Quantum Certificate Complexity

Scott Aaronson*

Abstract

Given a Boolean function f, we study two natural generalizations of the certificate complexity $\mathrm{C}(f)$: the randomized certificate complexity $\mathrm{RC}(f)$ and the quantum certificate complexity $\mathrm{QC}(f)$. Using Ambainis' adversary method, we exactly characterize $\mathrm{QC}(f)$ as the square root of $\mathrm{RC}(f)$. We then use this result to prove the new relation $\mathrm{R}_0(f) = O\left(\mathrm{Q}_2(f)^2 \mathrm{Q}_0(f) \log n\right)$ 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 $\mathrm{C}(f)$ is superquadratic in $\mathrm{QC}(f)$, and a symmetric partial f for which $\mathrm{QC}(f) = O(1)$ yet $\mathrm{Q}_2(f) = \Omega(n/\log n)$.

Most of what is known about the power of quantum computing can be cast in the query or decision-tree model [1, 3, 4, 7, 6, 9, 10, 11, 20, 25, 24]. 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 $f : \mathcal{S} \to \{0,1\}$ be a Boolean function with $\mathcal{S} \subseteq \{0,1\}^n$, that takes input $Y = y_1 \ldots y_n$. Then the deterministic query complexity $\mathrm{D}(f)$ 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, $\mathrm{R}_2(f)$, is the minimum expected number of queries needed by a randomized algorithm that, for each Y, 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 $\mathrm{R}_0(f)$, or zero-error randomized query complexity.

Analogously, $\mathrm{Q}_2(f)$ 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, let $\mathrm{Q}_0(f)$ be the minimum number of queries needed by a quantum algorithm that outputs $f(Y)$ with probability at least $1/2$, and otherwise outputs "I don't know" (it can never output an incorrect value). If we require the algorithm to succeed with probability 1 after a fixed number of queries, we obtain $\mathrm{Q}_E(f)$, or exact quantum query complexity. See Buhrman and de Wolf [10] for a more detailed survey of these measures.

It is immediate that

$$\mathrm{Q}_2(f) \leq \mathrm{R}_2(f) \leq \mathrm{R}_0(f) \leq \mathrm{D}(f) \leq n,$$

that $\mathrm{Q}_E(f) \leq \mathrm{D}(f)$, and that $\mathrm{Q}_0(f) \leq \mathrm{R}_0(f)$.[1] If f is partial (i.e. $\mathcal{S} \neq \{0,1\}^n$), then $\mathrm{Q}_2(f)$ can be superpolynomially smaller than $\mathrm{R}_2(f)$; this is what makes Shor's period-finding algorithm [21] possible. For total f, by contrast, the largest known gap even between $\mathrm{D}(f)$ and $\mathrm{Q}_2(f)$ is quadratic, and is achieved by the OR function on n bits: $\mathrm{D}(OR) = n$ (indeed $\mathrm{R}_2(\mathrm{OR}) = \Omega(n)$), whereas $\mathrm{Q}_2(\mathrm{OR}) = \Theta(\sqrt{n})$ because of Grover's search algorithm [11]. Furthermore, for total f, Beals et al. [6] showed that $\mathrm{D}(f) = O\left(\mathrm{Q}_2(f)^6\right)$, while de Wolf [24] showed that $\mathrm{D}(f) = O\left(\mathrm{Q}_2(f)^2 \mathrm{Q}_0(f)^2\right)$.

The result of Beals et al. [6] relies on two intermediate complexity measures, the *certificate complexity* $\mathrm{C}(f)$ and *block sensitivity* $\mathrm{bs}(f)$, which are defined as follows.

*Institute for Advanced Study, Princeton, NJ 08540 USA. Email: aaronson@ias.edu. This work was done while the author was a graduate student at UC Berkeley, supported by an NSF Graduate Fellowship and by ARO grant DAAD19-03-1-0082.

[1] For $\mathrm{Q}_0(f) \leq \mathrm{R}_0(f)$: by Markov's inequality, any randomized algorithm that succeeds in finding a 0- or 1-certificate after an expected number of queries T, has found such a certificate with probability at least $1/2$ after $2T$ queries. So it suffices for the quantum algorithm to simulate the first $2T$ queries of the randomized algorithm.

	Deterministic	Randomized	Quantum
Query complexity	$\mathrm{D}(f)$	$\mathrm{R}_2(f)$	$\mathrm{Q}_2(f)$
Certificate complexity	$\mathrm{C}(f)$	$\mathrm{RC}(f)$	$\mathrm{QC}(f)$

Table 1: Query complexity measures and their certificate complexity analogues.

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

Clearly $\mathrm{bs}(f) \leq \mathrm{C}(f) \leq \mathrm{D}(f)$. For total f, these measures are all polynomially related: Nisan [14] showed that $\mathrm{C}(f) \leq \mathrm{bs}(f)^2$, while Beals et al. [6] showed that $\mathrm{D}(f) \leq \mathrm{C}(f)\,\mathrm{bs}(f)$. Combining these results with $\mathrm{bs}(f) = O\left(\mathrm{Q}_2(f)^2\right)$ (from the optimality of Grover's algorithm), one obtains $\mathrm{D}(f) = O\left(\mathrm{Q}_2(f)^6\right)$.

1 Summary of Results

We investigate $\mathrm{RC}(f)$ and $\mathrm{QC}(f)$, the bounded-error randomized and quantum generalizations of the certificate complexity $\mathrm{C}(f)$ (see Table 8.1). My motivation is that, just as $\mathrm{C}(f)$ was used to show a polynomial relation between $\mathrm{D}(f)$ and $\mathrm{Q}_2(f)$, so $\mathrm{RC}(f)$ and $\mathrm{QC}(f)$ can lead to new relations among fundamental query complexity measures.

What the certificate complexity $\mathrm{C}(f)$ 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 $\mathrm{C}(f)$, 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[2]—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 $\mathrm{RC}(f)$ as follows.

Definition 3 *A randomized verifier for input X is a randomized algorithm that, on input Y to 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 $\mathrm{RC}^X(f)$ is the minimum expected number of queries used by a randomized verifier for X, and $\mathrm{RC}(f)$ is the maximum of $\mathrm{RC}^X(f)$ over all X.*

We define $\mathrm{QC}(f)$ analogously, with quantum instead of randomized algorithms. The following justifies the definition (the $\mathrm{RC}(f)$ part was originally shown by Raz et al. [17]).

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

Proof. For $\mathrm{RC}(f)$, 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 $\Pr\left[r_V^Y\right] \leq \varepsilon_0$ if $Y = X$ and $\Pr\left[r_V^Y\right] \geq 1 - \varepsilon_1$ if $f(Y) \neq f(X)$. We wish to lower-bound $\Pr\left[d_V^Y\right]$ for all Y such that $f(Y) \neq f(X)$. Observe that any time V rejects on Y without having encountered a disagreement with X, the same sequence of coin tosses would also cause it to reject on X. So

$$\begin{aligned}\Pr\left[r_V^Y \wedge \neg d_V^Y\right] &\leq \Pr\left[r_V^X \wedge \neg d_V^X\right] \\ &= \Pr\left[r_V^X\right] \\ &\leq \varepsilon_0,\end{aligned}$$

[2]Throughout this chapter, I use Y to denote the 'actual' input being queried, and X to denote the 'claimed' input.

where the second line follows since $\Pr\left[\neg d_V^X\right] = 1$. Hence for $f(Y) \neq f(X)$,

$$\begin{aligned}\Pr\left[d_V^Y\right] &\geq \Pr\left[r_V^Y\right] - \Pr\left[r_V^Y \wedge \neg d_V^Y\right] \\ &\geq 1 - \varepsilon_1 - \varepsilon_0.\end{aligned}$$

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 $f(Y) \neq f(X)$,

$$\begin{aligned}\Pr\left[r_{V^*}^Y\right] &= \Pr\left[d_V^Y\right] \\ &\geq 1 - \varepsilon_1 - \varepsilon_0.\end{aligned}$$

The result follows since $O(1)$ repetitions suffice to boost any constant error probability to any other constant error probability.

For $\mathrm{QC}(f)$, assume without loss of generality that all amplitudes are real. 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 $\mathrm{QC}(f) \leq \mathrm{RC}(f) \leq \mathrm{C}(f)$, that $\mathrm{QC}(f) = O(\mathrm{Q}_2(f))$, and that $\mathrm{RC}(f) = O(\mathrm{R}_2(f))$. We also have $\mathrm{RC}(f) = \Omega(\mathrm{bs}(f))$, since a randomized verifier for X must query each sensitive block on X with $1/2$ probability. This suggests viewing $\mathrm{RC}(f)$ as an 'alloy' of block sensitivity and certificate complexity, an interpretation for which Section 5 gives some justification.

The results of this paper are as follows. In Section 3 we show that $\mathrm{QC}(f) = \Theta\left(\sqrt{\mathrm{RC}(f)}\right)$ 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 $\mathrm{RC}(f)$, and then apply the adversary method of Ambainis [4] to lower-bound $\mathrm{QC}(f)$ in terms of this characterization. Then, in Section 4, we extend results on polynomials due to de Wolf [24] and to Nisan and Smolensky (as described by Buhrman and de Wolf [10]), to show that $\mathrm{R}_0(f) = O(\mathrm{RC}(f)\,\mathrm{ndeg}(f)\log n)$ for all total f, where $\mathrm{ndeg}(f)$ 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 3 and 4 leads to a new lower bound on quantum query complexity: that $\mathrm{R}_0(f) = O\left(\mathrm{Q}_2(f)^2\,\mathrm{Q}_0(f)\log n\right)$ 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 5, we exhibit asymptotic gaps between $\mathrm{RC}(f)$ and other query complexity measures, including a total f for which $\mathrm{C}(f) = \Theta\left(\mathrm{QC}(f)^{2.205}\right)$, and a symmetric partial f for which $\mathrm{QC}(f) = O(1)$ yet $\mathrm{Q}_2(f) = \Omega(n/\log n)$. We conclude in Section 6 with some open problems.

2 Related Work

Raz et al. [17] studied a query complexity measure they called $\mathrm{ma}(f)$, for Merlin-Arthur. In our notation, $\mathrm{ma}(f)$ equals the maximum of $\mathrm{RC}^X(f)$ over all X with $f(X)=1$. Raz et al. observed that $\mathrm{ma}(f)=\mathrm{ip}(f)$, where $\mathrm{ip}(f)$ 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 $\mathrm{ma}(f)=O(1)$ but $\mathrm{C}(f)=\Omega(n)$. This has similarities to the construction, in Section 5.2, of a symmetric partial f for which $\mathrm{QC}(f)=O(1)$ but $\mathrm{Q}_2(f)=\Omega(n/\log n)$.

Very recently Midrijanis [13] has shown that $\mathrm{D}(f)=O\left(\mathrm{Q}_2(f)^2\,\mathrm{Q}_0(f)\right)$ for all total f. This improves on our $\mathrm{R}_0(f)=O\left(\mathrm{Q}_2(f)^2\,\mathrm{Q}_0(f)\log n\right)$ result in two ways: first, the simulation is deterministic instead of randomized, and second, there is no $\log n$ factor. By modifying our simulation procedure in a simple but critical respect, Midrijanis was able to use the ordinary block sensitivity $\mathrm{bs}(f)$ instead of $\mathrm{RC}(f)$.

Watrous [22] has investigated a different notion of "quantum certificate complexity"—whether certificates that are quantum states can be superpolynomially smaller than any classical certificate. Raz and Shpilka [16] have further considered quantum query complexity and quantum communication complexity in the QMA (Quantum Merlin Arthur) model. Also, de Wolf [25] 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 $f(Y)=1$.

3 Characterization of Quantum Certificate Complexity

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

Lemma 5 *Call a randomized verifier for X nonadaptive if, on input Y, it queries each y_i with independent probability λ_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 $\mathrm{RC}^X_{na}(f)$ be the minimum of $\lambda_1+\cdots+\lambda_n$ over all nonadaptive verifiers for X. Then $\mathrm{RC}^X_{na}(f)=\Theta\left(\mathrm{RC}^X(f)\right)$.*

Proof. Clearly $\mathrm{RC}^X_{na}(f)=\Omega\left(\mathrm{RC}^X(f)\right)$. 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 $T=\left\lceil 2\,\mathrm{RC}^X(f)\right\rceil$ queries. So by the union bound

$$p_1(Y)+\cdots+p_T(Y)\geq\frac{1}{2}$$

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 λ_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 λ_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 $\mathrm{QC}(f)$, we will use the following simple reformulation of Ambainis's quantum adversary method [4].

Theorem 6 (Ambainis) *Given a function $f : \mathcal{S} \rightarrow \{0,1\}$ with $\mathcal{S} \subseteq \{0,1\}^n$, let β be a function from $\mathcal{S}$ to nonnegative reals, and let $R : \mathcal{S}^2 \rightarrow \{0,1\}$ 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 $X \in \mathcal{S}$ 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 $\mathrm{Q}_2(f) = \Omega\left(\sqrt{\frac{1}{\delta_0 \delta_1}}\right)$.

We now prove the main result of the section.

Theorem 7 *For all f (partial or total) and all X,*

$$\mathrm{QC}^X(f) = \Theta\left(\sqrt{\mathrm{RC}^X(f)}\right).$$

Proof. Let $(\lambda_1,\ldots,\lambda_n)$ be an optimal nonadaptive randomized verifier for $X = x_1 \ldots x_n$, and let

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

We first show that $\mathrm{QC}^X(f) = O\left(\sqrt{S}\right)$. Given an input $Y = y_1 \ldots y_n$, the goal is to find an i such that $y_i \neq x_i$. To do so, we run a weighted version of Grover's search algorithm, in which there are $\lceil n\lambda_i/S \rceil$ basis states querying y_i (and which consider it marked if $y_i \neq x_i$). Thus, the total number of basis states is

$$\begin{aligned}\sum_{i=1}^n \left\lceil \frac{n\lambda_i}{S} \right\rceil &= \left(\sum_{i=1}^n \frac{n\lambda_i}{S}\right) + O(n) \\ &= O(n),\end{aligned}$$

and the proportion of basis states that query y_i is

$$\frac{\lceil n\lambda_i/S \rceil}{\sum_{j=1}^n \lceil n\lambda_j/S \rceil} = \Omega\left(\frac{\lambda_i}{S}\right).$$

Let $\mathcal{Y} = \{Y : f(Y) \neq f(X)\}$. Then for any $Y \in \mathcal{Y}$, the expected number of iterations needed to find a disagreement with X with probability $\Omega(1)$ is just $O\left(\sqrt{S}\right)$, the square root of the number needed classically.

We now show that $\mathrm{QC}^X(f) = \Omega\left(\sqrt{S}\right)$. 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 Alice and Bob both play optimally, then Alice can win this game with probability at most $O(1/S)$. For otherwise Alice's strategy would yield a verifier $(\lambda'_1,\ldots,\lambda'_n)$ with

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

contradicting the optimality of $(\lambda_1,\ldots,\lambda_n)$. Hence, by the minimax theorem, there exists a distribution μ over $\mathcal{Y}$ such that for all $i \in \{1,\ldots,n\}$,

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

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. It follows that the quantum query complexity of distinguishing X from an arbitrary $Y \in \mathcal{Y}$ is $\Omega\left(\sqrt{S}\right)$. ■

4 Quantum Lower Bound for Total Functions

The goal of this section is to show that

$$\mathrm{R}_0(f) = O\left(\mathrm{Q}_2(f)^2 \mathrm{Q}_0(f) \log n\right)$$

for all total f. 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 $\mathrm{ndeg}(f)$ 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. A monomial M is called 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 the polynomial q that nondeterministically represents it 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 [24] showed that $\mathrm{D}(f) \leq \mathrm{C}(f)\,\mathrm{ndeg}(f)$ for all total f, slightly improving the result $\mathrm{D}(f) \leq \mathrm{C}(f)\deg(f)$ due to Buhrman and de Wolf [10]. In Theorem 10, we will give an analogue 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. Let A be a set of nontrivial (degree 1 or higher) monomials, and consider the weighting function

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

Let S be the set of nontrivial monomials of p. Initially $\omega(S) \leq n^{\deg(p)} \deg(p)!$, and we are done when $\omega(S) = 0$ (or equivalently S is empty, p having been restricted to a constant polynomial). The claim is 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 $\binom{\deg(M)}{\ell}$ distinct M^* with $\deg(M^*) = \ell$. Hence

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

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 $\deg(M) = 1$). When this occurs, the contribution of M is at least halved. 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 $1/2$. ■

We can now prove the main result.[3]

[3] The proof of Theorem 10 that I gave previously [2] makes a claim that is both superfluous for proving the theorem and false. I am grateful to Gatis Midrijanis for pointing this out to me.

Theorem 10 *For total f,*

$$\mathrm{R}_0(f) = O\left(\mathrm{RC}(f)\,\mathrm{ndeg}(f)\log n\right).$$

Proof. The algorithm is as follows.

```
Repeat
    Choose a 0-input X compatible with all queries made so far[4]
    Query a randomized 0-certificate for X
Until f has been restricted to a constant function
```

Let p be a polynomial that nondeterministically represents f. Then the key fact is that for every 0-input X, when we query a randomized 0-certificate for X we "hit" each maxonomial M of p with probability at least $1/2$. Here hitting M means querying a variable in M. This is because, by Lemma 8, it is possible to change $f(X)$ from 0 to 1 just by flipping variables in M. So a randomized certificate would be incorrect if it probed those variables with probability less than $1/2$.

Therefore, each iteration of the algorithm shrinks each maxonomial of p with probability at least $1/2$. It follows from Lemma 9 that the algorithm terminates after an expected number of iterations $O(\deg(p)\log n)$. ■

Buhrman et al. [6] showed that $\mathrm{ndeg}(f) \leq 2\,\mathrm{Q}_0(f)$ (indeed $\mathrm{ndeg}(f) = \mathrm{Q}_0(f)$, as shown by Høyer and de Wolf [12]). Combining this with Theorems 7 and 10 yields a new relation between classical and quantum query complexity.

Theorem 11 *For all total f,*

$$\mathrm{R}_0(f) = O\left(\mathrm{Q}_2(f)^2\,\mathrm{Q}_0(f)\log n\right).$$

The best previous relation of this kind was $\mathrm{R}_0(f) = O\left(\mathrm{Q}_2(f)^2\,\mathrm{Q}_0(f)^2\right)$, due to de Wolf [24]. It is worth mentioning another corollary of Theorems 7 and 10, this one purely classical:

Corollary 12 *For all total f,*

$$\mathrm{R}_0(f) = O\left(\mathrm{R}_2(f)\,\mathrm{ndeg}(f)\log n\right)$$

Previously, no relation between R_0 and R_2 better than $\mathrm{R}_0(f) = O\left(\mathrm{R}_2(f)^3\right)$ was known (although no asymptotic gap between R_0 and R_2 is known either [19]). Subsequent to this work, Midrijanis [13] has also shown that $\mathrm{R}_0(f) = O\left(\mathrm{R}_2(f)^2\log n\right)$ for all total f.

5 Asymptotic Gaps

Having related $\mathrm{RC}(f)$ and $\mathrm{QC}(f)$ to other query complexity measures in Section 4, in what follows we seek the largest possible asymptotic gaps among the measures. In particular, we give a total f for which $\mathrm{RC}(f) = \Theta\left(\mathrm{C}(f)^{0.907}\right)$ and hence $\mathrm{C}(f) = \Theta\left(\mathrm{QC}(f)^{2.205}\right)$, as well as a total f for which $\mathrm{bs}(f) = \Theta\left(\mathrm{RC}(f)^{0.922}\right)$. Although these gaps are the largest of which we know, Section 5.1 shows that no 'local' technique can improve the relations $\mathrm{C}(f) = O\left(\mathrm{RC}(f)^2\right)$ and $\mathrm{RC}(f) = O\left(\mathrm{bs}(f)^2\right)$. Finally, Section 5.2 uses combinatorial designs to construct a symmetric partial f for which $\mathrm{RC}(f)$ and $\mathrm{QC}(f)$ are $O(1)$, yet $\mathrm{Q}_2(f) = \Omega(n/\log n)$.

Wegener and Zádori [23] exhibited total Boolean functions with asymptotic gaps between $\mathrm{C}(f)$ and $\mathrm{bs}(f)$. In similar fashion, we give a function family $\{g_t\}$ with an asymptotic gap between $\mathrm{C}(g_t)$ and $\mathrm{RC}(g_t)$. 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

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

[4] Clearly, as long as f is not a constant function, there *exists* a 0-input X compatible with all queries made so far.

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

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

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

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

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

Proposition 13 $\mathrm{RC}(g_t) = \Theta\left(\mathrm{C}(g_t)^{0.907}\right)$.

Proof. Since $\mathrm{bs}(g_t) = \Omega\left(\mathrm{C}(g_t)^{0.907}\right)$, it suffices to show that $\mathrm{RC}(g_t) = O(\mathrm{bs}(g_t))$. 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 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 the verifier detects the change with probability at least $1/17^t$, and $\mathrm{RC}(g_t) = O(17^t)$. ■

By Theorem 7, it follows that $\mathrm{C}(g_t) = \Theta\left(\mathrm{QC}(g_t)^{2.205}\right)$. This offers a surprising contrast with the query complexity setting, where the best known gap between the deterministic and quantum measures is quadratic ($\mathrm{D}(f) = \Theta\left(\mathrm{Q}_2(f)^2\right)$).

The family $\{g_t\}$ happens *not* to yield an asymptotic gap between $\mathrm{bs}(f)$ and $\mathrm{RC}(f)$. 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, one can have $\mathrm{bs}(f) = o(\mathrm{RC}(f))$. As reported by Bublitz et al. [8], M. Paterson found a total Boolean function $h_1(x_1,\ldots,x_6)$ such that $\mathrm{C}^X(h_1) = 5$ and $\mathrm{bs}^X(h_1) = 4$ for all X. Composing h_1 recursively yields $\mathrm{bs}(h_t) = \Theta\left(\mathrm{C}(h_t)^{0.861}\right)$ and $\mathrm{bs}(h_t) = \Theta\left(\mathrm{RC}(h_t)^{0.922}\right)$, both of which are the largest such gaps of which we know.

5.1 Local Separations

It is a longstanding open question whether the relation $\mathrm{C}(f) \leq \mathrm{bs}(f)^2$ due to Nisan [14] is tight. As a first step, one can ask whether the relations $\mathrm{C}(f) = O\left(\mathrm{RC}(f)^2\right)$ and $\mathrm{RC}(f) = O\left(\mathrm{bs}(f)^2\right)$ are tight. In this section we introduce a notion of *local proof* in query complexity, and then show there is no local proof that $\mathrm{C}(f) = o\left(\mathrm{RC}(f)^2\right)$ or that $\mathrm{RC}(f) = o\left(\mathrm{bs}(f)^2\right)$. This implies that proving either result would require techniques unlike those that are currently known. My inspiration comes from computational complexity, where researchers first formalized known methods of proof, including *relativizable proofs* [5] and *natural proofs* [18], 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,

$$G(f) = \max_X G^X(f),$$
$$H(f) = \max_X H^X(f).$$

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 actually shows the stronger statement that for every input X,

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

As a canonical example, Nisan's proof [14] that $\mathrm{C}(f) \leq \mathrm{bs}(f)^2$ 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 $\mathrm{bs}^X(f)$ blocks, and (iii) each block can have size at most $\max_{Y \in \mathcal{N}(X)} \mathrm{bs}^Y(f)$. Another example of a local proof is the proof in Section 3 that $\mathrm{RC}(f) = O\left(\mathrm{QC}(f)^2\right)$.

Admittedly, "local proof" is not a mathematically precise notion. But to show that no proof of a statement P can proceed by showing the stronger statement Q, all one needs to show is that Q is false! This is similar to how one shows that there is no relativizable proof of $\mathsf{P} \neq \mathsf{NP}$: by exhibiting an oracle relative to which $\mathsf{P} = \mathsf{NP}$.

Proposition 14 *There is no local proof showing that* $\mathrm{C}(f) = o\left(\mathrm{RC}(f)^2\right)$ *or that* $\mathrm{RC}(f) = o\left(\mathrm{bs}(f)^2\right)$ *for all 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 $\mathrm{C}^{0^n}(f) = n - \lceil\sqrt{n}\rceil + 1$, but $\mathrm{RC}^{0^n}(f) = O(\sqrt{n})$, and indeed $\mathrm{RC}^Y(f) = O(\sqrt{n})$ 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 3×3, 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 $\mathrm{bs}^{0^n}(g) = \Theta\left(n^{1/3}\right)$, since there can be at most n/m^2 disjoint 1-squares of size $m \times m$. Also, $\mathrm{bs}^Y(g) = \Theta\left(n^{1/3}\right)$ 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 $\mathrm{RC}^{0^n}(g) = \Omega\left(n^{2/3}\right)$. ■

5.2 Symmetric Partial Functions

If f is partial, then $\mathrm{QC}(f)$ can be much smaller than $\mathrm{Q}_2(f)$. This is strikingly illustrated by the collision problem: let $\mathrm{Col}(Y) = 0$ if $Y = y_1 \ldots y_n$ is a one-to-one sequence and $\mathrm{Col}(Y) = 1$ if Y is a two-to-one sequence, promised that one of these is the case. Then $\mathrm{RC}(\mathrm{Col}) = \mathrm{QC}(\mathrm{Col}) = O(1)$, 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 $\mathrm{Q}_2(\mathrm{Col}) = \Omega\left(n^{1/5}\right)$.

¿From the example of the collision problem, it is tempting to conjecture that (say) $\mathrm{Q}_2(f) = O\left(n^{1/3}\right)$ whenever $\mathrm{QC}(f) = O(1)$—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. (Given a finite set $\mathcal{H}$, a function $f : \mathcal{S} \to \{0,1\}$ where $\mathcal{S} \subseteq \mathcal{H}^n$ is called symmetric if $x_1 \ldots x_n \in \mathcal{S}$ implies $x_{\sigma(1)} \ldots x_{\sigma(n)} \in \mathcal{S}$ and $f(x_1 \ldots x_n) = f\left(x_{\sigma(1)} \ldots x_{\sigma(n)}\right)$ for every permutation σ.)

The proof uses the following lemma, which can be found in Nisan and Wigderson [15] for example.

Lemma 15 (Nisan-Wigderson) *For any $\gamma > 1$, there exists a family of sets*

$$A_1, \ldots, A_m \subseteq \{1, \ldots, \lceil \gamma n \rceil\}$$

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

A lemma due to Ambainis [3] is also useful. Let $f : \mathcal{S} \to \{0,1\}$ where $\mathcal{S} \subseteq \{0,1\}^n$ be a partial Boolean function, and let $p : \{0,1\}^n \to \mathbb{R}$ be a real-valued multilinear polynomial. We say that p approximates f if (i) $p(X) \in [0,1]$ for every input $X \in \{0,1\}^n$ (not merely those in $\mathcal{S}$), and (ii) $|p(X) - g(X)| \leq 1/3$ for every $X \in \mathcal{S}$.

Lemma 16 (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, where $\Delta(n,d) = \sum_{i=0}^{d} \binom{n}{i}$.*

The result is an easy consequence of Lemmas 15 and 16.

Theorem 17 *There exists a symmetric partial function f from $\{1, \ldots, 3n\}^n$ to $\{0,1\}$, for which $\mathrm{QC}(f) = O(1)$ and $\mathrm{Q}_2(f) = \Omega(n/\log n)$. Here QC and Q_2 refer to the number of bits that must be queried (thus, the result is a factor $\log^2 n$ from optimal).*

Proof. Let $f : \mathcal{S} \to \{0,1\}$ where $\mathcal{S} \subseteq \{1, \ldots, 3n\}^n$, and let $m = \Omega\left(2^{n/3}\right)$. Let $A_1, \ldots, A_m \subseteq \{1, \ldots, 3n\}$ be as in Lemma 15. We put $x_1, \ldots, x_n$ in $\mathcal{S}$ if and only if $\{x_1, \ldots, x_n\} = A_j$ for some j. Clearly $\mathrm{QC}(f) = O(1)$, since if $i \neq j$ then every permutation of A_i differs from every permutation of A_j on at least $n/3$ indices. The number of symmetric f with $\mathcal{S}$ as above is $2^m = 2^{\Omega\left(2^{n/3}\right)}$. We can represent any such f as a Boolean function g on $O(n \log n)$ variables, with $\mathrm{Q}_2(g) = \mathrm{Q}_2(f)$ and $\mathrm{QC}(g) = \mathrm{QC}(f)$. But Beals et al. [6] showed that, if $\mathrm{Q}_2(g) = T$, then g is approximated by a polynomial of degree at most $2T$. So by Lemma 16, if $\mathrm{Q}_2(g) \leq T$ 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 $T = \Omega(n/\log n)$. ■

6 Open Problems

Is $\widetilde{\deg}(f) = \Omega\left(\sqrt{\mathrm{RC}(f)}\right)$, where $\widetilde{\deg}(f)$ is the minimum degree of a polynomial approximating f? In other words, can one lower-bound $\mathrm{QC}(f)$ using the polynomial method of Beals et al. [6], rather than the adversary method of Ambainis [4]?

Also, is $\mathrm{R}_0(f) = O\left(\mathrm{RC}(f)^2\right)$? If so we obtain the new relations $\mathrm{R}_0(f) = O\left(\mathrm{Q}_2(f)^4\right)$ and $\mathrm{R}_0(f) = O\left(\mathrm{R}_2(f)^2\right)$.

7 Acknowledgments

I thank Ronald de Wolf for comments on the manuscript and for pointing out that $\mathrm{Q}_E(f)$ can be replaced by $\mathrm{Q}_0(f)$ in Theorem 11; Gatis Midrijanis for finding an error in an earlier proof of Theorem 10; and Umesh Vazirani and Ashwin Nayak for helpful discussions.

References

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

[2] S. Aaronson. Quantum certificate complexity. In *Proc. IEEE Conference on Computational Complexity*, pages 171–178, 2003. ECCC TR03-005, quant-ph/0210020.

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

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

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

[6] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001. Earlier version in IEEE FOCS 1998, pp. 352-361. quant-ph/9802049.

[7] 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.

[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*, pages 358–368, 1999. cs.CC/9904019.

[10] H. Buhrman and R. de Wolf. Complexity measures and decision tree complexity: a survey. *Theoretical Comput. Sci.*, 288:21–43, 2002.

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

[12] P. Høyer and R. de Wolf. Improved quantum communication complexity bounds for disjointness and equality. In *Proc. Intl. Symp. on Theoretical Aspects of Computer Science (STACS)*, pages 299–310, 2002. quant-ph/0109068.

[13] G. Midrijanis. On randomized and quantum query complexities. In preparation, 2005.

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

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

[16] R. Raz and A. Shpilka. On the power of quantum proofs. In *Proc. IEEE Conference on Computational Complexity*, pages 260–274, 2004.

[17] 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.

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

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

[20] Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. In *Proc. IEEE FOCS*, pages 513–519, 2002. quant-ph/0112086.

[21] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. Earlier version in IEEE FOCS 1994. quant-ph/9508027.

[22] J. Watrous. Succinct quantum proofs for properties of finite groups. In *Proc. IEEE FOCS*, pages 537–546, 2000. cs.CC/0009002.

[23] 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.

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

[25] R. de Wolf. Characeterization of non-deterministic quantum query and quantum communication complexity. *SIAM J. Comput.*, 32(3):681–699, 2003. Earlier version in Proc. IEEE Complexity 2000. cs.CC/0001014.