Rational approximations and quantum algorithms with postselection

Urmila Mahadev* Ronald de Wolf†

Abstract

We study the close connection between rational functions that approximate some Boolean function, and quantum algorithms that compute the same function using postselection. We show that the minimal degree of the former equals (up to a factor of 2) the minimal query complexity of the latter. We give optimal (up to constant factors) quantum algorithms with postselection for the majority function, slightly improving upon an earlier algorithm of Aaronson. Finally we show how Newman's classic theorem about low-degree rational approximation of the absolute-value function follows from our algorithm.

1 Introduction

1.1 Background: low-degree approximations from efficient quantum algorithms

Since the introduction of quantum computing in the 1980s [Fey82, Deu85], most research in this area has focused on trying to find new quantum algorithms, quantum cryptography, communication schemes, uses of entanglement etc. One of the more surprising applications of quantum computing in the last decade has been its use, in some way or other, in obtaining results in *classical* computer science and mathematics (see [DW11a] for a survey). One direction here has been the use of quantum query algorithms to show the existence of low-degree polynomial approximations to various functions. This direction started with the observation [FR99, BBC$^+$01] that the acceptance probability of a T-query quantum algorithm with N-bit input can be written as an N-variate multilinear polynomial of degree at most $2T$. For example, Grover's $O(\sqrt{N})$-query algorithm for finding a 1 in an N-bit input [Gro96] implies the existence of an N-variate degree-$O(\sqrt{N})$ polynomial that approximates the N-bit OR-function, and (by symmetrization) of a single-variate polynomial p such that $p(0) = 0$ and $p(i) \approx 1$ for all $i \in \{1, \ldots, N\}$. Accordingly, one way to design (or prove existence of) a low-degree polynomial with a certain desired behavior, is to design an efficient quantum algorithm whose acceptance probability has that desired behavior. Some results based on this approach are tight bounds on the degree of low-error approximations for symmetric functions [Wol08], a new quantum-based proof of Jackson's theorem from approximation theory [DW11b], and tight upper bounds for sign-approximations of formulas [Lee09].

In this paper we focus on a related but slightly more complicated connection, namely the use of quantum query algorithms *with postselection* to show the existence of low-degree *rational* approximations to various functions. We will define both terms in more detail later, but for now let us just state that postselection is the unphysical ability of an algorithm to choose the outcome of a measurement, thus forcing a collapse of

*University of California, Berkeley, urmilamahadev@gmail.com.

†CWI and University of Amsterdam, rdewolf@cwi.nl. Supported by a Vidi grant from the Netherlands Organization for Scientific Research (NWO) and the European Commission IST STREP project Quantum Algorithms (QALGO) 600700.

the state to the corresponding subspace; and a rational function is the ratio of two polynomials (its degree is the max of the degrees of numerator and denominator polynomial). This connection was first made by Aaronson. In [Aar05], he provided a new proof of the breakthrough result of Beigel et al. [BRS95] that the complexity class PP is closed under intersection. He did this in three steps:

1. Define a new class PostBQP, corresponding to polynomial-time quantum algorithms augmented with postselection.
2. Prove that PP = PostBQP.
3. Observe that PostBQP is closed under intersection, which is obvious from its definition.

While very different from the proof of Beigel et al. (at least on the surface), Aaronson noted that his proof could actually be viewed as implicitly constructing certain low-degree rational approximations to the Majority function[1]; the fact that the resulting polynomial has low degree follows from the fact that Aaronson's algorithm makes only few queries to the input of Majority. Such rational approximations also form the key to the proof of Beigel et al.

Our goal in this paper is to work out this connection between rational functions and postselection-algorithms in much more detail, and to apply it elsewhere.

1.2 Definitions

In order to be able to state our results, let us be a bit more precise about definitions.

Polynomial approximation. An N-variate polynomial is a function $P : S^N \to \mathbb{R}$ that can be written as $P(x_1, \ldots, x_n) = \sum_{d_1,\ldots,d_n} c_{d_1,\ldots,d_n} \prod_{i=1}^N x_i^{d_i}$ with real coefficients $c_{d_1,\ldots,d_n}$. In our applications, the domain S of each input variable will be either $\mathbb{R}$ or $\{0, 1\}$. The *degree* of P is $\max\{\sum_{i=1}^N d_i \mid c_{d_1,\ldots,d_n} \neq 0\}$. When we only care about the behavior of the polynomial on the Boolean cube $\{0, 1\}^N$, then $x_i^d = x_i$ for all $d \geq 1$, so then we can restrict to *multilinear* polynomials, where the degree in each variable is at most 1. Let $\varepsilon \in [0, 1/2)$ be some fixed constant. A polynomial P *ε-approximates* $f : S^N \to \mathbb{R}$ if $|P(x) - f(x)| \leq \varepsilon$ for all $x \in S^N$. The ε-approximate degree of f (abbreviated $\deg_\varepsilon(f)$) is the minimal degree among all such polynomials P. The *exact* degree of f is $\deg(f) = \deg_0(f)$.

Rational approximation. A *rational function* is a ratio P/Q of two N-variate polynomials $P, Q : S^N \to \mathbb{R}$, where Q is required to be nonzero everywhere on S^N to prevent division by 0. Its degree is the maximum of the degrees of P and Q. A rational function P/Q *ε-approximates* f if $|P(x)/Q(x) - f(x)| \leq \varepsilon$ for all $x \in S^N$. The ε-approximate rational degree of f (abbreviated $\mathrm{rdeg}_\varepsilon(f)$) is the minimal degree among all such rational functions. The *exact* rational degree of f is $\mathrm{rdeg}_0(f)$.

Quantum query algorithms with postselection. A quantum query algorithm *with postselection* (short: postselection-algorithm) is a regular quantum query algorithm [BW02] with two output bits $a, b \in \{0, 1\}$. We say the postselection-algorithm computes a Boolean function $f : \{0, 1\}^N \to \{0, 1\}$ with error probability ε if for every $x \in \{0, 1\}^N$, we have $\Pr[a = 1] > 0$ and $\Pr[b = f(x) \mid a = 1] \geq 1 - \varepsilon$. The idea is that we can compute $f(x)$ with error probability ε if we could postselect on measurement outcome $a = 1$. In

[1] The N-bit Majority is the Boolean function defined by $\mathrm{MAJ}_N(x) = 1$ iff the Hamming weight $|x| := \sum_{i=1}^N x_i$ is $\geq N/2$.

other words, the second output bit b computes the function when the first is forced to output 1. This "forcing" is the postselection step, which is not something we can actually implement physically; in that respect the model of postselection is mostly a tool for theoretical analysis, not a viable model of actually-doable computation. The *postselection query complexity* $\mathrm{PostQ}_\varepsilon(f)$ of f is the minimal query complexity among such algorithms.[2]

1.3 Our results

Rational degree $\approx$ quantum query complexity with postselection. Our first result in this paper (Section 2) is to give a very tight connection between rational approximations of a Boolean function $f : \{0,1\}^N \to \{0,1\}$ and potselection-algorithms computing f with small error probability. We show that the minimal degree needed for the former equals the minimal query complexity needed for the latter, to within a factor of 2:

$$\frac{1}{2}\mathrm{rdeg}_\varepsilon(f) \leq \mathrm{PostQ}_\varepsilon(f) \leq \mathrm{rdeg}_\varepsilon(f).$$

In other words, minimal rational degree is essentially equal to quantum query complexity with postselection. This should be contrasted with the better-studied case of polynomial approximation, where the approximate degree $\widetilde{\deg}_\varepsilon(f)$ equals the bounded-error quantum query complexity *to within a polynomial factor* [BBC$^+$01], and there are actually polynomial gaps [Amb03].

Optimal postselection-algorithm for Majority. Our second result in this paper is to optimize Aaronson's construction, modifying his postselection algorithm for Majority to have minimal query complexity up to a constant factor (and hence the induced rational approximation for majority will have minimal degree):

$$\mathrm{PostQ}_\varepsilon(\mathrm{MAJ}_N) = O\left(\log(N/\log(1/\varepsilon))\log(1/\varepsilon)\right).$$

This reproves the upper bound of Sherstov [She14, Theorem 1.7]. In fact, we could just have combined Sherstov's upper bound with the equivalence between rational degree and postselection-complexity mentioned above, but our derivation of minimal-degree polynomials by means of a postselection-algorithm is very different from Sherstov's proof. Sherstov's matching lower bound for the degree of rational approximations shows that also our algorithm is optimal (up to a constant factor).

Newman's Theorem. One of the most celebrated results in rational approximation theory is Newman's Theorem [New64]. This says that there is a degree-d rational function that approximates the absolute-value function $|x|$ on the interval $x \in [-1,1]$ up to error $2^{-\Omega(\sqrt{d})}$. In contrast, it can be shown that the smallest error achievable by degree-d polynomials is $\Theta(1/d)$. The proof of Newman's Theorem is not extremely complicated:

> Define $a = e^{-1/\sqrt{d}}$, $p(x) = \prod_{k=0}^{d-1}(a^k + x)$, and degree-$d$ rational function $r(x) = \frac{p(x)-p(-x)}{p(x)+p(-x)}$. Half a page of calculations shows that $r(x)$ ε-approximates the sign-function on the interval $[-1,-\varepsilon] \cup [\varepsilon, 1]$, for $\varepsilon = e^{-\Omega(\sqrt{d})}$. We have $r(x) \in [-1,1]$ and $\mathrm{sgn}(x) = \mathrm{sgn}(r(x))$ on the whole interval $[-1,1]$, hence the degree-$(d+1)$ rational function $x \cdot r(x)$ ε-approximates the absolute-value function on the whole interval $[-1,1]$.

[2] The way we defined it here, a postselection-algorithm involves only one postselection-step, namely selecting the value $a = 1$. However, we can also allow intermediate postselection steps without changing the power of this model, see [DW11a, Section 4.3].

In fact the optimal error ε achievable by degree-d rational functions is known much more precisely [PP87, Theorem 4.2]: it is $\Theta(e^{-\pi\sqrt{d}})$. The proof of this tighter bound is substantially more complicated.[3]

In Section 4 we show how our postselection-algorithm for Majority can be used to derive Newman's Theorem. While this proof is not easier than Newman's by any reasonable standard, it (like the reproof of Sherstov's result mentioned above) is still interesting because it gives a new, quantum-algorithmic perspective on these known results that may have other applications.

2 Query complexity with postselection $\approx$ degree of rational approximation

We first show that rational approximation degree and quantum query complexity with postselection are essentially the same for all Boolean functions.

Theorem 1 *For all* $\varepsilon \in [0, 1/2)$ *and* $f : \{0,1\}^N \to \{0,1\}$ *we have* $\mathrm{rdeg}_\varepsilon(f) \leq 2\mathrm{PostQ}_\varepsilon(f)$.

Proof. Consider a postselection-algorithm for f with $T = \mathrm{PostQ}_\varepsilon(f)$ queries and error ε. Then by [BBC+01], the probabilities $Q(x) = \Pr[a = 1]$ and $P(x) = \Pr[a = b = 1]$ can be written as polynomials of degree $\leq 2T$. Their ratio P/Q is a rational function that equals the conditional probability $\Pr[b = 1 \mid a = 1]$. By definition, the latter is in $[1-\varepsilon, 1]$ for inputs $x \in f^{-1}(1)$, and is in $[0, \varepsilon]$ for $x \in f^{-1}(0)$. Hence P/Q is a rational ε-approximation for f of degree $\leq 2T = 2\mathrm{PostQ}_\varepsilon(f)$. □

Theorem 2 *For all* $\varepsilon \in [0, 1/2)$ *and* $f : \{0,1\}^N \to \{0,1\}$ *we have* $\mathrm{PostQ}_\varepsilon(f) \leq \mathrm{rdeg}_\varepsilon(f)$.

Proof. Consider an ε-approximate rational approximation P/Q for f of degree $d = \mathrm{rdeg}_\varepsilon(f)$. It will be convenient to convert f to a ±1-valued function. Define $F(x) = 1 - 2f(x) \in \{\pm 1\}$ and $R(x) = Q(x) - 2P(x)$, then $R/Q = 1 - 2P/Q$ is in $[-1-2\varepsilon, -1+2\varepsilon]$ if $F(x) = -1$, and in $[1-2\varepsilon, 1+2\varepsilon]$ if $F(x) = 1$. We will write R and Q in their Fourier decompositions:

$$R(x) = \sum_{S\subseteq[N]} \widehat{R}(S)(-1)^{x\cdot S} \text{ and } Q(x) = \sum_{S\subseteq[N]} \widehat{Q}(S)(-1)^{x\cdot S}.$$

Now set up the following $(N+1)$-qubit state (up to a global normalizing constant):

$$|0\rangle \sum_S \widehat{Q}(S)|S\rangle + |1\rangle \sum_S \widehat{R}(S)|S\rangle,$$

where $|S\rangle$ is the N-bit basis state corresponding to the characteristic vector of S. Note that $\widehat{R}(S)$ and $\widehat{Q}(S)$ are 0 whenever $|S| > d$. Hence by making d queries to x, we can add the phases

$$|0\rangle \sum_S \widehat{Q}(S)(-1)^{x\cdot S}|S\rangle + |1\rangle \sum_S \widehat{R}(S)(-1)^{x\cdot S}|S\rangle.$$

[3] In fact, in the 19th century Zolotarev [Zol77] already gave the optimal polynomial for each degree d. Later, Akhiezer [Akh29] worked out the asymptotical decrease of the error as a function of d, stating Newman's Theorem much before the paper of Newman (who was apparently unaware of this Russian literature).

Now a Hadamard transform on each of the n qubits of the second register gives a state proportional to

$$|0\rangle\left(\sum_S \widehat{Q}(S)(-1)^{x\cdot S}|0^N\rangle+\cdots\right)+|1\rangle\left(\sum_S \widehat{R}(S)(-1)^{x\cdot S}|0^N\rangle+\cdots\right)$$
$$=|0\rangle\left(Q(x)|0^N\rangle+\cdots\right)+|1\rangle\left(R(x)|0^N\rangle+\cdots\right),$$

where the $\cdots$ indicates all the basis states other than $|0^N\rangle$. Postselect on measuring $|0^N\rangle$ in the second register (more precisely, set the bit a to 1 only for basis state $|0^N\rangle$). What is left in the first register is the following qubit:

$$|\beta_x\rangle = c(Q(x)|0\rangle + R(x)|1\rangle) = cQ(x)\left(|0\rangle+\frac{R(x)}{Q(x)}|1\rangle\right),$$

where $c = 1/\sqrt{Q(x)^2+R(x)^2}$ is a normalizing constant. Since $R(x)/Q(x)\approx F(x)\in\{\pm 1\}$, a Hadamard transform followed by a measurement will with high probability tell us the sign $F(x)$ of $R(x)/Q(x)$. If $F(x)=1$, the error probability equals

$$|\langle -|\beta_x\rangle|^2 = \frac{(Q(x)-R(x))^2}{2(Q(x)^2+R(x)^2)} = \frac{(1-R(x)/Q(x))^2}{2(1+(R(x)/Q(x))^2)} \leq \frac{(2\varepsilon)^2}{2(1+(1-2\varepsilon)^2)} = \frac{\varepsilon^2}{1-2\varepsilon+2\varepsilon^2}\leq\varepsilon,$$

where the last inequality used that $\varepsilon \leq 1-2\varepsilon+2\varepsilon^2$ for all $\varepsilon\in[0,1/2)$. If $F(x)=-1$ then an analogous calculation works. Hence we have found a d-query postselection-algorithm that computes f with error probability $\leq\varepsilon$. □

3 An optimal postselection-algorithm for Majority

In this section we give an optimized postselection-algorithm for Majority, slightly improving Aaronson's algorithm from [Aar05].

Theorem 3 *For every $t\in[N]$ there exists a postselection-algorithm that computes* MAJ_N *with error probability $\leq 1/3$ using $O(\log\frac{N}{t}+t)$ queries.*

Proof. Assume for simplicity N is a power of 2, $N=2^n$. Since there is an exact algorithm for MAJ_N using N queries, we can assume $t \ll N/2$. Our algorithm is a modification of Aaronson's [Aar05]. He shows that for any $\alpha,\beta>0$ satisfying $\alpha^2+\beta^2=1$, using one query and some postselection we can construct the following qubit:

$$c\left(\alpha|x||0\rangle+\beta\frac{1}{\sqrt{2}}(N-2|x|)|1\rangle\right), \tag{1}$$

where $c=1/\sqrt{\alpha^2|x|^2+\frac{\beta^2}{2}(N-2|x|)^2}$ is a normalizing constant. Our goal is to decide whether $|x|\geq N/2$ or not. Note that if $0<|x|<N/2$ then the above qubit is inside the first quadrant (i.e., both $|0\rangle$ and $|1\rangle$ have positive amplitude), and if $|x|\geq N/2$ then it's not. In the first case, for some choice of α,β the above qubit will be close to the state $|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, while in the second case it will be far from $|+\rangle$ for any choice of α,β. The algorithm tries out a number of α,β-pairs in order to distinguish between these two cases. Let $A=\{-\lceil\log\frac{N}{t}\rceil,\ldots,-1,0,1,\ldots,\lceil\log\frac{N}{t}\rceil\}$, and for all $i\in A$ let $|a_i\rangle$ be the above qubit (1) for

$\frac{\alpha}{\beta} = 2^i$. Let $B = \{1, \ldots, t-1\} \cup \{N/2 + 1 - t, \ldots, N/2 - 1\}$ for $t \geq 2$ and $B = \emptyset$ otherwise. For all $i \in B$ let $|b_i\rangle$ be the above qubit for $\frac{\alpha}{\beta} = \frac{N-2i}{\sqrt{2i}}$.

The algorithm is as follows. The intuition is that we are trying to eliminate from A and B all i corresponding to states whose squared inner product with $|+\rangle$ is at most 1/2. If $|x| \geq N/2$ (i.e., $\mathrm{MAJ}_N(x) = 1$) then we expect to eventually eliminate all i, while if $|x| < N/2$ (i.e., $\mathrm{MAJ}_N(x) = 0$) then for at least one i, the squared inner product with $|+\rangle$ will be close to 1, and this i will probably not be eliminated by the process. For simplicity we will assume $|x| \notin \{0, N\}$ (we can ensure this for instance by fixing the first two bits of x to 01, so then we would be effectively computing MAJ_{N-2}).

1. Initialize $A_1 = A$, $B_1 = B$ and $k = 1$.
2. Repeat the following until $558(\log \frac{N}{t} + t)$ queries have been used:
   (a) For all $i \in A_k$, create $9k$ copies of $|a_i\rangle$ and measure each in the $|+\rangle, |-\rangle$ basis. Set $M^A_{k,i} = 1$ if this step resulted in a majority of $|+\rangle$ outcomes.
   (b) For all $i \in B_k$, create $9k$ copies of $|b_i\rangle$ and measure each in the $|+\rangle, |-\rangle$ basis. Set $M^B_{k,i} = 1$ if this resulted in a majority of $|+\rangle$ outcomes.
   (c) Set $A_{k+1} = \{i \in A_k \mid M^A_{k,i} = 1\}$. Set $B_{k+1} = \{i \in B_k \mid M^B_{k,i} = 1\}$. Set k to $k+1$.
3. Output 0 if $|A_k| + |B_k| \geq 1$, and output 1 otherwise.

By definition, the algorithm uses at most $558(\log \frac{N}{t} + t)$ queries. We will now prove correctness by analyzing three cases:

Case 1: $|x| \in B$

Because $|b_{|x|}\rangle = |+\rangle$, index $|x|$ remains in B_k for all k and the algorithm outputs 0 with probability 1.

Case 2: $|x| < N/2$ **but** $|x| \notin B$ **(i.e.,** $t \leq |x| \leq \frac{N-t}{2}$**)**

Note that for these values of $|x|$, the ratio between $|x|$ and $N - 2|x|$ lies between t/N and N/t. Hence there exists an $i \in A$ such that $|a_i\rangle$ and $|a_{i+1}\rangle$ lie on opposite sides of $|+\rangle$. In the worst case, $\langle +|a_i\rangle = \langle +|a_{i+1}\rangle$. In this case, $|a_i\rangle = \sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$, so $\langle +|a_i\rangle = \frac{1+\sqrt{2}}{\sqrt{6}} =: \lambda$. We will show that this i is likely to remain in all A_k. Each iteration of step 2 will be called a "trial". Let m be the number of the trial being executed when the algorithm stops. The algorithm gives the correct output 0 iff $|A_m| + |B_m|$ is at least 1. First, by the Chernoff bound, for every k

$$\Pr[M^A_{k,i} = 0] \leq \exp(-2 \cdot 9k(\lambda^2 - \frac{1}{2})^2) \leq 2^{-(k+3)}.$$

Now by the union bound, the error probability in this case is at most

$$\Pr[i \notin A_m] = \Pr[\exists\, k \ s.t.\ M^A_{k,i} = 0] \leq \sum_{k=1}^{\infty} 2^{-(k+3)} \leq \frac{1}{8}.$$

Case 3: $|x| \geq N/2$

We will first show that the algorithm is likely to go through at least $2 \log N$ trials. Since $|x| \geq N/2$, for all $i \in A$ we have $|\langle +|a_i\rangle|^2 \leq \frac{1}{2}$ and hence $\Pr[M^A_{k,i} = 1] \leq \frac{1}{2}$ for all k. Similarly $\Pr[M^B_{k,i} = 1] \leq \frac{1}{2}$ for all k and $i \in B$. Hence we have

$$\mathbb{E}[|A_{k+1}| + |B_{k+1}|] = \sum_{i \in A} \prod_{\ell=1}^{k} \Pr[M^A_{\ell,i} = 1] + \sum_{i \in B} \prod_{\ell=1}^{k} \Pr[M^B_{\ell,i} = 1] \leq \frac{|A| + |B|}{2^k} \leq \frac{\log \frac{N}{t} + t}{2^{k-1}}.$$

Let $Q = \sum_{k=1}^{2\log N} 9k(|A_k| + |B_k|)$ be the number of queries used in the first $2\log N$ trials (with the number of queries set to 0 for the non-executed trials after the mth). Now:

$$\mathbb{E}[Q] \leq 9(\log \frac{N}{t} + t) \sum_{k=1}^{2\log N} \frac{k}{2^{k-1}} \leq 62(\log \frac{N}{t} + t).$$

By Markov's inequality, $\Pr[Q \geq 558(\log \frac{N}{t} + t)] \leq \frac{1}{9}$. So with probability at least $\frac{8}{9}$ we have $Q < 558(\log \frac{N}{t} + t)$, meaning the algorithm executes at least $2\log N$ trials before it terminates. In that case each element of A and B has probability at most $1/2^{2\log N} = 1/N^2$ to remain after $2\log N$ trials. Hence, by the union bound

$$\Pr[|A_{2\log N+1}| + |B_{2\log N+1}| \geq 1] \leq \frac{|A| + |B|}{N^2} \leq \frac{1}{4}.$$

Therefore the final error probability is at most $\frac{8}{9}\frac{1}{4} + \frac{1}{9} = \frac{1}{3}$.

□

If we modify step $2(a)$ using $\lceil 9k \log \frac{1}{\varepsilon} \rceil$ copies instead of $9k$, then the error probability is at most ε and the number of queries is $O(\log \frac{N}{t} \cdot \log(1/\varepsilon) + t)$. Choosing $t = \log(1/\varepsilon)$ gives

Corollary 1 *For every $\varepsilon \in (0, 1/2)$ there exists a postselection-algorithm that computes* MAJ_N *using* $O(\log(N/\log(1/\varepsilon)) \cdot \log(1/\varepsilon))$ *queries with error probability* $\leq \varepsilon$.

Sherstov [She14, Theorem 1.7] proved an $\Omega(\log(N/\log(1/\varepsilon)) \cdot \log(1/\varepsilon))$ lower bound on the degree of ε-approximating rational functions for MAJ_N. Together with our Theorem 1, this shows that the algorithms of this section have optimal query complexity up to a constant factor.

4 Deriving Newman's Theorem

We now use the above postselection-algorithm for Majority to derive a good, low-degree rational approximation for the sign-function:

Theorem 4 *For every d there exists a degree-d rational function that ε-approximates the sign-function* $\mathrm{sgn}(z)$ *on* $[-1, -\varepsilon] \cup [\varepsilon, 1]$ *for* $\varepsilon = 2^{-\Omega(\sqrt{d})}$ *(and which lies in* $[-1, 1]$ *for all* $z \in [-1, 1]$*).*

Proof. Set $\varepsilon = 2^{-\Omega(\sqrt{d})}$ with a sufficiently small constant in the $\Omega(\cdot)$, and $N = \lceil \frac{2}{\varepsilon} \rceil$. Consider the algorithm from Corollary 1 with error ε. It provides two N-variate multilinear polynomials P and Q, each of degree $d = O(\log(N/\log(1/\varepsilon)) \cdot \log(1/\varepsilon)) = O(\log(1/\varepsilon)^2)$, such that for all $x \in \{0,1\}^N$,

$$\left| \frac{P(x)}{Q(x)} - \mathrm{MAJ}_N(x) \right| \leq \frac{\varepsilon}{2}.$$

Note that P can be written as $\sum_j c_j (\sum_i x_i)^j$, as can Q, because the amplitudes of the states $|a_i\rangle$ and $|b_i\rangle$ are functions of $|x| = \sum_i x_i$. To convert P to a univariate polynomial p, replace $\sum_i x_i$ with real variable z to obtain $p(z) = \sum_j c_j z^j$. Similarly convert $Q(x)$ to $q(z)$. Let maj_N represent the univariate version of MAJ_N: maj_N returns 0 on input $x \in [0, \dots, \frac{N}{2})$ and returns 1 on $x \in [N/2, \dots, N]$. We now have:

$$\left| \frac{p(x)}{q(x)} - \mathrm{maj}_N(x) \right| \leq \frac{\varepsilon}{2}$$

for $x \in \{0, \ldots, N\}$. Observe that the above inequality also holds for $x \in [1, \frac{N}{2} - 1] \cup [\frac{N}{2}, N]$. This is because we can modify the analysis of the above algorithm by replacing $|x|$ with x. The analysis for cases 2 and 3 in the proof of Theorem 3 still holds, since these two cases do not require x to be an integer value. The analysis for case 1 does not hold, but this is not an issue since we set t to 1 which means that $B = \emptyset$. Since $\mathrm{sgn}(z) = 2\mathrm{maj}_N(\frac{N(z+1)}{2}) - 1$, we have

$$\left| \frac{2p(\frac{N(z+1)}{2}) - q(\frac{N(z+1)}{2})}{q(\frac{N(z+1)}{2})} - \mathrm{sgn}(z) \right| \leq \varepsilon$$

for all $z \in [-1, -\frac{2}{N}] \cup [0, 1]$. Since $N = \lceil \frac{2}{\varepsilon} \rceil$, we have the desired approximation on $[-1, -\varepsilon] \cup [\varepsilon, 1]$. □

It is easy to see that multiplying the above rational function by z gives an approximation of the absolute-value function $|z|$ on the whole interval $z \in [-1, 1]$. Thus we have reproved Newman's Theorem in a new, quantum-based way:

Corollary 2 (Newman) *For every integer $d \geq 1$ there exists a degree-d rational function that approximates $|z|$ on $[-1, 1]$ with error $\leq 2^{-\Omega(\sqrt{d})}$.*

5 Open questions

We mention a few open questions. First, we have very few techniques for quantum algorithms with post-selection. Basically Aaronson's techniques from [Aar05] (and our variations thereof) are the only thing we know. What other algorithmic tricks can we play using postselection?

Second, we showed here how a classical but basic theorem in rational approximation theory (Newman's theorem) could be reproved based on efficient quantum algorithms with postselection. Is it possible to prove *new* results in rational approximation theory using such algorithms?

Finally, the following is a long-standing open question attributed to Fortnow by Nisan and Szegedy [NS94, p. 312]: is there a polynomial relation between the *exact* rational degree of a Boolean function $f : \{0, 1\}^N \to \{0, 1\}$ and its usual polynomial degree? It is known that exact and bounded-error quantum query complexity and exact and bounded-error polynomial degree are all polynomially close to each other [BW02], so rephrased in our framework Fortnow's question is equivalent to the following: can we efficiently simulate an *exact* quantum algorithm with postselection by a bounded-error quantum algorithm without postselection?[4] We hope this more algorithmic perspective will help answer his question.

Acknowledgment. We thank André Chailloux for helpful discussions.

References

[Aar05] S. Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. In *Proceedings of the Royal Society*, volume A461(2063), pages 3473–3482, 2005. quant-ph/0412187.

[Akh29] N. Akhiezer. On a problem of E. I. Zolotarev. *Izv. Akad. Nauk SSSR*, 10:919–931, 1929.

[4]Note that we are asking about *exact* rational degree here; for ε-approximate rational degree the Majority function gives an example of an exponential gap between rational degree and the usual polynomial degree.

[Amb03] A. Ambainis. Polynomial degree vs. quantum query complexity. In *Proceedings of 44th IEEE FOCS*, pages 230–239, 2003. quant-ph/0305028.

[BBC$^+$01] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. *Journal of the ACM*, 48(4):778–797, 2001. Earlier version in FOCS'98. quant-ph/9802049.

[BRS95] R. Beigel, N. Reingold, and D. Spielman. PP is closed under intersection. *Journal of Computer and System Sciences*, 50(2):191–202, 1995. Earlier version in STOC'91.

[BW02] H. Buhrman and R. de Wolf. Complexity measures and decision tree complexity: A survey. *Theoretical Computer Science*, 288(1):21–43, 2002.

[Deu85] D. Deutsch. Quantum theory, the Church-Turing principle, and the universal quantum Turing machine. In *Proceedings of the Royal Society of London*, volume A400, pages 97–117, 1985.

[DW11a] A. Drucker and R. de Wolf. Quantum proofs for classical theorems. *Theory of Computing*, 2011. ToC Library, Graduate Surveys 2.

[DW11b] A. Drucker and R. de Wolf. Uniform approximation by (quantum) polynomials. *Quantum Information and Computation*, 11(3&4):215–225, 2011. arxiv/1008.1599.

[Fey82] R. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6/7):467–488, 1982.

[FR99] L. Fortnow and J. Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999. Earlier version in Complexity'98. Also cs.CC/9811023.

[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of 28th ACM STOC*, pages 212–219, 1996. quant-ph/9605043.

[Lee09] T. Lee. A note on the sign degree of formulas, 2009. arxiv/0909.4607.

[New64] D. Newman. Rational approximations to $|x|$. *Michigan Mathematical Journal*, 11(1):11–14, 1964.

[NS94] N. Nisan and M. Szegedy. On the degree of Boolean functions as real polynomials. *Computational Complexity*, 4(4):301–313, 1994. Earlier version in STOC'92.

[PP87] P. P. Petrushev and V. A. Popov. *Rational Approximation of Real Functions*. Cambridge University Press, 1987.

[She14] A. Sherstov. The intersection of two halfspaces has high threshold degree. *SIAM Journal on Computing*, 2014. To appear. Earlier version in FOCS'09.

[Wol08] R. de Wolf. A note on quantum algorithms and the minimal degree of ε-error polynomials for symmetric functions. *Quantum Information and Computation*, 8(10):943–950, 2008. quant-ph/0802.1816.

[Zol77] E. Zolotarev. Application of the elliptic functions to the problems on the functions of the least and most deviation from zero (Russian). *Zpaishkah Rossijskoi Akad. Nauk*, 1877.