SIAM J. COMPUT.
Vol. 26, No. 5, pp. 1524–1540, October 1997

011

QUANTUM COMPUTABILITY*

LEONARD M. ADLEMAN†, JONATHAN DEMARRAIS†, AND MING-DEH A. HUANG†

Abstract. In this paper some theoretical and (potentially) practical aspects of quantum computing are considered. Using the tools of transcendental number theory it is demonstrated that quantum Turing machines (QTM) with rational amplitudes are sufficient to define the class of bounded error quantum polynomial time (BQP) introduced by Bernstein and Vazirani [*Proc. 25th ACM Symposium on Theory of Computation*, 1993, pp. 11–20, *SIAM J. Comput.,* 26 (1997), pp. 1411–1473]. On the other hand, if quantum Turing machines are allowed unrestricted amplitudes (i.e., arbitrary complex amplitudes), then the corresponding BQP class has uncountable cardinality and contains sets of all Turing degrees. In contrast, allowing unrestricted amplitudes does not increase the power of computation for error-free quantum polynomial time (EQP). Moreover, with unrestricted amplitudes, BQP is not equal to EQP. The relationship between quantum complexity classes and classical complexity classes is also investigated. It is shown that when quantum Turing machines are restricted to have transition amplitudes which are algebraic numbers, BQP, EQP, and nondeterministic quantum polynomial time (NQP) are all contained in PP, hence in $P^{\#P}$ and PSPACE. A potentially practical issue of designing "machine independent" quantum programs is also addressed. A single ("almost universal") quantum algorithm based on Shor's method for factoring integers is developed which would run correctly on almost all quantum computers, even if the underlying unitary transformations are unknown to the programmer and the device builder.

Key words. quantum Turing machines, quantum complexity classes

AMS subject classifications. 68Q05, 68Q10, 68Q15

PII. S0097539795293639

1. Introduction.

In 1982, Feynman [F] considered computers based on quantum mechanical principles and speculated about the existence of a universal quantum simulator analogous to a universal Turing machine. That work was followed by a sequence of important papers by Deutsch [D1, D2], Deutch and Jouzsa [DJ], Bernstein and Vazirani [BV], and others which brought the topic to a state of development suitable for rigorous investigation [Y, Si]. Recently, the topic garnered great attention when Shor [Sh] argued that integer factoring (and the discrete logarithm problem) could be solved in polynomial time on a quantum machine. More formally, Shor asserted that a problem polynomial time equivalent to integer factoring was in the class BQP defined by Bernstein and Vazirani [BV]. Since much of public key cryptography is dependent on the difficulty of factoring and discrete logarithms, the existence of these machines could have a profound effect on cryptography. It is not yet known whether these machines can be built in practice.

In this paper we study some of the theoretical and (potentially) practical aspects of quantum computing. In addition to the class BQP, the classes EQP and NQP, the analogues of the classes P and NP, are also investigated.

The results in [BV] demonstrated that when considering BQP[1] one could restrict attention to QTMs which use rotations by the angle $R = 2\pi \sum_{i=1}^{\infty} 2^{-2^i}$. In this paper, the tools of transcendental number theory are used to demonstrate that, rather than R, the angle θ such that $\cos(\theta) = 3/5$ and $\sin(\theta) = 4/5$ is sufficient (the same result

*Received by the editors October 20, 1995; accepted for publication (in revised form) December 2, 1996. The research of the first and second authors was supported by NSF grant CCR-9403662. The research of the third author was supported by NSF grant CCR-9412383.

http://www.siam.org/journals/sicomp/26-5/29363.html

†Department of Computer Science, University of Southern California, Los Angeles, CA 90089-0781 (adleman@pollux.usc.edu, jed@pollux.usc.edu, huang@pollux.usc.edu).

[1] $BQP_{poly(1/\epsilon)}$ to be precise; see section 2.

has been announced by Solovay [So]). As a result, when considering BQP, one can restrict one's attention to QTMs with rational amplitudes.

We also address an issue concerning implementation of quantum computation. Building a physical device on which to run quantum algorithms apparently requires selecting from the physical universe a set of unitary transformations (e.g., rotations) which will be used as "primitive" operations. It is unclear to what extent the builder of such a device can choose or even know with arbitrary accuracy which unitary transformations have been selected. We show that a single ("almost universal") quantum algorithm based on Shor's result would run correctly on almost all devices (i.e., the set of unacceptable rotations has Lebesgue measure 0)—even if the underlying unitary transformations are unknown to the programmer and the device builder.

Whereas QTMs with rational amplitudes are sufficient for investigating BQP, it is of theoretical interest to understand the power of QTMs with no restrictions on the amplitudes allowed. It is shown that when QTMs are allowed "unrestricted" amplitudes (i.e., arbitrary complex amplitudes), the class of sets which are decidable with bounded error in polynomial time has uncountable cardinality and contains sets of all Turing degrees. In contrast, allowing unrestricted amplitudes does not increase the power of computation for the EQP class. In fact, it is shown that if a set is accepted in EQP by a QTM with unrestricted amplitudes, it is also accepted in EQP by a QTM with amplitudes that are (real) algebraic numbers. It is also shown that, with unrestricted amplitudes, BQP is not equal to EQP.

The relationship between quantum complexity classes and classical complexity classes is also investigated. It is shown that when QTMs are restricted to have transition amplitudes which are algebraic numbers, BQP, EQP, and NQP are all contained in PP, hence in $\mathrm{P}^{\#\mathrm{P}}$ and PSPACE. Finally, let EQP_θ consist of the sets in EQP accepted by QTMs equipped with a single primitive rotation by angle θ. It is demonstrated that for θ such that $\cos(\theta)$ is transcendental, $\mathrm{EQP}_\theta = \mathrm{P}$, in particular assuming $\cos(R)$ is transcendental, $\mathrm{EQP}_R = \mathrm{P}$.

2. Definitions and results. As defined in [BV], a QTM M is a Turing machine where each tuple specifying a transition is assigned an *amplitude* which is a complex number. As in [BV], we assume that M has no stationary transition. The transition function δ of M maps each transition tuple to its amplitude. It induces a linear map, called the *time evolution operator* of M, on the infinite-dimensional linear space $\mathcal{H}$ which has the set of all configurations as an orthonormal basis. A vector in $\mathcal{H}$ is a *superposition of configuration*. Thus, if, for example, $C_1, \ldots, C_m$ are the configurations M can reach in one step from a configuration C under δ, with amplitudes $a_1, \ldots, a_m$, then the time evolution operator maps C to $a_1C_1 + \cdots + a_mC_m$. A QTM M is *well formed* if its time evolution operator preserves the L_2-norm.[2]

Later we will have the need to refer to subsets of QTMs with restricted amplitudes. We introduce notation to facilitate this.

Given any field K, we define QTM_K to be the subset of QTMs whose amplitudes (i.e., the range of δ) are all in K. Examples include $\mathrm{QTM}_{\mathbf{C}}$, $\mathrm{QTM}_{\mathbf{R}}$, $\mathrm{QTM}_{\bar{\mathbf{Q}}}$, and $\mathrm{QTM}_{\mathbf{Q}}$. We will write QTM to refer to $\mathrm{QTM}_{\mathbf{C}}$.

According to [BV], one can assume without loss of generality that the amplitudes of δ are all real and that M enters any particular state from one direction. One can therefore define the local matrix $Ł_\delta$ whose columns are indexed by pairs of current state and symbol and rows by pairs of new state and symbol; and the entry

[2] A probabilistic Turing machine is in fact a Turing machine with a transition function δ whose amplitudes are restricted to 0,1 and 1/2 and whose time evolution operator preserves the L_1-norm.

corresponding to a column and a row is the amplitude for the associated transition.

If $\theta \in \mathbf{R}_{\geq 0}^{<2\pi}$, then we will define QTM_θ, to be the subset of QTM M whose local matrix is block diagonal (up to permutations of rows and columns) with each block either 1, -1, or 2 by 2 of the form

$$\begin{matrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta). \end{matrix}$$

Note that the 2×2 block represents rotation by angle θ. The universal QTM constructed by Bernstein and Vazirani [BV], for example, belongs to QTM_R, where $R = 2\pi \sum_{i=1}^{\infty} 2^{-2^i}$. We will also call this class QTM_{BV}. Another example is QTM_π, which consists of deterministic Turing machines with all entries either $0, \pm 1$.

On occasion we will use an ad hoc notation. For example, M is in $\mathrm{QTM}_{poly(1/\epsilon)}$ iff there exist an $f \in \mathbf{Z}[x]$ and a deterministic algorithm which, on input $1/\epsilon$, where $\epsilon \in \mathbf{Q}_{>0}^{<1}$, approximates all transition amplitudes of M within ϵ in $f(1/\epsilon)$ time.[3]

If Q_1 and Q_2 are subsets of QTM, then we will write $Q_1 \preceq Q_2$ iff for all $\epsilon \in \mathbf{Q}_{>0}^{<1}$, for all machines $M_1 \in Q_1$, there exists a machine $M_2 \in Q_2$ such that M_2 simulates M_1 to within ϵ with at most a polynomial slowdown, in the sense of [BV].[4] We use $\prec$, $\succ$, and $\asymp$ in the expected ways. For example, $\mathrm{QTM}_{\mathbf{C}} \asymp \mathrm{QTM}_{\mathbf{R}}$ as was shown by Bernstein and Vazirani [BV].

The classes BQP and EQP are due to Bernstein and Vazirani [BV]. The next definitions define restricted notions of BQP and EQP.

In this paper, $||$ denotes length in binary, except in section 3 where it denotes absolute value.

DEFINITION 2.1. *For all $T \subseteq$ QTM, for all $S \subseteq \mathbf{N}$, $S \in \mathrm{BQP}_T$ iff there exists an $f \in \mathbf{Z}[x]$ and an $M \in T$ such that, for all $x \in \mathbf{N}$,*

$x \in S \Rightarrow$ for input x, M accepts with probability greater than $2/3$ after $f(|x|)$ steps;

$x \in \overline{S} \Rightarrow$ for input x, M rejects with probability greater than $2/3$ after $f(|x|)$ steps.

DEFINITION 2.2. *For all $T \subseteq$ QTM, for all $S \subseteq \mathbf{N}$, $S \in \mathrm{EQP}_T$ iff there exists an $f \in \mathbf{Z}[x]$ and an $M \in T$ such that, for all $x \in \mathbf{N}$,*

$x \in S \Rightarrow$ for input x, M accepts with probability 1 after $f(|x|)$ steps;

$x \in \overline{S} \Rightarrow$ for input x, M rejects with probability 1 after $f(|x|)$ steps.

DEFINITION 2.3. *For all $T \subseteq$ QTM, for all $S \subseteq \mathbf{N}$, $S \in \mathrm{NQP}_T$ iff there exists an $f \in \mathbf{Z}[x]$ and an $M \in T$ such that, for all $x \in \mathbf{N}$,*

$x \in S \Rightarrow$ for input x, M accepts with positive probability after $f(|x|)$ steps;

$x \in \overline{S} \Rightarrow$ for input x, M accepts with probability 0 after $f(|x|)$ steps.

For convenience, for all fields K, when T=QTM_K, we will write BQP_K or EQP_K. For all $\theta \in \mathbf{R}_{\geq 0}^{<2\pi}$, when $T = \mathrm{QTM}_\theta$, we will write BQP_θ or EQP_θ. Similarly, when T=$\mathrm{QTM}_{poly(1/\epsilon)}$, we will write $\mathrm{BQP}_{poly(1/\epsilon)}$.

2.1. Results. Let $T_1, T_2 \subseteq$QTM . Then $T_1 \preceq T_2$ implies that $\mathrm{BQP}_{T_1} \subseteq \mathrm{BQP}_{T_2}$. (This is not merely an observation but requires a short proof which will not be given here.) The results in [BV] imply that $\mathrm{QTM}_{poly(1/\epsilon)} \preceq \mathrm{QTM}_R$, and since R is approximable in polynomial time within ϵ, it follows that $\mathrm{BQP}_{poly(1/\epsilon)} = \mathrm{BQP}_R$. Consequently, rotation by angle R serves as a universal primitive for $\mathrm{BQP}_{poly(1/\epsilon)}$. It is

[3] One can define $\mathrm{QTM}_{rpoly(1/\epsilon)}$ as above, but where instead of a deterministic algorithm a "probabilistic" one is used.

[4] That is, suppose in t steps M_1 produces, on input x, a superposition of configuration ϕ_1. Then in time polynomial in $1/\epsilon$ and t, M_2 produces, on the same input x, a superposition of configuration ϕ_2 such that the L_2-norm of $\phi_1 - \phi_2$ is less than ϵ.

natural to ask if R can be replaced by other angles, particularly an angle θ with rational $\cos(\theta)$ and $\sin(\theta)$. We show that for all angles θ in a set S of Lebesgue measure 1, $\mathrm{QTM}_R \preceq \mathrm{QTM}_\theta$, consequently any such θ can replace R as a universal angle. In particular the angle θ with $\cos(\theta) = 3/5$ is in S; hence, $\mathrm{BQP}_{poly(1/\epsilon)} = \mathrm{BQP}_{\mathbf{Q}}$. These results are presented in section 3.

The proof technique for the fact that $\mathrm{QTM}_R \preceq \mathrm{QTM}_\theta$ for all $\theta \in S$ can be applied to construct a program based on Shor's factoring algorithm which works universally for all QTM_θ with $\theta \in S$. This makes it possible to write a single program for a quantum computer without knowing the primitive rotation used by the machine. This is discussed in section 4.

The next set of results addresses the following question: would unrestricted amplitudes for transition functions increase the power of quantum computation? It is shown in section 5 that $\mathrm{BQP}_{\mathbf{C}}$ contains sets of arbitrary Turing degrees, hence undecidable sets in particular. In contrast, it is shown in section 6 that $\mathrm{EQP}_{\mathbf{C}} = \mathrm{EQP}_{\bar{\mathbf{Q}}}$. Moreover, $\mathrm{BQP}_{poly(1/\epsilon)}$, $\mathrm{EQP}_{\bar{\mathbf{Q}}}$, and $\mathrm{NQP}_{\bar{\mathbf{Q}}}$ are all contained in PP, hence in $\mathrm{P}^{\#\mathrm{P}}$ and PSPACE. As a result, $\mathrm{BQP}_{\mathbf{C}} \neq \mathrm{EQP}_{\mathbf{C}}$. The proofs for these equalities explore algebraic geometric structures underlying the EQP and NQP classes. The techniques also yield the following result: for angles θ with $\cos\theta$ transcendental, $\mathrm{EQP}_\theta = \mathrm{P}$. In particular, assuming $\cos(R)$ is transcendental, $\mathrm{EQP}_R = \mathrm{P}$.

3. $\mathbf{QTM_Q \asymp QTM_{BV}}$.

THEOREM 3.1. $\mathrm{QTM}_{BV} \asymp \mathrm{QTM}_{\mathbf{Q}} \asymp \mathrm{QTM}_{\bar{\mathbf{Q}}} \asymp \mathrm{QTM}_{poly(1/\epsilon)}$.

COROLLARY 3.2. $\mathrm{BQP}_{BV} = \mathrm{BQP}_{\mathbf{Q}} = \mathrm{BQP}_{\bar{\mathbf{Q}}} = \mathrm{BQP}_{poly(1/\epsilon)}$.

Essentially the same result has been announced by Solovay [So].

It can be easily demonstrated that $\mathrm{QTM}_{\mathbf{Q}} \preceq \mathrm{QTM}_{\bar{\mathbf{Q}}} \preceq \mathrm{QTM}_{poly(1/\epsilon)}$, and it follows from results on approximations [BV, BBBV] that $\mathrm{QTM}_{poly(1/\epsilon)} \preceq \mathrm{QTM}_{BV}$. Hence, Theorem 3.1 will follow from establishing that $\mathrm{QTM}_{BV} \preceq \mathrm{QTM}_\theta$ for some θ with rational $\cos\theta$ and $\sin\theta$. More generally, one would like to understand for what angles θ, $\mathrm{QTM}_{BV} \preceq \mathrm{QTM}_\theta$. The following theorem provides an answer.

THEOREM 3.3. *For all* $\theta \in \mathbf{R}_{\geq 0}^{<2\pi}$ *if either*

(a) $\theta/2\pi$ *is not rational and not Liouville*;

(b) $\theta/2\pi \in \bar{\mathbf{Q}} - \mathbf{Q}$;

(c) $e^{i\theta} \in \bar{\mathbf{Q}}$ *and* $e^{i\theta}$ *not a root of unity*;

(d) $\cos(\theta), \sin(\theta) \in \mathbf{Q} - \{0\}$;

(e) $\cos(\theta) = 3/5, \sin(\theta) = 4/5$;

then $\mathrm{QTM}_{BV} \preceq \mathrm{QTM}_\theta$.

Thus Theorem 3.1 follows from (e) of Theorem 3.3. It will be shown that (b)–(e) of Theorem 3.3 are actually subcases of (a). We also recall for Theorem 3.3 that (see, e.g., [Ni, B]) a real number ξ is a *Liouville number* if for every positive integer m there is a distinct rational number h_m/k_m with $k_m > 1$ such that $|\xi - h_m/k_m| < (k_m)^{-m}$.

COROLLARY 3.4. *For almost all* $\theta \in \mathbf{R}_{\geq 0}^{<2\pi}$, $\mathrm{QTM}_{BV} \preceq \mathrm{QTM}_\theta$, *where "almost all" means* $S = \{\theta | \theta \in \mathbf{R}_{\geq 0}^{<2\pi}$ *and* $\mathrm{QTM}_{BV} \preceq \mathrm{QTM}_\theta\}$ *has Lebesgue measure* 1.

Corollary 3.4 follows from Theorem 3.3 and the fact that the set of Liouville numbers has Lebesgue measure 0 (see, e.g., [B, p. 86]).

To prove Theorem 3.3 we will need the following lemma.

LEMMA 3.5. *For all* $\theta \in \mathbf{R}$ *with* $\theta/(2\pi)$ *not rational and not Liouville, there exists an* $f \in \mathbf{Z}[X]$ *such that for all* $\gamma \in \mathbf{R}$ *and all* $\epsilon \in \mathbf{R}_{>0}^{<1}$ *there exist* $x \in \mathbf{Z}_{\geq 0}$ *and* $w \in \mathbf{Z}$ *such that* $|x\theta - 2\pi w - \gamma| < \epsilon$ *and* $x < f(1/\epsilon)$.

Proof of Lemma 3.5. Given any irrational α and any positive integer n, there exist integers h and k with $0 < k \leq n$ such that $|k\alpha - h| < 1/n$ (see Theorem 4.2 of

[Ni, p. 44]). Since $\theta/2\pi$ is irrational, if $n = \lceil 2\pi/\epsilon \rceil$, then there exist $h, k \in \mathbf{Z}$ with $0 < k \leq n$ such that $|(k\theta/(2\pi)) - h| < 1/n$ or, equivalently, $|k\theta - 2\pi h| < 2\pi/n \leq \epsilon$.

Since $\theta/2\pi$ is not Liouville and not rational, there exists an $m \in \mathbf{Z}_{>0}$ such that for all $h', k' \in \mathbf{Z}$ with $k' > 1$, $|(\theta/(2\pi)) - h'/k'| \geq 1/k'^m$, and therefore $|k'\theta - 2\pi h'| \geq 2\pi/k'^{m-1}$. Hence $2\pi/k^{m-1} \leq |k\theta - 2\pi h| < \epsilon$.

Let $\beta = \gamma + 2\pi y'$ such that $y' \in \mathbf{Z}$, $-2\pi < \beta < 2\pi$, and $\beta/(k\theta - 2\pi h) \geq 0$. Let $x' = \lceil \beta/(k\theta - 2\pi h) \rceil$. Let $x = x'k$, and $y = x'h$, then $|x\theta - 2\pi y - \beta| = |(k\theta - 2\pi h)x' - \beta| < |(k\theta - 2\pi h)((\beta/(k\theta - 2\pi h)) + 1) - \beta| = |k\theta - 2\pi h| < \epsilon$. Also $|x'| < |\beta/(k\theta - 2\pi h)| + 1 \leq (|\beta|/|k\theta - 2\pi h|) + 1 \leq (|\beta|/(2\pi/k^{m-1})) + 1 < k^{m-1} + 1$ since $|\beta| < 2\pi$. Hence $|x| = x'k < k^m + k$, and since $k \leq n = \lceil 2\pi/\epsilon \rceil$, if $f = 8^m X^m + 8X$, then $x < f(1/\epsilon)$. Let $w = y + y'$, then $|x\theta - 2\pi w - \gamma| = |x\theta - 2\pi y - 2\pi y' - \gamma| = |x\theta - 2\pi y - \beta| < \epsilon$ as required. □

Remark. When $\theta, \gamma \in \mathbf{R}_{>0}^{<2\pi}$, then it follows easily from the lemma that $|w| \leq x + 2$.

The proof which follows demonstrates the capacity of a quantum computer to obtain an approximation to its intrinsic angle through experimentation. This capacity will also play an important role in the subsequent section on almost universal quantum programs.

Proof of Theorem 3.3(a). Given an $M \in \mathrm{QTM}_{BV}$ and $\epsilon \in \mathbf{Q}_{>0}^{<1}$, we will construct an $M' \in \mathrm{QTM}_\theta$ such that M' simulates M with accuracy ϵ and slowdown polynomial in $1/\epsilon$ and time t. The QTM M' will determine a natural number a such that $a\theta$ approximates the angle $R = 2\pi \sum_{i=1}^{\infty} 2^{-2^i}$ used by machines in QTM_{BV}. Once a is determined, M' simulates M by replacing each R-transition with a sequence of a θ-transitions.

In order to determine the number a, M' needs to compute an accurate enough rational approximation $\hat{\theta}$ of its underlying angle θ. Unlike R, the angle θ will not in general be easy to approximate deterministically. However, it is possible to have the QTM compute its own internal angle up to reflection about the x-axis and y-axis with arbitrary accuracy. That is, it is possible to compute approximations to $|\sin(\theta)|$ and $|\cos(\theta)|$. From these approximations an angle $\hat{\theta}$ which approximates θ can be determined. The correct $\hat{\theta}$ (of the four which are consistent with the approximated $|\sin(\theta)|$ and $|\cos(\theta)|$) depends on the quadrant that θ is in; however, in this existence proof, we may assume that this is known. For convenience, we will proceed under the assumption that θ is in the first quadrant. The other cases are handled in a similar manner.

Consider the following procedure that can be implemented on a machine in QTM_θ. On input $n, m \in \mathbf{Z}_{>0}$,

(i) begin with n, m on the tape;

(ii) place m^2n^2 0's on the tape, and for each 0 do a quantum step such that the symbol stays the same with probability $\cos^2(\theta)$ and becomes a 1 with probability $\sin^2(\theta)$;

(iii) observe the bits after the quantum flips and record the ratio r of the number of 0's to m^2n^2;

(iv) output $\hat{\theta} \in \mathbf{Q}$ such that $|\hat{\theta} - \theta'| < 1/n$, where $\theta' = \arccos(\sqrt{r})$.

In the above procedure, the number of 0's follows the binomial distribution with mean $\mu = m^2n^2\cos^2(\theta)$ and standard deviation $\sigma = mn\cos(\theta)\sin(\theta)$. From Chebyshev's inequality it follows that with probability at least $1 - 1/m^2$,

$$\left|r - \cos^2(\theta)\right| = |\cos^2(\theta') - \cos^2(\theta)| < m\sigma/m^2n^2 = \sin(2\theta)/2n < 1/2n.$$

Hence the ratio r approximates $\cos^2(\theta)$ better and better with increasing n. When n is large enough so that the recorded $r = \cos^2(\theta')$ is greater than $2/n$, we have $\cos^2(\theta) >$

$\cos^2(\theta') - 1/2n > 1/n$, and it also follows that $\cos^2(\theta') > \cos^2(\theta) - 1/2n > \cos^2(\theta)/2$. Since θ is in the first quadrant, it follows that $\cos(\theta') > \cos(\theta)/\sqrt{2}$. A similar argument shows that $\sin(\theta') > \sin(\theta)/\sqrt{2}$. Moreover if ψ is an angle between θ and θ', then $\cos(\psi) > \cos(\theta)/\sqrt{2}$ and $\sin(\psi) > \sin(\theta)/\sqrt{2}$; hence $2\sin(\psi)\cos(\psi) > \sin(\theta)\cos(\theta)$. By the mean value theorem,

$$|\theta - \theta'| = |\cos^2(\theta) - \cos^2(\theta')|/2\sin(\psi)\cos(\psi)$$

for some ψ between θ and θ'. It follows that

$$|\theta - \theta'| < |\cos^2(\theta) - \cos^2(\theta')|/\sin(\theta)\cos(\theta) < 1/n.$$

Hence

$$|\theta - \hat{\theta}| \leq |\theta - \theta'| + |\hat{\theta} - \theta'| < 2/n.$$

Consequently the probability that $|\theta - \hat{\theta}| < 2/n$ is at least $1 - 1/m^2$.

We will choose m so that $m > 1/\epsilon$. Let $\delta = \frac{\epsilon}{6t}$. We will run the above procedure on input m and increasing value of n, until the following conditions are met:

(a) the recorded number $r > 2/n$;

(b) there are integers a, b with $0 \leq a, |b| < (n\delta)/6$ such that $|a\hat{\theta} - b2\hat{\pi} - \hat{R}| < 2\delta$, where $\hat{R}, \hat{\pi} \in \mathbf{Q}$ such that $|R - \hat{R}| < \delta/3$ and $|2\pi - 2\hat{\pi}| < 1/n$.

Let f be the polynomial in Lemma 3.5 for θ. We argue that the condition (b) will be met before n exceeds $\frac{6(f(1/\delta)+2)}{\delta}$, which is polynomial in t and $1/\epsilon$.

Indeed let $n = \frac{6(f(1/\delta)+2)}{\delta}$. Then Lemma 3.5 implies the existence of a, b with $0 \leq a, |b| < f(1/\delta) + 2 = (n\delta)/6$ such that $|a\theta - b2\pi - R| < \delta$. With such a and b, $|a||\theta - \hat{\theta}|$, $|b||2\pi - 2\hat{\pi}|$, and $|R - \hat{R}|$ are all bounded by $\delta/3$. Since $|a\hat{\theta} - b2\hat{\pi} - \hat{R}| \leq |a\theta - b2\pi - R| + |a||\theta - \hat{\theta}| + |b||2\pi - 2\hat{\pi}| + |R - \hat{R}|$, it follows that $|a\hat{\theta} - b2\hat{\pi} - \hat{R}| < 2\delta$ as required.

With the computed $\hat{\theta}$ and a, b, we have

$$|a\theta - b2\pi - R| \leq |a\hat{\theta} - b2\hat{\pi} - \hat{R}| + |a||\theta - \hat{\theta}| + |b||2\pi - 2\hat{\pi}| + |R - \hat{R}| < 3\delta.$$

Hence rotation by the angle θ a times approximates rotation by angle R to within $3\delta = \epsilon/(2t)$.

Now on input x, M' can simulate M on input x by replacing each R-transition with a sequence of a θ-transitions appropriately.

Finally, the following argument adapted from [BBBV] (see also [BV]) shows that the superposition of configurations produced by M in t steps is approximated by M' within ϵ after the t steps of M are all simulated.

Let $\{C_1, C_2, ...\}$ be the set of configurations and $\mathcal{H}$ be the space of superpositions of configurations of M. Let U be the time evolution operator of M. Let $\hat{U}$ be the linear map on $\mathcal{H}$ determined by the local matrix which is obtained from the local matrix of M by replacing each 2×2 block representing rotation by angle R with a 2×2 block representing rotation by angle $a\theta$. Suppose at a certain time that ϕ is the superposition of configurations that M has. Then $U^t\phi$ is the superposition of configurations M arrives at after t steps, and $\hat{U}^t\phi$ is the superposition of configurations M' arrives at after simulating these t steps of M. Hence it suffices to show that $\|\hat{U}^t\phi - U^t\phi\| < \epsilon$, for all $\phi \in \mathcal{H}$ with $\|\phi\| = 1$, where $\| \|$ denotes the L_2-norm.

First we show that $\|\hat{U}\phi - U\phi\|^2 < \epsilon^2/t^2$. To see this, let $I(i)$ be the set of C_j such that there is a transition from C_j to C_i with nonzero amplitude; let $E(i)$ be the set

of C_j such that there is a transition from C_i to C_j with nonzero amplitude. Since the local matrix is block diagonal with each block of size at most 2×2, the cardinality of $I(i)$ and $E(i)$ are bounded by 2. Let $UC_i = \sum_j \alpha_{ij} C_j$ and $\hat{U}C_i = \sum_j \hat{\alpha}_{ij} C_j$. Then $|\alpha_{ij} - \hat{\alpha}_{ij}| < \Delta$ where $\Delta = 3\delta = \epsilon/(2t)$. Let $\phi = \sum_j \beta_j C_j$ be of L_2-norm equal to 1. Then

$$U\phi = \sum_i \left(\sum_{j \in I(i)} \alpha_{ji} \beta_j \right) C_i;$$

hence

$$\begin{aligned} \|\hat{U}\phi - U\phi\|^2 = \sum_i \left| \sum_{j \in I(i)} (\hat{\alpha}_{ji} - \alpha_{ji}) \beta_j \right|^2 &\leq \sum_i |I(i)| \sum_{j \in I(i)} |(\hat{\alpha}_{ji} - \alpha_{ji}) \beta_j|^2 \\ &< 2\Delta^2 \sum_i \sum_{j \in I(i)} \beta_j^2 = 2\Delta^2 \sum_j |E(j)| \beta_j^2 \leq 4\Delta^2 \sum_j \beta_j^2 = 4\Delta^2 = \epsilon^2/t^2. \end{aligned}$$

It is easy to see by induction that

$$\hat{U}^t \phi - U^t \phi = \sum_{i=1}^{t} \hat{U}^{t-i} E_i,$$

where $E_i = \hat{U}U^{i-1}\phi - U^i\phi$. Since $U^{i-1}\phi$ is of L_2-norm equal to 1,

$$\|E_i\|^2 = \|\hat{U}(U^{i-1}\phi) - U(U^{i-1}\phi)\|^2 \leq \epsilon^2/t^2.$$

So

$$\|\hat{U}^t \phi - U^t \phi\|^2 = \left\| \sum_{i=1}^{t} \hat{U}^{t-i} E_i \right\|^2 \leq t \sum_{i=1}^{t} \|\hat{U}^{t-i} E_i\|^2 = t \sum_{i=1}^{t} \|E_i\|^2 < \epsilon^2. \qquad \square$$

For the proof of Theorem 3.3(b)–(e), we need a lemma and proof which were generously provided to us by Harold Stark.

LEMMA 3.6. *For all $\theta \in \mathbf{R}_{>0}^{<2\pi}$, if $e^{i\theta} \in \bar{\mathbf{Q}}$ and $e^{i\theta}$ is not a root of unity, then $\theta/(2\pi)$ is not Liouville.*

Note that if θ satisfies the conditions in Lemma 3.6, then $\theta/(2\pi)$ is also not rational. Lemma 3.6 is a consequence of the next theorem which follows from results of Feldman [Fe].

THEOREM 3.7. *For all $a = \cos(b) + i\sin(b) = \exp(ib) \in \bar{\mathbf{Q}}$, with a not a root of unity, there exists a $C, N \in \mathbf{Z}_{>0}$ such that for all $p \in \mathbf{Z}$, $q \in \mathbf{Z}_{>1}$, $|p2\log(-1) - q\log(a)| > Cq^{-N}$, where C and N depend only on a and on the choice of the branch of logarithms used.*

Since $e^{i\theta}$ is algebraic and not a root of unity, by choosing the branch of logarithm such that $2\log(-1) = 2\pi i$, and $\log(e^{i\theta}) = i\theta$, we have that for all $p \in \mathbf{Z}$, $q \in \mathbf{Z}_{>1}$, $|p2\pi i - qi\theta| = |p2\pi - q\theta| > Cq^{-N}$. Hence $|\theta/2\pi - p/q| > C/(2\pi q^{N+1})$ from which it follows that $\theta/2\pi$ is not Liouville. This proves Lemma 3.6. $\square$

Proof of Theorem 3.3(b)–(e). (b) follows from (a) since Liouville numbers are transcendental (see, e.g., [Ni, p. 92]). (c) follows from (a) and Lemma 3.6. (d) follows from (c) and the fact that the only roots of unity with rational real and imaginary parts are 1 and i. Finally, (e) follows from (d). $\square$

4. Almost universal quantum programs. Shor's quantum factoring method is of interest for purely mathematical reasons. However, it is unclear whether devices can be built which will actually implement Shor's method. It follows from the previous section that apparently it is enough to build a device capable of a rotation θ with $\cos(\theta) = 3/5$. But can such a device be built? To what extent can a device builder choose the angles of rotations which will be provided? To what accuracy can the device builder or the programmer know the angles of rotation inherent in the device? It turns out that these questions may be irrelevant and that one can write a single "program" which will factor with high probability on virtually any device which can be built.

This is done essentially as indicated in the proof of Theorem 3.3. One starts with a program for Shor's method which will factor with high probability on a device with rotation by the angle θ with $\cos(\theta) = 3/5$ as primitive. One then writes a new "almost universal program" which will, in the manner described in the proof of Theorem 3.3, calculate "on line" a sufficiently accurate estimation of whatever angle of rotation γ the underlying physical device provides and then use that estimate to simulate the original program with sufficient accuracy to insure factoring. Since the estimate of γ is only unique up to the sign of $\cos(\gamma)$ and $\sin(\gamma)$, we will simultaneously run all four possible approximations; however, this will neither increase the running time significantly nor decrease the probability of a successful factorization substantially. It follows from Corollary 3.4 that the "almost universal program" will factor with high probability on all but those devices with an angle of rotation in a set of Lebesgue measure 0.

5. Unrestricted quantum computation. We have demonstrated that restricting attention to quantum machines with rational amplitudes is sufficient to define the class BQP. However, it is of theoretical interest to understand the power of "unrestricted" quantum computation. In this section, it is shown that $\mathrm{BQP}_{\mathbf{C}}$ has sets of all possible Turing degrees.

THEOREM 5.1. *For all $S \subseteq \mathbf{N}$, there exists an $S' \subseteq \mathbf{N}$ such that*

1. *$S \equiv_T S'$ (Turing equivalent);*
2. *$S' \in \mathrm{BQP}_{\mathbf{C}}$.*

Proof. Throughout this proof, for all $x \in \mathbf{N}$, $|x|$ will denote the length of x. Let $S \subseteq \mathbf{N}$ and let $H : \mathbf{N} \to \{1, -1\}$ be such that for all $x \in \mathbf{N}$, $H(x) = 1$ if $x \in S$, $H(x) = -1$ if $x \in \overline{S}$. Let $S' \subseteq \mathbf{N}$ such that for all $x \in \mathbf{N}$, $x \in S'$ if and only if $H(i+1) = 1$ where i is the greatest integer such that $8^i \leq |x|$. It is clear from the definition that S and S' are Turing equivalent.

Let $\theta = 2\pi(\sum_{x=1}^{\infty} H(x)/8^x)$. Then $\theta \in \mathbf{R}$ (i.e., the series converges).

Let M be a QTM which on input $x \in \mathbf{N}$.

1. Calculate the greatest l such that $l \leq |x|$ and $l = 8^i$ for some $i \in \mathbf{N}$.
2. Place a 0 on the tape.
3. Perform l rotations by the angle θ on this tape location followed by a single rotation by the angle $\pi/4$, so that the amplitude of the configuration with 0 on the tape is $\cos(l\theta + \pi/4)$, and the amplitude with 1 on the tape is $\sin(l\theta + \pi/4)$. This is done in a manner similar to the method used by Bernstein and Vazirani [BV].
4. Output 0 or 1 based on the value of the given tape location. If the output is 1, the machine accepts, and if the output is 0, the machine rejects.

It is clear from the algorithm that for all $x \in \mathbf{N}$, the number of steps taken by M on input x is polynomially bounded in $|x|$.

After the third step of the algorithm, the configuration that corresponds to an output of 0 has amplitude $\cos(l\theta + \pi/4)$, and the configuration that corresponds to

an output of 1 has amplitude $\sin(l\theta + \pi/4)$ for the greatest l such that $l \leq |x|$ and l is power of 8. Let $l = 8^i$. Then

$$l\theta = 2\pi(H(1)8^{i-1} + H(2)8^{i-2} + \cdots + H(i) + H(i+1)/8 + H(i+2)/8^2 + \cdots).$$

Let $k = \pi/4 + l\theta \bmod 2\pi$. If $H(i+1) = 1$, then $\pi/2 - \pi/28 \leq k \leq \pi/2 + \pi/28$, in this case $\sin^2(\pi/4 + l\theta) > 0.98$; hence the input x is accepted with probability greater than 0.98. On the other hand if $H(i+1) = -1$, then $-\pi/28 \leq k \leq \pi/28$, in this case $\cos^2(\pi/4 + l\theta) > 0.98$; hence x is rejected with probability greater than 0.98. Therefore M accepts S' in $\mathrm{BQP}_{\mathbf{C}}$ and the theorem follows. □

Since there are uncountably many subsets of N and each Turing class can contain at most countably many subsets of N (since there are only this many TM), it follows that $\mathrm{BQP}_{\mathbf{C}}$ has uncountable cardinality. From this it follows that $\mathrm{BQP}_{\mathbf{Q}}$ (which clearly has countable cardinality) is a proper subset of $\mathrm{BQP}_{\mathbf{C}}$. From this in turn (see section 2) it follows that $\mathrm{QTM}_{\mathbf{Q}} \prec \mathrm{QTM}_{\mathbf{C}}$ and not $\mathrm{QTM}_{\mathbf{Q}} \succeq \mathrm{QTM}_{\mathbf{C}}$.

6. EQP and NQP. Let M be a QTM with transition function δ. Following [BV] we can assume without loss of generality that δ is a real-valued function.

Suppose there are N tuples $T_1, \ldots, T_N$ in the domain of δ. Let $v = (v_1, \ldots, v_N)$ where $v_i = \delta(T_i)$, the amplitude of δ on transition T_i, for $i = 1, \ldots, N$. We shall call v the *amplitude vector* of δ.

Replacing v by $x = (x_1, \ldots, x_N)$, where x_i are distinct complex variables, we obtain a "symbolic" QTM $M(x)$. By assigning a vector $u \in \mathbf{C}^N$ to x we obtain a QTM denoted by $M(u)$, in particular, $M = M(v)$. The QTMs obtained in this way have transition functions with the same domain, the same set of configurations, hence the same space of superpositions of configurations. They are distinguished by having different amplitude vectors associated with the transition function.

For $u \in \mathbf{R}^N$, $M(u)$ is well formed iff u satisfies a finite set of polynomial equations which can be obtained as follows.

Let $A(x)$ denote the infinite-dimensional matrix representing the (symbolic) time evolution operator of $M(x)$, the linear map induced by δ, on the infinite-dimensional space of superpositions of configurations [BV] with respect to the basis consisting of the whole set of configurations of $M(x)$. The rows and columns of $A(x)$ are labelled by the set of configurations. If upon applying the ith transition, a configuration C yields C', then x_i will be the entry corresponding to column labelled by C and the row labelled by C'. If no such transition exists, the corresponding entry will be 0. Thus each entry of $A(x)$ is one of the variables $x_1, \ldots, x_N$, and for all $u = (u_1, \ldots, u_N) \in \mathbf{R}^N$, by substituting x_i with u_i for $i = 1, \ldots, N$, we obtain the time evolution matrix $A(u)$ for $M(u)$. For all $i, j \in \mathbf{Z}_{>0}$, let $P_{ij}(x)$ denote the dot product of the ith and jth columns of $A(x)$. Then since each column of $A(x)$ has at most N nonzero entries, P_{ij} is the sum of at most N monomials in $x_1, \ldots, x_N$ of degree 2. In particular the set of P_{ij} is finite.

By [BV], $M(u)$ is well formed iff $A(u)^*A(u) = A(u)A(u)^* = I$, where $A(u)^*$ denotes the transpose conjugate of $A(u)$. Since u is real, $A(u)^*$ is just the transpose of $A(u)$. Hence $M(u)$ is well formed iff for all i, j, if $i \neq j$, then $P_{ij}(u) = 0$; if $i = j$, then $P_{ij}(u) = 1$. Hence let J_W be the set of polynomials P_{ij} for $i \neq j$ and $1 - P_{ii}$ for all i. Then $M(u)$ is well formed iff u is a zero to all polynomials in J_W. Note that J_W is finite since the set of P_{ij} is finite.

As will be demonstrated below, whether $M(u)$ accepts or rejects an input with probability 1 can also be characterized algebraically.

For all $i \in \mathbf{Z}_{>0}$, let $A^i(x)$ denote the product of $A(x)$ by itself i times. We note that each entry in $A^i(x)$ is a polynomial (possibly 0) in $\mathbf{Z}[X]$. Let α be an input string.

Let C_α be the initial configuration of $M(x)$ (hence of M and for all $u \in \mathbf{R}^N$, of $M(u)$) on input α. Then for all configurations C, for all $t \in \mathbf{Z}_{>0}$, we denote by $amp_{\alpha,t,C}$ the polynomial which is in the entry of $A^t(x)$ corresponding to the column labelled by C_α and the row labelled by C. For all $u \in \mathbf{C}^N$, $amp_{\alpha,t,C}(u)$ is the amplitude for C at time t on input α to $M(u)$.

Let $\mathcal{C}_A$ denote the set of accepting configurations and $\mathcal{C}_R = \mathcal{C} - \mathcal{C}_A$ the set of rejecting configurations. Suppose $u \in \mathbf{R}^N$, and assuming $M(u)$ is well formed, then an input α is accepted at time t with probability 1 iff

$$\sum_{C \in \mathcal{C}_R} |amp_{\alpha,t,C}(u)|^2 = \sum_{C \in \mathcal{C}_R} amp^2_{\alpha,t,C}(u) = 0,$$

iff $amp_{\alpha,t,C}(u) = 0$ for all $C \in \mathcal{C}_R$. Hence let

$$J_A(t,\alpha) = \{amp_{\alpha,t,C} : C \in \mathcal{C}_R\}.$$

Then $M(u)$ accepts α at time t with probability 1 iff u is a zero of all polynomials in $J_A(t,\alpha)$. Similarly, let

$$J_R(t,\alpha) = \{amp_{\alpha,t,C} : C \in \mathcal{C}_A\}.$$

Then $M(u)$ rejects α with probability 1 iff u is a zero of all polynomials in $J_R(t,\alpha)$.

Let L be a language over the input alphabet of M. Let p be a polynomial function where $p(n)$ is a positive integer for all $n \in \mathbf{Z}_{>0}$. For all inputs α, let $t_\alpha = p(n)$ where n is the length of α. Let

$$J(p,L) = J_W \cup_{\alpha \in L} J_A(t_\alpha,\alpha) \cup_{\alpha \notin L} J_R(t_\alpha,\alpha).$$

From the discussion above we see that for all $u \in \mathbf{R}^N$, $M(u)$ is well formed and accepts L in EQP at time $p(n)$ iff u is a zero of all polynomials in $J(p,L)$.

We recall the following proposition.

PROPOSITION 6.1. *Let I be an ideal in $\mathbf{Q}[x_1,\ldots,x_N]$. If the polynomials in I have a common zero in $\mathbf{R}^N$, then they have a common zero in $(\bar{\mathbf{Q}} \cap \mathbf{R})^N$.*

The proposition follows immediately from Tarski's theorem (see, e.g., [J, p. 323]), noting the fact that I is finitely generated and that both $\mathbf{R}$ and $\bar{\mathbf{Q}} \cap \mathbf{R}$ are real closed fields. It is a direct consequence of the mathematical principle implied by Tarski's theorem that any elementary sentence of algebra which is true in one real closed field is true in every real closed field.

Suppose L is accepted by $M = M(v)$ in EQP at time $p(n)$. Then v is a real zero of polynomials in the ideal I of $\mathbf{Q}[x_1,\ldots,x_N]$ generated by $J(p,L)$. From Proposition 6.1 it follows that the polynomials in I also have a common zero $u \in (\bar{\mathbf{Q}} \cap \mathbf{R})^N$. Since u is a zero of all polynomials in $J(p,L)$, it follows that $M(u)$ is well formed and accepts L in EQP at time $p(n)$.

Hence we have the following.

THEOREM 6.2. $\mathrm{EQP}_{\mathbf{C}} = \mathrm{EQP}_{\bar{\mathbf{Q}} \cap \mathbf{R}}$.

Finally, we give two results which relate quantum complexity classes to classical complexity classes.

THEOREM 6.3. *For all $\theta \in \mathbf{R}^{<2\pi}_{\geq 0}$ such that $\cos\theta$ is transcendental,* $\mathrm{EQP}_\theta = \mathrm{P}$. *In particular assuming $\cos(R)$ is transcendental,* $\mathrm{EQP}_R = \mathrm{P}$.

Proof. Let $M \in \mathrm{EQP}_\theta$ with amplitude vector $v = (v_1,\ldots,v_N) \in \mathbf{R}^N$. Then v_i is 0, ± 1, $\pm\cos\theta$, or $\pm\sin\theta$. Suppose $v_i \in \{0,\pm 1\}$ for all i. Since the time evolution

operator of M preserves the L_2-norm, there is at most one transition tuple with amplitude ± 1 for every pair of current state and symbol. Hence M is deterministic.

Suppose on the other hand that v contains some transcendental coordinates. Let L be accepted by M in EQP at time $p(n)$ for some polynomial p. Let $x = (x_1, \ldots, x_N)$. Form the symbolic QTM $M(x)$ and the set of polynomials $J(p, L)$ as before. Then for $u \in \mathbf{R}^N$, $M(u)$ is well formed and accepts L in EQP at time $p(n)$ iff u is a common zero of all polynomials in $J(p, L)$. Let s and t be variables and $u(s, t)$ be the N-vector obtained from x as follows: for all i, replace x_i by v_i if v_i is 0 or ± 1, replace x_i by $\pm s$ if $v_i = \pm \cos\theta$, and replace x_i by $\pm t$ if $v_i = \pm \sin\theta$. Let $J'(p, L) \subset \mathbf{Q}[s, t]$ be obtained from $J(p, L)$ by specializing each polynomial $F(x)$ in $J(p, L)$ to $F(u(s, t))$. Then for all $a, b \in \mathbf{R}$, $M(u(a, b))$ accepts L in EQP at time $p(n)$ iff a, b is a common zero of all polynomials in $J'(p, L)$. In particular we note that $v = u(\cos\theta, \sin\theta)$ and that $(\cos\theta, \sin\theta)$ is a common zero of all polynomials in $J'(p, L)$. Since $(\cos\theta, \sin\theta)$ is generic for the curve $s^2 + t^2 = 1$, it follows that every polynomial in $J'(p, L)$ is in the ideal generated by $s^2 + t^2 - 1$. But since $(1, 0)$ is a zero of $s^2 + t^2 - 1$, it follows that $(1, 0)$ is also a zero of all polynomials in $J'(p, L)$. This implies that $M(u(1, 0))$ accepts L in EQP. As $u(1, 0) \in \{0, \pm 1\}^N$, $M(u(1, 0))$ is deterministic as observed before, and the theorem follows. □

THEOREM 6.4. $\mathrm{BQP}_{poly(1/\epsilon)}, \mathrm{EQP}_{\mathbf{C}}, \mathrm{NQP}_{\bar{\mathbf{Q}} \cap \mathbf{R}} \subseteq \mathrm{PP} \subseteq \mathrm{P}^{\#\mathrm{P}}$.

From Theorems 5.1 and 6.4 we have the following.

COROLLARY 6.5. $\mathrm{BQP}_{\mathbf{C}} \neq \mathrm{EQP}_{\mathbf{C}}$.

We remark that the result $\mathrm{BQP}_{poly(1/\epsilon)} \subseteq \mathrm{P}^{\#\mathrm{P}}$ was first announced by Valiant (see [BV]). The rest of this section is devoted to the proof of Theorem 6.4. We begin by deriving some additional facts about QTMs with real algebraic amplitudes.

Let M be a QTM with real algebraic amplitude; that is, $M \in \mathrm{QTM}_{\bar{\mathbf{Q}} \cap \mathbf{R}}$. Let the local matrix L_δ of M be an $n \times m$ matrix with $\lambda_{i,j}$ as the entry corresponding to the ith row and jth column for $1 \leq i \leq n$ and $1 \leq j \leq m$. Let K be the field generated by all $\lambda_{i,j}$ over $\mathbf{Q}$. Let D be the degree of K over $\mathbf{Q}$. Then $K = \mathbf{Q}[\beta]$ for some $\beta \in \bar{\mathbf{Q}} \cap \mathbf{R}$, and the irreducible polynomial for β over $\mathbf{Q}$ is of degree D. We will call K the *field of amplitudes* for M.

For all $i, j, k \in \mathbf{Z},\ 1 \leq i \leq n,\ 1 \leq j \leq m,\ 0 \leq k \leq D-1$, let $r_{i,j,k} \in \mathbf{Q}$ be the values such that $\lambda_{i,j} = \sum_{k=0}^{D-1} r_{i,j,k}\beta^k$. For all $i, j, k \in \mathbf{Z},\ 0 \leq i \leq D-1,\ 0 \leq j \leq D-1,\ 0 \leq k \leq D-1$, let $s_{i,j,k} \in \mathbf{Q}$ be the values such that $\beta^i\beta^j = \sum_{k=0}^{D-1} s_{i,j,k}\beta^k$. Let $d_1 \in \mathbf{Z}$ be a common denominator of the $r_{i,j,k}$ and $d_2 \in \mathbf{Z}$ be a common denominator of the $s_{i,j,k}$. These values will be used below.

Let $\mathcal{C}$ be the set of all possible configurations of the machine M. Consider running machine M for t steps on input α. We can define a path of length t for input α leading to configuration C as a sequence of t configurations $\langle C_0, C_1, C_2, \ldots, C_t\rangle$ such that C_0 corresponds to the initial configuration for input α, $C_t = C$, and C_{i+1} can be reached from C_i with one step of the machine (including 0 amplitude moves) for $0 \leq i \leq t-1$. Let $P_{\alpha,t,C}$ be the set of paths of length t for input α leading to configuration C. For all paths $p = \langle C_0, C_1, \ldots, C_t\rangle$, there is an associated amplitude $\rho_p = \prod_{k=0}^{t-1} \lambda_{i_{p,k},j_{p,k}}$ where $i_{p,k}$ and $j_{p,k}$ are the row and column in the local matrix that correspond to moving from configuration C_k to configuration C_{k+1}. Let $d_t = d_1^t d_2^{t-1}$, and let $a_{p,i} \in \mathbf{Q}$ be the values such that $\rho_p = \sum_{i=0}^{D-1}(a_{p,i}/d_t)\beta^i$. The following lemma shows that the $a_{p,i}$'s are integers.

LEMMA 6.6. *There exists a $g \in \mathbf{Z}$ such that for all input strings α, for all configurations $C \in \mathcal{C}$, for all $t \in \mathbf{Z}_{>0}$, for all $p \in P_{\alpha,t,C}$, for all $i \in \mathbf{Z}_{\geq 0}^{<D}$, $a_{p,i} \in \mathbf{Z}$, and $abs(a_{p,i}) \leq g^t$.*

Proof of Lemma 6.6.

$$\rho_p = \prod_{k=0}^{t-1} \lambda_{i_{p,k},j_{p,k}} = \prod_{k=0}^{t-1} \sum_{l=0}^{D-1} r_{i_{p,k},j_{p,k},l}\beta^l = \sum_{0\le l_0,\ldots,l_{t-1}\le D-1} \prod_{k=0}^{t-1} r_{i_{p,k},j_{p,k},l_k} \prod_{k=0}^{t-1} \beta^{l_k}.$$

Since d_1 is the common denominator of the $r_{i,j,k}$, d_1^t will be a common denominator of any product of t $r_{i,j,k}$'s. Since d_2 is a common denominator of the $s_{i,j,k}$'s, it is possible to show by induction that d_2^{t-1} is a common denominator of the product of t β^i's. Hence $d_t = d_1^t d_2^{t-1}$ is a common denominator of the sum above and for all paths p and $i \in \mathbf{Z}_0^{D-1}$, $a_{p,i} \in \mathbf{Z}$.

Let

$$m_1 = \max\{abs(r_{i,j,k}) \mid 0 \le i \le n, 0 \le j \le m, 0 \le k \le D-1\}$$

and

$$m_2 = \max\{abs(s_{i,j,k}) \mid 0 \le i,j,k \le D-1\}.$$

Then it can also be shown from the above equation that

$$abs(a_{p,i}) \le d_t D^t m_1^t D^{t-1} m_2^{t-1}.$$

Hence there exists a $g \in \mathbf{Z}$ such that $abs(a_{p,i}) < g^t$. □

We summarize the constants that we have associated with a QTM M with real algebraic amplitudes. Let $K = \mathbf{Q}[\beta] \subseteq \bar{Q} \cap \mathbf{R}$ be the field of amplitudes for M. Let the local matrix of M be an $n \times m$ matrix with $\lambda_{i,j}$ as the (i,j)th entry. Then

$D = D(M)$ be the degree of K over $\mathbf{Q}$;

$d_1 = d_1(M)$ is the least natural number such that $\lambda_{i,j} \in \frac{1}{d_1}\mathbf{Z}[\beta]$ for all i,j with $1 \le i \le n$, $1 \le j \le m$;

$d_2 = d_2(M)$ is the least natural number such that $\beta^i\beta^j \in (1/d_2)\mathbf{Z}[\beta]$ for all i,j with $1 \le i,j \le D$;

$g = g(M)$ is the least natural number determined in Lemma 6.6 such that for all $\alpha \in \mathbf{N}$ and all $t \in \mathbf{Z}_{>0}$ and for all paths p of t steps on input α, the amplitude ρ_p associated with p has the form $\rho_p = \sum_{i=0}^{D-1}(a_{p,i}/d_t)\beta^i$, where $d_t = d_1^t d_2^{t-1}$, $a_{p,i} \in \mathbf{Z}$, and $abs(a_{p,i}) \le g^t$ for all i.

LEMMA 6.7. *For all inputs α, for all $t \in \mathbf{Z}_{>0}$, the following hold.*

1. *If α is accepted in time t with probability* 0, *then*

$$\sum_{i=0}^{D-1} \sum_{C\in\mathcal{C}_\mathcal{A}} \left(\sum_{p\in P_{\alpha,t,C}} a_{p,i} \right)^2 = 0.$$

2. *If α is accepted in time t with probability > 0, then*

$$\sum_{i=0}^{D-1} \sum_{C\in\mathcal{C}_\mathcal{A}} \left(\sum_{p\in P_{\alpha,t,C}} a_{p,i} \right)^2 > 0.$$

Proof of Lemma 6.7. For all configurations, $C \in \mathcal{C}$, for all $t \in \mathbf{Z}_{>0}$, for input strings α, then

$$amp_{\alpha,t,C}(u) = \sum_{p\in P_{\alpha,t,C}} \rho_p = \sum_{p\in P_{\alpha,t,C}} \sum_{i=0}^{D-1} (a_{p_i}/d_t)\beta^i.$$

Switching the sums we get

$$amp_{\alpha,t,C}(u) = \sum_{i=0}^{D-1} \left(\left(\sum_{p \in P_{\alpha,t,C}} a_{p,i} \right) / d_t \right) \beta^i.$$

For all inputs α and $t \in \mathbf{Z}_{>0}$, if input α is accepted in time t with probability 0, then

$$\sum_{C \in \mathcal{C}_A} amp^2_{\alpha,t,C}(u) = 0,$$

and for all $C \in \mathcal{C}_A$, $amp_{\alpha,t,C}(u) = 0$. Hence, for all $i \in \mathbf{Z}_{\geq 0}^{<D}$, $\sum_{p \in P_{\alpha,t,C}} a_{p,i} = 0$, and therefore

$$\sum_{i=0}^{D-1} \sum_{C \in \mathcal{C}_\mathcal{A}} \left(\sum_{p \in P_{\alpha,t,C}} a_{p,i} \right)^2 = 0,$$

which proves case 1.

For all inputs α and $t \in \mathbf{Z}_{>0}$, if input α is accepted in time t with probability > 0, then

$$\sum_{C \in \mathcal{C}_A} amp^2_{\alpha,t,C}(u) > 0,$$

so there exists a $C \in \mathcal{C}_A$ such that $amp_{\alpha,t,C}(u) \neq 0$, which implies that there exists an $i \in \mathbf{Z}_{\geq 0}^{<D}$ such that $\sum_{p \in P_{\alpha,t,C}} a_{p,i} \neq 0$, and, therefore,

$$\sum_{i=0}^{D} \sum_{C \in \mathcal{C}_\mathcal{A}} \left(\sum_{p \in P_{\alpha,t,C}} a_{p.i} \right)^2 > 0,$$

which proves case 2. □

Theorem 6.4 will be proved by the three lemmas given below.

LEMMA 6.8. $\mathrm{NQP}_{\bar{\mathbf{Q}} \cap \mathbf{R}} \subseteq \mathrm{PP} \subseteq \mathrm{P}^{\#\mathrm{P}}$.

Proof of Lemma 6.8. For all $S \subseteq \mathbf{N}$ such that $S \in \mathrm{NQP}_{\bar{\mathbf{Q}} \cap \mathbf{R}}$, we will show that there exists a nondeterministic Turing machine M' that for all $x \in \mathbf{N}$ the following hold:

if $x \in S$, then M' on input x says "yes" on more than 1/2 its paths;

if $x \in \overline{S}$, then M' on input x says "no" on more than 1/2 its paths.

It will follow that $S \in \mathrm{PP}$ and hence $\mathrm{NQP}_{\bar{\mathbf{Q}} \cap \mathbf{R}} \subseteq \mathrm{PP} \subseteq \mathrm{P}^{\#\mathrm{P}}$.

From the definition of $\mathrm{NQP}_{\bar{\mathbf{Q}} \cap \mathbf{R}}$, there exist a $c \in \mathbf{N}_{>0}$ and an M membership $\mathrm{QTM}_{\bar{\mathbf{Q}} \cap \mathbf{R}}$ such that for all $x \in \mathbf{N}$ the following hold:

$x \in S \rightarrow$ after $|x|^c$ steps M on input x accepts with probability > 0;

$x \in \overline{S} \rightarrow$ after $|x|^c$ steps M on input x rejects with probability 0.

Let $K = \mathbf{Q}[\beta] \subseteq \bar{Q} \cap \mathbf{R}$ be the field of amplitudes for M. Let $n = n(M)$, $D = D(M)$, $d_1 = d_1(M)$, $d_2 = d_2(M)$, and $g = g(M)$ be the constants associated with M as defined before.

We observe that for all $x \in \mathbf{N}$, for all $t \in \mathbf{Z}_{>0}$, a path $< C_0, \ldots, C_t >$ of M of length t on input x can be specified by a natural number $P < n^t$ as follows. Write $P = \sum_{i=0}^{t-1} m_i n^i$ with $0 \leq m_i \leq n-1$. Inductively for $i = 0, \ldots, t-1$, from C_i one

chooses the $(m_i + 1)$st entry from the corresponding column in the local matrix for transition to determine the next configuration C_{i+1}. We shall identify P with the path determined by it on input x, and let ρ_P denote the amplitude associated with P. Let $d_t = d_1^t d_2^{t-1}$. Then from Lemma 6.6, $\rho_P = \sum_{i=0}^{D-1} (a_{P,i}/d_t)\beta^i$, where $a_{P,i} \in \mathbf{Z}$, and $abs(a_{P,i}) \leq g^t$ for all i. We will call $a_{P,i}$ the *ith integral coefficient* of ρ_P for $i = 0, \ldots, D-1$.

Let M' on input x proceed as follows.

1. Compute $t = |x|^c$.

2. Guess seven numbers $\langle P_1, G_1, P_2, G_2, E, i, F\rangle$ ("$\langle$" denotes any "reasonable" pairing function) where $P_1, P_2 \in \mathbf{Z}_{\geq 0}^{\leq n^t}$, $G_1, G_2 \in \mathbf{Z}_{\geq 0}^{\leq g^t+1}$, E, F are 0 or 1 and $i \in \mathbf{Z}_{\geq 0}^{<D}$.

3. Use P_1 to choose a path of length t for M on input x. Compute the configuration C_1, which results along this path, and $a_{P_1,i}$, the ith integral coefficient of the amplitude ρ_{P_1} associated with P_1. Similarly, use P_2 to choose a second path of length t for M on input x, and compute C_2 and $a_{P_2,i}$.

4. (trivial guesses)

(i) If $C_1 \neq C_2$, then output "yes" if $E = 0$ and "no" if $E = 1$.

(ii) If $C_1 \in \mathcal{C}_{\mathcal{R}}$, then output "yes" if $E = 0$ and "no" if $E = 1$, except when $P_1 = P_2 = E = i = F = 0$ and $G_1 = G_2 = g^t + 1$.

(iii) If $G_1 \geq abs(a_{P_1,i})$ or $G_2 \geq abs(a_{P_2,i})$, then output "yes" if $E = 1$ and "no" if $E = 0$, except when $P_1 = P_2 = E = i = F = 0$ and $G_1 = G_2 = g^t + 1$.

5. Else (nontrivial guesses)

(i) If $P_1 = P_2 = E = i = F = 0$ and $G_1 = G_2 = g^t + 1$, output "no."

(ii) If $a_{P_1,i}$ and $a_{P_2,i}$ have the same sign, then output "yes."

(iii) If $a_{P_1,i}$ and $a_{P_2,i}$ have opposite signs, then output "no."

Any path with $G_1 = g^t + 1$ or $G_2 = g^t + 1$ is trivial since $G_1 \geq abs(a_{P_1,i})$ or $G_2 \geq abs(a_{P_2,i})$, respectively, except for the special case when $P_1 = P_2 = E = i = F = 0$ and $G_1 = G_2 = g^t + 1$. The number of trivial guesses plus this additional special guess give two more "no" outputs than "yes" outputs.

For all configurations $C \in \mathcal{C}_{\mathcal{A}}$ which can be reached with t steps of M (including transitions that have amplitude of 0), for all $P_1, P_2 \in P_{x,t,C}$, for all $i \in \mathbf{Z}_{\geq 0}^{<D}$, for all $G_1 \in \mathbf{Z}_{\geq 0}^{<abs(a_{P_1,i})}$, for all $G_2 \in \mathbf{Z}_{\geq 0}^{<abs(a_{P_2,i})}$, the guess is nontrivial. In all other cases (except one) the guess will be trivial.

If we count the number of "yes" outputs minus the number of "no" outputs we get

$$\left(4 \sum_{C \in \mathcal{C}_{\mathcal{A}}} \sum_{i=0}^{D-1} \sum_{P_1 \in P_{x,t,C}} \sum_{P_2 \in P_{x,t,C}} a_{P_1,i} a_{P_2,i}\right) - 2,$$

since for a fixed set of paths P_1, P_2 leading to the same configuration, there are $abs(a_{P_1,i} a_{P_2,i})$ sets of pairs G_1, G_2 for each value of E and F.

The above equation can be rewritten as

$$\left(4 \sum_{C \in \mathcal{C}_{\mathcal{A}}} \sum_{i=0}^{D-1} \left(\sum_{p \in P_{x,t,C}} a_{p,i}\right)^2\right) - 2.$$

If $x \in S$ then x is accepted with positive probability, so from part 2 of Lemma 6.7 the sum is greater than 0, and there are more "yes" outputs than "no" outputs.

If $x \in \overline{S}$ then x is accepted with probability 0, so from part 1 of Lemma 6.7 this sum is -2 and there are more "no" outputs than "yes" outputs. □

LEMMA 6.9. $\mathrm{EQP}_{\mathbf{C}} \subseteq \mathrm{PP} \subseteq \mathrm{P}^{\#\mathrm{P}}$.

Proof of Lemma 6.9. By Theorem 6.2, $\mathrm{EQP}_{\mathbf{C}} = \mathrm{EQP}_{\bar{\mathbf{Q}} \cap \mathbf{R}}$. Since $\mathrm{EQP}_K \subseteq \mathrm{NQP}_K$ for any field K, it follows from Lemma 6.8 that

$$\mathrm{EQP}_{\mathbf{C}} = \mathrm{EQP}_{\bar{\mathbf{Q}} \cap \mathbf{R}} \subseteq \mathrm{NQP}_{\bar{\mathbf{Q}} \cap \mathbf{R}} \subseteq \mathrm{PP} \subseteq \mathrm{P}^{\#\mathrm{P}}. \qquad \square$$

LEMMA 6.10. $\mathrm{BQP}_{poly(1/\epsilon)} \subseteq \mathrm{PP} \subseteq \mathrm{P}^{\#\mathrm{P}}$.

Proof of Lemma 6.10. From section 3, $\mathrm{BQP}_{poly(1/\epsilon)} = \mathrm{BQP}_\theta$, where $\cos(\theta) = 3/5$.

For all $S \subseteq \mathbf{N}$ such that $S \in \mathrm{BQP}_\theta$, we will show that there exists a nondeterministic Turing machine M' that for all $x \in \mathbf{N}$ the following hold:

if $x \in S$, then M' on input x says "yes" on more than $1/2$ its paths;

if $x \in \overline{S}$, then M' on input x says "no" on more than $1/2$ its paths.

It will follow that $S \in \mathrm{PP}$ and hence $\mathrm{BQP}_{poly(1/\epsilon)} = BQP_\theta \subseteq \mathrm{PP} \subseteq \mathrm{P}^{\#\mathrm{P}}$.

From the definition of BQP_θ, there exists a $c \in \mathbf{N}_{>0}$ and M a QTM_θ such that for all $x \in \mathbf{N}$ the following hold:

$x \in S \rightarrow$ after $|x|^c$ steps M on input x accepts with probability $> 2/3$,

$x \in \overline{S} \rightarrow$ after $|x|^c$ steps M on input x rejects with probability $> 2/3$.

Let $n = n(M)$, $D = D(M)$, $d_1 = d_1(M)$, $d_2 = d_2(M)$, and $g = g(M)$ be the constants associated with M as defined before.

Let M' on input x proceed as follows.

1. Compute $t = |x|^c$.

2. Guess five numbers $\langle P_1, G_1, P_2, G_2, E \rangle$ ("$\langle$" denotes any "reasonable" pairing function) where $P_1, P_2 \in \mathbf{Z}_{\geq 0}^{\leq n^t}$, $G_1, G_2 \in \mathbf{Z}_{\geq 0}^{\leq g^t}$, and E is 0 or 1.

3. Use P_1 to choose a path of length t for M on input x. Compute the configuration C_1, which results along this path, and $a_{P_1,i}$, the ith integral coefficient of the amplitude ρ_{P_1} associated with P_1. Similarly, use P_2 to choose a second path of length t for M on input x, and compute C_2 and $a_{P_2,i}$.

4. (trivial guesses)

(i) If $C_1 \neq C_2$, then output "yes" if $E = 0$ and "no" if $E = 1$.

(ii) If $G_1 \geq abs(a_{P_1,0})$ or $G_2 \geq abs(a_{P_2,0})$, then output "yes" if $E = 0$ and "no" if $E = 1$.

5. Else (nontrivial guesses)

(i) If $a_{P_1,0}$ and $a_{P_2,0}$ have the same sign, then output "yes" if C_1 is an accept configuration and "no" if C_1 is a reject configuration.

(ii) If $a_{P_1,0}$ and $a_{P_2,0}$ have opposite signs, then output "yes" if C_1 is a reject configuration and "no" if C_1 is an accept configuration.

Since the entries in the local matrix are rational, the degree of $K = \mathbf{Q}$ equals 1, and so

$$amp_{\alpha,t,C}(u) = \sum_{p \in P_{\alpha,t,C}} a_{p,0}/d_t.$$

Again all the trivial paths have equal "yes" and "no" results.

For all configurations $C \in \mathcal{C}$ which can be reached with t steps of M (including transitions that have amplitude of 0), for all $P_1, P_2 \in P_{x,t,C}$, for all $G_1 \in \mathbf{Z}_{\geq 0}^{<abs(a_{P_1,0})}$, for all $G_2 \in \mathbf{Z}_{\geq 0}^{<abs(a_{P_2,0})}$, the guess is nontrivial. In all other cases the guess will be trivial.

If we count the number of "yes" outputs minus the number of "no" outputs we get

$$2\left(\sum_{C\in\mathcal{C}_{\mathcal{A}}}\sum_{P_1\in P_{x,t,C}}\sum_{P_2\in P_{x,t,C}}a_{P_1,0}a_{P_2,0}-\sum_{C\in\mathcal{C}_{\mathcal{R}}}\sum_{P_1\in P_{x,t,C}}\sum_{P_2\in P_{x,t,C}}a_{P_1,0}a_{P_2,0}\right),$$

since for a fixed set of paths P_1, P_2 leading to the same configuration, there are $abs(a_{P_1,0}a_{P_2,0})$ sets of pairs G_1, G_2 for each value of E.

The above equation can be rewritten as

$$2\left(\sum_{C\in\mathcal{C}_{\mathcal{A}}}\left(\sum_{p\in P_{x,t,C}}a_{p,i}\right)^2-\sum_{C\in\mathcal{C}_{\mathcal{R}}}\left(\sum_{p\in P_{x,t,C}}a_{p,i}\right)^2\right)$$

$$=2d_t^2\left(\sum_{C\in\mathcal{C}_{\mathcal{A}}}\left(amp^2_{\alpha,t,C}(u)\right)-\sum_{C\in\mathcal{C}_{\mathcal{R}}}\left(amp^2_{\alpha,t,C}(u)\right)\right).$$

If $x \in S$, then x is accepted with probability greater than $2/3$ and rejected with probability less than $1/3$ and so the above sum is greater than 0, giving more paths in M' with a "yes" result than a "no" result.

If $x \in \overline{S}$, then x is rejected with probability greater than $2/3$ and accepted with probability less than $1/3$ and so the above sum is less than 0, giving more paths in M' with a "no" result than a "yes" result.

This concludes the proof of Lemma 6.10 and therefore Theorem 6.4. □

7. Discussion. If one is concerned about minimizing (or precisely calculating) the polynomial slowdown in the approximations implicit in Theorem 3.3, then more recent results of Baker and others on transcendental numbers may be useful. Angles θ with $\theta/2\pi \in \bar{\mathbf{Q}} - \mathbf{Q}$ may be particularly good in this regard.

There are many unsettled issues and open questions involving quantum computation. For example, letting K be a field, is $\mathrm{BQP}_K = \mathrm{EQP}_K$? We have shown that $\mathrm{BQP}_{\mathbf{C}} \neq \mathrm{EQP}_{\mathbf{C}}$. It seems unlikely that $\mathrm{BQP}_{\mathbf{Q}} = \mathrm{EQP}_{\mathbf{Q}}$.

One can ask whether $\mathrm{NQP}_K = \mathrm{EQP}_K$, an analogue of the $NP = P$ question.

One can consider the relationship between classical classes and quantum classes. For example does EQP=P? We suspect not, but since EQP$\subseteq$ PSPACE, a yes answer would not be entirely out of the question. Does $\mathrm{BQP}_{\mathbf{Q}}$=BPP?

One can generalize the notion of a "classical" probabilistic Turing machine to allow for amplitudes in $\mathbf{C}$ and consider the relationship between natural classes on a classical probabilistic Turing machine and on a quantum machine. For example, is it the case that $\mathrm{BQP}_{\mathbf{C}} = \mathrm{BPP}_{\mathbf{C}}$ (when BPP_K is appropriately defined)? Does $\mathrm{BQP}_{\mathbf{Q}} = \mathrm{BPP}_{\mathbf{Q}}$? An affirmative answer would inform us that the power of quantum computation is not found in the use of the L_2-norm but rather in the use of general (possibly negative) amplitudes.

One can ask similar questions for QTM_θ rather than QTM_K. For example, let θ and θ' have cos = 3/5 and 5/12, respectively. Then $\mathrm{QTM}_\theta \asymp \mathrm{QTM}_{\theta'}$ and hence $\mathrm{BQP}_\theta = \mathrm{BQP}_{\theta'}$; however, does $\mathrm{EQP}_\theta = \mathrm{EQP}_{\theta'}$? If $\theta/2\pi \notin \mathbf{Q}$, does EQP_θ =P?

To what extent would demonstrating relationships between various complexity classes over various fields (or with various angles) have implications similar to those which arise when relationships between classical classes are demonstrated with respect to an oracle?

One could consider very general notions of machines (amplitudes in $\mathbf{C}$, arbitrary norms, for example). Would an investigation of these shed light on the basic open problems of computational complexity?

On a more concrete level, is the "shortest vector in a lattice" problem in $\mathrm{BQP}_{\mathbf{Q}}$ (this has been asked by numerous researchers)? Is primality in $\mathrm{EQP}_{\mathbf{C}}$? Is primality in $\mathrm{EQP}_{\mathbf{Q}}$? Can integers be multiplied in linear time on a QTM?

Acknowledgments. We thank Harold Stark for providing us with Lemma 3.6, Charles Bennett for contributing to our understanding of methods of approximating θ used in the proof of Theorem 3.3, and Don Coppersmith for enlightening comments regarding a previous version of this paper. Finally, we thank the anonymous referees for bringing Proposition 6.1 to our attention, for pointing out a mistake in an earlier version, and for many valuable comments.

REFERENCES

[B] A. Baker, *Transcendental Number Theory*, Cambridge University Press, London, 1979.

[Be] C. H. Bennett, *Logical reversibility of computation*, IBM J. Res. Develop., 17 (1973), pp. 525–532.

[BBBV] C. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, *Strengths and weaknesses of quantum computing*, SIAM J. Comput., 26(1997), pp. 1510–1523.

[BV] E. Bernstein and U. Vazirani, *Quantum complexity theory*, in Proc. 25th ACM Symposium on Theory of Computation, San Diego, CA, 1993, pp. 11–20; SIAM J. Comput., 26 (1997), pp. 1411–1473.

[D1] D. Deutsch, *Quantum theory, the Church–Turing principle and the universal quantum computer*, Proc. Roy. Soc. London Ser. A, 400 (1985), pp. 96–117.

[D2] D. Deutsch, *Quantum computational networks*, Proc. Roy. Soc. London Ser. A., 425 (1989), pp. 73–90.

[DJ] D. Deutsch and R. Jouzsa, *Rapid solution of problems by quantum computation*, Proc. Roy. Soc. London Ser. A, 439 (1992), pp. 553–558.

[F] R. Feynman, *Simulating physics with computers*, Internat. J. Theoret. Phys., 21 (1982), pp. 467–488.

[Fe] N. I. Feldman, *An improvement of the estimate of a linear form in the logarithms of algebraic numbers*, Mat. Sb. (N.S.), 77 (119) (1968), pp. 423–436 (in Russian).

[J] N. Jacobson, *Basic Algebra* I, W. H. Freeman, San Francisco, 1980.

[Ni] I. Niven, *Irrational Numbers*, The Mathematics Association of America, Rahway, NJ, 1956.

[Sh] P. Shor, *Algorithms for quantum computation: Discrete log and factoring*, in Proc. 35th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, 1994, pp. 124–134.

[Si] D. Simon, *On the power of quantum computation*, SIAM J. Comput., 26 (1997), pp. 1474–1483.

[So] R. Solovay, *Virtual Reading Group Communication*, Internet, 14 August 1994.

[Y] A. Yao, *Quantum circuit complexity*, in Proc. 34th IEEE Symposium on Foundations of Computer Science, Palo Alto, CA, IEEE Computer Society Press, Los Alamitos, CA, 1993, pp. 352–361.