where it is vital to discriminate between relevant and irrelevant features to the learning process [26, 27].

The first quantum $k$-junta $\epsilon$-tester [28] for Boolean function and based on Fourier Sampling [29], due to Atıcı and Servedio in 2008, used $O(k/\epsilon)$ queries to the tested function, given the number of variables $k$ that the function depends on in advance. In addition, a quantum learning algorithm was introduced for $k$-junta Boolean functions to accuracy $\epsilon$ that required $O(k/\epsilon \log k)$ quantum examples and $O(2^k \log \epsilon^{-1})$ random examples.

In 2015, Li and Yang introduced a quantum algorithm [30] based on Bernstein-Vazirani algorithm [29] to measure the influence of variables in Boolean functions. They also discussed other learning probabilistic quantum algorithms for quadratic and cubic functions of simple forms.

Ambainis et al. presented a quantum algorithm [31] for testing junta func-
In 2017, we introduced a quantum algorithm [33] to test junta variables in Boolean functions, based on a quantum search algorithm [11] with reliable behavior. This algorithm required two oracle calls to the black-box representing the function to create a superposition with certain properties for junta variable testing. This algorithm required $O(\sqrt{2^n})$ oracle calls, where $n$ is the number of input variables to the Boolean function.

The aim of this paper is to present a quantum algorithm for testing variables in Boolean functions for the junta property. The proposed algorithm transforms the problem of testing junta property in variables to measuring entanglement between qubits, using a reliable entanglement measure. The proposed algorithm uses a quantum operator $U_{\lambda}$ that creates entanglement between the tested variable $x_i$ for the junta property and an auxiliary qubit, if and only if the tested qubit is in superposition. The proposed algorithm is further used to find variables residing with the tested variable $x_i$ in function definition, and to discriminate between constant, balanced or Boolean functions of other form.

This paper is organized as follows: Section 2 introduces the basic necessary concepts. Section 3 describes the proposed operator $U_{\lambda}$. Section 4 will cover the proposed algorithm along with the analysis. Section 5 introduces applications of the proposed algorithm for learning Boolean functions, followed by a conclusion in Section 6.

2 Preliminaries

2.1 Problem Definition

One of the important classical properties that might exist in a data set is the junta property. We define the problem of finding whether a variable is relevant or irrelevant to a given Boolean function as follows:

**Definition 2.1.** Given a data set $\Lambda$ of all possible vectors of size $N = 2^n$, and a Boolean function $f(x_0, x_1, \cdots, x_{n-1})$ which is used to map each vector $x \in \Lambda$ to either $\{0, 1\}$, it is required to find whether the variable $x_i$ in the Boolean function contributes to mapping the input $x \in \Lambda$ to either 0 or 1.

For $k$ input variables such that $k \leq n$, we say that a Boolean function $f$ is a $k$-junta function, if this Boolean function depends on at most $k$ out of its $n$ input variables.

For a linear Boolean function represented in positive polarity Reed-Muller [34]:

$$f(x_0, x_1, \cdots, x_{n-1}) = c_0x_0 \oplus c_1x_1 \oplus \cdots \oplus c_{n-1}x_{n-1}$$

$$= \bigoplus_{i=0}^{n-1} c_ix_i$$

(2.1)
where $⊕$ is the addition modulo 2 and the coefficient $c_i$ dictates whether the variable $x_i$ resides in the function definition or not, Bernstein-Vazirani algorithm [29] can be used to find the exact solution of this form of functions in $O(1)$, from which we can identify the junta variables. In this paper, we are interested to test if a given variable is junta in a general form function [34]:

$$f(x_0, x_1, \ldots, x_i, \ldots, x_{n-1}) = \bigoplus_{q=0}^{N-1} c_q P_q ,$$  \hspace{1cm} (2.2)

where

$$P_q : \text{product term}$$

$$c_q = \begin{cases} 
0 : \text{product term does not exist} \\
1 : \text{product term exists}
\end{cases}$$

2.2 Measures of Entanglement

**Definition 2.2.** Given a quantum system $|\varphi\rangle$ of 2 qubits, the pure bipartite state $|\varphi\rangle$ is called separable or a product state, if we can find states $|\phi_A\rangle$ and $|\phi_B\rangle$ in Hilbert space $\mathcal{H}$ of dimension 2 such that

$$|\varphi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle,$$  \hspace{1cm} (2.3)

otherwise, the state $|\varphi\rangle$ is called entangled.

Concurrence measure [35] is considered one of the most popular measures of entanglement quantification of bipartite systems, and can be defined as follows [36]:

$$C(|\varphi\rangle) = |\langle \varphi | \sigma_y \otimes \sigma_y | \varphi \rangle|^\frac{1}{2}$$  \hspace{1cm} (2.4)

where $\sigma_y = -i|1\rangle\langle 0| + i|0\rangle\langle 1|$, such that $i = \sqrt{-1}$.

3 The Proposed Operator

**Definition 3.1.** Let’s assume having a quantum register of $n$ qubits and given 2 qubits indexed $i$ and $j$ in this quantum register. An entanglement measure device $D_{i,j}$ is a device which measures the entanglement between those designated qubits. This defined device can be illustrated as in Figure [1].
Our proposed operator $U_i^\lambda$ to check whether a variable $x_i$ is a junta variable or not, will act on a given qubit indexed $i$ and an auxiliary qubit initialized to state $|1\rangle$, as depicted in Figure 2.

The operator $U_\lambda$, firstly, applies CNOT gate on $x_i$ as the control qubit and the auxiliary qubit as a target qubit, and then measures the entanglement between those qubits. It is worth noting that the entanglement will happen if and only if the tested qubit is in a superposition. For further elaboration, let’s examine a system $|\varphi\rangle$ of 2 qubits one of which is in a superposition. The system can be described as follows:

$$|\varphi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |1\rangle,$$

where $\alpha$ and $\beta$ are complex numbers named the amplitudes and satisfy the relation $|\alpha|^2 + |\beta|^2 = 1$.

When we apply CNOT on the system as described earlier, the effect can be illustrated as follows:

$$|\varphi^*\rangle = CNOT|\varphi\rangle = \alpha|01\rangle + \beta|10\rangle,$$
where the second qubit is entangled with the first qubit. According to Equation (2.4) and for the given bipartite quantum state $|\varphi^*\rangle$, the concurrence can be restated as follows [30]:

$$C(|\varphi^*\rangle) = 2|\alpha\beta|.$$  

(3.3)

4 A Quantum Algorithm for Testing Variables for the Junta Property

4.1 The Proposed Algorithm

In this section, we propose a quantum algorithm that tests whether a variable $x_i$ is a junta variable or not, utilizing the entanglement between the tested qubit and an auxiliary qubit.

$$|\psi_0\rangle = |0\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle.$$  

(4.1)

The algorithm is carried quantum mechanically as follows:

1. **Linearity Check.** Check whether the variable $x_i$ exists in a linear term, as follows:

   (a) Prepare a vector $v_0$ of size $n$ initialized with the state $|0\rangle$. If $f(v_0) = 1$, this will mean that the black-box $U_f$ has a constant term.

   (b) Prepare a vector $v_1$ of size $n$ initialized with the state $|0\rangle$ except for a $|1\rangle$ at position $i$.

   (c) If $f(v_1) = 0$ and $f(v_0) = 1$, or $f(v_1) = 1$ and $f(v_0) = 0$, this will mean that the black-box $U_f$ has the variable $x_i$ in a linear term. The variable $x_i$ is then considered not a junta variable, and exit.

2. **Register Preparation.** Prepare a quantum register of $n + 2$ qubits. The first $n$ qubits in the state $|0\rangle$ and the extra two qubits in the state $|1\rangle$:

$$|\psi_0\rangle = |0\rangle^\otimes n \otimes |1\rangle \otimes |1\rangle.$$  

(4.1)

3. **Register Initialization.** Apply the Hadamard gate on each qubit of the first $n + 1$ qubits to create a uniform superposition of all the possible $N$ states:
\[ |\psi_1\rangle = H^\otimes (n+1)|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} |l\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes |1\rangle. \quad (4.2) \]

4. **Apply the oracle \( U_f \).** Applying the oracle \( U_f \) will mark the solutions satisfying the Boolean function \( f \) with a phase shift:

\[ |\psi_2\rangle = U_f |\psi_1\rangle = \frac{1}{\sqrt{N}} \left( \sum_{l=0}^{N-1} \hat{f}(l) |l\rangle - \sum_{l=0}^{N-1} l |l\rangle \right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes |1\rangle, \quad (4.3) \]

where \( \sum' \) are the states that satisfy the oracle and marked with a phase shift, and \( \sum'' \) otherwise.

5. **Apply Hadamard on the Register.** Applying Hadamard gates on the first \( n+1 \) qubits will put the system in a state that can be described using the language of Fourier analysis as follows:

\[ |\psi_3\rangle = \sum_{l=0}^{N-1} \hat{f}(l) |l\rangle \otimes |1\rangle \otimes |1\rangle, \quad (4.4) \]

where \( \hat{f}(l) \) is the Fourier coefficient of the quantum state \( |l\rangle \) and is defined as follows:

\[ \hat{f}(l) = \frac{1}{N} \sum_{s=0}^{2^n-1} (-1)^{f(l)+l \cdot s}, \quad (4.5) \]

and \( l \cdot s = \sum_{a=0}^{n-1} l_a s_a \) is the inner product of the binary strings \( l \) and \( s \).

6. **Apply the Operator \( U_{\lambda} \).** Ignoring the other qubits when applying the oracle \( U_{\lambda} \) on the qubit indexed \( i \) and the auxiliary qubit, the subsystem \( |\psi_4^i\rangle \) can be described as follows:

\[ |\psi_4^i\rangle = (\alpha_i |0\rangle + \beta_i |1\rangle) \otimes |1\rangle, \quad (4.6) \]

and the effect of \( U_{\lambda} \) on \( |\psi_3\rangle \) can be viewed for \( |\psi_5^i\rangle \) as:

(a) **Apply the CNOT gate.**

\[ |\psi_5^i\rangle = CNOT(\alpha_i |0\rangle + \beta_i |1\rangle) \otimes |1\rangle \]

\[ = \alpha_i |0, 1 \oplus CNOT(0)\rangle + \beta_i |1, 1 \oplus CNOT(1)\rangle. \quad (4.7) \]
(b) Measure the entanglement between the qubit indexed \( i \) and the auxiliary qubit. If there is no entanglement measured, then the variable \( x_i \) is considered a junta variable, otherwise the variable \( x_i \) is not junta variable.

### 4.2 Analysis of the Proposed Algorithm

In this section, we discuss the proposed algorithm with the suggested operator introduced in Section 3. We will analyze the proposed algorithm assuming that the given oracle is a black-box.

In [30], Yang et al. was able to formulate an expression of the influence of the variable \( x_i \) on the Boolean function \( f \) using Bernstein-Vazirani algorithm:

\[
I_f(x_i) = \frac{|\nu_1|}{N},
\]

where \( \nu_1 \) is the set of all states \( x \in \Lambda \) that satisfies the relation [30]:

\[
x \in \{0, 1\}^n f(x \oplus \tau) + f(x) = 1,
\]

and \( \tau \) is a binary string of 0s except for a 1 at position \( i \).

We can say as well that

\[
|\nu_0| + |\nu_1| = N,
\]

where \( \nu_0 \) is the set of all states \( x \in \{0, 1\}^n \) that satisfies the relation [30]:

\[
x \in \{0, 1\}^n f(x \oplus \tau) + f(x) \neq 1.
\]

From Equation (4.10), we have

\[
\frac{|\nu_0|}{N} + \frac{|\nu_1|}{N} = 1,
\]

and for a single qubit indexed \( i \) in a quantum system \( |\psi\rangle \), we can state the following:

\[
|\psi_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle,
\]

where \( |\alpha_i|^2 = |\nu_0|/N \) and \( |\beta_i|^2 = |\nu_1|/N \).

#### In case the function \( f \) is independent of the variable \( x_i \)

When the function \( f \) is independent from the variable \( x_i \), i.e. the variable \( x_i \) is a junta variable, then the variable \( x_i \) will have no influence on the function \( f \), i.e. \( |\nu_1| = 0 \), thus the subsystem described in Equation (4.7) will be:

\[
|\psi_i^4\rangle = |01\rangle,
\]

and will produce no measurable entanglement between the indicated qubits, i.e. \( C(|\psi_i^4\rangle) = 0 \).
In case the function \( f \) is dependent on the variable \( x_i \). When the function \( f \) is dependent on the variable \( x_i \), i.e. \( x_i \) is not junta, then the variable \( x_i \) will have an influence \( I_f(x_i) \neq 0 \) on the function \( f \), and the subsystem in Equation (4.7) can be described as follows:

\[
\psi_4^{i} = \alpha_i|01\rangle + \beta_i|10\rangle,
\] (4.15)

and will produce a measurable entanglement between the indicated qubits, and the concurrence between those qubits:

\[
C(|\psi_4^i\rangle) = \frac{2 \times |\nu_0| \times |\nu_1|}{N^2}.
\] (4.16)

In the case that the variable \( x_i \) exists in the function \( f \) but only as a linear term, the final state will be \( |\psi_4^i\rangle = |10\rangle \) with no measurable entanglement. This case can be handled by detecting whether or not the variable \( x_i \) exists as a linear term in the function \( f \), as covered in Step 1 of the proposed algorithm.

5 Applications of the Proposed Operator for Learning Boolean Functions

5.1 Finding Variables within the Same Terms

In [33], we constructed an oracle \( U_g \) using 2 copies of a given black-box \( U_f \), and acting on \( n + 1 \) qubits. The oracle \( U_g \) is defined as follows:

\[
U_g = U_{f_x} U_f.
\] (5.1)

An illustration of this circuit is shown in Figure 4.

![Quantum Circuit](image)

Figure 4: A quantum circuit for the constructed oracle \( U_g \) [33].

This oracle \( U_g \) has a unique property: \( U_g = I_n \), if and only if \( x_i \) is a junta variable, where \( I_n \) is the identity matrix of size \( 2^n \times 2^n \). The effect of the
constructed oracle $U_g$ can be illustrated as follows. For any general Boolean function $f$ of $n$ input variables, the function $f$ can be generally defined in terms of a variable $x_i$ as follows [33]:

$$f(x_0, \cdots, x_i, \cdots, x_{n-1}) = f_{+x_i} \oplus f_{-x_i}, \tag{5.2}$$

such that $f_{+x_i}$ are the terms which contain the variable $x_i$, and $f_{-x_i}$ are the terms which do not contain the variable $x_i$. We define the function $g$ such that

$$g = f \oplus f_{\bar{x}_i}, \tag{5.3}$$

where $f_{\bar{x}_i} = f(x_0, \cdots, \bar{x}_i, \cdots, x_{n-1})$ and $f$ as in Equation (5.2).

The function $g$ can be defined as Equation (5.2) as follows [33]:

$$g = f_{+x_i} \oplus f_{+\bar{x}_i}, \tag{5.4}$$

such that $f_{+\bar{x}_i}$ are the terms which had the variable $x_i$ and are decomposed to lower order terms that do not have the variable $x_i$.

In this section, we will propose an algorithm to find the variables that exist in the same terms with the variable $x_i$, if there is any. Consider the proposed algorithm in Section 4 as a subroutine $PA(Oracle \ U, Index \ p)$ that takes an oracle $U$ and the index $p$ of the desired variable for the junta test and returns true if and only if $x_p$ is junta. The steps of the proposed algorithm is carried as follows:

1. If $PA(U_f, i) = true$, exit.
2. Create a set $\mathcal{S} = \{\}$.  
3. Construct the oracle $U_g$ for the variable $x_i$.
4. Set $t = 0$.
5. $Q = PA(U_g, t)$.
6. If $Q \neq true$, add $t$ to the set $\mathcal{S}$.
7. If $t < n$, $t = t + 1$ and go to step 5.

5.2 Boolean Function Categorization

A balanced Boolean function is a function which outputs as many 1s as 0s over its possible input $\Lambda$, meanwhile, a constant Boolean function is such a function which always yield either 1 or 0, i.e. $\forall x \in \Lambda. f : x \to \{0\}$ or $f : x \to \{1\}$. Deutsch and Jozsa introduced an exact quantum algorithm [37] that solved the problem of identifying whether a given black-box is a balanced Boolean function or a constant Boolean function. Given a black-box, we propose an application of the proposed procedure that can test whether that given black-box represents a constant, balanced or Boolean function of other form, using a variation of Bernstein-Vazirani algorithm. The algorithm is carried quantum mechanically as follows:
1. **Register Preparation.** Prepare a quantum register of \( n + 2 \) qubits and set the first \( n + 1 \) with the state \( |0\rangle \) and the extra qubit with the state \( |1\rangle \).

\[
|\psi_0\rangle = |0\rangle^{\otimes n+1} \otimes |1\rangle.
\] (5.5)

2. **Register Initialization.** Apply Hadamard gates on the first \( n \) qubits to get a perfect superposition of all \( N \) states.

\[
|\psi_1\rangle = H^{\otimes n} |\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} |l\rangle \otimes |0\rangle \otimes |1\rangle.
\] (5.6)

3. **Apply the Oracle \( U_f \).** Applying the oracle \( U_f \) will yield a quantum system that can be generally expressed as follows:

\[
|\psi_2\rangle = U_f |\psi_1\rangle = \left( \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} |l\rangle \otimes |f(l)\rangle \otimes |1\rangle \right) \otimes |1\rangle
\]

\[
= \left( \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} |l\rangle \otimes |0\rangle + H \sum_{l=0}^{N-1} |l\rangle \otimes |1\rangle \right) \otimes |1\rangle
\] (5.7)

where \( \sum' \) represents the \( M \) states that satisfy the oracle \( U_f \) marked with entanglement, and \( \sum'' \) otherwise.

4. **Apply Hadamard on the Register.** Applying Hadamard gates on the first \( n \) qubits of the system will transform the system to the following:

\[
|\psi_3\rangle = H^{\otimes n} |\psi_2\rangle = \left( \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} H|l\rangle \otimes |0\rangle + \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} H|l\rangle \otimes |1\rangle \right) \otimes |1\rangle
\]

\[
= \left( \sum_{l=0}^{N-1} \hat{f}_0(l)|l\rangle \otimes |0\rangle + \sum_{l=0}^{N-1} \hat{f}_1(l)|l\rangle \otimes |1\rangle \right) \otimes |1\rangle,
\] (5.8)

where \( \hat{f}_0 \) and \( \hat{f}_1 \) are

\[
\hat{f}_0(l) = \frac{1}{N} \sum_{s=0}^{N-1} ''(-1)^{l \cdot s},
\]

\[
\hat{f}_1(l) = \frac{1}{N} \sum_{s=0}^{N-1} '(-1)^{l \cdot s}.
\]
5. **Apply the Operator** $U_n^\lambda$. Applying $U_n^\lambda$ on the quantum system, will yield a subsystem:

$$|\psi_n^4\rangle = \alpha_n |01\rangle + \beta_n |10\rangle,$$

and the measured concurrence $C(|\psi_n^4\rangle)$ can be expressed as follows:

$$C(|\psi_n^4\rangle) = 2 \times \frac{M(N - M)}{N^2}. \quad (5.10)$$

If $C = 0$, then the given oracle represents a constant Boolean function, and if $C = 1/2$ then the oracle represents a balanced Boolean function, but otherwise this will mean that the black-box represents a Boolean function of other form.

One of the potential applications of the proposed Boolean function categorization algorithm is that it can be utilized to know the number of solutions $M$ to any given black-box by solving Equation (5.10) for unknown $M$.

### 6 Conclusion

In this paper, we proposed a fast quantum algorithm that uses entanglement to test the junta property of a certain variable in a Boolean function given as a black-box. We transformed the junta variable testing to measuring entanglement between the variable being tested and an auxiliary qubit.

The algorithm creates entanglement between the tested variable and the auxiliary qubit if the variable being tested is not a junta variable. If the variable being tested is a junta variable, there will be no measurable entanglement using concurrence measure, otherwise the variable is considered not junta. To test whether a Boolean function is a $k$-junta function or not will require $O(n)$ oracle calls.

The paper also introduced applications for learning any black-box that represents an unknown Boolean function regardless of its form. The first learning algorithm finds the variables in the same product terms with the variable under test using $O(n)$ oracle calls. The second application is to categorize any given black-box representing an unknown Boolean function to either constant, balanced or a Boolean function of other form.

### Acknowledgment

We would like to thank Prof. Mahmoud Abdel-Aty, Dr. Abdel-Haleem Abdel-Aty and Mohammed Zidan for their valuable suggestions on entanglement concurrence measure.

### References

[1] R. P. Feynman and I. Meeting, “Quantum Mechanical Computers 1,” vol. 16, no. 6, pp. 507–531, 1986.
[2] D. Deutsch, “Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer,” Proc. Roy. Soc. A, vol. 400, no. 1818, pp. 97–117, 1985. [Online]. Available: http://rspa.royalsocietypublishing.org/cgi/doi/10.1098/rspa.1985.0070

[3] S. Lloyd, “A potentially realizable quantum computer.” Science, vol. 261, no. 5128, pp. 1569–1571, 1993. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/17798117

[4] H. Buhrman, R. Cleve, and A. Wigderson, “Quantum vs. Classical Communication and Computation,” pp. 63–68, 1998. [Online]. Available: http://arxiv.org/abs/quant-ph/9802040

[5] L. K. Grover, “Quantum Mechanics Helps in Searching for a Needle in a Haystack,” Phys. Rev. Lett., vol. 79, p. 325, 1997. [Online]. Available: http://arxiv.org/abs/quant-ph/9706033

[6] C. Zalka, “Grover’s quantum searching algorithm is optimal.” Phys. Rev. A, vol. 60, no. 4, pp. 2746–2751, 1999. [Online]. Available: http://arxiv.org/abs/quant-ph/9711070

[7] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, “Tight bounds on quantum searching,” arXiv preprint quant-ph/9605034, vol. 46, no. May, p. 8, 1996. [Online]. Available: http://arxiv.org/abs/quant-ph/9605034

[8] P. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” SIAM J. Comput., vol. 26, no. 5, pp. 1484–1509, 1997. [Online]. Available: http://epubs.siam.org/doi/pdf/10.1137/S0097539795293172

[9] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?” Phys. Rev., vol. 47, no. 10, p. 777, 1935.

[10] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, 2010.

[11] A. Younes, J. Rowe, and J. Miller, “Enhanced quantum searching via entanglement and partial diffusion,” Physica D., vol. 237, no. 8, pp. 1074–1078, 2008.

[12] A. Younes, “Constant-Time Quantum Algorithm For The Unstructured Search Problem,” p. 11, 2008. [Online]. Available: http://arxiv.org/abs/0811.4247

[13] C. J. Pugh, S. Kaiser, J.-P. Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B. L. Higgins, and T. Jennewein, “Airborne demonstration of a quantum key distribution receiver payload,” 2016. [Online]. Available: http://arxiv.org/abs/1612.06396
[14] S.-k. Liao, W.-q. Cai, W.-y. Liu, L. Zhang, Y. Li, J.-g. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, “Satellite-to-ground quantum key distribution,” Arxiv, 2017. [Online]. Available: http://arxiv.org/abs/1707.00542

[15] Q.-C. Sun, Y.-L. Mao, S.-J. Chen, W. Zhang, Y.-F. Jiang, Y.-B. Zhang, W.-J. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang, T.-Y. Chen, L.-X. You, X.-F. Chen, Z. Wang, J.-Y. Fan, Q. Zhang, and J.-W. Pan, “Quantum teleportation with independent sources and prior entanglement distribution over a network,” Nat. Photonics, vol. 10, no. 10, pp. 671–675, 2016. [Online]. Available: http://www.nature.com/doifinder/10.1038/nphoton.2016.179

[16] J. Hald, J. L. Sørensen, C. Schori, and E. S. Polzik, “Spin Squeezed Atoms: A Macroscopic Entangled Ensemble Created by Light,” Phys. Rev. Lett., vol. 83, no. 7, pp. 1319–1322, 1999.

[17] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-al kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt, “Scalable multiparticle entanglement of trapped ions,” Nature, vol. 438, no. 7068, pp. 643–646, 2005. [Online]. Available: http://www.nature.com/doifinder/10.1038/nature04279

[18] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan, “Experimental entanglement of six photons in graph states,” Nat. Phys., vol. 3, no. 2, pp. 91–95, 2007. [Online]. Available: http://www.nature.com/doifinder/10.1038/nphys507

[19] M. Li, M. J. Zhao, S. M. Fei, and Z. X. Wang, “Experimental detection of quantum entanglement,” Front. Phys., vol. 8, no. 4, pp. 357–374, 2013.

[20] L. Zhou and Y. B. Sheng, “Concurrence measurement for the two-qubit optical and atomic states,” Entropy, vol. 17, no. 6, pp. 4293–4322, 2015.

[21] L. H. Zhang, M. Yang, and Z. L. Cao, “Direct measurement of the concurrence for two-photon polarization entangled pure states by parity-check measurements,” Phys. Lett. A, vol. 377, no. 21-22, pp. 1421–1424, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.physleta.2013.04.018

[22] B. Regula and G. Adesso, “Entanglement Quantification Made Easy: Polynomial Measures Invariant under Convex Decomposition,” Phys. Rev. Lett., vol. 116, no. 7, pp. 1–5, 2016.

[23] O. Gühne and G. Tóth, “Entanglement detection,” Phys. Rep., vol. 474, no. 1-6, pp. 1–75, 2009. [Online]. Available: http://dx.doi.org/10.1016/j.physrep.2009.02.004
[24] McKinsey & Company, “Big data: The next frontier for innovation, competition, and productivity,” *McKinsey Global Institute*, no. June, p. 156, 2011.

[25] A. Montanaro and R. D. Wolf, “A Survey of Quantum Property Testing,” pp. 1–66, 2014.

[26] A. L. Blum, “Relevant Examples and Relevant Features: Thoughts from Computational Learning Theory,” *AAAI Fall Symposium on Relevance*, 1994.

[27] A. L. Blum and P. Langley, “Selection of relevant features and examples in machine learning,” *Artificial Intelligence*, vol. 97, no. 1-2, pp. 245–271, 1997.

[28] A. Acai and R. A. Servedio, “Quantum algorithms for learning and testing juntas,” *Quantum Inf. Process.*, vol. 6, no. 5, pp. 323–348, 2007.

[29] E. Bernstein and U. Vazirani, “Quantum Complexity Theory,” *SIAM J. Comput.*, vol. 26, no. 5, pp. 1411–1473, 1997.

[30] H. Li and L. Yang, “A quantum algorithm for approximating the influences of Boolean functions and its applications,” *Quantum Inf. Process.*, vol. 14, no. 6, pp. 1787–1797, 2015.

[31] A. Ambainis, A. Belovs, O. Regev, and R. de Wolf, “Efficient Quantum Algorithms for (Gapped) Group Testing and Junta Testing,” pp. 903–922, 2015. [Online]. Available: [http://arxiv.org/abs/1507.03126](http://arxiv.org/abs/1507.03126)

[32] A. Sterrett, “On the detection of defective members of large populations,” *The Annals of Mathematical Statistics*, vol. 28, no. 4, pp. 1033–1036, 1957.

[33] K. El-Wazan, A. Younes, and S. B. Doma, “A Quantum Algorithm for Testing Juntas in Boolean Functions,” pp. 1–13, 2017. [Online]. Available: [http://arxiv.org/abs/1701.02143](http://arxiv.org/abs/1701.02143)

[34] A. Younes and J. Miller, “Representation of Boolean Quantum Circuits as Reed-Muller Expansions,” pp. 1–12, 2003. [Online]. Available: [http://arxiv.org/abs/quant-ph/0305134](http://arxiv.org/abs/quant-ph/0305134)

[35] S. Hill and W. K. Wootters, “Entanglement of a Pair of Quantum Bits,” *Phys. Rev. Lett.*, vol. 78, no. 26, pp. 5022–5025, 1997. [Online]. Available: [https://link.aps.org/doi/10.1103/PhysRevLett.78.5022](https://link.aps.org/doi/10.1103/PhysRevLett.78.5022)

[36] S. P. Walborn, P. H. Souto Ribeiro, L. Davidovich, F. Mintert, and A. Buchleitner, “Experimental determination of entanglement with a single measurement,” *Nature*, vol. 440, no. 7087, pp. 1022–1024, 2006. [Online]. Available: [http://www.nature.com/doifinder/10.1038/nature04627](http://www.nature.com/doifinder/10.1038/nature04627)

15
[37] D. Deutsch and R. Jozsa, “Rapid Solution of Problems by Quantum Computation,” Proc. Roy. Soc. A, vol. 439, no. 1907, pp. 553–558, 1992. [Online]. Available: http://rspa.royalsocietypublishing.org/cgi/doi/10.1098/rspa.1992.0167