Exact quantum query algorithms

Ashley Montanaro, Richard Jozsa and Graeme Mitchison

Centre for Quantum Information and Foundations, University of Cambridge

Abstract

- *We present several families of total boolean functions which have exact quantum query complexity which is a constant multiple (between $1/2$ and $2/3$) of their classical query complexity, and show that optimal quantum algorithms for these functions cannot be obtained by simply computing parities of pairs of bits.*
- *These results were originally inspired by numerically solving the semidefinite programs characterising quantum query complexity for small problem sizes.*
- *We include numerical results giving the optimal success probabilities achievable by quantum algorithms computing all boolean functions on up to 4 bits, and all symmetric boolean functions on up to 6 bits.*
- *We also characterise the model of nonadaptive exact quantum query complexity in terms of coding theory and completely characterise the query complexity of symmetric boolean functions in this context.*

Exact quantum query complexity

Let $f : \{0,1\}^n \to \{0,1\}$ be a boolean function.

- Define $D(f)$ ($Q_E(f)$) as the minimum number of classical (quantum) queries required to compute f with certainty.
- It was shown by Midrijanis [4] that for total functions f, $D(f) = O(Q_E(f)^3)$.
- On the other hand, exact quantum algorithms can indeed be better than classical algorithms: Cleve et al [2] showed that the parity of n bits,
$$f(x) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$$
can be computed exactly using only $\lceil n/2 \rceil$ quantum queries, simply by computing the parity of 2 bits using 1 quantum query.
- Some authors have used the algorithm for parity as a subroutine, e.g. [3] uses it to compute the majority function using $n - O(\log n)$ queries.
- But to our knowledge there are no other (non-trivial) exact quantum query algorithms for total functions known! It has been open for 14+ years whether there exists a total function f such that $Q_E(f) < D(f)/2$.

Quantum query complexity SDP

Given $f : \{0,1\}^n \to \{0,1\}$ and $t \in \mathbb{N}$, find a sequence of 2^n-dim real symmetric matrices $(M_i^{(j)})$, where $0 \le i \le n$ and $0 \le j \le t-1$, and 2^n-dim real symmetric matrices Γ_0, Γ_1, such that
$$\sum_{i=0}^{n} M_i^{(0)} = E_0$$
$$\sum_{i=0}^{n} M_i^{(j)} = \sum_{i=0}^{n} E_i \circ M_i^{(j-1)} \text{ (for } 1 \le j \le t-1)$$
$$\Gamma_0 + \Gamma_1 = \sum_{i=0}^{n} E_i \circ M_i^{(t-1)}$$
$$F_0 \circ \Gamma_0 \ge (1-\epsilon)F_0, \quad F_1 \circ \Gamma_1 \ge (1-\epsilon)F_1.$$
Here E_i is the matrix $\langle x|E_i|y\rangle = (-1)^{x_i + y_i}$, F_0 and F_1 are diagonal 0/1 matrices where $\langle x|F_z|x\rangle = 1$ if and only if $f(x) = z$, and $\circ$ is the Hadamard (entrywise) product of matrices.

Theorem (Barnum, Saks and Szegedy [1]). *There is a quantum query algorithm that uses t queries to compute a function $f : \{0,1\}^n \to \{0,1\}$ within error ϵ if and only if the above SDP is feasible. Further, given a solution to the above SDP, one can write down an explicit quantum algorithm achieving the same parameters.*

Exact quantum query algorithms

- Using the CVX package for Matlab, we solved the Barnum-Saks-Szegedy SDP numerically for all boolean functions up to 4 bits, and all symmetric functions on up to 6 bits.
- Based on the (inexact) output of the SDP solver, one can try to find an exact quantum algorithm achieving the same parameters.
- We have done this for the functions $x_1 \wedge (x_2 \vee x_3)$, EXACT$_2$ and $(x_1 \wedge x_2) \vee (\bar{x}_1 \wedge \bar{x}_2 \wedge x_3)$, for all of which the optimal quantum algorithm is provably not based on computing parities.
- We also have a simpler exact quantum algorithm which solves EXACT$_2$ on 4 bits using 2 queries. This algorithm generalises to a 2-query algorithm for determining whether the Hamming weight of the input is $n/2$ or in the set $\{0, 1, n-1, n\}$.
- These separations scale up to give constant factor quantum-classical query separations.

Numerical results for small functions

For example, we have the following results for all boolean functions depending on 3 input bits, up to isomorphism.

ID	Function	1 query	2 queries	$\mathbb{F}_2$ deg.	D(f)
1	$x_1 \wedge x_2 \wedge x_3$	0.800	0.980	3	3
6	$x_1 \wedge (x_2 \oplus x_3)$	0.667	1	2	3
7	$x_1 \wedge (x_2 \vee x_3)$	0.773	1	3	3
22	EXACT$_2$	0.571	1	3	3
23	MAJ	0.667	1	2	3
30	$x_1 \oplus (x_2 \vee x_3)$	0.667	1	2	3
53	SEL(x_1, x_2, x_3)	0.854	1	2	2
67	see below	0.773	1	3	3
105	PARITY	0.500	1	1	3
126	NAE	0.900	1	2	3

In this table:

- The ID of each function is the integer obtained by converting its truth table from binary.
- Columns give the optimal success probability that can be achieved by quantum algorithms making 1 or 2 queries.
- Function 67 is $(x_1 \wedge x_2) \vee (\bar{x}_1 \wedge \bar{x}_2 \wedge x_3)$.

Nonadaptive quantum query complexity

- A nonadaptive (classical or quantum) query algorithm cannot choose queries based on the result of previous queries. In other words, the queries must all be made up front, in parallel.
- Let $D^{na}(f)$, $Q_E^{na}(f)$ be the nonadaptive classical and quantum exact query complexities of f.

For any total boolean function f depending on n variables, $D^{na}(f) = n$. Nonadaptive quantum query complexity is more complicated.

- For any $f : \{0,1\}^n \to \{0,1\}$, define the subspace
$$S_f := \{z : \forall x, f(x) = f(x+z)\}.$$
- For any subspace $S \subseteq \{0,1\}^n$, let $S^\perp$ denote the orthogonal subspace to S, i.e.
$$S^\perp = \{x : x \cdot s = 0, \forall s \in S\}.$$

Theorem. *For any function $f : \{0,1\}^n \to \{0,1\}$,*
$$Q_E^{na}(f) = \min_{x \in \{0,1\}^n} \max_{y \in S_f^\perp} d(x,y).$$

This allows us to prove the following quadrichotomy for symmetric boolean functions.

Corollary. *If $f : \{0,1\}^n \to \{0,1\}$ is symmetric, then exactly one of the following four possibilities is true.*

1. *f is constant and $Q_E^{na}(f) = 0$.*
2. *f is the PARITY function or its negation and $Q_E^{na}(f) = \lceil n/2 \rceil$.*
3. *f satisfies $f(x) = f(\bar{x})$ (but is not constant, the PARITY function or its negation) and $Q_E^{na}(f) = n-1$.*
4. *f is none of the above and $Q_E^{na}(f) = n$.*

Open questions

As always, the basic open question still remains: can we achieve $Q_E(f) < D(f)/2$? Our numerical results inspire many other tantalising conjectures. For example:

Conjecture. *For any n, the EXACT$_k$ function on n bits can be computed exactly using $\max\{k, n-k\}$ quantum queries.*

This conjecture holds numerically for $n \le 6$.

References

[1] H. Barnum, M. Saks, and M. Szegedy. Quantum query complexity and semi-definite programming. In *Proc. 18th CCC*, pages 179–193, 2003.

[2] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proc. R. Soc. Lond. A*, 454(1969):339–354, 1998. `quant-ph/9708016`.

[3] T. Hayes, S. Kutin, and D. van Melkebeek. The quantum black-box complexity of majority. *Algorithmica*, 34(4):480–501, 2002. `quant-ph/0109101`.

[4] G. Midrijānis. Exact quantum query complexity for total Boolean functions, 2004. `quant-ph/0403168`.

arXiv:1111.0475