Characterizations of symmetric partial Boolean functions with exact quantum query complexity ——Deutsch-Jozsa Problem

Daowen Qiu

School of Data and Computer Science

Sun Yat-sen University, China

Joint work with Shenggen Zheng

arXiv:1603.06505(Qiu and Zheng)

2017AQIS

September 4-8, 2017, NUS, Singapore

Abstract

In this talk, I would like to report a recent work regarding:

1. An optimal exact quantum query algorithm for generalized Deutsch-Jozsa problem

2. The characterization of all symmetric partial Boolean functions with exact quantum 1-query complexity

Basic background

- **Discover more problems to show that quantum computing is more powerful than classical computing**
- **These problems have the potential of applications in other areas such as cryptography.**

Outline

- 1. Motivations, Problems, Results
- 2. Preliminaries
- 3. Main Results
- 4. Methods of Proofs
- 5. Conclusions & Further Problems

1. Motivations, Problems, Results

- **(1) Generalized Deutsch-Jozsa**
- **(2) Problems with exact quantum 1-query complexity**

Motivation I

- The Deutsch-Jozsa promise problem [DJ'92]:

$x \in \{0,1\}^n$, $|\mathrm{x}|$ is the Hamming weight of x,

$$DJ(x) = \begin{cases} 0 & if\,|\mathrm{x}| = 0 \; or \; |\mathrm{x}| = n \\ 1 & if\;|\mathrm{x}| = n/2 \end{cases}$$

$$Q_E(DJ) = 1, D(DJ) = \frac{n}{2} + 1$$

- $DJ_n^1 = \begin{cases} 0 & if\,|\mathrm{x}| \le 1 \;\; or\,|\mathrm{x}| \ge n-1 \\ 1 & if\,|\mathrm{x}| = n/2 \end{cases}$ [MJM'15]

$$Q_E(DJ_n^1) \le 2$$

[DJ'92] D. Deutsch, R. Jozsa, Rapid solution of problems by quantum computation, In Proceedings of the Royal Society of London, 439A (1992): 553—558.
[MJM'15] A. Montanaro, R. Jozsa, G. Mitchison, On exact quantum query complexity, Algorithmica**419** (2015) 775--796.

Problem I

- $DJ_n^k = \begin{cases} 0 & if\,|\mathrm{x}| \leq k \;\; or\;|\mathrm{x}| \geq n-k \\ 1 & if\,|\mathrm{x}| = n/2 \end{cases}$ **?**

➢Our result:

Theorem 1 $Q_E\left(DJ_n^k\right) = k+1$ and $D\left(DJ_n^k\right) = n/2+k+1$.

Motivation II

Deutsch-Jozsa problem that is a symmetric partial Boolean function can be solved by DJ algorithm (exact quantum 1-query algorithm). Then how to characterize the other symmetric partial Boolean functions with exact quantum 1-query complexity? Can such functions be solved by DJ algorithm?

Problem and Result II

- What can be solved with exact quantum 1-query complexity?

Our result:

- Theorem 2 Any symmetric partial Boolean function f has $Q_E(f) = 1$ if and only if f can be computed by the Deutsch-Jozsa algorithm.

Preliminaries

- Symmetric partial Boolean functions
- Classical query complexity
- Quantum query complexity
- Multilinear polynomials

Symmetrical partial Boolean functions

- Let f be a Boolean function from $D \subseteq \{0,1\}^n$ to $\{0,1\}$. If $D = \{0,1\}^n$, then f is called a total Boolean function. Otherwise, f is called a partial Boolean function or a promise problem.
- A Boolean function f is called symmetric if $f(x)$ only depends on the Hamming weight (i.e. $|x|$) of x, that is, if $|x| = |y|$, then $f(x) = f(y)$.
- Given a partial Boolean function f with its domain of definition $D \subseteq \{0,1\}^n$, if for any $x \in D$, and $y \in \{0,1\}^n$, with $|x| = |y|$, we have $y \in D$, and $f(x) = f(y)$, then f is called a symmetrical partial Boolean function.

Representation of symmetric partial Boolean functions

- Given a partial symmetric function $f:\{0,1\}^n \to \{0,1\}$, with the domain D of definition, it can be equivalently described by a vector $(b_0, b_1, \dots, b_n) \in \{0,1,*\}^{n+1}$, where $f(x) = b_{|x|}$, i.e. b_k is the value of $f(x)$ when $|x| = k$, and $f(x)$ is `undefined' for $b_{|x|} = *$.

- Example

$$f(x) = x_1 \vee x_2 \qquad b = (b_0, b_1, b_2) = (0,1,1)$$

$$f(x) = x_1 \wedge x_2 \qquad b = (b_0, b_1, b_2) = (0,0,1)$$

Isomorphism of symmetric partial Boolean functions

- Two symmetric partial functions f and g over $\{0,1\}^n$ are isomorphic if they are equal up to negations and permutations of the input variables, and negation of the output variable.
- Concerning the n-bit symmetric partial functions, it is clear that the following four functions are isomorphic to each other:

$$(b_0, b_1, \ldots, b_n) \, ; \qquad (b_n, b_{n-1}, \ldots, b_0);$$
$$(\bar{b}_0, \bar{b}_1, \ldots, \bar{b}_n); \qquad (\bar{b}_n, \bar{b}_{n-1}, \ldots, \bar{b}_0).$$

Another simple example:

$$f(x) = x_1 \vee x_2 \qquad b = (b_0, b_1, b_2) = (0,1,1)$$
$$g(x) = x_1 \wedge x_2 \qquad b = (b_0, b_1, b_2) = (0,0,1)$$

Classical query complexity

- An exact classical (deterministic) query algorithm to compute a Boolean function $f: \{0,1\}^n \to \{0,1\}$ can be described by a decision tree.

- If the output of a decision tree is $f(x)$, for all $x \in \{0,1\}^n$, the decision tree is said to "compute" f. The depthof a tree is the maximum number of queries that can happen before a leaf is reached and a result obtained.
- $D(f)$, the deterministic decision tree complexity of f is **the smallest depth** among all deterministic decision trees that compute f.

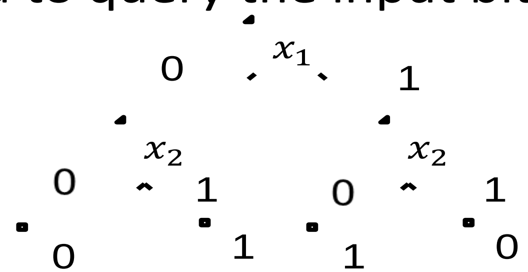
Example

- Deterministic query complexity

  (how many times we need to query the input bits)

- Example:

  $f(x_1, x_2) = x_1 \oplus x_2$



- Decision tree

The minimal depth over all decision trees computing f is the exact classical query complexity (deterministic query complexity, decision tree complexity) $D(f)$.

Quantum query algorithms

- Quantum T -query algorithm (its complexity is T)

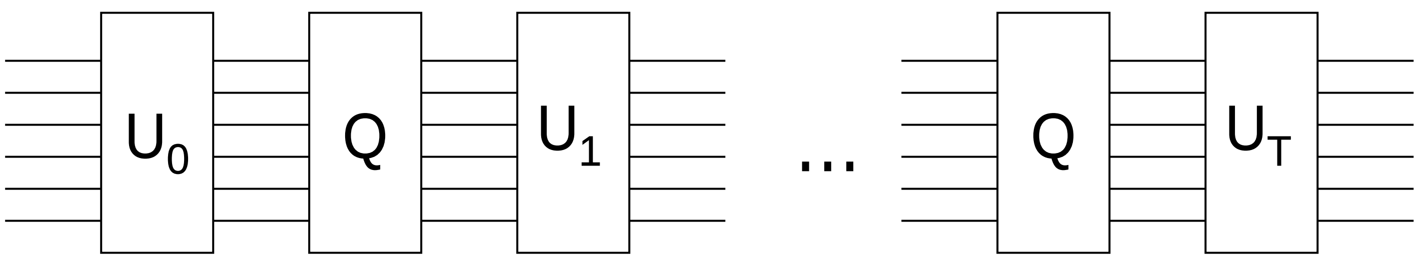
$f:\{0,1\}^n \rightarrow \{0,1\}$, input bit string $x = x_1 \cdots x_n$

We consider a Hilbert space $\mathcal{H}$ with basis state $|i, j\rangle$ for

$i \in \{0,1, \dots, n\}, j \in \{1, \dots, m\}$ (m can be chosen arbitrarily)

A T-query quantum algorithm:

$$|\psi_f\rangle = U_T Q_x U_{T-1} Q_x \cdots Q_x U_1 Q_x U_0 \, |\psi_s\rangle,$$



Black box

A T-query quantum algorithm:

$$|\psi_f\rangle = U_T Q_x U_{T-1} Q_x \cdots Q_x U_1 Q_x U_0 \, |\psi_s\rangle,$$

and then the algorithm performs a measurement,

where

$Q_x|i,j\rangle = (-1)^{x_i}|i,j\rangle$ for $i \in \{1, \dots, n\}$

$Q_x|0,j\rangle = |0,j\rangle$

$$|i,j\rangle \longrightarrow \boxed{Q_x} \longrightarrow (-1)^{x_i}|i,j\rangle$$

- Deutsch-Jozsa's query box, Grover's query box

$$|i\rangle \longrightarrow \boxed{Q_x} \longrightarrow (-1)^{x_i}|i\rangle$$

Quantum query complexity

The final state is then measured with a measurement $\{M_0, M_1\}$. For an input $x \in \{0,1\}^n$, we denote $A(x)$ the output of the quantum query algorithm A.

- We say that the quantum query algorithm A computes f within an error ε if for every input $x \in \{0,1\}^n$ it holds that $\Pr[A(x) = f(x)] \geq 1 - \varepsilon$.
- If ε=0, we says that the quantum algorithm is **exact**.
- $Q_\varepsilon(f), Q(f), Q_E(f)$ are **the smallest T** among all quantum query algorithms that compute f (with error ε, bounded-error, exact, respectively).

Multilinear polynomials

Every Boolean function $f: \{0,1\}^n \rightarrow \{0,1\}$ has a unique representation as an n-variate multilinear polynomial over the reals, i.e., there exist real coefficients a_S such that

$$f(x_1, \dots, x_n) = \sum_{S \subseteq [n]} a_S \prod_{i \in S} x_i$$

The degree of f is the degree of its largest monomial:

$\deg(f) = \max\{|S| : a_S \neq 0\}$.

For example, $AND_2(x_1, x_2) = x_1 \cdot x_2$ and

$$OR_2(x_1, x_2) = x_1 + x_2 - x_1 \cdot x_2.$$

Multilinear polynomials representing symmetric partial Boolean functions

- Let f be a partial function with a domain of definition $D \subseteq \{0,1\}^n$. For $0 \le \varepsilon < 1/2$, we say a real multilinear polynomial p approximates f with error ε if:

(1) $|p(x) - f(x)| \le \varepsilon$ for all $x \in D$;

(2) $0 \le p(x) \le 1$ for all $x \in \{0,1\}^n$.

- The approximate degree of f with error ε, denoted by $\widetilde{deg}_{\varepsilon}(f)$, is the minimum degree among all real multilinear polynomials that approximate f with error ε. In particular,

$$\widetilde{deg}_{0}(f) \triangleq \deg(f)$$

Methods of Proofs

We would like to outline the basic ideas and methods for the proofs of main results.

$$DJ_n^k = \begin{cases} 0 & if|x| \le k \;\; or \; |x| \ge n-k \\ 1 & if|x| = n/2 \end{cases}$$

Theorem 1 $Q_E(DJ_n^k) = k+1$ and $D(DJ_n^k) = \frac{n}{2} + k + 1$.

Proof method:

- Using the exact quantum query algorithms for computing $EXACT_n^k$ and due to Ambainis *et al.* (TQC'13), we can give an exact quantum $(k+1)$-query algorithm for computing DJ_n^k
- On the other hand, we will prove that $\deg(DJ_n^k) \ge 2k+2$, and therefore

$$Q_E(DJ_n^k) \ge \deg(DJ_n^k)/2 = k+1$$

$Q_E\left(DJ_n^k\right) \le k+1$

Subroutine: Xquery(m, x) 【from Ambainis *et al.* (TQC'13)】

Input: $x = x_1, x_2, \ldots, x_m$.

Output: $(0,0) \Rightarrow |x| \neq \frac{m}{2}$

$(i,j) \Rightarrow x_i \neq x_j$

Algorithm 2 Algorithm for DJ_n^k

```
procedure DJ(integer n, integer k, array x)
    integer l:=1
    while l ≤ k do
        Output ←Xquery(n, x)
        if Output=(0,0) then return 0
        end if
        if Output=(i, j) then
            x ← x \ {x_i, x_j}
            l ← l + 1
            n ← n − 2
        end if
    end while
    Output ←Xquery(n, x)
    if Output=(0,0) then return 0
    end if
    if Output=(i, j) then return 1
    end if
end procedure
```

$\deg(DJ_n^k) \geq 2k+2$

Lemma: For any symmetrically partial Boolean function f over $\{0,1\}^n$ with domain of definition D, suppose $\deg_\varepsilon(f) = d$. Then there exists a real multilinear polynomial q approximates f with error ε and q can be written as

$$q(x) = c_0 + c_1 V_1 + c_2 V_2 + \cdots + c_d V_d,$$

where $c_i \in R, V_1 = x_1 + \cdots + x_n, V_2 = x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n, \cdots$

Suppose that $\deg(DJ_n^k) \leq 2k+1$. Then we can get a contradiction. So, $\deg(DJ_n^k) \geq 2k+2$ follows.

Theorem: $Q_E(f) = 1$ *if and only if* f can be computed by DJ algorithm

Lemma 1 Let $n > 1$ and let $f: \{0,1\}^n \to \{0,1\}$ be an n-bit symmetrically partial Boolean function. Then:

(1) $\deg(f) = 1$ iff f is isomorphic to the function $f_{n,n}^{(1)}$

(2) $\deg(f) = 2$ iff f is isomorphic to one of the functions

$$f_{n,k}^{(1)}(x) = \begin{cases} 0 & \text{if } |x| = 0, \\ 1 & \text{if } |x| = k, \end{cases} \qquad f_{n,l}^{(3)}(x) = \begin{cases} 0 & \text{if } |x| = 0 \text{ or } |x| = n, \\ 1 & \text{if } |x| = l, \end{cases}$$

$$f_{n,k}^{(2)}(x) = \begin{cases} 0 & \text{if } |x| = 0, \\ 1 & \text{if } |x| = k \text{ or } |x| = k+1, \end{cases} \qquad f_{n}^{(4)}(x) = \begin{cases} 0 & \text{if } |x| = 0 \text{ or } |x| = n, \\ 1 & \text{if } |x| = \lfloor n/2 \rfloor \text{ or } |x| = \lceil n/2 \rceil, \end{cases}$$

where $n - 1 \geq k \geq \lfloor n/2 \rfloor$, and $\lceil n/2 \rceil \geq l \geq \lfloor n/2 \rfloor$.

Two Lemmas

- Lemma. Let n be even. Then $QE(f) = 1$ if and only if f is isomorphic to one of these functions: $f_{n,k}^{(1)}$ and $f_{n,n/2}^{(3)}$, $k \geq \frac{n}{2}$.
- Lemma. Let n be odd. Then $QE(f) = 1$ if and only if f is isomorphic to one of these functions: $f_{n,k}^{(1)}$, $k \geq \lceil n/2 \rceil$.

Equivalence transformation

- **Indeed, these functions with exact quantum 1-query complexity can be essentially transformed into DJ problem by padding some zeros into the input string. So, $QE(f) = 1$ if and only if f can be computed by DJ algorithm.**

Conclusions

- $DJ_n^k = \begin{cases} 0 & if\,|\mathrm{x}| \le k \;\; or\; |\mathrm{x}| \ge n-k \\ 1 & if\,|\mathrm{x}| = n/2 \end{cases}$

Theorem. $Q_E\left(DJ_n^k\right) = k+1$ and $D\left(DJ_n^k\right) = n/2+k+1.$

Theorem. Any symmetric partial Boolean function f has $Q_E(f) = 1$ if and only if f can be computed by the Deutsch-Jozsa algorithm.

Theorem. Any classical deterministic algorithm that solves Simon's problem requires $\Omega(\sqrt{\mathbf{2^n}})$ queries.

Problems

- Let $f: \{0,1\}^n \rightarrow \{0,1\}$ be an n-bit symmetric partial Boolean function with domain of definition D, and let $0 \leq k < \lfloor\frac{n}{2}\rfloor$. Then, for $2k+1 \leq \deg(f) \leq 2(k+1)$, how to characterize f by giving all functions with degrees from $2k+1$ to $2k+2$?
- For the function $DW_n^{k,l}$ defined as:

$$\mathrm{DW}_n^{k,l}(x) = \begin{cases} 0 & \text{if } |x| = k, \\ 1 & \text{if } |x| = l, \end{cases}$$

can we give optimal exact quantum query algorithms for any k and l?

Thank you for your attention！