Impossibility of Succinct Quantum Proofs for Collision-Freeness

Scott Aaronson*

Abstract

We show that any quantum algorithm to decide whether a function $f : [n] \to [n]$ is a permutation or far from a permutation must make $\Omega\left(n^{1/3}/w\right)$ queries to f, even if the algorithm is given a w-qubit quantum witness in support of f being a permutation. This implies that there exists an oracle A such that $\mathsf{SZK}^A \not\subset \mathsf{QMA}^A$, answering an eight-year-old open question of the author. Indeed, we show that relative to some oracle, SZK is not in the counting class $\mathsf{A_0PP}$ defined by Vyalyi. The proof is a fairly simple extension of the quantum lower bound for the collision problem.

1 Introduction

The *collision problem* is to decide whether a black-box function $f : [n] \to [n]$ is one-to-one (i.e., a permutation) or two-to-one function, promised that one of these is the case. Together with its close variants, the collision problem is one of the central problems studied in quantum computing theory; it abstractly models numerous other problems such as graph isomorphism and the breaking of cryptographic hash functions.

In this paper, we will mostly deal with a slight generalization of the collision problem that we call the *Permutation Testing Problem*, or PTP. This is a property testing problem, in which we are promised that $f : [n] \to [n]$ is either a permutation or far from any permutation, and are asked to decide which is the case.

In 1997, Brassard, Høyer, and Tapp [8] gave a quantum algorithm for the collision problem that makes $O\left(n^{1/3}\right)$ queries to f, an improvement over the $\Theta\left(\sqrt{n}\right)$ randomized query complexity that follows from the birthday paradox. Brassard et al.'s algorithm is easily seen to work for the PTP as well.

Five years later, Aaronson [1] proved the first non-constant lower bound for these problems: namely, any bounded-error quantum algorithm to solve them needs $\Omega\left(n^{1/5}\right)$ queries to f. Aaronson and Shi [4] subsequently improved the lower bound to $\Omega\left(n^{1/3}\right)$, for functions $f : [n] \to [3n/2]$; then Ambainis [5] and Kutin [11] proved the optimal $\Omega\left(n^{1/3}\right)$ lower bound for functions $f : [n] \to [n]$. All of these lower bounds work for both the collision problem and the PTP, though they are slightly easier to prove for the latter.

The collision problem and the PTP are easily seen to admit Statistical Zero-Knowledge (SZK) proof protocols. Thus, one consequence of the collision lower bound was the existence of an oracle A such that $\mathsf{SZK}^A \not\subset \mathsf{BQP}^A$.

*MIT. Email: aaronson@csail.mit.edu. This material is based upon work supported by the National Science Foundation under Grant No. 0844626. Also supported by a DARPA YFA grant, a Sloan Fellowship, a TIBCO Chair, and an NSF STC on Science of Information.

In talks beginning in 2002,[1] the author often raised the following question:

> *Suppose a function $f : [n] \to [n]$ is a permutation, rather than far from a permutation. Is there a small (*$\operatorname{polylog}(n)$*-qubit) quantum proof $|\varphi_f\rangle$ of that fact, which can be verified using* $\operatorname{polylog}(n)$ *quantum queries to f?*

In this paper, we will answer the above question in the negative. As a consequence, we will obtain an oracle A such that $\mathsf{SZK}^A \not\subset \mathsf{QMA}^A$. This implies, for example, that any QMA protocol for graph non-isomorphism would need to exploit something about the problem structure beyond its reducibility to the collision problem.

Given that the relativized SZK versus QMA problem remained open for eight years, our solution is surprisingly simple. We first use the in-place amplification procedure of Marriott and Watrous [12] to "eliminate the witness," and reduce the question to one about quantum algorithms with extremely small acceptance probabilities. We then use a relatively-minor adaptation of the polynomial degree argument that was used to prove the original collision lower bound. Our proof actually yields an oracle A such that $\mathsf{SZK}^A \not\subset \mathsf{A_0PP}^A$, where $\mathsf{A_0PP}$ is a class defined by Vyalyi [15] that sits between QMA and PP.

Despite the simplicity of our result, to our knowledge it constitutes *the first nontrivial lower bound on* QMA *query complexity*, where "nontrivial" means that it doesn't follow immediately from earlier results unrelated to QMA.[2] We hope it will serve as a starting point for stronger results in the same vein.

2 Preliminaries

We assume familiarity with quantum query complexity, as well as with complexity classes such as QMA (Quantum Merlin-Arthur), QCMA (Quantum Merlin-Arthur with classical witnesses), and SZK (Statistical Zero-Knowledge). See Buhrman and de Wolf [9] for a good introduction to quantum query complexity, and the Complexity Zoo[3] for definitions of complexity classes.

We now define the main problem we will study.

Problem 1 (Permutation Testing Problem or PTP) *Given black-box access to a function $f : [n] \to [n]$, and promised that either*

(i) f is a permutation (i.e., is one-to-one), or

(ii) f differs from every permutation on at least $n/8$ coordinates.

The problem is to accept if (i) holds and reject if (ii) holds.

[1] See for example: *Quantum Lower Bounds*, www.scottaaronson.com/talks/lower.ppt; *The Future (and Past) of Quantum Lower Bounds by Polynomials*, www.scottaaronson.com/talks/future.ppt; *The Polynomial Method in Quantum and Classical Computing*, www.scottaaronson.com/talks/polymeth.ppt.

[2] From the BBBV lower bound for quantum search [6], one immediately obtains an oracle A such that $\mathsf{coNP}^A \not\subset \mathsf{QMA}^A$: for if there exists a witness state $|\varphi\rangle$ that causes a QMA verifier to accept the all-0 oracle string, then that same $|\varphi\rangle$ must also cause the verifier to accept some string of Hamming weight 1. Also, since $\mathsf{QMA} \subseteq \mathsf{PP}$ relative to all oracles, the result of Vereshchagin [14] that there exists an oracle A such that $\mathsf{AM}^A \not\subset \mathsf{PP}^A$ implies an A such that $\mathsf{AM}^A \not\subset \mathsf{QMA}^A$ as well.

[3] www.complexityzoo.com

In the above definition, the choice of $n/8$ is arbitrary; it could be replaced by cn for any $0 < c < 1$.

As mentioned earlier, Aaronson [1] defined the collision problem as that of deciding whether f is *one-to-one or two-to-one*, promised that one of these is the case. In this paper, we are able to prove a QMA lower bound for PTP, but not for the original collision problem.

Fortunately, however, most of the desirable properties of the collision problem carry over to PTP. As an example, we now observe a simple SZK protocol for PTP.

Proposition 2 *PTP has an (honest-verifier) Statistical Zero-Knowledge proof protocol, requiring $O(\log n)$ time and $O(1)$ queries to f.*

Proof. The protocol is the following: to check that $f : [n] \to [n]$ is one-to-one, the verifier picks an input $x \in [n]$ uniformly at random, sends $f(x)$ to the prover, and accepts if and only if the prover returns x. Since the verifier already knows x, it is clear that this protocol has the zero-knowledge property.

If f is a permutation, then the prover can always compute $f^{-1}(f(x))$, so the protocol has perfect completeness.

If f is $n/8$-far from a permutation, then with at least $1/8$ probability, the verifier picks an x such that $f(x)$ has no unique preimage, in which case the prover can find x with probability at most $1/2$. So the protocol has constant soundness. ■

2.1 Upper Bounds

To build intuition, we now give a simple QMA *upper* bound for the collision problem. Indeed, this will actually be a QCMA upper bound, meaning that the witness is classical, and only the verification procedure is quantum.

Theorem 3 *For all $w \in [0, n]$, there exists a QCMA protocol for the collision problem—i.e., for verifying that $f : [n] \to [n]$ is one-to-one rather than two-to-one—that uses a $w \log n$-bit classical witness and makes $O\left(\min\left\{\sqrt{n/w}, n^{1/3}\right\}\right)$ quantum queries to f.*

Proof. If $w = O\left(n^{1/3}\right)$, then the verifier V can just ignore the witness and solve the problem in $O\left(n^{1/3}\right)$ queries using the Brassard-Høyer-Tapp algorithm [8]. So assume $w \geq Cn^{1/3}$ for some suitable constant C.

The witness will consist of claimed values $f'(1), \ldots, f'(w)$ for $f(1), \ldots, f(w)$ respectively. Given this witness, V runs the following procedure.

(Step 1) Choose a set of indices $X \subset [w]$ with $|X| = O(1)$ uniformly at random. Query $f(x)$ for each $x \in X$, and reject if there is an $x \in X$ such that $f(x) \neq f'(x)$.

(Step 2) Choose a set of indices $Y \subset \{w+1, \ldots, n\}$ with $|Y| = n/w$ uniformly at random. Use Grover's algorithm to look for a $y \in Y$ such that $f(y) = f'(x)$ for some $x \in [w]$. If such a y is found, then reject; otherwise accept.

Clearly this procedure makes $O\left(\sqrt{n/w}\right)$ quantum queries to f. For completeness, notice that if f is one-to-one, and the witness satisfies $f'(x) = f(x)$ for all $x \in [w]$, then V accepts with probability 1. For soundness, suppose that Step 1 accepts. Then with high probability, we have $f'(x) = f(x)$ for at least (say) a $2/3$ fraction of $x \in [w]$. However, as in the analysis of Brassard et al. [8], this means that, if f is two-to-one, then with high probability, a Grover search over n/w randomly-chosen indices $y \in \{w+1, \ldots, n\}$ will succeed at finding a y such that $f(y) = f'(x) = f(x)$ for some $x \in [w]$. So if Step 2 does *not* find such a y, then V has verified to within constant soundness that f is one-to-one. $\blacksquare$

For the Permutation Testing Problem, we do not know whether there is a QCMA protocol that satisfies both $T = o\left(n^{1/3}\right)$ and $w = o(n \log n)$. However, notice that if $w = \Omega(n \log n)$, then the witness can just give claimed values $f'(1), \ldots, f'(n)$ for $f(1), \ldots, f(n)$ respectively. In that case, the verifier simply needs to check that f' is indeed a permutation, and that $f'(x) = f(x)$ for $O(1)$ randomly-chosen values $x \in [n]$. So if $w = \Omega(n \log n)$, then the QMA, QCMA, and MA query complexities are all $T = O(1)$.

3 Main Result

In this section, we prove a lower bound on the QMA query complexity of the Permutation Testing Problem. Given a QMA verifier V for PTP, the first step will be to amplify V's success probability. For this, we use the by-now standard procedure of Marriott and Watrous [12], which amplifies without increasing the size of the quantum witness.

Lemma 4 (In-Place Amplification Lemma [12]) *Let V be a QMA verifier that uses a w-qubit quantum witness, makes T oracle queries, and has completeness and soundness errors $1/3$. Then for all $s \geq 1$, there exists an amplified verifier V_s' that uses a w-qubit quantum witness, makes $O(Ts)$ oracle queries, and has completeness and soundness errors $1/2^s$.*

Lemma 4 has a simple consequence that will be the starting point for our lower bound.

Lemma 5 (Guessing Lemma) *Suppose a language L has a QMA protocol, which makes T queries and uses a w-qubit quantum witness. Then there is also a quantum algorithm for L (with no witness) that makes $O(Tw)$ queries, accepts every $x \in L$ with probability at least $0.75/2^w$, and accepts every $x \notin L$ with probability at most $0.25/2^w$.*

Proof. Let V_s' be the amplified verifier from Lemma 4. Set $s := w + 2$, and consider running V_s' with the w-qubit maximally mixed state I_w in place of the QMA witness $|\varphi_x\rangle$. Then given any yes-instance $x \in L$,

$$\Pr\left[V_s'(x, I_w) \text{ accepts}\right] \geq \frac{1}{2^w} \Pr\left[V_s'(x, |\varphi_x\rangle) \text{ accepts}\right] \geq \frac{1 - 2^{-s}}{2^w} \geq \frac{0.75}{2^w},$$

while given any no-instance $x \notin L$,

$$\Pr\left[V_s'(x, I_w) \text{ accepts}\right] \leq \frac{1}{2^s} \leq \frac{0.25}{2^w}.$$

$\blacksquare$

Now let Q be a quantum algorithm for PTP, which makes T queries to f. Then just like in the collision lower bound proofs of Aaronson [1], Aaronson and Shi [4], and Kutin [11], the crucial fact we will need is the so-called "Symmetrization Lemma": namely, *Q's acceptance probability* *can be written as a polynomial, of degree at most $2T$, in a small number of integer parameters characterizing f.*

In more detail, call an ordered pair of integers (m,a) *valid* if

(i) $0 \leq m \leq n$,

(ii) $1 \leq a \leq n-m$, and

(iii) a divides $n-m$.

Then for any valid (m,a), let $S_{m,a}$ be the set of all functions $f:[n] \rightarrow [n]$ that are one-to-one on m coordinates and a-to-one on the remaining $n-m$ coordinates (with the two ranges not intersecting, so that $|\operatorname{Im} f| = m + \frac{n-m}{a}$). The following version of the Symmetrization Lemma is a special case of the version proved by Kutin [11].

Lemma 6 (Symmetrization Lemma [1, 4, 11]) *Let Q be a quantum algorithm that makes T queries to $f:[n] \rightarrow [n]$. Then there exists a real polynomial $p(m,a)$, of degree at most $2T$, such that*

$$p(m,a) = \operatorname*{E}_{f \in S_{m,a}} \left[\Pr \left[Q^f \text{ accepts} \right] \right]$$

for all valid (m,a).

Finally, we will need a standard result from approximation theory, due to Paturi [13].

Lemma 7 (Paturi [13]) *Let $q:\mathbb{R} \rightarrow \mathbb{R}$ be a univariate polynomial such that $0 \leq q(j) \leq \delta$ for all integers $j \in [a,b]$, and suppose that $|q(\lceil x \rceil) - q(x)| = \Omega(\delta)$ for some $x \in [a,b]$. Then* $\deg(q) = \Omega\left(\sqrt{(x-a+1)(b-x+1)}\right)$.

Intuitively, Lemma 7 says that $\deg(q) = \Omega\left(\sqrt{b-a}\right)$ if x is close to one of the endpoints of the range $[a,b]$, and that $\deg(q) = \Omega(b-a)$ if x is close to the middle of the range.

We can now prove the QMA lower bound for PTP.

Theorem 8 (Main Result) *Let V be a QMA verifier for the Permutation Testing Problem, which makes T quantum queries to the function $f:[n] \rightarrow [n]$, and which takes a w-qubit quantum witness $|\varphi_f\rangle$ in support of f being a permutation. Then $Tw = \Omega\left(n^{1/3}\right)$.*

Proof. Assume without loss of generality that n is divisible by 4. Let $\varepsilon := 0.25/2^w$. Then by Lemma 5, from the hypothesized QMA verifier V, we can obtain a quantum algorithm Q for the PTP that makes $O(Tw)$ queries to f, and that satisfies the following two properties:

(i) $\Pr\left[Q^f \text{ accepts}\right] \geq 3\varepsilon$ for all permutations $f:[n] \rightarrow [n]$.

(ii) $\Pr\left[Q^f \text{ accepts}\right] \leq \varepsilon$ for all $f:[n] \rightarrow [n]$ that are at least $n/8$-far from any permutation.

Now let $p(m,a)$ be the real polynomial of degree $O(Tw)$ from Lemma 6, such that

$$p(m,a) = \operatorname*{E}_{f \in S_{m,a}} \left[\Pr \left[Q^f \text{ accepts} \right] \right]$$

for all valid (m,a). Then p satisfies the following two properties:

(i') $p(m,1) \geq 3\varepsilon$ for all $m \in [n]$. (For any $f \in S_{m,1}$ is one-to-one on its entire domain.)

(ii') $0 \leq p(m,a) \leq \varepsilon$ for all integers $0 \leq m \leq 3n/4$ and $a \geq 2$ such that a divides $n-m$. (For in this case, (m,a) is valid and every $f \in S_{m,a}$ is at least $n/8$-far from a permutation.)

So to prove the theorem, it suffices to show that any polynomial p satisfying properties (i') and (ii') above has degree $\Omega\left(n^{1/3}\right)$.

Let $g(x) := p(n/2, 2x)$, and let k be the least positive integer such that $|g(k)| > 2\varepsilon$ (such a k must exist, since g is a non-constant polynomial). Notice that $g(1/2) = p(n/2,1) \geq 3\varepsilon$, that $g(1) = p(n/2,2) \leq \varepsilon$, and that $|g(i)| \leq 2\varepsilon$ for all $i \in [k-1]$. By Lemma 7, these facts together imply that $\deg(g) = \Omega\left(\sqrt{k}\right)$.

Now let $c := 2k$, and let $h(i) := p(n-ci, c)$. Then for all integers $i \in \left[\frac{n}{4c}, \frac{n}{c}\right]$, we have $0 \leq h(i) \leq \varepsilon$, since $(n-ci, c)$ is valid, $n - ci \leq 3n/4$, and $c \geq 2$. On the other hand, we also have

$$h\left(\frac{n}{2c}\right) = p\left(\frac{n}{2}, c\right) = p\left(\frac{n}{2}, 2k\right) = g(k) > 2\varepsilon.$$

By Lemma 7, these facts together imply that $\deg(h) = \Omega(n/c) = \Omega(n/k)$.

Clearly $\deg(g) \leq \deg(p)$ and $\deg(h) \leq \deg(p)$. So combining,

$$\deg(p) = \Omega\left(\max\left\{\sqrt{k}, \frac{n}{k}\right\}\right) = \Omega\left(n^{1/3}\right).$$

■

4 Oracle Separations

Using Theorem 8, we can exhibit an oracle separation between SZK and QMA, thereby answering the author's question from eight years ago.

Theorem 9 *There exists an oracle A such that $\mathsf{SZK}^A \not\subset \mathsf{QMA}^A$.*

Proof Sketch. The oracle A will encode an infinite sequence of instances $f_n : [2^n] \rightarrow [2^n]$ of the Permutation Testing Problem, one for each input length n. Define a unary language L_A by $0^n \in L_A$ if f_n is a permutation, and $0^n \notin L_A$ if f_n is far from a permutation. Then Proposition 2 tells us that $L_A \in \mathsf{SZK}^A$ for all A. On the other hand, Theorem 8 tells us that we can choose A in such a way that $L_A \notin \mathsf{QMA}^A$, by diagonalizing against all possible QMA verifiers. ■

In the rest of the section, we explain how our lower bound actually places SZK outside of a larger complexity class than QMA. First let us define the larger class in question.

Definition 10 (Vyalyi [15]) $\mathsf{A_0PP}$ *is the class of languages L for which there exists a #P function g, as well as polynomials p and q, such that for all inputs $x \in \{0,1\}^n$:*

(i) If $x \in L$ then $\left|g(x) - 2^{p(n)}\right| \geq 2^{q(n)}$.

(ii) If $x \notin L$ then $\left|g(x) - 2^{p(n)}\right| \leq 2^{q(n)-1}$.

We now make some elementary observations about $\mathsf{A_0PP}$. First, $\mathsf{A_0PP}$ is contained in PP, and contains not only MA but also the slightly-larger class SBP (Small Bounded-Error Polynomial-Time) defined by Böhler et al. [7]. Second, it is not hard to show that $\mathsf{P}^{\mathsf{PromiseA_0PP}} = \mathsf{P}^{\mathsf{PP}} = \mathsf{P}^{\#\mathsf{P}}$. The reason is that, by varying the polynomial p, we can obtain a multiplicative estimate of the difference $\left|g(x) - 2^{p(n)}\right|$, which then implies that we can use binary search to determine $g(x)$ itself.

By adapting the result of Aaronson [2] that $\mathsf{PP} = \mathsf{PostBQP}$, Kuperberg [10] gave a beautiful alternate characterization of $\mathsf{A_0PP}$ in terms of quantum computation. Let SBQP (Small Bounded-Error Quantum Polynomial-Time) be the class of languages L for which there exists a polynomial-time quantum algorithm that accepts with probability at least $2^{-p(n)}$ if $x \in L$, and with probability at most $2^{-p(n)-1}$ if $x \notin L$, for some polynomial p.

Theorem 11 (Kuperberg [10]) $\mathsf{A_0PP} = \mathsf{SBQP}$.

By combining Theorem 11 with Lemma 4, it is not hard to reprove the following result of Vyalyi [15].

Theorem 12 (Vyalyi [15]) $\mathsf{QMA} \subseteq \mathsf{A_0PP}$.

Proof. Similar to Lemma 5. Given a language L, suppose L has a QMA verifier V that takes a w-qubit quantum witness. Then first apply Marriott-Watrous amplification (Lemma 4), to obtain a new verifier V' with completeness and soundness errors $0.25/2^w$, which also takes a w-qubit quantum witness. Next, run V' with the w-qubit maximally mixed state I_w in place of the witness. The result is a quantum algorithm that accepts every $x \in L$ with probability at least $0.75/2^w$, and accepts every $x \notin L$ with probability at most $0.25/2^w$. This implies that $L \in \mathsf{SBQP}$. ■

We now observe that our results from Section 3 yield, not only an oracle A such that $\mathsf{SZK}^A \not\subset \mathsf{QMA}^A$, but an oracle A such that $\mathsf{SZK}^A \not\subset \mathsf{A_0PP}^A$, which is a stronger separation.

Theorem 13 *There exists an oracle A such that* $\mathsf{SZK}^A \not\subset \mathsf{A_0PP}^A$.

Proof Sketch. As in Theorem 9, the oracle A encodes an infinite sequence of instances $f_n : [2^n] \to [2^n]$ of the Permutation Testing Problem. The key observation is that Theorem 8 rules out, not merely any QMA protocol for PTP, but also any SBQP algorithm: that is, any polynomial-time quantum algorithm that accepts with probability at least 2ε if f_n is a permutation, and with probability at most ε if f_n is far from a permutation, for some $\varepsilon > 0$. This means that we can use Theorem 8 to diagonalize against SBQP (or equivalently $\mathsf{A_0PP}$) machines. ■

5 Open Problems

(1) It is strange that our lower bound works only for the Permutation Testing Problem, and not for the original collision problem (i.e., for certifying that f is one-to-one rather than two-to-one). Can we rule out succinct quantum proofs for the latter?

(2) Even for PTP, there remains a large gap between the upper and lower bounds that we can prove on QMA query complexity. Recall that our lower bound has the form $Tw = \Omega\left(n^{1/3}\right)$, where T is the query complexity and w is the number of qubits in the witness. By contrast,

if $w = o(n \log n)$, then we do not know of *any* QMA protocol that achieves $T = o\left(n^{1/3}\right)$—i.e., that does better than simply ignoring the witness and running the Brassard-Høyer-Tapp algorithm. It would be extremely interesting to get sharper results on the tradeoff between T and w. (As far as we know, it is open even to get a sharp tradeoff for *classical* MA protocols.)

(3) For the collision problem, the PTP, or any other black-box problem, is there a gap (even just a polynomial gap) between the QMA query complexity and the QCMA query complexity? This seems like a difficult question, since currently, the one lower bound technique that we have for QCMA—namely, the reduction to SBQP exploited in this paper—*also* works for QMA. It follows that a new technique will be needed to solve the old open problem of constructing an oracle A such that $\mathsf{QCMA}^A \neq \mathsf{QMA}^A$. (Currently, the closest we have is a *quantum* oracle separation between QMA and QCMA, shown by Aaronson and Kuperberg [3].)

(4) Watrous (personal communication) asked whether there exists an oracle A such that $\mathsf{SZK}^A \not\subset \mathsf{PP}^A$. Since $\mathsf{PP} \subseteq \mathsf{P}^{\mathsf{PromiseA_0PP}}$, our oracle separation between SZK and $\mathsf{A_0PP}$ comes "close" to answering Watrous's question. However, a new technique seems needed to get from $\mathsf{A_0PP}$ to PP.

6 Acknowledgments

I thank the anonymous reviewer for helpful comments.

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 computing, postselection, and probabilistic polynomial-time. *Proc. Roy. Soc. London*, A461(2063):3473–3482, 2005. quant-ph/0412187.

[3] S. Aaronson and G. Kuperberg. Quantum versus classical proofs and advice. *Theory of Computing*, 3(7):129–157, 2007. Previous version in Proceedings of CCC 2007. quant-ph/0604056.

[4] S. Aaronson and Y. Shi. Quantum lower bounds for the collision and the element distinctness problems. *J. ACM*, 51(4):595–605, 2004.

[5] A. Ambainis. Polynomial degree and lower bounds in quantum complexity: collision and element distinctness with small range. *Theory of Computing*, 1:37–46, 2005. quant-ph/0305179.

[6] 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.

[7] E. Böhler, C. Glaßer, and D. Meister. Error-bounded probabilistic computations between MA and AM. *J. Comput. Sys. Sci.*, 72(6):1043–1076, 2006.

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

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

[10] G. Kuperberg. How hard is it to approximate the Jones polynomial? arXiv:0908.0512, 2009.

[11] S. Kutin. Quantum lower bound for the collision problem with small range. *Theory of Computing*, 1:29–36, 2005. quant-ph/0304162.

[12] C. Marriott and J. Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005.

[13] R. Paturi. On the degree of polynomials that approximate symmetric Boolean functions. In *Proc. ACM STOC*, pages 468–474, 1992.

[14] N. Vereshchagin. On the power of PP. In *Proc. IEEE Conference on Computational Complexity*, pages 138–143, 1992.

[15] M. Vyalyi. QMA=PP implies that PP contains PH. ECCC TR03-021, 2003.