Asynchronous Cellular Automata and Brownian Motion

Quantum random walks in one dimension via generating functions

Andrew Bressler and Robin Pemantle [†]

University of Pennsylvania, Department of Mathematics, 209 S. 33rd Street, Philadelphia, PA 19104. pemantle,bressler@math.upenn.edu

We analyze nearest neighbor one-dimensional quantum random walks with arbitrary unitary coin-flip matrices. Using a multivariate generating function analysis we give a simplified proof of a known phenomenon, namely that the walk has linear speed rather than the diffusive behavior observed in classical random walks. We also obtain exact formulae for the leading asymptotic term of the wave function and the location probabilities.

Keywords: Hadamard, asymptotics, rational generating function

Subject classification: Primary: 81P68, 05A15.

1 Introduction

The classical random walk is a well-understood system with many important applications to computer science. Well-known examples of algorithms based on random walks include algorithms for counting, sampling, and testing properties such as satisfiability of Boolean formulae or graph connectivity. One of the most basic and useful random walks is a simple random walk on $\mathbb{Z}$. Here, a single particle moves on the one-dimensional integer lattice. At each step the particle moves one position to the left or right with equal probability. As the time t increases, the probability distribution describing the particle's location can be approximated increasing well by a normal distribution. The particle's expected location is at the origin, and its standard deviation is $\frac{1}{2}\sqrt{t}$, so its distribution is $O(\sqrt{t})$ in probability. That is to say that $\Pr(x \in [-M\sqrt{t}, M\sqrt{t}]) \to 1$ uniformly in t as $M \to \infty$.

Throughout the last century mankind has developed an increasing appreciation for the fact that Newton's laws alone do not describe our world. Among man's most recent attempts to harness the power of his quantum reality has been the field of quantum information theory, bringing with it the potential to devise instruments of extraordinary power [NC00]. For example, in 1994 Peter Shor [Sho97] discovered an algorithm to factor numbers on a quantum computer in a number of steps which is polynomial in the length of the number to be factored. This problem is not known to be solvable in polynomial time on a classical computer. Similarly, in [Gro96], Lov Grover determined a quantum mechanical algorithm reducing the time for searching a database of N entries from $O(N)$ steps to $O(\sqrt{N})$ steps. Algorithms such as these have brought researchers from a variety of scientific fields to focus on quantum information theory.

With the application of the classical random walk to information theory, as well as the growing promise of quantum information theory, it is clearly of interest to define the quantum random walk. This was first done by Y. Aharanov, L. Davidovich and N. Zagury [ADZ93] who introduced the quantum random walk and first discussed differences with the classical random walk due to quantum interference. Shortly thereafter,

[†]Research supported in part by National Science Foundation grant # DMS 0603821

David Meyer [Mey96] pointed out that the simple classical random walk described above does not translate into a quantum framework. Semigroup operators, such as the combination $\frac{1}{2}\sigma_+ + \frac{1}{2}\sigma_-$ of shifts defining the classical simple random walk, are positive operators of norm 1 over the classical state space $l_1(\mathbb{Z})$, but fail to be unitary over the quantum space $l_2(\mathbb{Z})$. In fact, it is easy to verify that the only translation-invariant positive real operators on $l_2(\mathbb{Z})$ are trivial (powers of the shift operator).

In order to construct unitary operators that disperse the position of a particle, it is necessary to introduce an extra degree of freedom, known as *chirality*. At any position on the lattice the particle's chirality takes either the value R (for RIGHT) or L (for LEFT). The elementary states are thus $\mathbb{Z} \times \Sigma$ where $\Sigma := \{R, L\}$, and the state space is $l_2(\mathbb{Z} \times \Sigma) = l_2(\mathbb{Z}) \otimes l_2(\Sigma)$. While this is the convention established by Ambainis *et al.* in [ABN$^+$01], we will refer to particles in the LEFT and RIGHT positions with the vector notation $\binom{1}{0}$ and $\binom{0}{1}$, respectively. We will denote the unit basis vector of $l_2(\mathbb{Z}) \otimes l_2(\Sigma)$ at position i with LEFT chirality as $e(i, L)$ and we define $e(i, R)$ analogously. We will order this basis as

$$\ldots e(i-1, L), e(i-1, R), e(i, L), e(i, R), e(i+1, L), e(i+1, R) \ldots .$$

Ambainis *et al.* focus on the Hadamard walk. This is based on the Hadamard transformation, a unitary operator on $l_2(\Sigma)$ whose matrix with respect to the standard basis is

$$U_{\sqrt{\frac{1}{2}}} := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

We then extend this transformation to $l_2(\mathbb{Z}) \otimes l_2(\Sigma)$ as $I \otimes U_{\sqrt{\frac{1}{2}}}$ where I is the identity, resulting in a transformation which acts as the block diagonal matrix:

$$\begin{pmatrix} \ddots & \vdots & \vdots & \vdots & \\ \ldots & U_{\sqrt{\frac{1}{2}}} & 0 & 0 & \ldots \\ \ldots & 0 & U_{\sqrt{\frac{1}{2}}} & 0 & \ldots \\ \ldots & 0 & 0 & U_{\sqrt{\frac{1}{2}}} & \ldots \\ & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

We then define a translation operator $\tilde{T}$ which shifts a particle with chirality R to the right one step and shifts a particle with chirality L to the left one step. More formally, we have

$$\tilde{T} : e(i, L) \mapsto e(i-1, L), \ \tilde{T} : e(i, R) \mapsto e(i+1, R)$$

and in the basis described above,

$$\tilde{T} = \begin{pmatrix} \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ \ldots & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \ldots \\ \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\ \ldots & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & \ldots \\ \ldots & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\ \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \ldots \\ \ldots & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \ldots \\ \ldots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\ \ldots & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & \ldots \\ & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

in which every fourth diagonal alternates in 0's and 1's and all other entries are 0. We then define the operator $\tilde{W}$ as $\tilde{W} = \tilde{T} \cdot (I \otimes U_{\sqrt{\frac{1}{2}}})$. As each of $\tilde{T}$ and $I \otimes U_{\sqrt{\frac{1}{2}}}$ are unitary, $\tilde{W}$ is unitary as well. This unitary composition of operators represents one step of the Hadamard walk.

These days, it is not so hard to compute the 200^{th} power of a large matrix. Computing the 200^{th} power of W and plotting the square moduli of the entries of the row whose index is (0,R) yields a graph of the probabilities, starting from a single particle in state $e(0, R)$ to be in position k at time 200 (see Figure 1). (Note: The range of the particle is 0 to 200, in accordance with the adjustment made in Section 2. Also note that the upper envelope is the prediction made by Theorem 2.1, excluding the $\cos^2(\rho)$ term.)

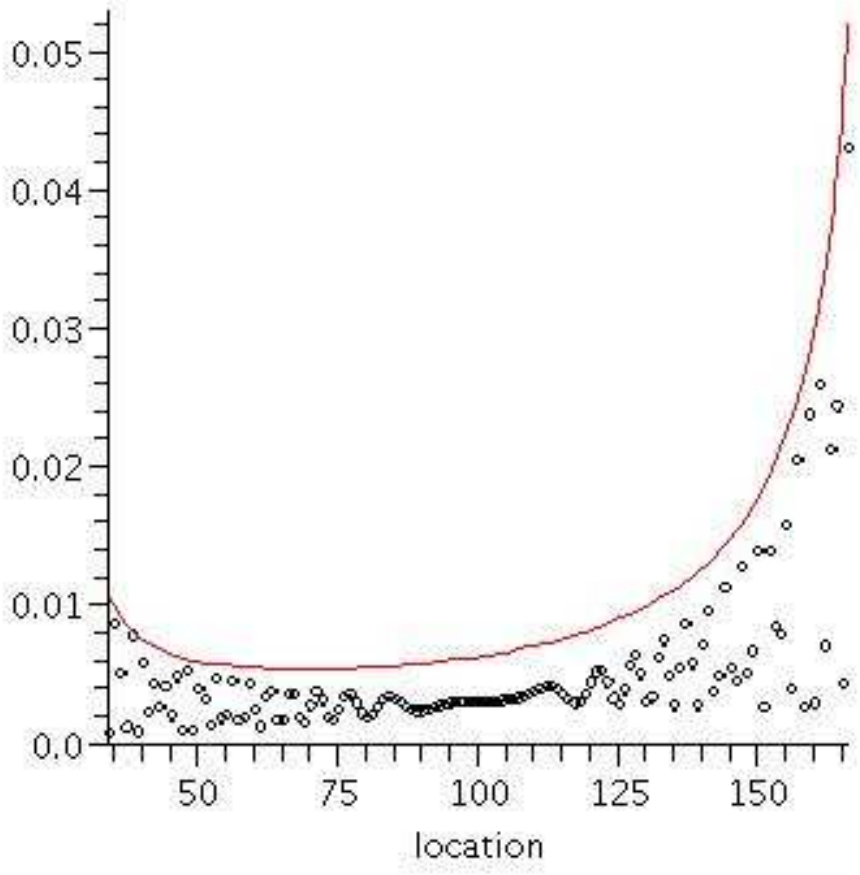

Fig. 1: Time $t = 200$ probability $(p_{\downarrow\uparrow} + p_{\downarrow\downarrow})$ values by location and their upper envelope obtained by dropping the $\cos^2(\rho)$ term

Such illustrations appear in earlier works on QRW such as [ABN$^+$01]. One may generalize the QRW, replacing $U_{\sqrt{\frac{1}{2}}}$ by any unitary matrix U. Except for degenerate choices of U, such as diagonal matrices, the picture remains roughly the same. To be more precise, given a 2×2 unitary matrix U, define $\mathsf{width} = \mathsf{width}(U)$ to be the magnitude of either diagonal entry. For example, the real orthogonal matrix

$$U_c := \begin{pmatrix} c & \sqrt{1-c^2} \\ \sqrt{1-c^2} & -c \end{pmatrix}$$

has $\mathsf{width}(U_c) = c$.

2 Further notation and main results

Given c, we define the interval

$$J := \left[\frac{1-c}{2}, \frac{1+c}{2}\right]. \tag{2.1}$$

Let us relabel our chiralities as $\{\uparrow, \downarrow\}$ instead of $\{L, R\}$ (to avoid collision of notation with the literature). We will also change the shift operator so that one chirality moves right but the other stands still instead of moving left. Doing this removes periodicity from the QRW, which reduces the algebraic complexity of our computations. Letting T denote this shift operator, we then define the general unitary nearest-neighbor QRW on $\mathbb{Z}^1$ to be the operator

$$W := T \cdot (I \otimes U).$$

For any chiralities ξ_0 and ξ, let $\psi_{\xi_0\xi}(r, s)$ denote the amplitude at time s of state (r, ξ) given a delta function at $(0, \xi_0)$ at time zero. Let $p_{\xi_0,\xi}(r, s) := |\psi_{\xi_0,\xi}(r, s)|^2$ denote the corresponding probabilities. Our results may be stated as follows.

Theorem 2.1 (asymptotics inside the interval J) *Given a general unitary walk with transformation U, let c denote* $\mathsf{width}(U)$ *and define J by* (2.1)*. Assume that $0 < c < 1$. Let $\lambda := \frac{r}{s}$. Then there are phase functions $\rho_{\xi_0,\xi}(r, s)$ described in equation* (3.11) *below, such that*

$$p_{\downarrow\downarrow}(r,s) \sim \frac{2}{\pi}\frac{\lambda\sqrt{1-c^2}}{(1-\lambda)s\sqrt{-((1-c^2)-4\lambda+4\lambda^2)}}\cos^2(\rho_{\downarrow\downarrow}(r,s)) \tag{2.2}$$

$$p_{\uparrow\uparrow}(r,s) \sim \frac{2}{\pi}\frac{(1-\lambda)\sqrt{1-c^2}}{\lambda s\sqrt{-((1-c^2)-4\lambda+4\lambda^2)}}\cos^2(\rho_{\uparrow\uparrow}(r,s)) \tag{2.3}$$

$$p_{\downarrow\uparrow}(r,s) \sim \frac{2}{\pi}\frac{\sqrt{1-c^2}}{s\sqrt{-((1-c^2)-4\lambda+4\lambda^2)}}\cos^2(\rho_{\downarrow\uparrow}(r,s)) \tag{2.4}$$

$$p_{\uparrow\downarrow}(r,s) \sim \frac{2}{\pi}\frac{\sqrt{1-c^2}}{s\sqrt{-((1-c^2)-4\lambda+4\lambda^2)}}\cos^2(\rho_{\uparrow\downarrow}(r,s)) \tag{2.5}$$

uniformly as λ varies over any compact subset of the interior of J.

Theorem 2.2 (rapid decay beyond J) *Consider the quantities $p_{\xi_0,\xi}$ for a general unitary QRW with $0 < c < 1$. For each compact $K \subseteq J^c$ and each integer $N > 0$ there is a $C > 0$ such that for any chiralities ξ_0 and ξ,*

$$p_{\xi_0,\xi}(r,s) \le Cs^{-N}$$

whenever $\lambda = r/s \in K$.

Such results have appeared already in the literature. The first rigorous proof of this result (in the special case of the Hadamard QRW) appears in [ABN$^+$01, Theorems 1 and 2]. A better analysis, giving asymptotics near the endpoints of J as well, is given in [CIR03]. The main purpose of this paper is to give a greatly simplified analysis via generating functions, which illuminates the reason for the observed phenomena and which will serve as a basis for analyses of generalizations to higher dimensions, more varied increments, introduction of barriers, and so forth.

The work of [ABN$^+$01] spurred on much related analysis, including that in [AAKV01], [Kem05], [CFG02], and [BMSS02]. The new methods of [CIR03] have simplified analysis and results. Certain generalizations of Hadamard QRW's to more general unitary QRW's were already introduced in [Kon05]. Throughout this paper, we often restrict our attention to the work of Ambainis *et al.* [ABN$^+$01] for means of comparison, as their paper has served as a benchmark since they rediscovered the quantum random walk for its use in quantum computing [Sev03].

3 Proofs

3.1 Generating functions

For any fixed pair of chiralities $(\xi_0, \xi) \in \{\uparrow, \downarrow\} \times \{\uparrow, \downarrow\}$ we can form the bivariate generating function $F_{\xi_0,\xi}(x, y) := \sum_{r,s\in\mathbb{Z}^+} \psi_{\xi_0,\xi}(r, s)x^r y^s$, enumerating paths from $(0, 0)$ with chirality ξ_0 to (r, s) with chirality ξ by position (indexed by $r \in \mathbb{N}$) and time (indexed by $s \in \mathbb{N}$). We then form the generating matrix $\mathbf{F}(x, y)$, defined as:

$$\mathbf{F}(x, y) := \begin{pmatrix} F_{\uparrow\uparrow}(x, y) & F_{\downarrow\uparrow}(x, y) \\ F_{\uparrow\downarrow}(x, y) & F_{\downarrow\downarrow}(x, y) \end{pmatrix}$$

Let us write M for the diagonal matrix of monomials

$$M := \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}.$$

Although we do not consider it in this paper, these notions generalize as follows. Let $\mathbf{v}(1), \ldots \mathbf{v}(k) \in \mathbb{Z}^d$ be any k integer vectors. Let M denote the diagonal matrix with j^{th} diagonal entry $\mathbf{x}^{\mathbf{v}(j)} = x_1^{\mathbf{v}(j)_1} \ldots x_d^{\mathbf{v}(j)_d}$. Then the QRW on $\mathbb{Z}^d$ with increment $\mathbf{v}(j)$ on chirality j, with unitary chirality operator U has generating matrix

$$F_{\xi_0,\xi}(\mathbf{x}, y) := \sum_{\mathbf{r}\in\mathbb{Z}^d, s\in\mathbb{Z}^+} \psi_{\xi_0,\xi}(\mathbf{r}, s)\mathbf{x}^{\mathbf{r}} y^s .$$

A simple application of the transfer matrix method yields the following proposition.

Proposition 3.1 *For any QRW in any dimension,*

$$\mathbf{F}(x, y) = (I - yMU)^{-1} .$$

□

The formula for the entries of the inverse of a matrix allows us to write the entries of $\mathbf{F}$ as rational functions, all with the same denominator $H := \det(I - yMU)$. The numerators will in general differ, thus we have

$$\mathbf{F} = \frac{\mathbf{G}}{H} .$$

Any unitary matrix U with $\mathsf{width}(U) = c$ may be written as

$$U = \begin{pmatrix} ce^{i\alpha} & \sqrt{1-c^2}e^{i\beta} \\ \sqrt{1-c^2}e^{i\gamma} & -ce^{i(\beta+\gamma-\alpha)} \end{pmatrix} .$$

Computing G and H explicitly for this matrix U leads to

$$\mathbf{G}(x, y) = \begin{pmatrix} 1 + ce^{(\beta+\gamma-\alpha)i}xy & e^{\beta i}xy\sqrt{1-c^2} \\ e^{\gamma i}y\sqrt{1-c^2} & 1 - ce^{\alpha i}y \end{pmatrix} \tag{3.1}$$

and

$$H(x, y) = 1 - ce^{\alpha i}y + ce^{(\beta+\gamma-\alpha)i}xy - e^{(\beta+\gamma)i}xy^2 . \tag{3.2}$$

In the case that $U = U_c$ is real, this specializes to

$$\mathbf{G}_c = \begin{pmatrix} 1 + cxy & xy\sqrt{1-c^2} \\ y\sqrt{1-c^2} & 1 - cy \end{pmatrix},$$

$$H_c = 1 - cy + cxy - xy^2 .$$

To see why the only physically relevant parameter is c, observe that the general denominator which we denote $H_{c,\alpha,\beta,\gamma}$ satisfies

$$H_{c,\alpha,\beta,\gamma}(x,y) = H_c\left(e^{i(\beta+\gamma-2\alpha)}x, e^{i\alpha}y\right) \tag{3.3}$$

while the entries of the general numerator $\mathbf{G}_{c,\alpha,\beta,\gamma}(x,y)$ are equal to unit complex multiples of $\mathbf{G}_c(e^{i(\beta+\gamma-2\alpha)}x, e^{i\alpha}y)$. It follows that the coefficients of the generating function $F_{c,\alpha,\beta,\gamma}$ for a general unitary matrix have the same magnitudes as the coefficients of F_c.

3.2 Asymptotics from generating functions

Derivation of the asymptotics of a_{rs} when the generating function is rational is well understood for many cases including the one at hand. The theory was developed in [PW02] and further explained in [PW07]. In those works, a number of concepts are introduced including classification of critical points of pole varieties and conditions under which these can always be found. In our case, the only necessary notation is as follows.

Given a rational generating function $F(x,y) = G(x,y)/H(x,y)$, let $\mathcal{V}$ denote the complex (affine) algebraic curve $\{(x,y) \in \mathbb{C}^2 : H(x,y) = 0\}$. For $(x_0,y_0) \in \mathcal{V}$, denote

$$\mathbf{dir}\,(x_0,y_0) := \left.\frac{yH_y}{xH_x}\right|_{x=x_0,y=y_0}. \tag{3.4}$$

For $a,b > 0$, let $D_{a,b}$ denote the closed polydisk $\{(x,y \in \mathbb{C}^2 : |x| \le a, |y| \le b\}$, let C_a denote the circle $\{x \in \mathbb{C} : |x| = a\}$, and let $T_{a,b}$ denote the torus $C_a \times C_b$. Let

$$\mathcal{V}_1 := \mathcal{V} \cap T_{1,1}$$

denote the intersection of $\mathcal{V}$ with the unit torus. Define

$$Q(x,y) := -y^2H_y^2xH_x - yH_yx^2H_x^2 - x^2y^2(H_y^2H_{xx} + H_x^2H_{yy} - 2H_xH_yH_{xy})\,. \tag{3.5}$$

The main result we need is the upcoming Theorem 3.2. Theorems 2.1 and 2.2 follow from this result together with a short computation that evaluates the expression (3.6) given in Theorem 3.2. We stress that Theorem 3.2 is essentially proved in [PW02]. Therefore, the behavior of one-dimensional QRW as described in Theorem 2.1 and Theorem 2.2 emerge with almost no work. However, because the hypotheses of [PW02, Theorem 3.1] require $\mathcal{V}_1$ to be finite, they exclude the present case. We therefore give a proof of Theorem 3.2 that adapts the proof of [PW02, Theorem 3.1] to the infinite case.

Theorem 3.2 *Suppose that the following conditions hold:*

(i) F *is analytic on* $D_{1,1-\epsilon}$*;*

(ii) $|x| = 1 \Rightarrow |y| = 1$ *on* $\mathcal{V}$*;*

(iii) For each x *the set* $\{y_1(x), \ldots, y_k(x)\}$ *of values for which* $H(x,y) = 0$ *is finite;*

(iv) H_y *is nonvanishing on* $\mathcal{V} \cap T_{1,1}$.

Then the following two conclusions hold.

1. *If* $\lambda := \frac{r}{s}$ *is not in the image under* $\mathbf{dir}$ *of* $\mathcal{V}_1$*, then* a_{rs} *is rapidly decreasing. Specifically, as* λ *varies over a compact set disjoint from the range of* $\mathbf{dir}$*, for every integer* $N > 0$ *there is a* $C > 0$ *such that* $a_{rs} \le Cs^{-N}$.

2. *Conversely, let Λ be a compact subset of the range of* $\mathbf{dir}$ *such that for any $\lambda \in \Lambda$, the set $\Xi(\lambda)$ of points $(x,y) \in \mathcal{V}_1$ for which $\mathbf{dir}\,(x,y) = \lambda$ is finite and neither Q nor G vanishes there. Then*

$$a_{rs} \sim \sum_{(x,y)\in\Xi(r/s)} \frac{G(x,y)}{\sqrt{2\pi}} x^{-r} y^{-s} \sqrt{\frac{-yH_y}{sQ(x,y)}} \tag{3.6}$$

as $r, s \to \infty$, uniformly as r/s varies over Λ.

PROOF: The following successive estimates for a_{rs} mimic the reasoning in [PW02], though they occur in a different order due to differing geometry. We will write down the estimates and then see what is needed to justify them in our case.

$$a_{rs} = \left(\frac{1}{2\pi}\right)^2 \int_{C_1} \int_{C_{1-\epsilon}} x^{-r-1} y^{-s-1} F(x,y)\, dy\, dx\,. \tag{3.7}$$

$$\begin{aligned} a_{rs} &= \left(\frac{1}{2\pi}\right)^2 \left[\int_{C_1} \int_{C_{1+\epsilon}} x^{-r-1} y^{-s-1} F(x,y)\, dy\, dx \right. \\ &\quad \left. - \int_{C_1} \left(\int_{C_{1+\epsilon}} - \int_{C_{1-\epsilon}} \right) x^{-r-1} y^{-s-1} F(x,y)\, dy\, dx \right]\,. \end{aligned} \tag{3.8}$$

$$a_{rs} = \frac{1}{2\pi} \int_{C_1} x^{-r-1} \sum_j y_j^{-s-1} \mathrm{Res}(F; y = y_j)\, dx + O((1+\epsilon)^{-s})\,. \tag{3.9}$$

$$a_{rs} = \frac{1}{2\pi} \int_{C_1} x^{-r-1} \sum_j y_j^{-s-1} \frac{G(x, y_j(x))}{H_y(x, y_j(x))} + O((1+\epsilon)^{-s})\, dx\,. \tag{3.10}$$

The first of these is Cauchy's integral formula. It is valid as long as F is analytic on $D_{1,1-\epsilon}$, which is guaranteed by hypothesis (i). The second is true whenever F is analytic on the torus $T_{1,1+\epsilon}$ as well, which is guaranteed by hypothesis (ii). In the third equation, we have set $y_j = y_j(x)$ to enumerate the values of y making $H(x,y) = 0$ for the given value of x. The third equation is true as long as $F(x,\cdot)$ has finitely many poles on the annulus $1-\epsilon < |y| < 1+\epsilon$ for every $x \in C_1$. This is guaranteed by hypothesis (iii). The fourth of these is true as long as the poles of $H(x,\cdot)$ are always simple, which is guaranteed by hypothesis (iv).

We now observe that $\mathcal{V}_1$ is a smooth 1-manifold and that

$$\eta := x^{-1} y^{-1} \frac{G}{\partial H/\partial y}\, dx$$

pulls back to a smooth form on $\mathcal{V}_1$. In fact, smoothness of the form and the manifold follow from hypothesis (iv) and the implicit function theorem. We therefore arrive at

$$a_{rs} = \frac{1}{2\pi} \int_{\mathcal{V}_1} x^{-r} y^{-s} \eta + O((1+\epsilon)^{-s})\,.$$

It now follows from Proposition 1 of Chapter VIII of [Ste93] that the integral is rapidly decreasing when the function $\log y + \lambda \log x$ on $\mathcal{V}_1$ has no critical points (any branch of the log will yield the same critical points). Critical points of $\log y + \lambda \log x$ on $\mathcal{V}_1$ are exactly those $(x,y) \in \mathcal{V}_1$ for which $\mathbf{dir}\,(x,y) = \lambda$, so the first conclusion of the theorem is established.

Continuing, suppose now that there are critical points $\{(x_l, y_l) : 1 \le l \le L\}$. A partition of unity argument together with Proposition 1 of [Ste93, Chapter VIII] shows that $a_{rs} - \frac{1}{2\pi} \sum_{l=1}^{L} \Xi_l$ is rapidly decreasing, where

$$\Xi_l := \int_{\mathcal{N}_l} x^{-r} y^{-s} \eta$$

and $\mathcal{N}_l$ is a neighborhood of (x_l, y_l) in $\mathcal{V}_1$. The assumption $Q \neq 0$ is equivalent to the critical point for the phase function $\log y + \lambda \log x$ to be quadratically nondegenerate. It remains to plug in a standard stationary phase estimate for Ξ_l. Lemma 4.3 of [PW02] does exactly this: it evaluates the stationary phase integral Ξ_l and shows it to differ from

$$x_l^{-r} y_l^{-s} G(x_l, y_l) \sqrt{\frac{-y_l H_y(x_l, y_l)}{sQ(x_l, y_l)}}$$

by a rapidly decreasing quantity. This establishes the second conclusion of the theorem. □

3.3 Application of asymptotics methods to QRW

We now establish the hypotheses of Theorem 3.2 and apply it to the generating function for QRW. Observe first, using the relation (3.3) and the subsequent discussion, that it suffices to prove both Theorem 2.2 and Theorem 2.1 in the real case, $U = U_c$. Thus we assume throughout this section that $\alpha = \beta = \gamma = 0$ and $U = U_c$.

Proposition 3.3 *The power series F is absolutely convergent on $D_1 \times D_{1-\epsilon}$ for any $\epsilon > 0$.*

PROOF: This is equivalent to finiteness of the sums $\sum_s (1-\epsilon)^s \sum_r |\psi_{\xi_0,\xi}(r,s)|$ for each ξ_0, ξ. Since $|\psi|$ is bounded by 1, the inner sum is bounded by the number of nonzero terms which is $s+1$. Hence the sums converge. □

Proposition 3.4 *For any QRW in any dimension, if $(\mathbf{x}, y) \in \mathcal{V}$ and $|x_j| = 1$ for all j then $|y| = 1$.*

PROOF: When $|x_j| = 1$ for all j, the monomial matrix M is unitary. Therefore the matrix MU is also unitary and the eigenvalues of MU all have modulus 1. Since $\mathbf{H}_{c,\alpha,\beta,\gamma} = \det(I - yMU)$, we see that $\mathbf{H}_{c,\alpha,\beta,\gamma}$ vanishes precisely when $\frac{1}{y}$ is an eigenvalue of MU. Thus $|y| = 1$. □

Proposition 3.5 *For QRW on Z^1 with matrix U_c for $0 < c < 1$, the quantity H_y is nonvanishing on $\mathcal{V}_1$.*

PROOF: Solving $H = 0, H_y = 0$, for example by using Maple to compute a Gröbner basis for `[H , diff(H,y)]`, shows that there are precisely two pairs (x, y); the possible values of y are not on the unit circle except in the degenerate case $c = 1$. □

Lemma 3.6 *Let $(x(\lambda), y(\lambda))$ be any point (x, y) where $H(x, y) = 0$ and $\mathbf{dir}\,(x, y) = \lambda$. Then*

$$(x(\lambda), y(\lambda)) \in T_{1,1} \iff \lambda \in J\,.$$

PROOF: First assume $(x(\lambda), y(\lambda)) \in T_{1,1}$. If we let X and Y be the arguments of x and y respectively, then implicit differentiation of the equation

$$e^{iX} = \frac{1 - ce^{iY}}{e^{iY}(e^{iY} - c)}$$

results in

$$-\mathbf{dir}\,(x, y) = -\frac{xH_x}{yH_y} = \frac{d(\log y)}{d(\log x)} = \frac{dY}{dX} = -\frac{1}{\frac{ce^{iY}}{1-ce^{iY}} + 1 + \frac{e^{iY}}{e^{iY}-c}} = -\left(1 + \frac{c^2 - 1}{2 - 2c \cdot \cos(Y)}\right)$$

when (x, y) is on the unit torus. Thus $\lambda = 1 + \dfrac{c^2 - 1}{2 - 2c \cdot \cos(Y)}$. It is not hard from here to check that as y varies over the unit circle, λ is decreasing in $\mathrm{Re}\,\{y\}$, so that the minimum value of λ is $\lambda(1) = (1-c)/2$, while the maximum is $\lambda(-1) = (1+c)/2$, proving that the image of $\mathcal{V}_1$ under $\mathbf{dir}$ is equal to J.

For the other direction, we choose $\lambda \in J$ and solve for all possible points $(x(\lambda), y(\lambda))$. These solve $H(x,y) = 0$ and $K(x,y) := xH_x - \lambda y H_y = 0$. A convenient way to solve these simultaneous polynomial equations is with Maple's Groebner package. The command `Basis([H,K], plex(y,x))` results in a reduced Groebner basis whose first polynomial is the polynomial satisfied by x over $\mathbb{Z}[\lambda]$:

$$\lambda(1-\lambda)c^2x^2 - [(1-c^2) - (4-2c^2)\lambda + (4-2c^2)\lambda^2]\, x + \lambda(1-\lambda)c^2\,.$$

Viewed as a polynomial in x, the roots are conjugate (possibly equal) if and only if the discriminant is nonpositive, which happens exactly when $\lambda \in J$. The product of the roots is the ratio of the constant to the quadratic coefficient, in this case 1, therefore $\lambda \in J$ implies the two conjugate roots are on the unit circle, hence by Proposition 3.4, $|x| = |y| = 1$ for all critical points. □

PROOF OF THEOREM 2.2: This is immediate from Lemma 3.6 and the first conclusion of Theorem 3.2 once one observes that the hypotheses of Theorem 3.2 are satisfied. The first hypothesis was verified in Proposition 3.3, the second in Proposition 3.4, the third follows whenever H has no factor $P(x)$, and the fourth is Proposition 3.5. □

PROOF OF THEOREM 2.1: Having verified the hypotheses of Theorem 3.2, it remains to compute (3.6) in the case where $\lambda \in J$. The hypothesis $Q \neq 0$ is then equivalent to λ being in the interior of J. Assuming this, we finish the computation as follows.

Consider the first estimate (2.2) in Theorem 2.1. Recalling that $G_{\downarrow\downarrow}(x,y) = 1 - cy$ and observing that the two summands in (3.6) are conjugates, we see that

$$\psi_{\downarrow\downarrow}(r,s) \sim 2\mathrm{Re}\left\{\frac{1-cy}{\sqrt{2\pi}} x^{-r} y^{-s} \sqrt{\frac{-yH_y}{sQ(x,y)}}\right\}$$

where Q is given in (3.5). Letting

$$\rho_{\downarrow\downarrow}(r,s) := \mathrm{Arg}\left(\frac{1-cy}{\sqrt{2\pi}} x^{-r} y^{-s} \sqrt{\frac{-yH_y}{sQ(x,y)}}\right)\,, \tag{3.11}$$

allows us to rewrite this as

$$p_{\downarrow\downarrow}(r,s) \sim \frac{2}{\pi}\cos^2\rho_{\downarrow\downarrow}(r,s)\left|(1-cy)^2\frac{-yH_y}{sQ(x,y)}\right|\,.$$

Instead of solving for x and y and plugging into expressions for H_y and Q, the computations are simplified by finding directly the minimal polynomial for $w := (1-cy)^2\frac{-yH_y}{sQ(x,y)}$.

Recalling that (x,y) satisfies $H(x,y) = K(x,y) = 0$, we introduce a variable $z := 1/(sQ)$ so that w may be expressed as the first coordinate of the simultaneous root (w,x,y,z) of four polynomials: $H, K, zsQ - 1$ and $w + (1-cy)^2 y H_y z$. To obtain a polynomial in w alone, we use the `Basis` command with term order `plex(x,y,z,w)`, resulting in the polynomial

$$r^2(1-c^2) + 4\left(\frac{s(1+c)}{2} - r\right)\left(r - \frac{s(1-c)}{2}\right)(s-r)^2w^2\,.$$

After dividing by s^2 and letting $\lambda = \frac{r}{s}$, it follows that

$$|w| = \frac{\sqrt{1-c^2}\lambda}{(1-\lambda)s\sqrt{-((1-c^2) - 4\lambda + 4\lambda^2)}}\,.$$

This proves (2.2). The computations for the other three cases are slight variations, the only difference being the value of $G_{\xi_0,\xi}(x,y)$. □

References

[AAKV01] Dorit Aharonov, Andris Ambainis, Julia Kempe, and Umesh Vazirani. Quantum walks on graphs. *arXiv*, quant-ph/0012090:10, 2001.

[ABN+01] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J Watrous. One-dimensional quantum random walk. In *Proceedings of the 33rd Annual AMC Symposium on Theory of Computing*, pages 37–49. ACM Press, New York, 2001.

[ADZ93] Y. Aharonov, L. Davidovich, and N. Zagury. Quantum random walks. *Phys. Rev. A*, 48:1687–1690, 1993.

[BMSS02] S. D. Bartlett, T. D. Mackay, B. C. Sanders, and L. T. Stephenson. Quantum walks in higher dimensions. *J. Phys. A*, 35:2745–2753, 2002.

[CFG02] Andrew M. Childs, Edward Farhi, and Sam Gutmann. An example of the difference between quantum and classical random walks. *Quantum Information Processing*, 1:35–43, 2002.

[CIR03] Hilary A. Carteret, Mourad E. H. Ismail, and Bruce Richmond. Three routes to the exact asymptotics for the one-dimensional quantum walk. *J. Phys. A*, 36:8775–8795, 2003.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. *Annual ACM Symposium on Theory of Computing*, pages 212–219, 1996. Proceedings of the twenty-eighth annual ACM symposium on Theory of computing.

[Kem05] Julia Kempe. Quantum random walks hit exponentially faster. *Prob. Theory Related Fields*, 133(2):215–235, 2005.

[Kon05] Norio Konno. A new type of limit theorems for the one-dimensional quantum random walk. *Journal of the Mathematical Society of Japan*, 57:1179–1195, 2005.

[Mey96] D. Meyer. From quantum cellular automata to quantum lattice gases. *Journal Stat. Phys.*, 85:551–574, 1996.

[NC00] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[PW02] R. Pemantle and M. Wilson. Asymptotics of multivariate sequences. I. Smooth points of the singular variety. *J. Combin. Theory Ser. A*, 97(1):129–161, 2002.

[PW07] R. Pemantle and M. Wilson. Twenty combinatorial examples of asymptotics derived from multivariate generating functions. *SIAM Review*, to appear, 2007.

[Sev03] Simone Severini. On the digraph of a unitary matrix. *SIAM Journal on Matrix Analysis and Applications*, 25:295–300, 2003.

[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.*, 26:1484–1509, 1997.

[Ste93] Elias M. Stein. *Harmonic Analysis: Real-Variable Methods, Orthogonality, and Oscillatory Integrals*. Princeton University Press, Princeton, NJ, 1993. With the assistance of Timothy S. Murphy, Monographs in Harmonic Analysis, III.