# Quantum Certificate Complexity

Scott Aaronson*
Computer Science Department
University of California, Berkeley

**Abstract**

Given a Boolean function $f$, we study two natural generalizations of the certificate complexity $C(f)$: the randomized certificate complexity $RC(f)$ and the quantum certificate complexity $QC(f)$. Using Ambainis' adversary method, we exactly characterize $QC(f)$ as the square root of $RC(f)$. We then use this result to prove the new relation $R_0(f) = O\left(Q_2(f)^2 Q_0(f) \log n\right)$ for total $f$, where $R_0$, $Q_2$, and $Q_0$ are zero-error randomized, bounded-error quantum, and zero-error quantum query complexities respectively. Finally we give asymptotic gaps between the measures, including a total $f$ for which $C(f)$ is superquadratic in $QC(f)$, and a symmetric partial $f$ for which $QC(f) = O(1)$ yet $Q_2(f) = \Omega(n/\log n)$.

## 1 Background

Most of what is known about the power of quantum computing can be cast in the query or decision-tree model [1, 2, 3, 5, 6, 9, 10, 11, 18, 22, 23]. Here one counts only the number of queries to the input, not the number of computational steps. The appeal of this model lies in its extreme simplicity—in contrast to (say) the Turing machine model, one feels the query model ought to be 'completely understandable.' In spite of this, open problems abound.

Let $f : Dom(f) \rightarrow \{0,1\}$ be a Boolean function with $Dom(f) \subseteq \{0,1\}^n$, that takes input $Y = y_1 \ldots y_n$. Then the deterministic query complexity $D(f)$ is the minimum number of queries to the $y_i$'s needed to evaluate $f$, if $Y$ is chosen adversarially and if queries can be adaptive (that is, can depend on the outcomes of previous queries). Also, the bounded-error randomized query complexity, $R_2(f)$, is the minimum expected number of queries needed by a randomized algorithm that, for each $Y \in Dom(f)$, outputs $f(Y)$ with probability at least $2/3$. Here the '2' refers to two-sided error; if instead we require $f(Y)$ to be output with probability 1 for every $Y$, we obtain $R_0(f)$, or zero-error randomized query complexity.

Analogously, $Q_2(f)$ is the minimum number of queries needed by a quantum algorithm that outputs $f(Y)$ with probability at least $2/3$ for all $Y$. Also, for $k \in \{0,1\}$ let $Q_0^k(f)$ be the minimum number of queries needed by a quantum algorithm that outputs $f(Y)$ with probability 1 if $f(Y) = k$, and with probability at least $1/2$ if $f(Y) \neq k$. Then let $Q_0(f) = \max\left\{Q_0^0(f), Q_0^1(f)\right\}$. If we require a single algorithm that succeeds with probability 1 for all $Y$, we obtain $Q_E(f)$, or exact quantum query complexity. See [10] for detailed definitions and a survey of these measures.

It is immediate that $Q_2(f) \leq R_2(f) \leq R_0(f) \leq D(f) \leq n$, that $Q_0(f) \leq R_0(f)$, and that $Q_E(f) \leq D(f)$. If $f$ is partial (i.e. $Dom(f) \neq \{0,1\}^n$), then $Q_2(f)$ can be superpolynomially smaller than $R_2(f)$; this is what makes Shor's period-finding algorithm [19] possible. For total $f$, by contrast, the largest known gap even between $D(f)$ and $Q_2(f)$ is quadratic, and is achieved by the $OR$ function on $n$ bits:

*Email: aaronson@cs.berkeley.edu. Supported by an NSF Graduate Fellowship and by the Defense Advanced Research Projects Agency (DARPA) and Air Force Laboratory, Air Force Materiel Command, USAF, under agreement number F30602-01-2-0524.

$D(OR) = n$ (indeed $R_2(OR) = \Omega(n)$), whereas $Q_2(OR) = \Theta(\sqrt{n})$ because of Grover's search algorithm [11]. Furthermore, for total $f$, Beals et al. [6] showed that $D(f) = O\left(Q_2(f)^6\right)$, while de Wolf [23] showed that $D(f) = O\left(Q_2(f)^2 Q_0(f)^2\right)$.

The result of Beals et al. [6] relies on two intermediate complexity measures, the *certificate complexity* $C(f)$ and *block sensitivity* $bs(f)$, which we now define.

**Definition 1** *A certificate for an input $X$ is a set $S \subseteq \{1,\ldots,n\}$ such that for all $Y \in Dom(f)$, if $y_i = x_i$ for all $i \in S$ then $f(Y) = f(X)$. Then $C^X(f)$ is the minimum size of a certificate for $X$, and $C(f)$ is the maximum of $C^X(f)$ over all $X$.*

**Definition 2** *A sensitive block on input $X$ is a set $B \subseteq \{1,\ldots,n\}$ such that $f\left(X^{(B)}\right) \neq f(X)$, where $X^{(B)}$ is obtained from $X$ by flipping $x_i$ for each $i \in B$. Then $bs^X(f)$ is the maximum number of disjoint sensitive blocks on $X$, and $bs(f)$ is the maximum of $bs^X(f)$ over all $X$.*

Clearly $bs(f) \leq C(f) \leq D(f)$. For total $f$, these measures are all polynomially related: Nisan [12] showed that $C(f) \leq bs(f)^2$, while Beals et al. [6] showed that $D(f) \leq C(f)\, bs(f)$. Combining these results with $bs(f) = O\left(Q_2(f)^2\right)$ (from the optimality of Grover's algorithm), one obtains $D(f) = O\left(Q_2(f)^6\right)$.

## 2 Our Results

We investigate $RC(f)$ and $QC(f)$, the bounded-error randomized and quantum generalizations of the certificate complexity $C(f)$ (see Table 1). Our motivation is that, just as $C(f)$ was used to show a polynomial relation between $D(f)$ and $Q_2(f)$, so $RC(f)$ and $QC(f)$ can lead to new relations among fundamental query complexity measures.

| **Table 1** | | | |
|---|---|---|---|
| Query complexity | $D(f)$ | $R_2(f)$ | $Q_2(f)$ |
| Certificate complexity | $C(f)$ | $RC(f)$ | $QC(f)$ |

What the certificate complexity $C(f)$ measures is the number of *queries* used to verify a certificate, not the number of *bits* used to communicate it. Thus, if we want to generalize $C(f)$, we should assume the latter is unbounded. A consequence is that without loss of generality, a certificate is just a claimed value $X$ for the input $Y$[1]—since any additional information that a prover might provide, the verifier can compute for itself. The verifier's job is to check that $f(Y) = f(X)$. With this in mind we define $RC(f)$ as follows.

**Definition 3** *A randomized verifier for input $X$ is a randomized algorithm that, on input $Y \in Dom(f)$, (i) accepts with probability 1 if $Y = X$, and (ii) rejects with probability at least $1/2$ if $f(Y) \neq f(X)$. (If $Y \neq X$ but $f(Y) = f(X)$, the acceptance probability can be arbitrary.) Then $RC^X(f)$ is the minimum expected number of queries used by a randomized verifier for $X$, and $RC(f)$ is the maximum of $RC^X(f)$ over all $X$.*

We define $QC(f)$ analogously, with quantum instead of randomized algorithms. The following justifies the definition (the $RC(f)$ part was originally shown by Raz et al. [15]).

**Proposition 4** *Making the error probability two-sided rather than one-sided changes $RC(f)$ and $QC(f)$ by at most a constant factor.*

[1] Throughout this paper, we use $Y$ to denote the 'actual' input being queried, and $X$ to denote the 'claimed' input (whose randomized certificate complexity, block sensitivity, and so on we want to study).

**Proof.** For $RC(f)$, let $r_V^Y$ be the event that verifier $V$ rejects on input $Y$, and let $d_V^Y$ be the event that $V$ encounters a disagreement with $X$ on $Y$. We may assume $\Pr\left[r_V^Y \mid d_V^Y\right] = 1$. Suppose that $Y = X$ and $f(Y) \neq f(X)$ both occur with probability $1/2$, and that $\Pr\left[r_V^Y\right] \leq \varepsilon_0$ in the former case and $\Pr\left[r_V^Y\right] \geq 1-\varepsilon_1$ in the latter. Then

$$\Pr\left[\neg d_V^Y \mid r_V^Y\right] = \frac{\Pr\left[r_V^Y \mid \neg d_V^Y\right] \Pr\left[\neg d_V^Y\right]}{\Pr\left[r_V^Y\right]} \leq \frac{2\varepsilon_0}{1-\varepsilon_1}.$$

Now let $V^*$ be identical to $V$ except that, whenever $V$ rejects despite having found no disagreement with $X$, $V^*$ accepts. Clearly $\Pr\left[r_{V^*}^X\right] = 0$. Also, in the case $f(Y) \neq f(X)$,

$$\Pr\left[r_{V^*}^Y\right] = \Pr\left[d_V^Y\right] \geq \Pr\left[r_V^Y\right] \Pr\left[d_V^Y \mid r_V^Y\right] \geq (1-\varepsilon_1)\left(1 - \frac{2\varepsilon_0}{1-\varepsilon_1}\right).$$

For $QC(f)$, suppose the verifier's final state given input $Y$ is

$$\sum_z \alpha_z^Y |z\rangle \left(\beta_z^Y |0\rangle + \gamma_z^Y |1\rangle\right)$$

where $|0\rangle$ is the reject state, $|1\rangle$ is the accept state, and $\left|\beta_z^Y\right|^2 + \left|\gamma_z^Y\right|^2 = 1$ for all $z$. Suppose also that $A^X \geq 1-\varepsilon_0$ and that $A^Y \leq \varepsilon_1$ whenever $f(Y) \neq f(X)$, where $A^Y = \sum_z \left|\alpha_z^Y \gamma_z^Y\right|^2$ is the probability of accepting. Then the verifier can make $A^X = 1$ by performing the conditional rotation

$$\begin{pmatrix} \gamma_z^X & -\beta_z^X \\ \beta_z^X & \gamma_z^X \end{pmatrix}$$

on the second register prior to measurement. In the case $f(Y) \neq f(X)$, this produces

$$\begin{aligned} A^Y &= \sum_z \left|\alpha_z^Y\right|^2 \left|\beta_z^X \beta_z^Y + \gamma_z^X \gamma_z^Y\right|^2 \\ &\leq 2\sum_z \left|\alpha_z^Y\right|^2 \left(\left|\beta_z^X\right|^2 + \left|\gamma_z^Y\right|^2\right) \\ &\leq 2(\varepsilon_0 + \varepsilon_1). \end{aligned}$$

■

It is immediate that $QC(f) \leq RC(f) \leq C(f)$, that $QC(f) = O(Q_2(f))$, and that $RC(f) = O(R_2(f))$. We also have $RC(f) = \Omega(bs(f))$, since a randomized verifier for $X$ must query each sensitive block on $X$ with $1/2$ probability. This suggests viewing $RC(f)$ as an 'alloy' of block sensitivity and certificate complexity, an interpretation for which Section 6 gives some justification.

Our results are as follows. In Section 4 we show that $QC(f) = \Theta\left(\sqrt{RC(f)}\right)$ for all $f$ (partial or total), precisely characterizing quantum certificate complexity in terms of randomized certificate complexity. To do this, we first give a nonadaptive characterization of $RC(f)$, and then apply the adversary method of Ambainis [3] to lower-bound $QC(f)$ in terms of this characterization. Then, in Section 5, we extend results on polynomials due to de Wolf [23] and to Nisan and Smolensky (as described by Buhrman and de Wolf [10]), to show that $R_0(f) = O(RC(f)\, ndeg(f) \log n)$ for all total $f$, where $ndeg(f)$ is the minimum degree of a polynomial $p$ such that $p(X) \neq 0$ if and only if $f(X) \neq 0$. Combining the results of Sections 4 and 5 leads to a new lower bound on quantum query complexity: that $R_0(f) = O\left(Q_2(f)^2 Q_0(f) \log n\right)$ for all total $f$. To our knowledge, this is the first quantum lower bound to use both the adversary method and the polynomial method at different points in the argument.

Finally, in Section 6, we exhibit asymptotic gaps between $RC(f)$ and other query complexity measures, including a total $f$ for which $C(f) = \Theta\left(QC(f)^{2.205}\right)$, and a symmetric partial $f$ for which $QC(f) = O(1)$ yet $Q_2(f) = \Omega(n/\log n)$. We conclude in Section 7 with some open problems.

# 3 Related Work

Raz et al. [15] studied a query complexity measure they called $ma(f)$, for Merlin-Arthur. In our notation, $ma(f)$ equals the maximum of $RC^X(f)$ over all $X$ with $f(X) = 1$. Raz et al. observed that $ma(f) = ip(f)$, where $ip(f)$ is the number of queries needed given arbitrarily many rounds of interaction with a prover. They also used error-correcting codes to construct a total $f$ for which $ma(f) = O(1)$ but $C(f) = \Omega(n)$. This has similarities to our construction, in Section 6.3, of a symmetric partial $f$ for which $QC(f) = O(1)$ but $Q_2(f) = \Omega(n/\log n)$. Aside from that and from Proposition 4, Raz et al.'s results do not overlap with ours.

Watrous [20] has investigated a different notion of 'quantum certificate complexity'—whether certificates that are quantum states can be superpolynomially smaller than any classical certificate. Also, de Wolf [22] has investigated 'nondeterministic quantum query complexity' in the alternate sense of algorithms that accept with zero probability when $f(Y) = 0$, and with positive probability when $f(Y) = 1$.

# 4 Characterization of Quantum Certificate Complexity

We wish to show that $QC(f) = \Theta\left(\sqrt{RC(f)}\right)$, precisely characterizing quantum certificate complexity in terms of randomized certificate complexity. The first step is to give a simpler characterization of $RC(f)$.

**Lemma 5** *Call a randomized verifier for $X$ nonadaptive if, on input $Y$, it queries each $y_i$ with independent probability $\lambda_i$, and rejects if and only if it encounters a disagreement with $X$. (Thus, we identify such a verifier with the vector $(\lambda_1, \ldots, \lambda_n)$.) Let $RC^X_{na}(f)$ be the minimum of $\lambda_1 + \cdots + \lambda_n$ over all nonadaptive verifiers for $X$. Then $RC^X_{na}(f) = \Theta\left(RC^X(f)\right)$.*

**Proof.** Clearly $RC^X_{na}(f) = \Omega\left(RC^X(f)\right)$. For the upper bound, we can assume that a randomized verifier rejects immediately on finding a disagreement with $X$, and accepts if it finds no disagreement. Let $\mathcal{Y} = \{Y : f(Y) \neq f(X)\}$. Let $V$ be an optimal randomized verifier, and let $p_t(Y)$ be the probability that $V$, when given input $Y \in \mathcal{Y}$, finds a disagreement with $X$ on the $t^{th}$ query. By Markov's inequality, $V$ must have found a disagreement with probability at least $1/2$ after $T = \left\lceil 2RC^X(f) \right\rceil$ queries. So by the union bound

$$p_1(Y) + \cdots + p_T(Y) \geq 1/2$$

for each $Y \in \mathcal{Y}$. Suppose we choose $t \in \{1, \ldots, T\}$ uniformly at random and simulate the $t^{th}$ query, pretending that queries $1, \ldots, t-1$ have already been made and have returned agreement with $X$. Then we must find a disagreement with probability at least $1/2T$. By repeating this procedure $4T$ times, we can boost the probability to $1 - e^{-2}$. For $i \in \{1, \ldots, n\}$, let $\lambda_i$ be the probability that $y_i$ is queried at least once. Then $\lambda_1 + \cdots + \lambda_n \leq 4T$, whereas for each $Y \in \mathcal{Y}$,

$$\sum_{i : y_i \neq x_i} \lambda_i \geq 1 - e^{-2}.$$

It follows that, if each $y_i$ is queried with independent probability $\lambda_i$, then the probability that at least one $y_i$ disagrees with $X$ is at least

$$1 - \prod_{i : y_i \neq x_i} (1 - \lambda_i) \geq 1 - \left(1 - \frac{1 - e^{-2}}{n}\right)^n > 0.57.$$

■

To obtain a lower bound on $QC(f)$, we use the following simple reformulation of the adversary method of Ambainis [3].

**Theorem 6 (Ambainis)** *Let $\beta$ be a function from $Dom(f)$ to nonnegative reals, and let $R : Dom(f)^2 \rightarrow \{0,1\}$ be a relation such that $R(X,Y) = R(Y,X)$ for all $X,Y$ and $R(X,Y) = 0$ whenever $f(X) = f(Y)$. Let $\delta_0, \delta_1 \in (0,1]$ be such that for every $X \in Dom(f)$ and $i \in \{1,\ldots,n\}$,*

$$\sum_{Y\,:\,R(X,Y)=1} \beta(Y) \geq 1,$$

$$\sum_{Y\,:\,R(X,Y)=1, x_i \neq y_i} \beta(Y) \leq \delta_{f(X)}.$$

*Then $Q_2(f) = \Omega\left(\sqrt{\frac{1}{\delta_0 \delta_1}}\right)$.*

We now prove the main result of the section.

**Theorem 7** *For all $f$ (partial or total) and all $X$, $QC^X(f) = \Theta\left(\sqrt{RC^X(f)}\right)$.*

**Proof.** Let $(\lambda_1,\ldots,\lambda_n)$ be an optimal nonadaptive randomized verifier for $X$, and let

$$S = \lambda_1 + \cdots + \lambda_n.$$

First, $QC^X(f) = O\left(\sqrt{S}\right)$. We can run a "weighted Grover search," in which the proportion of basis states querying index $i$ is within a constant factor of $\lambda_i/S$. (It suffices to use $n^2$ basis states.) Let $\mathcal{Y} = \{Y : f(Y) \neq f(X)\}$; then for any $Y \in \mathcal{Y}$, $O\left(\sqrt{S}\right)$ iterations suffice to find a disagreement with $X$ with probability $\Omega(1)$.

Second, $QC^X(f) = \Omega\left(\sqrt{S}\right)$. Consider a matrix game in which Alice chooses an index $i$ to query and Bob chooses $Y \in \mathcal{Y}$; Alice wins if and only if $y_i \neq x_i$. If both players are rational, then Alice wins with probability $O(1/S)$, since otherwise Alice's strategy would yield a verifier $(\lambda'_1,\ldots,\lambda'_n)$ with

$$\lambda'_1 + \cdots + \lambda'_n = o(S).$$

Hence by the minimax theorem, there exists a distribution $\mu$ over $\mathcal{Y}$ such that for every $i$,

$$\Pr_{Y \in \mu}[y_i \neq x_i] = O(1/S).$$

Let $\beta(X) = 1$ and let $\beta(Y) = \mu(Y)$ for each $Y \in \mathcal{Y}$. Also, let $R(Y,Z) = 1$ if and only if $Z = X$ for each $Y \in \mathcal{Y}$ and $Z \notin \mathcal{Y}$. Then we can take $\delta_{f(Y)} = 1$ and $\delta_{f(X)} = O(1/S)$ in Theorem 6. So the quantum query complexity of distinguishing $X$ from an arbitrary $Y \in \mathcal{Y}$ is $\Omega\left(\sqrt{S}\right)$. ■

# 5 Quantum Lower Bound for Total Functions

Our goal is to show that

$$R_0(f) = O\left(Q_2(f)^2 Q_0(f) \log n\right).$$

Say that a real multilinear polynomial $p(x_1,\ldots,x_n)$ nondeterministically represents $f$ if for all $X \in \{0,1\}^n$, $p(X) \neq 0$ if and only if $f(X) \neq 0$. Let $ndeg(f)$ be the minimum degree of a nondeterministic polynomial for $f$. Also, given such a polynomial $p$, say that a monomial $M_1 \in p$ is *covered* by $M_2 \in p$ if $M_2$ contains every variable in $M_1$. We call $M$ a *maxonomial* if it is not covered by any other monomial of $p$. The following is a simple generalization of a lemma attributed in [10] to Nisan and Smolensky.

**Lemma 8 (Nisan-Smolensky)** *Let $p$ nondeterministically represent $f$. Then for every maxonomial $M$ of $p$ and $X \in f^{-1}(0)$, there is a set $B$ of variables in $M$ such that $f\left(X^{(B)}\right) \neq f(X)$, where $X^{(B)}$ is obtained from $X$ by flipping the variables in $B$.*

**Proof.** Obtain a restricted function $g$ from $f$, and a restricted polynomial $q$ from $p$, by setting each variable outside of $M$ to $x_i$. Then $g$ cannot be constant, since its representing polynomial $q$ contains $M$ as a monomial. Thus there is a subset $B$ of variables in $M$ such that $g\left(X^{(B)}\right) = 1$, and hence $f\left(X^{(B)}\right) = 1$. ■

Using Lemma 8, de Wolf [23] showed that $D(f) \leq C(f)\, ndeg(f)$ for all total $f$ (slightly improving the result $D(f) \leq C(f) \deg(f)$ due to Buhrman and de Wolf [10]). In Theorem 10, we will give an analog of this result for *randomized* query and certificate complexities. However, we first need a probabilistic lemma.

**Lemma 9** *Suppose we repeatedly apply the following procedure: first identify the set $B$ of maxonomials of $p$, then 'shrink' each $M \in B$ with (not necessarily independent) probability at least $1/2$. Shrinking $M$ means replacing it by an arbitrary monomial of degree $\deg(M) - 1$. Then with high probability $p$ is a constant polynomial after $O(\deg(p) \log n)$ iterations.*

**Proof.** For any set $A$ of monomials, consider the weighting function

$$\omega(A) = \sum_{M \in A} \deg(M)!$$

Let $S$ be the set of monomials of $p$. Initially

$$\omega(S) \leq n^{\deg(p)} \deg(p)!$$

and we are done when $\omega(S) = 0$. We claim that at every iteration, $\omega(B) \geq \frac{1}{e}\omega(S)$. For every $M^* \in S \setminus B$ is covered by some $M \in B$, but a given $M \in B$ can cover at most $\binom{\deg(M)}{l}$ distinct $M^*$ with $\deg(M^*) = l$. Hence

$$\begin{aligned}
\omega(S \setminus B) &\leq \sum_{M \in B} \sum_{l=0}^{\deg(M)-1} \binom{\deg(M)}{l} l! \\
&\leq \sum_{M \in B} \deg(M)! \left(\frac{1}{1!} + \frac{1}{2!} + \cdots\right) \\
&\leq (e-1)\,\omega(B).
\end{aligned}$$

At every iteration, the contribution of each $M \in B$ to $\omega(A)$ has at least $1/2$ probability of shrinking from $\deg(M)!$ to $(\deg(M) - 1)!$ (or to 0 if $\deg(M) = 1$). Hence $\omega(S)$ decreases by an expected amount at least $\frac{1}{4e}\omega(S)$. Thus after

$$\log_{4e/(4e-1)}\left(2n^{\deg(p)} \deg(p)!\right) = O(\deg(p) \log n)$$

iterations, the expectation of $\omega(S)$ is less than $1/2$, so $S$ is empty with probability at least $1/2$. ■

**Theorem 10** *For total $f$,*

$$R_0(f) = O(RC(f)\, ndeg(f) \log n).$$

**Proof.** Choose an $X$ with $f(X) = 0$, and let $(\lambda_1, \ldots, \lambda_n)$ be a nonadaptive randomized verifier for $X$. Form $I \subseteq \{1, \ldots, n\}$ by placing each $i$ in $I$ with independent probability $\lambda_i$. Then for any $Z \in \{0,1\}^n$, let $Z^{[I]}$ be obtained from $Z$ by setting $z_i$ to $x_i$ for each $i \in I$. We have $\Pr_I\left[f\left(Z^{[I]}\right) = 0\right] \geq 1/2$. But by Lemma 8, for every maxonomial $M$ of $f$, there exists a $Z$ that disagrees with $X$ only on variables occurring in $M$,

such that $f(Z) = 1$. It follows that for every $M$, $I$ contains the index of a variable in $M$ with probability at least $1/2$.

Given input $Y$, the randomized algorithm is as follows. First query the indices in $I$, and let $f_1$ be the restriction of $f$ induced by this. Then repeat the above procedure on $f_1$—that is, choose an $X_1$ with $f_1(X_1) = 0$ (assuming one exists), and then query a set $I_1$ drawn using a nonadaptive randomized verifier for $X_1$. Continue in this manner until $f$ is restricted to a constant function $f_T$. At this point, if $f_T$ is identically 0 then we know $f(Y) = 0$; otherwise we know $f(Y) = 1$.

Each iteration of the algorithm uses an expected number of queries at most $RC(f)$, since $RC(g) \leq RC(f)$ for every restriction $g$ of $f$. Furthermore, since an iteration shrinks each maxonomial with probability at least $1/2$, Lemma 9 implies that with $\Omega(1)$ probability, $f_T$ is constant after $T = O(ndeg(f) \log n)$ iterations. ■

Buhrman et al. [6] showed that $ndeg(f) \leq 2Q_0(f)$. Combining this with Theorems 7 and 10, we obtain a new relation between classical and quantum query complexity.

**Theorem 11** *For total $f$,*

$$R_0(f) = O\left(Q_2(f)^2 Q_0(f) \log n\right).$$

The best previous relation of this kind was $R_0(f) = O\left(Q_2(f)^2 Q_0(f)^2\right)$, due to de Wolf [23]. It is worth remarking that we also obtain

$$R_0(f) = O(R_2(f)\, ndeg(f) \log n)$$

for total $f$, since no relation between $R_0$ and $R_2$ better than $R_0(f) = O\left(R_2(f)^3\right)$ is currently known (although no asymptotic gap between $R_0$ and $R_2$ is known either [17]).

# 6 Asymptotic Gaps

Having related $RC(f)$ and $QC(f)$ to other query complexity measures in Section 5, in what follows we seek the largest possible asymptotic gaps among the measures. In particular, Section 6.1 gives a total $f$ for which $RC(f) = \Theta\left(C(f)^{0.907}\right)$ and hence $C(f) = \Theta\left(QC(f)^{2.205}\right)$, as well as a total $f$ for which $bs(f) = \Theta\left(RC(f)^{0.922}\right)$. Although these gaps are the largest of which we know, Section 6.2 shows that no 'local' technique can improve the relations $C(f) = O\left(RC(f)^2\right)$ and $RC(f) = O\left(bs(f)^2\right)$. Finally, Section 6.3 uses combinatorial designs to construct a symmetric partial $f$ for which $RC(f)$ and $QC(f)$ are $O(1)$, yet $Q_2(f) = \Omega(n/\log n)$.

## 6.1 Certificate Complexity, Randomized Certificate Complexity, and Block Sensitivity

Wegener and Zádori [21] exhibited total Boolean functions with asymptotic gaps between $C(f)$ and $bs(f)$. In similar fashion, we give a function family $\{g_t\}$ with an asymptotic gap between $C(g_t)$ and $RC(g_t)$. Let $g_1(x_1, \ldots, x_{29})$ equal 1 if and only if the Hamming weight of its input is 13, 14, 15, or 16. (The parameter 29 was found via computer search to produce a maximal separation.) Then for $t > 1$, let

$$g_t(x_1, \ldots, x_{29^t}) = g_0[g_{t-1}(X_1), \ldots, g_{t-1}(X_{29})]$$

where $X_1$ is the first $29^{t-1}$ input bits, $X_2$ is the second $29^{t-1}$, and so on. For $k \in \{0,1\}$, let

$$bs^k(f) = \max_{f(X)=k} bs^X(f),$$
$$C^k(f) = \max_{f(X)=k} C^X(f).$$

Then since $bs^0(g_1) = bs^1(g_1) = 17$, we have $bs(g_t) = 17^t$. On the other hand, $C^0(g_1) = 17$ but $C^1(g_1) = 26$, so

$$C^1(g_t) = 13C^1(g_{t-1}) + 13C^0(g_{t-1}),$$
$$C^0(g_t) = 17\max\left\{C^1(g_{t-1}), C^0(g_{t-1})\right\}.$$

Solving this recurrence yields $C(g_t) = \Theta(22.725^t)$. We can now show a gap between $C$ and $RC$.

**Proposition 12** $RC(g_t) = \Theta\left(C(g_t)^{0.907}\right)$.

**Proof.** Since $bs(g_t) = \Omega\left(C(g_t)^{0.907}\right)$, it suffices to show that $RC(g_t) = O(bs(g_t))$. The randomized verifier $V$ chooses an input variable to query as follows. Let $X$ be the claimed input, and let $K = \sum_{i=1}^{29} g_{t-1}(X_i)$. Let $I_0 = \{i : g_{t-1}(X_i) = 0\}$ and $I_1 = \{i : g_{t-1}(X_i) = 1\}$. With probability $p_K$, $V$ chooses an $i \in I_1$ uniformly at random; otherwise $A$ chooses an $i \in I_0$ uniformly at random. Here $p_K$ is as follows.

| $K$ | $[0,12]$ | 13 | 14 | 15 | 16 | $[17,29]$ |
|---|---|---|---|---|---|---|
| $p_K$ | 0 | $\frac{13}{17}$ | $\frac{7}{12}$ | $\frac{5}{12}$ | $\frac{4}{17}$ | 1 |

Once $i$ is chosen, $V$ repeats the procedure for $X_i$, and continues recursively in this manner until reaching a variable $y_j$ to query. One can check that if $g_t(X) \neq g_t(Y)$, then $g_{t-1}(X_i) \neq g_{t-1}(Y_i)$ with probability at least $1/17$. Hence $x_j \neq y_j$ with probability at least $1/17^t$, and $RC(g_t) = O(17^t)$. ■

By Theorem 7, it follows that $C(g_t) = \Theta\left(QC(g_t)^{2.205}\right)$. This offers a surprising contrast with the query complexity setting, where the best known gap between the deterministic and quantum measures is quadratic $(D(f) = \Theta\left(Q_2(f)^2\right))$.

The family $\{g_t\}$ happens *not* to yield an asymptotic gap between $bs(f)$ and $RC(f)$. The reason is that any input to $g_0$ can be covered perfectly by sensitive blocks of minimum size, with no variables left over. In general, though, we can have $bs(f) = o(RC(f))$. As reported by Bublitz et al. [8], M. Paterson found a total Boolean function $h_1(x_1,\ldots,x_6)$ such that $C^X(h_1) = 5$ and $bs^X(h_1) = 4$ for all $X$. Composing $h_1$ recursively yields $bs(h_t) = \Theta\left(C(h_t)^{0.861}\right)$ and $bs(h_t) = \Theta\left(RC(h_t)^{0.922}\right)$, both of which are the largest such gaps of which we know.

## 6.2 Local Separations

It is a longstanding open question whether the relation $C(f) \leq bs(f)^2$ due to Nisan [12] is tight. As a first step, one can ask whether the relations $C(f) = O\left(RC(f)^2\right)$ and $RC(f) = O\left(bs(f)^2\right)$ are tight. In this section we introduce a notion of *local proof* in query complexity, and then show there is no local proof that $C(f) = o\left(RC(f)^2\right)$ or that $RC(f) = o\left(bs(f)^2\right)$. This implies that proving either result would require techniques unlike those that are currently known. Our inspiration comes from computational complexity, where researchers first formalized known methods of proof, including *relativizable proofs* [4] and *natural*

*proofs* [16], and then argued that these methods were not powerful enough to resolve the field's outstanding problems.

Let $G(f)$ and $H(f)$ be query complexity measures obtained by maximizing over all inputs—that is, $G(f) = \max_{X \in Dom(f)} G^X(f)$ and $H(f) = \max_{X \in Dom(f)} H^X(f)$. Call $B \subseteq \{1, \ldots, n\}$ a *minimal block* on $X$ if $B$ is sensitive on $X$ (meaning $f\left(X^{(B)}\right) \neq f(X)$), and no sub-block $B' \subset B$ is sensitive on $X$. Also, let $X$'s *neighborhood* $\mathcal{N}(X)$ consist of $X$ together with $X^{(B)}$ for every minimal block $B$ of $X$. Consider a proof that $G(f) = O(t(H(f)))$ for some nondecreasing $t$. We call the proof *local* if it proceeds by showing that for every $X \in Dom(f)$,

$$G^X(f) = O\left(\max_{Y \in \mathcal{N}(X)} \left\{t\left(H^Y(f)\right)\right\}\right).$$

As a canonical example, Nisan's proof [12] that $C(f) \leq bs(f)^2$ is local. For each $X$, Nisan observes that (i) a maximal set of disjoint minimal blocks is a certificate for $X$, (ii) such a set can contain at most $bs^X(f)$ blocks, and (iii) each block can have size at most $\max_{Y \in \mathcal{N}(X)} bs^Y(f)$. Another example of a local proof is our proof in Section 4 that $RC(f) = O\left(QC(f)^2\right)$.

**Proposition 13** *There is no local proof that* $C(f) = o\left(RC(f)^2\right)$ *or that* $RC(f) = o\left(bs(f)^2\right)$ *for total* $f$.

**Proof.** The first part is easy: let $f(X) = 1$ if $|X| \geq \sqrt{n}$ (where $|X|$ denotes the Hamming weight of $X$), and $f(X) = 0$ otherwise. Consider the all-zero input $0^n$. We have $C^{0^n}(f) = n - \lceil\sqrt{n}\rceil + 1$, but $RC^{0^n}(f) = O(\sqrt{n})$, and indeed $RC^Y(f) = O(\sqrt{n})$ for all $Y \in \mathcal{N}(0^n)$.

For the second part, arrange the input variables in a lattice of size $\sqrt{n} \times \sqrt{n}$. Take $m = \Theta\left(n^{1/3}\right)$, and let $g(X)$ be the monotone Boolean function that outputs 1 if and only if $X$ contains a 1-*square* of size $m \times m$. This is a square of 1's that can wrap around the edges of the lattice; note that only the variables along the sides must be set to 1, not those in the interior. An example input, with a 1-square of size $3 \times 3$, is shown below.

$$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{array}$$

Clearly $bs^{0^n}(g) = \Theta\left(n^{1/3}\right)$, since there can be at most $n/m^2$ disjoint 1-squares of size $m \times m$. Also, $bs^Y(g) = \Theta\left(n^{1/3}\right)$ for any $Y$ that is 0 except for a single 1-square. On the other hand, if we choose uniformly at random among all such $Y$'s, then at any lattice site $i$, $\Pr_Y[y_i = 1] = \Theta\left(n^{-2/3}\right)$. Hence $RC^{0^n}(g) = \Omega\left(n^{2/3}\right)$. ■

## 6.3 Symmetric Partial Functions

If $f$ is partial, then $QC(f)$ can be much smaller than $Q_2(f)$. This is strikingly illustrated by the *collision problem*: let $Y = (y_1, \ldots, y_n)$ be a sequence of integers in the range $\left\{1, \ldots, n^2\right\}$, each of which can be retrieved by a single query. Let $Col(Y) = 0$ if $Y$ is one-to-one (each $y_i$ is unique), and $Col(Y) = 1$ if $Y$ is two-to-one (each $y_i$ appears exactly twice), under the promise that one of these is the case. Then $RC(Col) = QC(Col) = O(1)$, since every one-to-one input differs from every two-to-one input on at least $n/2$ of the $y_i$'s. On the other hand, Aaronson [1] showed that $Q_2(Col) = \Omega\left(n^{1/5}\right)$, and Shi [18] improved this to $\Omega\left(n^{1/3}\right)$, which is tight [7].

From the example of the collision problem, it is tempting to conjecture that (say) $Q_2(f) = O\left(n^{1/3}\right)$ whenever $QC(f) = O(1)$—that is, 'if every 0-input is far from every 1-input, then the quantum query

complexity is sublinear.' Here we disprove this conjecture, even for the special case of symmetric functions such as $Col$. (For a finite set $\mathcal{H}$, we say that $f : \mathcal{H}^n \rightarrow \{0,1\}$ is symmetric if $y_1 \ldots y_n \in Dom(f)$ implies $y_{\sigma(1)} \ldots y_{\sigma(n)} \in Dom(f)$ and $f(y_1 \ldots x_n) = f\left(y_{\sigma(1)} \ldots y_{\sigma(n)}\right)$ for every permutation $\sigma$.)

Our proof uses the following lemma, due to Nisan and Wigderson [14].

**Lemma 14 (Nisan-Wigderson)** *For any $\gamma > 1$, there exists a family of sets*

$$S_1, \ldots, S_m \subseteq \{1, \ldots, \lceil \gamma n \rceil\}$$

*such that $m = \Omega\left(2^{n/\gamma}\right)$, $|S_i| = n$ for all $i$, and $|S_i \cap S_j| \leq n/\gamma$ for all $i \neq j$.*

We will also need to adapt a lemma of Ambainis [2]. For $Z \in \{0,1\}^N$, say that a multivariate polynomial $p(Z)$ approximates $g(Z)$ if (i) $p(Z) \in [0,1]$ for *every* input $Z$ (not merely those in $Dom(f)$), and (ii) $|p(Z) - g(Z)| \leq 1/3$ for every $Z \in Dom(f)$. Also, let $\Delta(N,d) = \sum_{i=0}^{d} \binom{N}{i}$.

**Lemma 15 (Ambainis)** *At most $2^{O\left(\Delta(N,d)dN^2\right)}$ distinct Boolean functions (partial or total) can be approximated by polynomials of degree $d$.*

We can now prove the main result.

**Theorem 16** *There exists a symmetric partial $f$ for which $QC(f) = O(1)$ and $Q_2(f) = \Omega(n/\log n)$.*

**Proof.** Let $f : \mathcal{H}^n \rightarrow \{0,1\}$ where $\mathcal{H} = \{1, \ldots, 3n\}$, and let $m = \Omega\left(2^{n/3}\right)$. Let $S_1, \ldots, S_m \subseteq \mathcal{H}$ be as in Lemma 14. We put $(y_1, \ldots, y_n)$ in $Dom(f)$ if and only if $\{y_1, \ldots, y_n\} = S_j$ for some $j$. Clearly $QC(f) = O(1)$, since if $i \neq j$ then every permutation of $S_i$ differs from every permutation of $S_j$ on at least $n/3$ indices.

The number of symmetric $f$ with $Dom(f)$ as above is $2^m = 2^{\Omega\left(2^{n/3}\right)}$. We can convert any such $f$ to a Boolean function $g$ on $O(n \log n)$ variables. But Beals et al. [6] showed that, if $Q_2(g) = T$, then $g$ is approximated by a polynomial of degree at most $2T$. So by Lemma 15, if $Q_2(g) \leq T$ for every $g$ then

$$2T \cdot \Delta(n \log n, 2T) \cdot (n \log n)^2 = \Omega\left(2^{n/3}\right)$$

and we solve to obtain $T = \Omega(n/\log n)$. ■

# 7 Open Problems

Is $\widetilde{\deg}(f) = \Omega\left(\sqrt{RC(f)}\right)$, where $\widetilde{\deg}(f)$ is the minimum degree of a polynomial approximating $f$? In other words, can one lower-bound $QC(f)$ using the polynomial method of Beals et al. [6], rather than the adversary method of Ambainis [3]?

Also, is $R_0(f) = O\left(RC(f)^2\right)$? If so we obtain the new relations $R_0(f) = O\left(Q_2(f)^4\right)$ and $R_0(f) = O\left(R_2(f)^2\right)$.

# 8 Acknowledgments

I thank Ronald de Wolf for comments on the manuscript and for pointing out that $Q_E(f)$ can be replaced by $Q_0(f)$ in Theorem 11; and Umesh Vazirani and Ashwin Nayak for helpful discussions.

## References


[1] S. Aaronson. Quantum lower bound for the collision problem, in *Proc. ACM STOC'2002*, pp. 635–642, 2002. quant-ph/0111102.

[2] A. Ambainis. A note on quantum black-box complexity of almost all Boolean functions, *Inform. Proc. Lett.* 71:5–7, 1999. quant-ph/9811080.

[3] A. Ambainis. Quantum lower bounds by quantum arguments, *J. Comput. Sys. Sci.* 64:750–767, 2002. Earlier version in *STOC'2000*. quant-ph/0002066.

[4] T. Baker, J. Gill, and R. Solovay. Relativizations of the P=?NP question, *SIAM J. Comput.* 4(4):431–442, 1975.

[5] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing, *SIAM J. Comput.* 26(5):1510–1523, 1997. quant-ph/9701001.

[6] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials, in *Proc. IEEE FOCS'98*, pp. 352–361, 1998. quant-ph/9802049.

[7] G. Brassard, P. Høyer, and A. Tapp. Quantum algorithm for the collision problem, *SIGACT News (Cryptology Column)* 28:14–19, 1997. quant-ph/9705002.

[8] S. Bublitz, U. Schürfeld, B. Voigt, and I. Wegener. Properties of complexity measures for PRAMs and WRAMs, *Theoretical Comput. Sci.* 48:53–73, 1986.

[9] H. Buhrman, R. Cleve, R. de Wolf, and Ch. Zalka. Bounds for small-error and zero-error quantum algorithms, in *Proc. IEEE FOCS'99*, pp. 358–368, 1999. cs.CC/9904019.

[10] H. Buhrman and R. de Wolf. Complexity measures and decision tree complexity: a survey, to appear in *Theoretical Comput. Sci.*

[11] L. K. Grover. A fast quantum mechanical algorithm for database search, in *Proc. ACM STOC'96*, pp. 212–219, 1996. quant-ph/9605043.

[12] N. Nisan. CREW PRAMs and decision trees, *SIAM J. Comput.* 20(6):999–1007, 1991.

[13] N. Nisan and M. Szegedy. On the degree of Boolean functions as real polynomials, *Comput. Complexity* 4(4):301–313, 1994.

[14] N. Nisan and A. Wigderson. Hardness vs. randomness, *J. Comput. Sys. Sci.* 49(2):149–167, 1994.

[15] R. Raz, G. Tardos, O. Verbitsky, and N. Vereshchagin. Arthur-Merlin games in Boolean decision trees, *J. Comput. Sys. Sci.* 59(2):346–372, 1999.

[16] A. A. Razborov and S. Rudich. Natural proofs, *J. Comput. Sys. Sci.* 55(1):24–35, 1997.

[17] M. Santha. On the Monte-Carlo decision tree complexity of read-once formulae, *Random Structures and Algorithms* 6(1):75–87, 1995.

[18] Y. Shi. Quantum lower bounds for the collision and the element distinctness problems, in *Proc. IEEE FOCS'2002*, 2002. quant-ph/0112086.

[19] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* 26(5):1484–1509, 1997. quant-ph/9508027.

[20] J. Watrous. Succinct quantum proofs for properties of finite groups, in *Proc. IEEE FOCS'2000*, pp. 537–546, 2000. cs.CC/0009002.

[21] I. Wegener and L. Zádori. A note on the relations between critical and sensitive complexity, *EIK: Journal of Information Processing and Cybernetics* 25:417-421, 1989.

[22] R. de Wolf. Nondeterministic quantum query and communication complexities, to appear in *SIAM J. Comput.* Earlier version in *Proc. IEEE Complexity'2000*. cs.CC/0001014.

[23] R. de Wolf. *Quantum Computing and Communication Complexity*, PhD thesis, University of Amsterdam, 2001.