Quantum Random Walks and the Analysis of Discrete Quantum Processes

Andris Ambainis* Eric Bach† John Watrous‡

October 31, 2000

Abstract

We define and analyze quantum computational variants of random walks on one-dimensional lattices. Several striking differences between the quantum and classical cases are observed. In our analyses we employ techniques that may find further use in analyzing discrete quantum processes.

1 Introduction

Classical random walks on the line are very well-studied processes. In the simplest variation, a single particle moves on a two-way infinite, one-dimensional lattice. At each step, the particle moves one position left or right, depending on the flip of a fair coin. Such random walks may be generalized to more complicated lattices and to finite or infinite graphs, and have had several interesting applications in computer science (see, for instance, [2, 3, 8, 10]). We refer the reader to Kemeny and Snell [9] for basic facts regarding random walks.

In this paper we consider quantum variations of random walks on one-dimensional lattices—we refer to such quantum processes as *quantum random walks*. Although our basic definition looks quite similar to the classical random walk, the quantum random walk has strikingly different behavior. The reason for this is quantum interference. Whereas there cannot be destructive interference in a classical random walk, in a quantum random walk two separate paths leading to the same point may be out of phase and cancel one another out.

We study three basic quantum variations of classical random walks, which correspond to random walks with zero, one, or two absorbing boundaries. We call these *infinite*, *semi-infinite*, and *finite* quantum random walks. Each of the three cases illustrates surprising behavior that underscores the differences between quantum and classical processes.

For the infinite random walk, it is well-known that the classical random walk is at the expected distance $\Theta(\sqrt{t})$ from the origin at time t. The probability of the classical random walk being at a distance $\Omega(t)$ is exponentially small. In contrast, the quantum random walk spreads quadratically faster and is quite evenly distributed over an interval of size $\Theta(t)$. The expected distance from the origin is $\Theta(t)$ after t steps.

In the semi-infinite case, we assume we have an absorbing boundary one location to the left of the origin; the process is terminated if the particle reaches this location. Again, it is well known that in the classical case the random walk stops with probability 1. In contrast, the quantum random walk

*Computer Science Division, University of California, Berkeley, CA 94720.

†Computer Sciences Department, University of Wisconsin, Madison, WI 53706.

‡Department of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4.

stops with probability $2/\pi$. Thus, a considerable part of the quantum state keeps going infinitely in the other direction (to the right) without ever returning to the origin.

Finally, in the finite case, we assume there is a second absorbing boundary n positions to the right of the origin for arbitrary n. Again, in the classical and quantum cases, the process is terminated if the particle reaches an absorbing boundary. Naturally, the presence of the second boundary decreases the probability of reaching the left boundary in the classical case. Again surprisingly, in the quantum case, adding the second boundary on the right actually *increases* the chance of reaching the boundary on the left (as long as the second boundary allows the particle at least two non-boundary locations on which to walk). In the limit for large n, the probability of reaching the left boundary tends to $1/\sqrt{2}$ (and **not** $2/\pi$). The reason for this strange behavior is, again, the quantum interference. Adding a right boundary removes a part of the quantum state (the part which reaches the right boundary), which would otherwise have interfered destructively with another part of the state reaching the left boundary. Thus, removing a part of the quantum state at the right boundary *increases* the chance of reaching the left boundary.

To obtain our results, we express the amplitudes of the quantum random walk by recurrence relations and solve the recurrences. In two cases, this requires sophisticated techniques. The recurrences for the infinite line are obtained by first expressing the amplitudes by a sum of binomial coefficients and then generating a recurrence from this sum by Gosper-Zeilberger method. For the two-sided bounded case, we require methods from real and complex analysis, including a (possibly new) nonlinear version of the Riemann-Lebesgue lemma.

Our primary motivation for studying quantum random walks is to develop techniques for analyzing discrete quantum processes. Indeed, while our quantum random walks are very simple to describe, they appear to be quite difficult to analyze. Analysis of various more complicated quantum processes, such as certain definitions for quantum random walks on arbitrary finite graphs, seem to be out of our reach at the present time. However, as quantum algorithm design and quantum complexity theory become more and more sophisticated, we believe it will be inevitable to develop methods for accurately analyzing discrete quantum processes. This paper represents one step toward this goal.

In this paper we are only considering one way to define quantum random walks, and it should be noted that we are not suggesting that this is the only definition—there are several ways one can define quantum variations on random walks (see, for instance, the quantum processes considered by Farhi and Gutmann [4]).

1.1 Related work

Quantum random walks have been studied by Meyer [11] and Farhi and Gutmann [4] but their results are mostly unrelated to ours. Meyer's model (quantum lattice gas automata or QLGA) is the same as our two-way infinite quantum random walk but the questions that he asks are quite different from ours. The only overlapping result is the formula for the amplitudes as the sum of binomial coefficients (our Lemma 6). After obtaining this result, he proceeds to analyzing the continuous-time limit of QLGA and shows that this limit is given by the Dirac equation [5]. The results about the continuous-time limit does not imply anything for the discrete case which we study in this paper.

Farhi and Gutmann [4] analyze quantum random walks on trees and exhibit a collection of trees on which the quantum process hits one particular leaf exponentially faster than the corresponding classical process. Their model, results, and methods seem to be quite different from ours.

Watrous [15] considered quantum processes on graphs that mimic classical random walks in order to obtain results about space-bounded quantum computation. In this case, however, the quantum processes are designed so that quantum effects do not ruin the behavior given by classical random walks on graphs, and so give a much less natural definition for quantum random walks.

Recently, inspired by a preliminary version of this paper, Aharonov et.al. [1] have introduced and analyzed quantum random walks on other types of graphs—the particular questions they address and results they obtain, however, are of a different nature than those of this paper. Also, Nayak and Vishwanath [12] have obtained an another proof of some of our results regarding the infinite random walk using a different technique (eigenvector analysis).

2 Definitions and Statement of Results

In this paper we consider three different quantum processes that may be described as *quantum random walks* on a one-dimensional lattice. We now describe these processes in a unified framework.

Let $\mathbb{Z}$ denote the integers and let $\Sigma = \{0, 1\}$. Shortly we will make the identification $0 = \textit{right}$, $1 = \textit{left}$. The quantum systems we will consider will have the underlying classical state set $\mathbb{Z} \times \Sigma$. We view a state $(n, d) \in \mathbb{Z} \times \Sigma$ as consisting of a location n and a direction d.

The pure quantum states of our systems may be identified with unit vectors in the Hilbert space $\mathcal{H} = \ell_2(\mathbb{Z} \times \Sigma)$. This space consists of (square-summable) mappings of the form $\psi : \mathbb{Z} \times \Sigma \to \mathbb{C}$, along with the usual inner product. We will use the Dirac notation to represent elements of $\mathcal{H}$; $|n, d\rangle$ denotes the vector mapping (n, d) to 1 and all other elements of $\mathbb{Z} \times \Sigma$ to 0, and is identified with the classical state (n, d). Other vectors of $\mathcal{H}$ may be expressed as linear combinations of this basis (which will be referred to as the *computational basis*).

Let us define two unitary operators on $\mathcal{H}$. First, define U_{move} by the following action on computational basis states: $U_{move} |n, 0\rangle = |n + 1, 0\rangle$ and $U_{move} |n, 1\rangle = |n - 1, 1\rangle$. Extending this mapping to an operator on $\mathcal{H}$ clearly gives a unitary operator (since the operator is nothing more than a permutation of computational basis states). The second operator, which we will denote U_{twirl}, acts only on the direction component of quantum states, and has the following action on computational basis states:

$$U_{twirl} |n, 0\rangle = \frac{1}{\sqrt{2}}(|n, 0\rangle + |n, 1\rangle), \qquad U_{twirl} |n, 1\rangle = \frac{1}{\sqrt{2}}(|n, 0\rangle - |n, 1\rangle).$$

(Again we extend U_{twirl} to all of $\mathcal{H}$ by linearity.) In short, the operator U_{twirl} applies the Hadamard transform to the direction component of a quantum state, leaving the location unaffected. The operator U_{twirl} is obviously unitary. Finally, define U_{walk} as $U_{walk} = U_{move} U_{twirl}$.

It should be noted that there is nothing special about the choice of the Hadamard transform in defining U_{twirl}—other quantum operations on the direction component would simply yield different quantum processes having possibly very different behaviors from the processes we consider.

The action of U_{walk} on any state $|n, 0\rangle$ is as follows: $U_{walk} |n, 0\rangle = (|n - 1, 1\rangle + |n + 1, 0\rangle)/\sqrt{2}$. Similarly we have $U_{walk} |n, 1\rangle = (-|n - 1, 1\rangle + |n + 1, 0\rangle)/\sqrt{2}$.

We may imagine a system that starts in some classical state, such as $|0, 0\rangle$, and undergoes the evolution obtained by repeatedly applying the operator U_{walk}. If we consider the process obtained by alternately applying U_{walk} and observing the location of the system, then the system behaves precisely as a classical random walk. However, without such observations that serve to "collapse" the state of the system after each application of U_{walk}, the system evolves much differently because paths interfere with one another.

In order to discuss processes that may be categorized as above as quantum random walks in a physically meaningful way, we must consider observations of the system. The particular observations considered are what give rise to the three separate processes we consider. We now describe the three processes individually and state the main results obtained for each process.

2.1 Two-way infinite timed quantum random walk

The simplest process we consider is the *two-way infinite timed quantum random walk*. The process is as follows.

1. Initialize the system in classical state $|0,0\rangle$.

2. For any chosen number of steps t, apply U_{walk} to the system t times, then observe the location.

We show that the location of the quantum random walk after t steps is quite evenly distributed over $\Omega(n)$ locations. This sharply contrasts with the classical random walk which after t steps is at location within $O(\sqrt{t})$ of the origin with a high probability.

Theorem 1 *For any $\epsilon > 0$, there are $\Omega(t)$ values n such that the measurement of $U^t_{walk}|0,0\rangle$ gives $|n,0\rangle$ with probability at least $(1-\epsilon)\frac{1}{2\pi t}$ and $\Omega(t)$ values n such that the measurement gives $|n,1\rangle$ with probability at least $(1-\epsilon)\frac{1}{2\pi t}$.*

Theorem 2 *For any $\epsilon > 0$, there exists c such that, if $(-\frac{1}{\sqrt{2}}+\epsilon)t \leq n \leq (\frac{1}{\sqrt{2}}-\epsilon)t$, then the probability that the measurement of $U^t_{walk}|0,0\rangle$ gives $|n,0\rangle$ or $|n,1\rangle$ is at most $\frac{c}{n}$.*

It may still be possible that the probability of $|n,0\rangle$ or $|n,1\rangle$ grows faster than $\frac{c}{n}$ for any constant c when $n \approx -\frac{t}{\sqrt{2}}$ or $n \approx \frac{t}{\sqrt{2}}$.

Computer experiments suggest that the probability of location n grows fast from $n=-t$ to $n \approx -\frac{t}{\sqrt{2}}$, reaches a maximum at $n \approx -\frac{t}{\sqrt{2}}$, then oscillates between $n \approx -\frac{t}{\sqrt{2}}$ and $n \approx \frac{t}{\sqrt{2}}$ (with the amplitude of oscillations slightly decreasing from $n \approx -\frac{t}{\sqrt{2}}$ to $n=0$ and then slightly increasing from $n=0$ to $n \approx \frac{t}{\sqrt{2}}$), reaches another maximum at $n \approx \frac{t}{\sqrt{2}}$ and then rapidly decreases to 0 after that. Data from our experiments do not clearly indicate whether the probability of location n at the peaks $n \approx -\frac{t}{\sqrt{2}}$ and $n \approx \frac{t}{\sqrt{2}}$ is still $O(\frac{1}{t})$ or higher.

2.2 Semi-infinite quantum random walk

For the second process we introduce an absorbing boundary. This is done by considering a measurement that corresponds to the question "Is the system at location n?". This measurement may be described as corresponding to the projection operators $\Pi^n_{yes} = |n,0\rangle\langle n,0| + |n,1\rangle\langle n,1|$ and $\Pi^n_{no} = I - \Pi^n_{yes}$. For example, suppose a system is in the state

$$\frac{1}{2}|0,0\rangle - \frac{1}{2}|0,1\rangle + \frac{1}{2}|2,0\rangle + \frac{1}{2}|4,1\rangle$$

and is observed using the above measurement for $n=0$. The answer obtained is "yes" with probability

$$\left\|\Pi^0_{yes}\left(\frac{1}{2}|0,0\rangle - \frac{1}{2}|0,1\rangle + \frac{1}{2}|2,0\rangle + \frac{1}{2}|4,1\rangle\right)\right\|^2 = \left\|\frac{1}{2}|0,0\rangle - \frac{1}{2}|0,1\rangle\right\|^2 = \frac{1}{2},$$

in which case the system "collapses" to state $(|0,0\rangle - |0,1\rangle)/\sqrt{2}$, and the answer is "no" with probability 1/2, in which case the system "collapses" to state $(|2,0\rangle + |4,1\rangle)/\sqrt{2}$.

Now we are ready to define our second quantum process:

1. Initialize the system in classical state $|1,0\rangle$.

2. a. Apply U_{walk}.

   b. Observe the system according to $\{\Pi^0_{yes}, \Pi^0_{no}\}$ (i.e., measure the system to see whether it is or is not at location 0).

3. If the result of the measurement was "yes" (i.e., revealed that the system was at location 0), then terminate the process, otherwise repeat step 2.

There are several questions one might ask about this process. We will restrict our attention to the following simple question: *What is the probability that the system ever reaches location 0?* In other words, what is the probability that the measurement eventually results in the answer "yes"? Let p_∞ denote this probability. We have

Theorem 3 $p_\infty = 2/\pi$.

This theorem is in sharp contrast with the classical case, for which it is well-known that the probability of eventually reaching location 0 is 1.

2.3 Finite quantum random walk

The third and final process we consider is similar to the second, except that two absorbing boundaries are present rather than one. Specifically, using the same measurements as defined for the semi-infinite quantum random walk, we consider the following process:

1. Initialize the system in classical state $|1,0\rangle$.

2. a. Apply U_{walk}.

   b. Observe the system according to $\{\Pi^0_{yes}, \Pi^0_{no}\}$

   c. Observe the system according to $\{\Pi^n_{yes}, \Pi^n_{no}\}$ (for some fixed $n > 1$).

3. If the result of either measurement was "yes" (i.e., revealed that the system was either at location 0 or location n), then terminate the process, otherwise repeat step 2.

For fixed $n > 1$, let us define p_n to be the probability that the above process eventually exits from the left, i.e., the measurement in step 2b eventually results in "yes". Also define q_n to be the probability that the process exits from the right.

Proposition 4 *For all* $n > 1$, $p_n + q_n = 1$.

The asymptotic behavior of p_n is as follows.

Theorem 5 $\lim_{n\to\infty} p_n = 1/\sqrt{2}$.

Once again, this result is in sharp contrast to the classical case, for which the probability of exiting from the left is $1 - 1/n$.

When comparing this situation to the semi-infinite quantum random walk, it is interesting to note that $1/\sqrt{2} > 2/\pi$. ($1/\sqrt{2} = 0.7071\ldots$ while $2/\pi = 0.6366\ldots$.) This means that for sufficiently large n, terminating the walk at location n actually *increases* the probability of reaching location 0. (Indeed, since p_3 is easily shown to be $2/3$, this holds already for the case $n = 3$.)

We are not yet able to derive a closed form for p_n. However, we conjecture the following.

Conjecture 2.1 *The probabilities p_n obey the following recurrence.*

$$\begin{aligned} p_1 &= 0, \\ p_{n+1} &= \frac{1+2p_n}{2+2p_n}, \quad n \geq 1. \end{aligned}$$

3 Analysis of the two-way infinite timed quantum random walk

To obtain our results, we bound the amplitudes of $|x,0\rangle$ and $|x,1\rangle$ in the superposition $U_{walk}^t|0,0\rangle$. Since the probability of measuring $|x,i\rangle$ is a square of the absolute value of the amplitude, bounds on amplitudes imply bounds on the probabilities.

To reach $|x,0\rangle$ or $|x,1\rangle$ in t steps, there should be $m = \frac{x+t}{2}$ moves left and $t-m = \frac{t-x}{2}$ moves right. By counting the paths consisting of m moves left and $t-m$ moves right, one gets

Lemma 6 *[11] The amplitude of $|x,0\rangle$ after t applications of U_{walk} is*

$$\frac{1}{\sqrt{2^t}} \sum_k \binom{m-1}{k} \binom{t-m}{k} (-1)^{m-k}. \tag{1}$$

The amplitude of $|x,1\rangle$ after t applications of U_{walk} is

$$\frac{1}{\sqrt{2^t}} \sum_k \binom{m-1}{k-1} \binom{t-m}{k} (-1)^{m-k-1}. \tag{2}$$

This allows to calculate the amplitudes of $|x,0\rangle$ and $|x,1\rangle$ for any x. However, formulas (1) and (2) involve the difference of two numbers which are both much bigger than the amplitudes. For this reason, they cannot be directly used to bound the amplitudes.

If x is close to 0, a simple manipulation with binomial coefficients gives nice formulas for $|x,0\rangle$ and $|x,1\rangle$.

Lemma 7 *The amplitudes of $|0,0\rangle$ and $|0,1\rangle$ after t steps are:*

1. *0 if t is odd,*
2. *$\frac{1}{2^m}(-1)^{\frac{m}{2}}\binom{m-1}{m/2}$ if $t=2m$, m even,*
3. *$\frac{1}{2^m}(-1)^{\frac{m+1}{2}}\binom{m-1}{(m-1)/2}$ and $\frac{1}{2^m}(-1)^{\frac{m-1}{2}}\binom{m-1}{(m-1)/2}$ if $t=2m$, m odd.*

By Stirling's approximation, $\binom{m}{m/2} \approx \frac{2^m}{\sqrt{\pi m}}$. Therefore, the amplitudes of $|0,0\rangle$ and $|0,1\rangle$ after $t=2m$ steps is $\frac{1}{2^m}\binom{m-1}{(m-1)/2} \approx \frac{1}{2^m}\frac{2^{m-1}}{\sqrt{\pi m}} = \frac{1}{2\sqrt{\pi m}} = \frac{1}{\sqrt{2\pi t}}$ and the probabilities of measuring them are approximately $\frac{1}{2\pi t}$.

However, for an arbitrary x, applying the idea of Lemma 7 still gives a difference of two very large numbers.

3.1 Recurrences

We now focus on the sum

$$S_{m,n} = \sum_k \binom{m}{k}\binom{n}{k}(-1)^k.$$

Because of Lemma 6, calculating the amplitude of $|x, 0\rangle$ at time t is equivalent to calculating $S_{m,n}$ for $m = \frac{t+x}{2} - 1$, $n = \frac{t-x}{2}$.

Using Gosper-Zeilberger method[6, 7, 16] for generating recurrences from sums of binomial coefficients, we get

Lemma 8 $(n+2)S_{m,n+2} = (3n+4-m)S_{m,n+1} - (2n+2)S_{m,n}$.

Together with Lemma 6, this relates the amplitudes of $|x, 0\rangle$ at the time t, $|x-1, 0\rangle$ at the time $t+1$ and $|x-2, 0\rangle$ at the time $t+2$. We can also obtain a similar (but more complicated) recurrence that relates $S_{m-1,n+1}$, $S_{m,n}$ and $S_{m+1,n-1}$ (or, equivalently, amplitudes of $|x-1, 0\rangle$, $|x, 0\rangle$ and $|x+1, 0\rangle$ at time t).

3.2 Solving the recurrences

Let

$$S'_{m,n} = a_0 2^{n/2} \sin(\sum_{j=m}^{n-1} \theta_{m,j} + \alpha)$$

where $\theta_{m,j} = \arccos \frac{3j+4-m}{2\sqrt{2}(j+1)}$. Then, we have

Lemma 9 *Let $d < \frac{1}{3-2\sqrt{2}}$. If a_0 and α are such that $S_{m,m} = S'_{m,m}$ and $S_{m,m+1} = S'_{m,m+1}$, then, for any n satisfying $n < m < dn$,*

$$|S_{m,n} - S'_{m,n}| \leq f(d) 2^{n/2} a_0$$

for any n satisfying $n < m < dn$. $f(d)$ is such that $f(1+\delta) = \Theta(\delta)$ for small δ and $f(d) < \infty$ for all $d < \frac{1}{3-2\sqrt{2}}$.

Then, we use the method of Lemma 7 to obtain the precise values of $S_{m,m}$ and $S_{m,m+1}$ and use $S_{m,m}$ and $S_{m,m+1}$ to determine a_0 and α.

Because $f(1+\delta) = \Theta(\delta)$, this gives a good approximation of amplitudes of $|x, 0\rangle$ for $-\delta t < x < \delta t$. This approximation can be then used to show that, for any t and $\epsilon > 0$, $\Omega(t)$ amplitudes of $|x, 0\rangle$ must be at least $(1-\epsilon)$ times the amplitude of $|0, 0\rangle$, i.e., at least $(1-\epsilon)\frac{1}{\sqrt{2\pi t}}$. This implies Theorem 1.

Theorem 2 follows from the approximation of Lemma 9 and $f(d) < \infty$. (The requirement $m < \frac{1}{3-2\sqrt{2}} n$ is equivalent to $x \leq \frac{t}{\sqrt{2}}$ for location x and time t.)

4 Analysis of the semi-infinite quantum random walk

The probability p_∞ may be expressed as $p_\infty = \sum_{t\geq 1} \left\|\Pi^0_{yes} U^t_{walk}|1,0\rangle\right\|^2$. (Note that renormalizations do not appear in this expression because we are calculating an unconditional probability.) The sum will be evaluated by counting paths.

Let A_t be the set of t-tuples $(a_1,\ldots,a_t)\in\{-1,1\}^t$ for which (i) $\sum_{i\leq j} a_i \geq 0$, for all $j<t$, and (ii) $\sum_{i\leq t} a_i = -1$. The set A_t is in one-to-one correspondence with the set of all paths starting in state $|1,0\rangle$ and entering location 0 for the first time at time t (each a_i indicates $(-1)^{d_i}$ for d_i the direction after i applications of U_{walk}). Let A_t^+ denote the subset of A_t for which $\#\{i\,|\,1\leq i<t,\ a_i=a_{i+1}=-1\}$ is even and let A_t^- denote the subset of A_t for which $\#\{i\,|\,1\leq i<t,\ a_i=a_{i+1}=-1\}$ is odd. Now, the amplitude associated with each path in A_t^+ is $2^{-t/2}$, and the amplitude associated with each path in A_t^- is $-2^{-t/2}$. It follows that

$$p_\infty = \sum_{t\geq 1}\left(\#\left(A_t^+\right)-\#\left(A_t^-\right)\right)^2 2^{-t}. \tag{3}$$

We will evaluate the sum in (3) by defining a generating function for $\#\left(A_t^+\right)-\#\left(A_t^-\right)$. Let $f(z)=\sum_{t\geq 1}\left(\#\left(A_t^+\right)-\#\left(A_t^-\right)\right)z^t$. The function $f(z)$ obeys the equation

$$f(z) = z - z\left(zf(z)+(zf(z))^2+(zf(z))^3+\cdots\right) = z - \frac{z^2 f(z)}{1-zf(z)}, \tag{4}$$

which follows from the fact that $-z(zf(z))^k$ is a generating function similar to f, but restricted to paths which pass through location 1 exactly k times, $k\geq 1$. Solving for $f(z)$ we obtain

$$f(z) = \frac{1+2z^2-\sqrt{1+4z^4}}{2z}. \tag{5}$$

Equation (5) is similar in form to the generating function for the Catalan numbers. We have

$$\#\left(A_t^+\right)-\#\left(A_t^-\right) = \begin{cases} 1 & t=1\\ (-1)^{k+1}C_k & t=4k+3\\ 0 & \text{otherwise}\end{cases}$$

where $C_k=\frac{1}{k+1}\binom{2k}{k}$ is the kth Catalan number. Thus $p_\infty = 1/2+(\sum_{k\geq 0} C_k^2\, 2^{-4k})/8$. Using induction, it is straightforward to prove $\sum_{k\leq N} C_k^2\, 2^{-4k} = (16\,N^3+36\,N^2+24\,N+5)\,C_N^2\,2^{-4N}-4$, and hence

$$p_\infty = \frac{1}{2}+\frac{1}{8}\left(\lim_{N\to\infty}(16\,N^3+36\,N^2+24\,N+5)\,C_N^2\,2^{-4N}-4\right) = \frac{1}{2}+\frac{1}{8}\left(\frac{16}{\pi}-4\right) = \frac{2}{\pi}.$$

5 Analysis of the finite quantum random walk

The goal of this section is to show that p_n, the probability of exit to the right for the walk on $\{1,\ldots,n-1\}$, has the limiting value $1/\sqrt{2}$. The idea is to express p_n as an oscillatory integral, whose limit is a two-dimensional integral we can evaluate exactly.

As in the semi-infinite case, we count paths. Define A_t^+ and A_t^- as in Section 4, and let $A_{t,n}^+$ and $A_{t,n}^-$ denote the subsets of A_t^+ and A_t^-, respectively, for which paths are restricted to locations $1,\ldots,n-1$ before reaching location 0 on the last step. Defining

$$f_n(z) = \sum_{t\geq 0}\left(\#\left(A_{t,n}^+\right)-\#\left(A_{t,n}^-\right)\right)z^t, \tag{6}$$

we have for $n > 1$ that $p_n = \sum_{t\geq 0} \left(\#\left(A_{t,n}^+\right) - \#\left(A_{t,n}^-\right)\right)^2 2^{-t} = (f_n \odot f_n)(1/2)$, where $\odot$ denotes the Hadamard product [14, p. 157]. The generating functions f_n satisfy

$$f_n(z) = z\left(\frac{1-2zf_{n-1}}{1-zf_{n-1}}\right) \tag{7}$$

with $f_1(z) = 0$. The reasoning is similar to the semi-infinite case. We will let $z = e^{i\theta}/\sqrt{2}$ in the analysis that follows.

5.1 Integrals for exit probabilities

Lemma 10 *We have*

$$p_n = \frac{2}{\pi}\int_0^{\pi/2} |f_n(e^{i\theta}/\sqrt{2})|^2 \, d\theta.$$

Proof. (Sketch.) Use the integral for the Hadamard product [14, p. 157] and symmetries implied by (7). ∎

Lemma 11 *For $n \geq 1$ and $|z| = 1/\sqrt{2}$, we have $|f_n| \leq 1$.*

Proof. (Sketch.) Use the maximum modulus principle and (7) to show that $g_n = zf_n(z/\sqrt{2})$ satisfies $|g_n| \leq 1$ on the unit disk. ∎

Lemma 12 *Let*

$$\lambda_{1,2} = \frac{(2z^2-1) \pm \sqrt{1+4z^4}}{2} \tag{8}$$

(subscript 1 for +; principal branch taken) and

$$\mu_{1,2} = \frac{(2z^2+1) \pm \sqrt{1+4z^4}}{2z^2} \tag{9}$$

(ditto). Then for $n \geq 0$ we have

$$h_n := \frac{f_n}{z} = \mu_1\mu_2 \frac{(\lambda_1/\lambda_2)^n - 1}{\mu_2(\lambda_1/\lambda_2)^n - \mu_1}.$$

Proof. (Sketch.) Let φ_z denote the Möbius transformation $w \mapsto \frac{2z^2w-1}{z^2w-1}$, so that $h_n = \varphi_z^n(0)$. Evaluate this using the technique in [13]. ∎

Lemma 13 *Let $z = e^{i\theta}/\sqrt{2}$. Then we have: (i) $|\lambda_1/\lambda_2| = 1$ for $0 < \theta < \pi/4$; (ii) $|\lambda_1/\lambda_2| < 1$ for $\pi/4 < \theta < \pi/2$; (iii) $|\mu_2|^2 = 2$ for $\pi/4 < \theta < \pi/2$; and (iv) $\mu_1/\mu_2 = 1 + 2\cos 2\theta + 2\cos\theta\sqrt{2\cos 2\theta} \in \mathbb{R}$ for $0 < \theta < \pi/4$.*

Proof. Unenlightening computation; omitted from the abstract. ∎

5.2 A nonlinear Riemann-Lebesgue lemma

For a smooth function on the torus $T = \{|z| = 1\} \times \{|u| \leq \pi\}$, the following result is physically plausible. Our application motivates the precise assumptions.

Lemma 14 *Let $F : T \to \mathbf{R}$ be C^2 for $|u| < \pi$, bounded when $z = e^{iu}$, with radial average*

$$G(u) := \frac{1}{2\pi} \int_0^{2\pi} F(e^{i\phi}, u) d\phi$$

bounded and Riemann integrable on $|u| < \pi$. Then

$$\lim_{n\to\infty} \int_{-\pi}^{\pi} F(e^{inu}, u) du = \int_{-\pi}^{\pi} G(u) du.$$

Proof: Approximate the integral of F over intervals of length $2\pi/n$, to get a Riemann sum for G. ∎

5.3 The limiting exit probability.

In this section we prove Theorem 5. It follows from the two lemmas below.

Lemma 15 *We have*

$$\lim_{n\to\infty} p_n = \frac{1}{2} + \frac{4}{\pi} \int_0^{\pi/4} \frac{d\theta}{\mu_1/\mu_2 + 1}.$$

Proof. From Lemma 10 we have, since $|f_n|$ is even,

$$p_n = \frac{1}{\pi} \int_{-\pi/4}^{\pi/4} |f_n|^2 d\theta + \frac{1}{\pi} \int_{\pi/4}^{\pi/2} |f_n/z|^2 d\theta. \tag{10}$$

By Lemma 11 and (ii)-(iii) of Lemma 13, the second term has the limit 1/2 as $n \to \infty$.

In the first term, we consider θ to be a function of $u = \arg(\lambda_1/\lambda_2)$ (real by Lemma 13), choosing the branch that maps 0 to 0. This gives

$$\frac{1}{\pi} \int_{-\pi/4}^{\pi/4} |f_n|^2 d\theta = \frac{2}{\pi} \int_{-\pi}^{\pi} \left| \frac{(\lambda_1/\lambda_2)^n - 1}{\mu_2(\lambda_1/\lambda_2)^n - \mu_1} \right|^2 \frac{d\theta}{du} du.$$

Applying Lemma 14 with $F(z, u) = |(z-1)/(\mu_2 z - \mu_1)|^2 \, d\theta/du$ and undoing the substitution, this becomes

$$\frac{4}{\pi^2} \int_0^{\pi/4} d\theta \int_0^{2\pi} \frac{1 - \cos\phi}{|\mu_2 e^{i\phi} - \mu_1|^2} d\phi = \frac{4}{\pi^2} \int_0^{\pi/4} \frac{d\theta}{|\mu_2|^2} \int_0^{2\pi} \frac{1 - \cos\phi}{(\mu_1/\mu_2 - \cos\phi)^2 + (\sin\phi)^2} d\phi. \tag{11}$$

Now apply Poisson's integral formula [14, p. 124] to the inner integral and observe that $\mu_1 \overline{\mu_2} = 2$. ∎

Lemma 16 *We have*

$$\int_0^{\pi/4} \frac{d\theta}{\mu_1/\mu_2 + 1} = \frac{\pi}{4} \left(\frac{1}{\sqrt{2}} - \frac{1}{2} \right).$$

Proof. Use of)iv) of Lemma 13, followed by an orgy of substitutions ($\psi = 2\theta$, then $t = \tan\psi/2$, $\rho = \sin^{-1} t$, finally $u = \tan\rho/2$) reduces the integral to an arctangent. We omit the details. ∎

References

[1] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani. Quantum walks on graphs. Submitted to the 33nd ACM Symposium on Theory of Computing, 2000.

[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] E. Coffman and G. Lueker. *Probabilistic Analysis of Packing and Partitioning Algorithms.* Wiley, 1991.

[4] E. Farhi and S. Gutmann. Quantum computation and decision trees. *Physical Review A*, 58:915–928, 1998.

[5] R. Feynman and A. Hibbs. *Quantum Mechanics and Path Integrals.* McGraw–Hill, 1965.

[6] W. Gosper. Decision procedure for indefinite hypergeometric summation. In *Proceedings of the National Academy of Sciences of U.S.A.*, volume 75, pages 40–42, 1978.

[7] R. Graham, D. Knuth, and O. Patashnik. *Concrete Mathematics.* Addison-Wesley, 2nd edition, 1994.

[8] R. Karp, M. Luby, and A. Marchetti-Spaccamela. A probabilistic analysis of multidimensional bin packing problems. In *Proceedings of the Sixteenth Annual ACM Symposium on Theory of Computing*, pages 289–298, 1984.

[9] J. Kemeny and J. Snell. *Finite Markov Chains.* Springer-Verlag, 1983.

[10] G. Louchard. The brownian motion: a neglected tool for the complexity analysis of sorted tables manipulation. *RAIRO Inform. Th.*, 17(4), 1983.

[11] D. Meyer. From quantum cellular automata to quantum lattice gases. *Journal of Statistical Physics*, 85:551–574, 1996. Also available from the Los Alamos Preprint Archive, quant-ph/9604003.

[12] A. Nayak and A. Vishwanath. Manuscript, submitted to the 33rd ACM Symposium on Theory of Computing, 2000.

[13] M. Nodine. *Fibonacci Quarterly*, 28:102–106, 1990.

[14] E. C. Titchmarsh. *The Theory of Functions.* Oxford University Press, 2nd edition, 1979.

[15] J. Watrous. Quantum simulations of classical random walks and undirected graph connectivity. In *Proceedings of the 14th Annual IEEE Conference on Computational Complexity*, pages 180–187, 1999.

[16] D. Zeilberger. The method of creative telescoping. *Journal of Symbolic Computation*, 11:195–204, 1991.