Unbounded error quantum query complexity

Ashley Montanaro[1], Harumichi Nishimura[2] and Rudy Raymond[3]

[1]Department of Computer Science, University of Bristol, UK
[2]School of Science, Osaka Prefecture University, Japan
[3]Tokyo Research Laboratory, IBM Research, Japan

arXiv:0712.1446

University of BRISTOL

QICS

Abstract

We study the quantum query complexity of Boolean functions in an unbounded error scenario.

Main results:

- The unbounded error quantum query complexity is exactly half of its classical counterpart for any (partial or total) Boolean function.
- A known “black box” approach to convert quantum query algorithms into communication protocols is optimal even in the unbounded error setting.
- In a related weakly unbounded error setting, there is a tight multiplicative $\Theta(\log n)$ separation between quantum and classical query complexity for a partial Boolean function.

Motivation

- Many models in computational complexity have several settings where different restrictions are placed on the success probability to evaluate a Boolean function f.
- For example, in the polynomial-time complexity model, we have:

Model	**Complexity class**
Exact computation	P
Bounded error	BPP
Unbounded error	PP

- Can we understand how the gap between quantum and classical computation changes with different success probability restrictions?

Query complexity (1)

- The quantum/classical query complexity of a Boolean function $f : \{0,1\}^n \to \{0,1\}$ is the number of quantum/classical queries to its input that are required to compute f (with some error probability requirement).

- We have the following definitions:

Quantity	**Model**	**Success prob. required**
$D(f)$	Deterministic	1
$R(f)$	Randomised	2/3
$UC(f)$	Randomised	$> 1/2$
$Q_E(f)$	Quantum	1
$Q_2(f)$	Quantum	2/3
$UQ(f)$	Quantum	$> 1/2$

Query complexity (2)

- There can be an exponential separation between $R(f)$ and $Q_2(f)$ for partial f [Simon '97].
- For total f, separation at most polynomial [Beals et al '01].
- The only separation known between $D(f)$ and $Q_E(f)$ for total f is a factor of 2 [Beals et al '01, Farhi et al '98].

e.g. functions $OR_n(x) = 1 \Leftrightarrow \exists i, x_i = 1$, $PARITY_n(x) = \bigoplus_i x_i$:

Quantity	OR	PARITY
$D(f)$	n	n
$R(f)$	$\Theta(n)$	n
$UC(f)$	1	n
$Q_E(f)$	n	$n/2$
$Q_2(f)$	$O(\sqrt{n})$	$\Theta(n)$
$UQ(f)$	1	$n/2$

Sign-representing polynomials

- A polynomial $p(x) : \{0,1\}^n \to \mathbb{R}$ sign-represents f if $p(x) > 0$ when $f(x) = 1$, and $p(x) < 0$ when $f(x) = 0$.
- The minimum, over all polynomials p that sign-represent f, of $deg(p)$ is called $sdeg(f)$.

Lemma [Buhrman et al '07]

An unbounded error randomised algorithm for f using d queries is equivalent to a degree d polynomial p that sign-represents f, i.e. $UC(f) = sdeg(f)$.

Lemma [Beals et al '01]

The amplitude of the final basis states of a quantum algorithm using T queries can be written as a multilinear polynomial of degree at most T.

Unbounded error: quantum vs. classical

Theorem

For any Boolean function $f : X \to \{0,1\}$ such that $X \subseteq \{0,1\}^n$,

$$UQ(f) = \left\lceil \frac{UC(f)}{2} \right\rceil = \left\lceil \frac{sdeg(f)}{2} \right\rceil.$$

Proof: **[**$UQ(f) \geqslant sdeg(f)/2$**]**

- Let $\mathcal{A}$ be an unbounded-error quantum algorithm for f using $UQ(f)$ queries.
- By the lemma of Beals et al, the acceptance probability of $\mathcal{A}$ can be written as a multilinear polynomial of degree at most $2UQ(f)$.
- Hence $sdeg(f) \leqslant 2UQ(f)$.

$\mathbf{UQ(f) \leqslant \lceil sdeg(f)/2 \rceil}$

Lemma [Beals et al '01, Farhi et al '98]

Let $S \subseteq [n]$ be a set of indices of variables. Then there exists a quantum algorithm that computes $\bigoplus_{i \in S} x_i$ using $\lceil |S|/2 \rceil$ queries.

Proof sketch:

- Write the sign-representing polynomial p as $p(x) = \sum_{s \in \{0,1\}^n} \hat{p}(s)(-1)^{x \cdot s}$ (Fourier representation).
- Rewrite as normalised difference of 2 sums of +ve terms.
- Quantum algorithm picks a term s with probability $|\hat{p}(s)|$ and computes $(-1)^{x \cdot s}$.
- Uses at most $\lceil |sdeg(f)|/2 \rceil$ queries and succeeds with probability $> 1/2$.

Query algorithm $\mapsto$ communication protocol

Lemma [Buhrman et al '98]

Let $F : \{0,1\}^n \to \{0,1\}$, and $F^L : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ denote the distributed function of F induced by the bitwise function $L : \{0,1\} \times \{0,1\} \to \{0,1\}$. That is, $F^L(x,y) = F(z)$, where each bit of z is $z_i = L(x_i, y_i)$.

If there is a quantum algorithm that computes F using T queries, with success prob. p, then there is an $O(T \log n)$-qubit communication protocol for F^L, with success prob. p.

- So quantum query algorithms induce quantum communication protocols, and quantum communication lower bounds induce query lower bounds.
- Gives (e.g.) an $O(\sqrt{n} \log n)$ quantum protocol for disjointness [Buhrman et al '98].

Optimality of the reduction

This reduction has $\Theta(\log n)$ overhead... could we do better?

Theorem (1)

Let $\mathcal{A}$ be a procedure that, for any function $f : \{0,1\}^n \to \{0,1\}$, converts a nondeterministic (resp. exact) quantum algorithm for f using $T(n)$ queries into a nondeterministic (resp. exact) quantum communication protocol for $f^{\oplus}$ using $O(T(n)D(n))$ qubits. Then $D(n) = \Omega(\log(n/T(n)))$.

Theorem (2)

Let $\mathcal{A}$ be a procedure that, for any function $f : \{0,1\}^n \to \{0,1\}$, converts an unbounded error quantum algorithm for f using $T(n)$ queries into an unbounded error quantum communication protocol for $f^{\wedge}$ which uses $O(T(n)D(n))$ qubits. Then $D(n) = \Omega(\log(n/T(n)))$.

Proof idea

In both cases: find a function such that we can upper bound the quantum query complexity, and lower bound the communication complexity of the distributed variant.

1. Function used: a Fourier sampling problem [Bernstein and Vazirani '97]. Distributed variant gives rise to the equality function, for which exact/nondeterministic lower bounds are known.

2. Function used: ODD-MAX-BIT (evaluates to 1 if highest index of a 1 bit is odd). Easy to solve with one classical query. Distributed problem induces the INDEX problem, which then induces a solution to PARITY.

The weakly unbounded error model

What happens if we trade off success probability and the number of queries used?

- The bias β of a quantum or classical query algorithm which succeeds with probability $p > 1/2$ is $p - 1/2$.
- The weakly unbounded error cost of the algorithm is equal to the number of queries plus $\log 1/2\beta$.
- $WUC(f)$ is the minimum cost over all classical algorithms.
- $WUQ(f)$ is the minimum cost over all quantum algorithms.

Example:

- $WUC(OR_n) = \Theta(\log n)$, $WUQ(OR_n) = \Theta(\log n)$.

Weakly unbounded error: lower bound

Lemma

For any function $f : \{0,1\}^n \to \{0,1\}$, $WUC(f) \leqslant 2WUQ(f) \log n$.

Proof based on the following lemma:

Lemma [Buhrman et al '07]

Let p be a multilinear polynomial of degree d that sign-represents $f : \{0,1\}^n \to \{0,1\}$ with bias β. Define $N = \sum_{i=0}^{d} \binom{n}{i}$. Then there also exists a multilinear polynomial $q(x) = \sum_{S \in S_d} \hat{q}(S)(-1)^{x_S}$ of the same degree and bias $\beta/\sqrt{N}$ that sign-represents f, such that $\sum_{S \in S_d} |\hat{q}(S)| = 1$.

(Proof sketch: by lemma of Beals et al, quantum algorithm $\Rightarrow$ sign-representing polynomial. By this lemma, sign-representing polynomial $\Rightarrow$ classical algorithm.)

Weakly unbounded error: quantum-classical separation

Idea: Find a function for which the quantum query complexity is $O(1)$, but the classical query complexity is $\Omega(\log n)$.

We use the well-known Fourier Sampling problem of [Bernstein and Vazirani '97].

Definition: Fourier Sampling

For $x, r \in \{0,1\}^m$, let F^r be a bit string of length $n = 2^m$ whose x-th bit is $F^r_x = \sum_i x_i \cdot r_i \mod 2$. Let g be another bit string of length n.

Then the *Fourier Sampling* function is defined by $\mathrm{FS}(F^r, g) = g_r$.

Proof idea

Quantum upper bound is easy. Classical lower bound proof idea:

- Show that many queries are needed for any classical algorithm to achieve a high bias for the FS problem.
- Achieve this by picking the string g at random and using a probabilistic method by counting the number of classical algorithms that use a small number of queries.

We now have an additive $O(1)$ vs. $\Omega(\log n)$ separation. Convert this to be a multiplicative separation by replacing each input bit by the parity of T bits. We have:

Theorem

There is a partial function $f : \{0,1\}^n \to \{0,1\}$ such that $WUC(f) = \Omega(WUQ(f) \log n)$.

Conclusions and conjectures

- We exactly characterised unbounded error quantum query complexity.
- We have given a tight quantum-classical gap for weakly unbounded error QC for partial functions.
- We conjecture that for all total functions f, it holds that $WUC(f) = O(WUQ(f))$. We know:

Theorem

For the threshold function defined by $\mathrm{TH}_k(x) = 1$ iff $|x| > k$, $WUC(\mathrm{TH}_k) = WUQ(\mathrm{TH}_k) = \Theta(\log n)$.

- The factor of 2 separation between UQ and UC is the same as the maximal known separation between the exact quantum and classical QCs of total Boolean functions – is this optimal?