Quantum simulations of classical random walks and undirected graph connectivity

John Watrous[*]
Département d'informatique et de recherche opérationnelle
Université de Montréal
Montréal (Québec), Canada
watrous@iro.umontreal.ca

Abstract

There are a number of questions in quantum complexity that have been resolved in the time-bounded setting, but remain open in the space-bounded setting. For example, it is not currently known if space-bounded probabilistic computations can be simulated by space-bounded quantum machines without allowing measurements during the computation, while it is known that an analogous statement holds in the time-bounded case. A more general question asks if measurements during a quantum computation can allow for more space-efficient solutions to certain problems.

In this paper we show that space-bounded quantum Turing machines can efficiently simulate a limited class of random processes—random walks on undirected graphs—without relying on measurements during the computation. By means of such simulations, it is demonstrated that the undirected graph connectivity problem for regular graphs can be solved by one-sided error quantum Turing machines that run in logspace and require a single measurement at the end of their computations. It follows that symmetric logspace is contained in the quantum analogue of randomized logspace, i.e., $SL \subseteq QR_HL$.

1 Introduction

This paper addresses the problem of space-efficient quantum simulations of probabilistic computations. We take as our model of computation the quantum Turing machine, where we assume measurements may not occur during the computation, and that a single measurement (yielding one of the results: *accept* or *reject*) takes place at the end of the computation. One reason for studying such computations is that they may safely be used as subroutines in larger quantum computations, while computations allowing unrestricted intermediate measurements might spoil a larger quantum computation if used in this way. Another reason is purely academic: the resulting quantum classes are interesting from a complexity-theoretic point of view in their (possible) weaknesses. Since quantum computations are reversible except for measurements, it is also interesting to consider the power of quantum computations without intermediate measurements from the perspective of the thermodynamics of computation, in view of Landauer's Principle [8].

While it has been shown that restricting measurements as described above does not affect computational power with respect to time-bounded computation [1], it is not known if this restriction affects computational power in the space-bounded case. Indeed, while it can be shown that a quantum machine running in logspace that allows local measurements at any point in its computation can simulate a given logspace probabilistic machine, it is not known if this can be done in the case where measurements are not allowed during the computation. The apparent difficulty in simulating probabilistic computations with space-bounded quantum machines in this restricted setting by means of the most straightforward technique (i.e., directly simulating coin-flips with appropriately defined quantum transformations) lies in the problem of reusing the space required for each coin-flip, of which there may be a number exponential in the space-bound.

In a previous paper [14], we have investigated a number of space-bounded quantum complexity classes defined in terms of machines that allow a restricted class of measurements during their computations: after each step the internal state of the quantum Turing machine is observed, yielding one of the results

[*] Partially supported by Canada's NSERC. Part of this work was performed while the author was at the University of Wisconsin–Madison Computer Sciences Department under the support of NSF grant CCR-95-10244.

accept, *reject*, or *continue*. (Alternately this may be formulated by allowing for an output tape that is observed after each step.) The computation continues until one of the results *accept* or *reject* is obtained. As in the classical case, we may define a notion of *halting absolutely* for such computations; a computation halts absolutely if it has finite worst-case running time. It was proved that any logspace quantum Turing machine allowing for these limited intermediate measurements that halts absolutely can be simulated by one in which no intermediate measurements occur. Under the assumption that the running time in the single-measurement case is a logspace time-bound (i.e., the running time of some deterministic logspace Turing machine), the converse holds as well. Thus, the notion of a logspace quantum computation not allowing measurements during the computation and the notion of a logspace quantum computation that halts absolutely (with respect to measurements of the accept/reject/continue type during the computation) are equivalent.

In the present paper we prove that quantum Turing machines can simulate a limited class of random processes—random walks on regular, undirected graphs—in a time-efficient and space-efficient manner in the single-measurement (equivalently, halting absolutely) case. A random walk on a regular, undirected graph $G = (V, E)$ of degree d is a Markov chain defined as follows: the states of the Markov chain correspond to the vertices of G, and the transition probability from vertex u to vertex v is defined to be $1/d$ in case v is adjacent to u, and zero otherwise.

The study of random walks has had a number of interesting applications in complexity theory. From the perspective of this paper, the most important such application is due to Aleliunas, Karp, Lipton, Lovász and Rackoff [2], who used random walks to show that the undirected graph connectivity (USTCON) problem is in $\mathrm{R}_H\mathrm{L}$ (sometimes denoted RL^{poly} or just RL). Since USTCON is complete for symmetric logspace (SL) with respect to logspace reductions [10], the relation $\mathrm{SL} \subseteq \mathrm{R}_H\mathrm{L}$ follows. The most space-efficient known deterministic algorithm for USTCON requires space $O((\log n)^{4/3})$ [3]. We define d-regular undirected graph connectivity (d-USTCON) to be the variant of this problem in which the graph in question is regular of a fixed degree d:

<u>d-USTCON</u>

Instance: A regular, undirected graph $G = (V, E)$ of degree d and $s, t \in V$.

Question: Are s and t connected in G?

For $d \geq 3$, d-USTCON is SL-complete, as a straightforward reduction shows USTCON $\leq_m^{\log}$ d-USTCON.

By considering suitable quantum variants of random walks on graphs we prove d-USTCON $\in \mathrm{QR}_H\mathrm{L}$, which is the quantum analogue of $\mathrm{R}_H\mathrm{L}$ where intermediate measurements are not allowed. This is done in two steps. First we show d-USTCON can be solved with one-sided error logspace quantum Turing machines having considerably worse acceptance probability than 1/2 for positive instances. We then demonstrate that $\mathrm{QR}_H\mathrm{L}$ is robust with respect to acceptance probabilities, yielding d-USTCON $\in \mathrm{QR}_H\mathrm{L}$. This implies the following containment.

Theorem 1 $\mathrm{SL} \subseteq \mathrm{QR}_H\mathrm{L}$.

Symmetric logspace is closed under complementation [12], which, together with Theorem 1, implies $\mathrm{SL} \subseteq \mathrm{QR}_H\mathrm{L} \cap \text{co-}\mathrm{QR}_H\mathrm{L} =: \mathrm{ZQ}_H\mathrm{L}$.

From our technique to simulate classical random walks with logspace quantum Turing machines, we obtain the following somewhat stronger result: given an undirected, regular graph G and a vertex u, in polynomial time and logarithmic space we may approximate a uniform superposition over all vertices in the connected component of u in G with high probability and with a high degree of accuracy. This fact may be of use for developing efficient space-bounded quantum algorithms for other graph problems.

The remainder of this paper has the following organization. In Section 2 we review relevant facts concerning space-bounded quantum computation. In Section 3, we define a number of quantum operators and prove a lemma regarding these operators that will be useful in Section 4, which contains the construction of quantum Turing machines for simulating classical random walks on d-regular graphs. In Section 5, we address the issue of robustness of $\mathrm{QR}_H\mathrm{L}$ that, along with the machine constructed in Section 4, allows us to prove Theorem 1. Section 6 contains some concluding remarks.

2 Space-bounded QTMs

We begin by briefly discussing some relevant facts concerning space-bounded quantum computation; for further information see [14]. For background on quantum computation more generally, we refer the reader to [4] and [5], and for classical space-bounded computation see [13].

The model of computation we use is the quantum Turing machine (QTM). Our QTMs have two tapes: a read-only input tape and a work tape. The input and work tape alphabets are denoted Σ and Γ, respectively.

The internal states of a QTM are partitioned into two sets: accepting states and rejecting states.

As usual, the behavior of a QTM is determined by a transition function. There are strict conditions the transition function of a QTM must satisfy, as the evolution of a QTM must correspond to a unitary operator on the Hilbert space spanned by classical configurations of the machine (see [4, 14] for further discussion).

In order to define the language accepted by a particular QTM M, we associate with M a function T specifying the number of steps for which M is to be run on each input. The probability that a pair (M, T) accepts a given string x is the probability that an accepting state results if the internal state of M on input x is measured, given that the machine has run for precisely $T(x)$ steps. A QTM M runs in logspace with respect to a given T if there exists a function $f(n) = O(\log n)$ such that, for every input x, the position of the work tape head of M is never outside the range $[-f(|x|), f(|x|)]$ with nonzero amplitude during the first $T(x)$ steps of the computation of M on x.

The class $\mathrm{QR}_H\mathrm{L}$ consists of all languages A for which there exists a QTM M and a function T such that the following hold:

1. There exists a DTM M_T such that on each input x, M_T runs for precisely $T(x)$ steps (T is a logspace time-bound, for short).
2. M runs in logspace with respect to T.
3. If $x \in A$, then (M, T) accepts x with probability at least $1/2$.
4. If $x \notin A$, then (M, T) accepts x with probability 0.

As mentioned above, this definition is equivalent to the definition given in [14], stated in terms of QTMs allowing observations of the accept/reject/continue type on each step. Note also that the class $\mathrm{QR}_H\mathrm{L}$ does not change if we restrict T to depend only on the length of x. In Section 5 we show that the value $1/2$ in the above definition for $\mathrm{QR}_H\mathrm{L}$ may be replaced by any function $f(|x|)$ satisfying $1/g(|x|) \leq f(|x|) \leq 1 - 2^{-g(|x|)}$ for some polynomial $g(|x|) > 0$.

Substituting PTM for QTM in this definition yields the class $\mathrm{R}_H\mathrm{L}$. It is not currently known if $\mathrm{QR}_H\mathrm{L}$ and $\mathrm{R}_H\mathrm{L}$ are different, nor if one is contained in the other.

We will describe quantum Turing machines using pseudo-code in a manner typical for classical Turing machine descriptions. Computations will be composed of transformations of two types: *quantum transformations* and *reversible transformations*, both necessarily inducing unitary operators on the associated Hilbert space. Quantum transformations will consist of a single step, so it will be trivial to argue that each quantum transformation can be performed as claimed. For reversible transformations, we rely on the result of Lange, McKenzie, and Tapp [9], which implies that any logspace deterministic computation can be simulated reversibly in logspace. However, because the interference patterns produced by a given QTM depend greatly upon the precise lengths of the various computation paths comprising that machine's computation, we must take care to insure that these lengths are predictable in order to correctly analyze machines. In the remainder of this section, we discuss reversible transformations somewhat more formally, and state a theorem based on the main result of [9] that will simplify our analyses greatly.

For a given space-bound f and work tape alphabet Γ, define $W_{f(|x|)}(\Gamma)$ to be the set of all mappings of the form $w : \mathbb{Z} \to \Gamma$ taking the value # (blank) outside the interval $[-f(|x|), f(|x|)]$ (i.e., those mappings representing the possible contents of the work tape of a machine on input x having work tape alphabet Γ and running in space f). By a *reversible transformation*, we mean a one-to-one and onto mapping of the form $\Phi : W_{f(|x|)}(\Gamma) \to W_{f(|x|)}(\Gamma)$ for some f, x and Γ.

Let M be a deterministic Turing machine having internal state set Q, which includes an initial state q_0 and a final state q_f, and work tape alphabet $\Gamma' \supseteq \Gamma$. For $w \in W_{f(|x|)}(\Gamma)$, define $c(q, w)$ to be that configuration of M for which the work tape contents are described by w, the input and work tape heads are scanning the squares indexed by 0, and the internal state is q. We say that M on input x performs transformation Φ on $W_{f(|x|)}(\Gamma)$ if the following holds: if M on input x is placed in configuration $c(q_0, w)$ for any $w \in W_{f(|x|)}(\Gamma)$, then there exists $t = t(x, w)$ such that if M is run for precisely t steps, it will then be in configuration $c(q_f, \Phi(w))$. Furthermore, at no time prior to step number t is the internal state of M equal to q_f. Naturally, we say that t is the number of steps required for M on x to perform Φ. If the work tape head of M never leaves the region indexed by numbers in the range $[-g(|x|), g(|x|)]$ during this process, we say that M on x performs transformation Φ in space g.

Theorem 2 *Let $f(n) = O(\log n)$ and let M be a deterministic Turing machine that, on each input x, performs reversible transformation Φ_x on $W_{f(|x|)}(\Gamma)$ in space $O(\log |x|)$. Then there exists a reversible Turing machine M' that, on each input x, performs Φ_x on $W_{f(|x|)}(\Gamma)$ in space $O(\log |x|)$. Furthermore, the number of steps required for M' to perform Φ_x depends only on x and not on the particular argument of Φ_x.*

The proof of this theorem is based on the main result of [9], with added consideration payed to the number of steps required for transformations. See [14], along with [9] for details.

3 Quantum operators

In this section we define some operators and prove a lemma that will be used in the analysis of the machines presented in the next section.

Throughout this subsection, assume $G = (V, E)$ is an undirected, regular graph of degree d that is not necessarily connected. The Hilbert space upon which the operators we define act is $\mathcal{H} = \ell_2(V \times V)$, i.e., the classical states of our space consists of all ordered pairs of vertices of G. Let $n = |V|$, $m = |E|$, and for each $u \in V$ define $S(u) = \{v \in V : \{u, v\} \in E\}$ and $B(u) = S(u) \cup \{u\}$. Each operator we consider is linear: we define the action of operators on the basis $\{|u, v\rangle : u, v \in V\}$ and extend to $\mathcal{H}$ by linearity.

First, define F as follows:

$$F\,|u,v\rangle = \begin{cases} |u,v\rangle - \dfrac{2}{d+1} \displaystyle\sum_{v' \in B(u)} |u,v'\rangle & v \in B(u) \\ |u,v\rangle & v \notin B(u). \end{cases}$$

We now verify that F is both unitary and hermitian. Define

$$|\psi_u\rangle = \frac{1}{\sqrt{d+1}} \sum_{v \in B_u} |u,v\rangle$$

for each $u \in V$, and note that $\{|\psi_u\rangle : u \in V\}$ is an orthonormal set. We may rewrite F as follows:

$$F \;=\; I - 2 \sum_{u \in V} |\psi_u\rangle \langle\psi_u|\,.$$

Consequently, each vector $|\psi_u\rangle$ is an eigenvector of F with eigenvalue -1, and every vector orthogonal to $\{|\psi_u\rangle : u \in V\}$ is an eigenvector of F with eigenvalue 1. From this it follows that F is both unitary and hermitian: $F = F^\dagger = F^{-1}$. The operator F is related to the operator D defined on $\ell_2(\{0, \ldots, d\})$ as follows:

$$D\,|a\rangle = |a\rangle - \frac{2}{d+1} \sum_{b=0}^{d} |b\rangle\,.$$

Up to a sign change, this is the "diffusion" operator used in the Grover searching technique [7].

Next, define X as follows.

$$X = \sum_{u,v \in V} |v,u\rangle \langle u,v|\,.$$

The operator X simply exchanges the vertices u and v. Clearly $X = X^\dagger = X^{-1}$; X is unitary and hermitian.

Finally, define P as follows.

$$P = \sum_{u \in V} |u,u\rangle \langle u,u|\,.$$

The operator P is the projection onto the subspace of $\mathcal{H}$ spanned by self-loops.

Lemma 3 *Let $G = (V, E)$ be a regular graph of degree $d \geq 2$, let F, X and P be as defined above, define $Q = P\,F\,X\,F\,P$, and let $k \geq \frac{d(d+1)^2 n^2 \log(1/\epsilon)}{8}$ for given $\epsilon > 0$. For each $u \in V$, let $G_u = (V_u, E_u)$ denote the connected component of G containing u, and write $n_u = |V_u|$. Then for every $u \in V$ we have*

$$\left\| Q^k\,|u,u\rangle - \frac{1}{n_u} \sum_{v \in V_u} |v,v\rangle \right\| < \epsilon.$$

Proof. First, note that

$$\begin{aligned} &Q\,|u,u\rangle \\ &= \left(1 - \frac{2}{d+1}\right)^2 |u,u\rangle + \left(\frac{2}{d+1}\right)^2 \sum_{v \in S(u)} |v,v\rangle \qquad (1) \end{aligned}$$

for each $u \in V$, and that $Q\,|u,v\rangle = 0$ for $u \neq v$.

For given $u \in V$ we have that $v \notin V_u$ implies $\langle v,v \,|\, Q^l \,|\, u,u\rangle = 0$ for $l = 1$, and a simple induction shows that this holds for any $l \geq 1$. For each u, define P_u to be a projection operator as follows:

$$P_u = \sum_{v \in V_u} |v,v\rangle \langle v,v|\,.$$

Defining $Q_u = P_u Q P_u$, we therefore have $Q_u^l\,|u,u\rangle = Q^l\,|u,u\rangle$ for $l \geq 0$. Note that Q_u is hermitian: $Q_u^\dagger = (P_u PFXFPP_u)^\dagger = P_u PFXFPP_u = Q$, following from the fact that P_u, P, F, and X are hermitian.

Let A denote the adjacency matrix of G_u and let f_A denote the characteristic polynomial of A. By (1), we determine that f_{Q_u}, the characteristic polynomial of Q_u, satisfies

$$\begin{aligned} f_{Q_u}(z) \;=\; & z^{(n^2 - n_u)} \left(\frac{2}{d+1}\right)^{2n_u} \\ & \times f_A\left(\frac{(d+1)^2 z - (d-1)^2}{4}\right). \end{aligned}$$

Letting $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{n_u}$ be the eigenvalues of A, we see that Q_u has eigenvalues

$$\mu_j = \frac{4\lambda_j + (d-1)^2}{(d+1)^2},$$

for $j = 1, \ldots, n_u$, as well as eigenvalues $\mu_j = 0$ for $j = n_u + 1, \ldots, n^2$. Note that the eigenvalues of A (and hence the eigenvalues of Q_u) are real since A is symmetric. Since G_u is connected and regular of degree d, we have $\lambda_1 = d$, $\lambda_j < d$ for $j = 2, \ldots, n_u$, and $\lambda_{n_u} \geq -d$ (see, e.g., [6], page 14). Furthermore, it follows from [11] that

$$\lambda_j \;\leq\; d - \frac{2}{dn_u^2},$$

for $j = 2, \ldots, n_u$. Hence $\mu_1 = 1$, and

$$\mu_j \in \left[1 - \frac{8d}{(d+1)^2},\; 1 - \frac{8}{d(d+1)^2 n_u^2}\right]$$

for $j = 2, \ldots, n_u$. In particular, we have that $\mu_2, \ldots, \mu_{n_u}$ are bounded in absolute value by

$$1 - \frac{8}{d(d+1)^2 n_u^2}.$$

Next, define

$$|\phi_1\rangle = \frac{1}{\sqrt{n_u}} \sum_{u \in V_u} |u, u\rangle\,,$$

and note that $|\phi_1\rangle$ is an eigenvector of Q_u corresponding to the eigenvalue $\mu_1 = 1$. As Q_u is hermitian, we may choose eigenvectors $|\phi_2\rangle, \ldots, |\phi_{n^2}\rangle$ corresponding to eigenvalues $\mu_2, \ldots, \mu_{n^2}$ in such a way that $\{|\phi_1\rangle, \ldots, |\phi_{n^2}\rangle\}$ is an orthonormal basis of $\mathcal{H}$. Letting $c_j = \langle \phi_j \,|\, u, u\rangle$ for $j = 1, \ldots, n^2$, we may write $|u, u\rangle = \sum_{j=1}^{n^2} c_j |\phi_j\rangle$, and thus

$$Q_u^l |u, u\rangle \;=\; \sum_{j=1}^{n_u} c_j \mu_j^l |\phi_j\rangle$$

for $l \geq 1$. Consequently,

$$\begin{aligned} &\left\| Q_u^l |u, u\rangle - \frac{1}{n_u} \sum_{v \in V_u} |v, v\rangle \right\|^2 \\ &\quad = \left\| \sum_{j=2}^{n_u} c_j \mu_j^l |\phi_j\rangle \right\|^2 = \sum_{j=2}^{n_u} |c_j|^2 |\mu_j|^{2l} \\ &\quad \leq \left(1 - \frac{8}{d(d+1)^2 n_u^2}\right)^{2l}. \qquad (2) \end{aligned}$$

Since $k \geq \frac{d(d+1)^2 n^2 \log(1/\epsilon)}{8}$, for every u we have

$$\left(1 - \frac{8}{d(d+1)^2 n_u^2}\right)^k \leq \left(1 - \frac{8}{d(d+1)^2 n^2}\right)^k < \epsilon,$$

following from the fact that $(1 - 1/x)^x < 1/e$ for $x \geq 1$. Thus

$$\left\| Q_u^k |u, u\rangle - \frac{1}{n_u} \sum_{v \in V_u} |v, v\rangle \right\| < \epsilon$$

follows by (2). As $Q^k |u, u\rangle = Q_u^k |u, u\rangle$, this completes the proof. ■

By taking $\epsilon = \frac{1}{2n}$ in Lemma 3, we obtain the following corollary.

Corollary 4 *Let $G = (V, E)$ be a regular graph of degree $d \geq 2$ with $s, t \in V$, let Q be as defined in Lemma 3, and let $k \geq \lceil d(d+1)^2 n^2 \log(2n)/8 \rceil$. If s and t are connected in G, then*

$$\left|\langle t, t \,|\, Q^k \,|s, s\rangle\right|^2 \;\geq\; \frac{1}{4n^2},$$

and otherwise $\left|\langle t, t \,|\, Q^k \,|s, s\rangle\right|^2 = 0$.

4 QTM construction and analysis

We now construct, for each fixed degree $d \geq 2$, a logspace QTM solving d-USTCON that operates with one-sided error. Although the QTMs we construct have somewhat poor probabilities of acceptance for positive instances of d-USTCON, it will be demonstrated in the next section that these machines may be modified to yield logspace QTMs for d-USTCON having sufficiently small one-sided error to prove d-USTCON $\in$ QR$_H$L.

Lemma 5 *For $d \geq 2$, there exists a quantum Turing machine M and a logspace time-bound T such that M runs in logspace with respect to T and operates as follows. For any input (G, s, t), where $G = (V, E)$ is a regular, undirected graph of degree d, $s, t \in V$, and s is connected to t in G, (M, T) accepts with probability at least $\frac{1}{4|V|^2}$, and for all other inputs (M, T) accepts with probability zero.*

Proof. The work tape of M will consist of four tracks, one for each of the following variables: u, v, b and c. Each variable will contain an integer, with the exception of v, which will store either an integer or a single symbol in the set $\{0, \ldots, d\}$. Integers are assumed to be encoded as strings over the alphabet $\{0', 1'\}$, taken to be disjoint from $\{0, \ldots, d\}$. We make the assumption that each integer has exactly one encoding and that 0 is encoded by the empty string. Note that this implies u, v, b and c are all initially set to 0, as the work tape initially contains only blanks. Vertices of G are assumed to be labeled by integers having length at most logarithmic in the input size, and each vertex has a unique label. When u or v contains an integer, this integer is to be interpreted as the label of a vertex.

```
1. Reject if the input does not encode $(G, s, t)$ for $G$
   undirected and regular of degree $d$.
2. Copy $s$ to $u$ and $v$.
3. Loop with starting/stopping condition "b=0":
   i.    If $v \in B(u)$, replace $v$ with the symbol in
         $\{0, \ldots, d\}$ corresponding to its index in $B(u)$
         modulo $d + 1$.
   ii.   If $v \in \{0, \ldots, d\}$, perform transformation $D$
         (defined in Section 3) on $v$.
   iii   Invert step i.
   iv.   Exchange $u$ and $v$.
   v.    If $v \in B(u)$, replace $v$ with the symbol in
         $\{0, \ldots, d\}$ corresponding to its index in $B(u)$
         modulo $d + 1$.
   vi.   If $v \in \{0, \ldots, d\}$, perform transformation $D$
         on $v$.
   vii.  Invert step v.
   viii. If $u \neq v$, increment $c$ modulo $d(d+1)^2 n^3 + 1$.
   ix.   Increment $b$ modulo $d(d + 1)^2 n^3$.
4. If $c = 0$ and $u = t$, then accept, else reject.
```

Figure 1: Description of quantum Turing machine M for Lemma 5.

The execution of M is described in Figure 1. For each of the steps in Figure 1 we may define an appropriate reversible or quantum transformation corresponding to the action described. Each transformation is to maintain the invariant that all tracks contain strings having no embedded blanks and having leftmost symbol stored in the work tape square indexed by 0. The quantum transformations are steps ii and vi. These transformations require a single step and involve only the symbol in square 0 of the track corresponding to v. The remaining transformations are reversible transformations. It is straightforward to show that each such transformation may be performed by a DTM running in space $O(\log n)$ in the manner described in Section 2 for a suitable space-bound $f(n) = O(\log n)$. (It is for this reason that we increment c modulo $d(d + 1)^2 n^3 + 1$ instead of simply incrementing c in step viii, although the same effect results; each transformation must be defined on a bounded region of the work tape). We note that the quantity $d(d+1)^2 n^3$ is somewhat arbitrary in steps viii and ix; any quantity at least $\lceil d(d + 1)^2 n^2 \log(2n)/8 \rceil$ suffices. The loop may be implemented reversibly, in the manner described in [14]. By Theorem 2, it follows that each reversible step in Figure 1 may be performed reversibly in logspace, requiring time depending only on the input (G, s, t) and not on the particular contents of the work tape of M when the step is performed. This implies that each step in Figure 1 may be viewed as requiring unit time, insofar as the analysis of the machine is concerned. When we say *accept* or *reject*, we naturally mean enter an accepting or rejecting state, as appropriate. It is straightforward to define a function T, as in the definition of $\mathrm{QR}_H\mathrm{L}$, so that the observation of M takes place after the correct number of steps in order to yield acceptance or rejection accordingly. It is also straightforward to show that M runs in logspace with respect to this T.

Now we analyze the computation of M on a given input (G, s, t). When describing superpositions of M, we will restrict our attention to the variables u, v, b and c; since we will only care about superpositions between the transformations described above, all other aspects of M (specifically, tape head positions and internal state) are deterministic. It will be most convenient to express such superpositions in terms of classical states of the form $|u, v\rangle\, |c\rangle\, |b\rangle$ for $u, v \in V$, $c, b \in \mathbb{Z}$, which may be interpreted as being equivalent to classical states the form $|u, v, c, b\rangle$.

Assume that M does not reject during step 1, so that G is indeed regular of degree d and undirected. After step 2 is performed, the superposition of M is $|s, s\rangle\, |0\rangle\, |0\rangle$. Now the loop in step 3 is performed. After one iteration of the loop, the superposition of M is $(Q\, |s, s\rangle)\, |0\rangle\, |1\rangle + |\xi_{1,1}\rangle\, |1\rangle\, |1\rangle$, where Q is defined in Section 3 and $|\xi_{1,1}\rangle$ is some vector (that we don't care about). More generally, after $j < d(d + 1)^2 n^3$ iterations of the loop, the superposition is

$$\left(Q^j\, |s, s\rangle\right) |0\rangle\, |j\rangle + \sum_{c \geq 1} |\xi_{c,j}\rangle\, |c\rangle\, |j\rangle\,,$$

and after $k = d(d+1)^2 n^3$ iterations, the superposition is

$$\left(Q^k\, |s, s\rangle\right) |0\rangle\, |0\rangle + \sum_{c \geq 1} |\xi_{c,0}\rangle\, |c\rangle\, |0\rangle\,.$$

At this point, the loop terminates, so that upon completion of step 4 the probability of accepting is $\left|\langle t, t|\, Q^k\, |s, s\rangle\right|^2$. By Lemma 3, we conclude that M accepts (G, s, t) with probability at least $\frac{1}{4n^2}$ in case s is connected to t, and probability 0 otherwise. ■

5 Amplifying acceptance probabilities

The complexity class $\mathrm{R}_H\mathrm{L}$ is robust with respect to the probability with which positive instances are accepted: the probability $1/2$ in the definition of $\mathrm{R}_H\mathrm{L}$ may be replaced by any function $f(|x|)$ satisfying $1/g(|x|) \leq f(|x|) \leq 1 - 2^{-g(|x|)}$ for $g(|x|) > 0$ a polynomial. It is not immediate that the analogous fact holds for $\mathrm{QR}_H\mathrm{L}$; repeated simulation a given QTM computation requires that the simulated machine be in its initial configuration at the start of each simulation, but resetting this machine to its initial configuration constitutes an irreversible action that cannot be performed by the quantum machine performing the simulation. In this section we prove that this fact does indeed hold.

Lemma 6 *Let M be a QTM and let T be a logspace time-bound such that M runs in logspace with respect to T. Let $p(x)$ denote the probability that (M, T) accepts x. Then for any polynomial f, there exists a QTM M_f and a logspace time-bound T_f such that M_f runs in logspace with respect to T_f, and (M_f, T_f) accepts each input x with probability*

$$1 - (1 - p(x))(1 - 2p(x))^{2f(|x|)}.$$

Proof. Given M, T, and f as in the statement of the theorem, we let M_f be a quantum Turing machine functioning as described in Figure 2. The machine M_f will store an encoding of some configuration of M on its work tape, as well as an integer a, initially equal to zero. For each step in Figure 2, a sequence of reversible and quantum transformations may be defined that have the described effects. We will not describe in detail how this may be done, as this has been discussed in [14]. Each required transformation can be performed in logspace, so that we may assume M_f runs in logspace. It may also be assumed that each step in Figure 2 requires a number of steps depending only on the input and not on any other aspect of the computation path being followed. An appropriate logspace time-bound T_f can be defined so that the observation occurs when step 2 has finished, yielding acceptance or rejection appropriately.

```
1. Repeat the following $f(|x|) + 1$ times:
   i.   Simulate the computation of $M$ on $x$ for $T$ steps.
   ii.  If $M$ accepts $x$, increment $a$ modulo $f(|x|)+2$.
   iii. Invert step i.
   iv.  If the current configuration of $M$ is not the initial configuration, and if $a = 0$, multiply the current amplitude by -1.
2. Accept if $a \neq 0$, otherwise reject.
```

Figure 2: Description of quantum Turing machine M_f for Lemma 6.

We now determine the probability that (M_f, T_f) rejects. Let us denote by E the unitary operator corresponding to evolving M for T steps. Since the counter a is incremented modulo $f(|x|) + 2$ at most $f(|x|) + 1$ times, we may determine the probability (M_f, T_f) rejects by examining the superposition of M represented by the state of M_f projected onto the space spanned by classical configurations for which $a = 0$.

Initially, the state of M represented by M_f is $|c_0\rangle$, for c_0 the initial configuration of M. The first iteration of step i maps this state to $E\,|c_0\rangle = |\psi\rangle$. Write $|\psi\rangle = |\psi_{acc}\rangle + |\psi_{acc}^{\perp}\rangle$, where $|\psi_{acc}\rangle$ denotes the projection of $|\psi\rangle$ onto the space spanned by accepting configurations of M. During step ii, a is incremented if M is in an accepting configuration. Since we are interested in that part of the superposition for which $a = 0$, step ii effectively projects the superposition of M represented by M_f onto state $|\psi_{acc}^{\perp}\rangle$.

Now we consider the sequence of steps iii, iv, i, ii, which are at this point performed $f(|x|)$ times. The effect of each iteration of this sequence of operations is that $|\psi_{acc}^{\perp}\rangle$ is mapped to $(1 - 2p(x))|\psi_{acc}^{\perp}\rangle$, where still our attention is restricted to the subspace on which $a = 0$. This may be argued as follows. First, the effect of step iii is to map $|\psi_{acc}^{\perp}\rangle$ to $E^{\dagger}|\psi_{acc}^{\perp}\rangle$. Since

$$\langle c_0|E^{\dagger}|\psi_{acc}^{\perp}\rangle = \overline{\langle\psi_{acc}^{\perp}|E|c_0\rangle} = 1 - p(x),$$

we may write $E^{\dagger}|\psi_{acc}^{\perp}\rangle = (1 - p(x))\,|c_0\rangle + |\xi\rangle$, where $|\xi\rangle$ satisfies $\langle\xi|c_0\rangle = 0$. Step iv maps this state to $(1-p(x))\,|c_0\rangle - |\xi\rangle$, and step i maps this resulting state to $(2 - 2p(x))|\psi_{acc}\rangle + (1 - 2p(x))|\psi_{acc}^{\perp}\rangle$. Finally, step ii effectively projects this state onto the space of non-accepting configurations, yielding $(1 - 2p(x))|\psi_{acc}^{\perp}\rangle$.

Therefore $f(|x|)$ iterations of steps iii, iv, i, ii map $|\psi_{acc}^{\perp}\rangle$ to $(1 - 2p(|x|))^{f(|x|)}|\psi_{acc}^{\perp}\rangle$. During the last iteration of the loop, steps iii and iv do not affect the norm of this vector, and hence (M_f, T_f) rejects with probability

$$\left\|(1 - 2p(|x|))^{f(|x|)}|\psi_{acc}^{\perp}\rangle\right\|^2 \\ = (1 - p(x))(1 - 2p(x))^{2f(|x|)}$$

and accepts otherwise, which completes the proof. ■

By Lemmas 5 and 6, we have d-USTCON $\in \mathrm{QR}_H\mathrm{L}$.

Theorem 1 now follows in straightforward fashion, relying again on Theorem 2; given a particular language $A \in \mathrm{SL}$ we have a logspace many-one reduction to d-USTCON, and we may replace various reversible transformations of our machine for d-USTCON with appropriately defined reversible transformations based on compositions of the reduction with the replaced transformation. Details will appear in the final version of this paper.

6 Concluding remarks

We have shown that logspace quantum Turing machines can simulate a limited class of probabilistic computations in a time-efficient manner without relying on measurements during the computation. This leaves open the question of whether probabilistic computations can be simulated efficiently by space-bounded quantum machines in general (e.g., is $\mathrm{R}_H\mathrm{L}$ contained in $\mathrm{QR}_H\mathrm{L}$?)

We have defined in this paper quantum processes that attempt to mimic classical random walks on graphs. There are a number of ways in which to define *quantum walks on graphs* having properties quite different from classical random walks. It may be interesting to consider possible applications of such processes to quantum complexity theory.

Acknowledgments

I would like to thank an anonymous referee for providing a number of suggestions for improving the presentation of this paper.

References

[1] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing*, pages 20–30, 1998.

[2] R. Aleliunas, R. Karp, R. Lipton, L. Lovász, and C. Rackoff. Random walks, universal traversal sequences, and the time complexity of maze problems. In *Proceedings of the 20th Annual Symposium on Foundations of Computer Science*, pages 218–223, 1979.

[3] R. Armoni, A. Ta-Shma, A. Wigderson, and S. Zhou. $SL \subseteq L^{4/3}$. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing*, pages 230–239, 1997.

[4] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[5] A. Berthiaume. Quantum computation. In L. Hemaspaandra and A. Selman, editors, *Complexity Theory Retrospective II*, pages 23–50. Springer, 1997.

[6] N. Biggs. *Algebraic Graph Theory.* Cambridge University Press, 1974.

[7] L. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 212–219, 1996.

[8] R. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5:183–191, 1961.

[9] K. Lange, P. McKenzie, and A. Tapp. Reversible space equals deterministic space (extended abstract). In *Proceedings of the 12th Annual IEEE Conference on Computational Complexity*, pages 45–50, 1997.

[10] H. Lewis and C. Papadimitriou. Symmetric space-bounded computation. *Theoretical Computer Science*, 19:161–187, 1982.

[11] L. Lovász and P. Winkler. Mixing of random walks and other diffusions on a graph. In Peter Rowlinson, editor, *Surveys in Combinatorics*, volume 218 of *London Mathematical Society Lecture Note Series*, pages 119–154. Cambridge University Press, 1995.

[12] N. Nisan and A. Ta-Shma. Symmetric logspace is closed under complement. In *Proceedings of the 37th Annual Symposium on Foundations of Computer Science*, pages 140–146, 1995.

[13] M. Saks. Randomization and derandomization in space-bounded computation. In *Proceedings of the 11th Annual IEEE Conference on Computational Complexity*, pages 128–149, 1996.

[14] J. Watrous. Space-bounded quantum complexity. *Journal of Computer and System Sciences*, 1999. To appear. A preliminary version appeared in *Proceedings of the 13th Annual IEEE Conference on Computational Complexity*, 1998, pages 210–227.