Central European Science Journals
www.cesj.com

Central European Journal of Physics
Central European Science Journals
CEJP 4 (2003) 556–573

Two Models of Quantum Random Walk

Jozef Košík*

Research Centre for Quantum Information,
Slovak Academy of Sciences,
Dúbravská cesta 9, 845 11 Bratislava, Slovakia

Received 24 March 2003; accepted 24 June 2003

Abstract: We present an overview of two models of quantum random walk. In the first model, the discrete quantum random walk, we present the explicit solution for the recurring amplitude of the quantum random walk on a one-dimensional lattice. We also introduce a new method of solving the problem of random walk in the most general case and use it to derive the hitting amplitude for quantum random walk on the hypercube. The second is a special model based on a local interaction between neighboring spin-1/2 particles on a one-dimensional lattice. We present explicit results for the relevant quantities and obtain an upper bound on the speed of convergence to limiting probability distribution.

Keywords: quantum information, random walk, hypercube
PACS (2000): 03.67.-a,05.40.-a

1 Introduction

Random walks constitute an important tool used in computational mathematics to solve various problems, mostly connected to exploring large combinatorial structures. The randomized methods (Monte Carlo methods) provide some insight into problems which could not otherwise be handled using the brute computational force, such as finding the Hamiltonian or Eulerian cycle in a given graph, or finding the shortest Hamiltonian cycle in a weighted graph (the travelling salesman problem). Other examples include 2- and 3-SAT problems, to name a few. For more on problems of this sort, see [12], p. 141ff.

With the advent of quantum information theory a new way of running algorithms on physical hardware has emerged: by encoding the information in qubits, the two-level quantum systems, we can manipulate the qubits using unitary operations, and readout

* E-mail: jkosik@post.sk

the result of this manipulation thereafter. If we can simulate all the logic gates from classical computers, we can (in principle) run the classical software on this new basis. The fundamental difference is, that while the classical computer accepts only one input at a time, we can feed the quantum computers with the coherent superposition of many input states, and run the computation simultaneously, thus attaining exponential speedup (with respect to the length of bit string used at the input) over the classical computer. Unfortunately, there is no simple way to actually check all the parts of the superposition at the output: the projection postulate forbids this! However, some successful attempts have been made to find an effective quantum algorithm: the best known is the Shor algorithm for factoring of integers [4].

Still, the community of researchers is lacking good new algorithms. One direction of research is toward the investigation of random walks and the effort is made to implement them on the quantum level, and possibly to devise some real new algorithm. Quantum random walks (which is the term used to denote the yet unspecified process which mimic the classical random walks) have interesting properties, which may eventually turn out to be the basis of possible improvements in the performance with respect to classical algorithms.

Some distinct types of quantum random walk have been proposed in the literature. They may be discrete or continuous in time, i.e. their evolution may be governed either by a sequence of unitary operators, or a Hamiltonian. The first method has been proposed in [2].

1.1 Discrete quantum random walk

It may be conceived as a particle bound to a line (or any graph, in general), which may occupy a set of nodes, or vertices of the graph. The vertices are effectively the position states of the particle, denoted $|x\rangle$. The elements x form an additive group G. Now we may apply the unitary operator S_a on the position states to obtain new ones: $S_a|x\rangle = |x+e_a\rangle$. The set of elements $\{e_a\}$ generates the group G, i.e. any element x may be written as the sum of some e_a-s. For a random walk, it should be a matter of chance, which unitary operator S_a will be applied to the state $|x\rangle$ at a time. By including any random factor in the evolution, the state of the particle would be described by a density matrix rather than by a vector of Hilbert space – the coherence of the state would be lost. Instead, we augment the state of the particle by some internal degrees of freedom, which affect the route it will take in the next step: let $|\chi\rangle = \sum \gamma_a |e_a\rangle$ be the superposition of the states associated with the generators of G. Now if the particle is in the state $|x\rangle|\chi\rangle$, the step of the quantum random walk will be

$$S|x\rangle = \sum_a \gamma_a |x + e_a\rangle|a\rangle$$

that is, we move (in superposition) in each direction, determined by $\{e_a\}$. The Hilbert space spanned by $\{|e_a\rangle\}$ is sometimes called the coin space, since it effectively acts as the coin on which the result of the evolution in the next step depends. To include some quasi-randomness in the whole process, we shuffle the amplitudes of $|\chi\rangle$ at each step: we simply apply some unitary operator C like $|\chi\rangle \rightarrow C|\chi\rangle$. Now one step of this type of random walk is generated by the unitary operator

$$U = S(I \otimes C)$$

This type of quantum random walk is sometimes referred to as the coined quantum random walk.

The quantum random walk induces a probability distribution over the vertices, given by the expectation value of the observables $|x\rangle\langle x| \otimes I$. It has been shown [2] that the time-averaged probability distribution of the coined quantum random walk on Cayley graph, based on commutative group G converges to a limit, which is independent of the initial state of the particle. On the other hand, the probability distribution as such does not converge to a limit, unless $\langle\psi|U|\psi\rangle = 0$ for some initial state $|\psi\rangle$ of the particle. On the contrary, the classical random walk on an undirected graph, where the probability of a step along an edge which emanates from a vertex with degree d is $\frac{1}{d}$, always has a limit for the probability distribution. Moreover, the limiting distribution is uniform over the vertices of the graph, if the graph is d-regular, i.e. all its vertices have the same degree d.

There are not only qualitative, but also quantitative differences between classical and quantum random walks. While the classical random walk on the line is well known (its probability distribution is the Gaussian distribution with variance proportional to the number of steps), the coined quantum random walk on the line has been studied in [11] and [3]. Roughly speaking, they discovered, that the quantum random walk spreads quadratically faster than its classical counterpart (measured by the variance of the probability distribution); that, unlike the Gaussian distribution, the probability distribution of quantum random walk has sharp peaks near the front (whence the previous statement is more understandable), and that the probability distribution of quantum random walk may be asymmetric, depending on the initial state of the augmentation vector (in [6] the conditions for the symmetry are formulated).

1.2 Continuous quantum random walk

Another approach was sketched in [13]. The evolution of the particle depends on a continuously varying time parameter, and is generated by a Hamiltonian, which is chosen so as to mimic the stochastic matrix for a continuous classical random walk. We do not need any auxiliary degrees of freedom; we only need to identify the vertices of some graph on which the walk happens to be with position states of a quantum particle. In the original article [13] the authors have investigated how fast the particle will reach a given vertex, starting from a certain vertex, for a special graph. In general, this model has not been studied yet, though it seems more promising from the point of view of its physical implementation.

1.3 Our results

We will be dealing with both types of quantum random walks. For the discrete case, we will investigate (in the section 2) the walk on the line and give an explicit formula for the projection of the state of the particle on the vertex where the walk starts. We also present a new and simple formula (sec. 2.1), based on the path integral approach, which enables us to compute the state of the particle for any graph and any coin. Using this formula we show that the quantum random walk on the hypercube is in some respects faster than the corresponding one in classical case. For the continuous case, we present a new model based on the Ising-type interaction analogy (sec. 3), and give explicit formulas for its evolution. We show that the probability distribution associated with it converges to a limit, which (unlike the classical case) is biased, depending on the initial conditions. We also give an upper bound on the speed of convergence to the limiting distribution.

2 Discrete quantum random walk

We are going to deal with coined discrete quantum random walk on the line. We start with some rigorous notation.

Let $\mathcal{H}_X = \mathrm{span}\{|x\rangle : x \in \mathbb{Z}\}$ be the Hilbert space of the position of a particle (which is bounded to a line, and can only occupy a countable number of vertices), and $\mathcal{H}_A = \mathrm{span}\{|a\rangle : a = L, R\}$ be the Hilbert space of the internal degrees of freedom of the particle (the *chirality*). We also will refer to $\mathcal{H}_A$ as the *coin-space*. Now the state of the particle is $|\psi\rangle \in \mathcal{H}_X \otimes \mathcal{H}_A$, and it evolves in steps by application of the unitary operator $U = S(I \otimes C)$, where C is some unitary operator acting on $\mathcal{H}_A$ (we call it the *coin*) and

$$S = \sum_{x\in\mathbb{Z}} \sum_{a\in\{L,R\}} |x-1\rangle\langle x| \otimes |L\rangle\langle L| + |x+1\rangle\langle x| \otimes |R\rangle\langle R| \, .$$

Hence, the particle moves to the left ($|x\rangle \to |x-1\rangle$) if its internal state is L, and to the right ($|R\rangle \to |x+1\rangle$), if its internal state is R. Let $|\psi_n\rangle = U^n|\psi_0\rangle$, if $|\psi_0\rangle$ is the initial state of the particle. We choose the operator C to be the Hadamard matrix, the 2-dimensional Fourier transform. In the basis $(|L\rangle, |R\rangle)$, its matrix form is

$$C = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{1}$$

Since the operator U is translationally invariant ($UT = TU$, where T is translational matrix, $T = \sum_x |x\rangle\langle x+1| \otimes I$), we may use the Fourier transform [11]: first, if $|\psi\rangle = \sum_x |x\rangle|\chi_x\rangle$ then let

$$|\chi_x\rangle = \frac{1}{2\pi} \int_{-\pi}^{\pi} d\theta \; e^{i\theta x} |\tilde{\chi}_\theta\rangle \, . \tag{2}$$

Then the action of U on any state looks like

$$\begin{aligned} U|\psi\rangle &= S\sum_x |x\rangle C|\chi_x\rangle \\ &= S\sum_x |x\rangle\Big(\langle L|C|\chi_x\rangle|L\rangle + \langle R|C|\chi_x\rangle|R\rangle\Big) \\ &= \sum_x \Big(|x-1\rangle\langle L|C|\chi_x\rangle|L\rangle + |x+1\rangle\langle R|C|\chi_x\rangle|R\rangle\Big) \\ &= \sum_x |x\rangle\Big(\langle L|C|\chi_{x+1}\rangle|L\rangle + \langle R|C|\chi_{x-1}\rangle|R\rangle\Big). \end{aligned} \tag{3}$$

Substituting (2) into (3) we get

$$U|\psi\rangle = \sum_x |x\rangle \frac{1}{2\pi}\int_{-\pi}^{\pi} d\theta\, \Big(e^{i\theta}\langle L|C|\tilde{\chi}_\theta\rangle|L\rangle + e^{-i\theta}\langle R|C|\tilde{\chi}_\theta\rangle|R\rangle\Big)e^{i\theta x}. \tag{4}$$

Effectively, one step of quantum random walk rotates the transformed chirality $|\tilde{\chi}_\theta\rangle$ of the particle with the operator, which in the basis $(|L\rangle,|R\rangle)$ is the matrix

$$M = \frac{1}{\sqrt{2}}\begin{pmatrix} e^{i\theta} & e^{i\theta} \\ e^{-i\theta} & -e^{-i\theta}, \end{pmatrix} \tag{5}$$

hence to determine the operator U^n, we need to evaluate M^n and then to integrate over $[-\pi,\pi]$ with respect to $d\theta\, e^{i\theta x}$ to obtain the probability distribution $p(n,x) = \langle\psi_n||x\rangle\langle x|\otimes I|\psi_n\rangle$. Unless stated otherwise, we understand the initial state of the particle to be $|\psi_0\rangle = |0\rangle|\chi\rangle$, i.e. the particle is localized at the 0^{th} vertex at the beginning, and has some chirality $|\chi\rangle$. We obtain M^n in a straightforward manner using the eigenvector expansion of M. Denoting

$$M^n = \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix},$$

we obtain the coefficients in the above expression as follows:

$$\begin{aligned} \alpha_1 &= 2^{-1}\left\{\Big((-1)^n e^{-in\omega} + e^{in\omega}\Big) + \frac{\cos\theta}{\sqrt{1+\cos^2\theta}}\Big(-(-1)^n e^{-in\omega} + e^{in\omega}\Big)\right\} \\ \alpha_2 &= \frac{2^{-1}e^{i\theta}}{\sqrt{1+\cos^2\theta}}\left\{-(-1)^n e^{-in\omega} + e^{in\omega}\right\} \\ \alpha_3 &= \frac{2^{-1}e^{-i\theta}}{\sqrt{1+\cos^2\theta}}\left\{-(-1)^n e^{-in\omega} + e^{in\omega}\right\} \\ \alpha_4 &= 2^{-1}\left\{\Big((-1)^n e^{-in\omega} + e^{in\omega}\Big) - \frac{\cos\theta}{\sqrt{1+\cos^2\theta}}\Big(-(-1)^n e^{-in\omega} + e^{in\omega}\Big)\right\}. \end{aligned} \tag{6}$$

with $\omega \equiv \arctan\frac{\sqrt{2}\sin\theta}{\sqrt{3+\cos 2\theta}}$.

Now we need to evaluate the integral $\frac{1}{2\pi}\int_{-\pi}^{\pi} e^{i\theta x}\alpha_j\ d\theta;\ j = 1,\ldots,4$ (we omit the explicit dependence of α_j, ω on θ in the notation). This is hard to do except for $x = 0$. If the initial state is $|\psi_0\rangle = |0\rangle|\chi_0\rangle$, then $p(n, 0) = \|M^n|\chi_0\rangle\|^2$, since the inverse Fourier transform is $|\tilde{\chi}_\theta\rangle = \sum_x e^{-i\theta x}|\chi_x\rangle$.

The terms in (6) contain odd and even functions. The functions $\cos n\omega$, $\frac{1}{\sqrt{1+\cos^2\theta}}$ are even, while $\sin n\omega$ is odd. Their products may vanish if we integrate over $[-\pi, \pi]$. Then, we are left with the effective coefficients of M ($\alpha_1 \to \alpha_1'$, etc., and $\alpha_j'(e)$ $[\alpha_j'(o)]$ means that α_j takes the given value for n even [odd])

$$\begin{aligned}
\alpha_1'(e) &= \cos n\omega \\
\alpha_1'(o) &= \frac{\cos\theta}{\sqrt{1+\cos^2\theta}}\cos n\omega \\
\alpha_2'(e) &= \frac{-\sin n\omega}{\sqrt{1+\cos^2\theta}}\sin\theta \\
\alpha_2'(o) &= \frac{\cos n\omega}{\sqrt{1+\cos^2\theta}}\cos\theta \\
\alpha_3'(e) &= -\alpha_2'(e) \\
\alpha_3'(o) &= \alpha_2'(o) \\
\alpha_4'(e) &= \alpha_1'(e) \\
\alpha_4'(o) &= -\alpha_1'(o)\,.
\end{aligned} \tag{7}$$

This already seems to be fairly simple. Now all we need to do is to integrate two functions

$$f_A(\theta) = \cos n\omega \tag{8}$$

$$f_B(\theta) = \frac{\sin n\omega}{\sqrt{1+\cos^2\theta}}\sin\theta = \sin n\omega\tan\omega \tag{9}$$

We may expand the formula (8) using several identities. First note that †

$$\frac{i}{2}\left(\ln(1-ix) - \ln(1+ix)\right) = \arctan x$$

From the complex expansion of $\cos(n\arctan x)$ we get

$$\cos(n\arctan x) = \frac{(1-i\,x)^n + (1+i\,x)^n}{2\,(1+x^2)^{\frac{n}{2}}}\,. \tag{10}$$

Substituting $x = \frac{\sin\theta}{\sqrt{1+\cos^2\theta}}$ in (10) and from

$$\sqrt{1+x^2} = \sqrt{\frac{2}{1+\cos^2\theta}}\,, \tag{11}$$

we may transform the integral of $f_A(\theta)$ to the sum of integrals of the form

$$\int f_A(\theta)\,d\theta = \int R\left(\sin\theta, \cos\theta, \sqrt{1-r^2\sin^2\theta}\right)\,d\theta\,, \tag{12}$$

† We remind ourselves that the complex logarithm is $\ln(re^{i\theta}) = \ln r + i\theta$

where R is the rational function of the respective coefficients. These integrals have analytical solutions in many cases. The exact form of $R \equiv R_A$ is (with n even)

$$\begin{aligned} R_A &= 2^{-1-n/2}\left\{\left(\sqrt{2-\sin^2\theta}-i\sin\theta\right)^n+\left(\sqrt{2-\sin^2\theta}+i\sin\theta\right)^n\right\} \\ &= 2^{-1-n/2}\sum_{k=0}^{n}\binom{n}{k}\left(\sqrt{2-\sin^2\theta}\right)^{n-k}\sin^k\theta\left[(-i)^k+i^k\right] \\ &= 2^{-1-n/2}\sum_{k=0}^{n/2}\binom{n}{2k}\left(\sqrt{2-\sin^2\theta}\right)^{n-2k}\sin^{2k}\theta\; 2(-1)^k \\ &= 2^{-n/2}\sum_{k=0}^{n/2}\binom{n}{2k}(-1)^k\left(2-\sin^2\theta\right)^{(n-2k)/2}\sin^{2k}\theta\,. \end{aligned} \tag{13}$$

On integration we get

$$\begin{aligned} \alpha_1'(e) &= \frac{1}{2\pi}\int_{-\pi}^{\pi}R_A\,d\theta\frac{2^{1-n/2}}{\pi}\int_0^{\pi/2}d\theta\sum_{k=0}^{n/2}\binom{n}{2k}(-1)^k\left(2-\sin^2\theta\right)^{(n-2k)/2}\sin^{2k}\theta \\ &= \frac{2^{1-n/2}}{\pi}\sum_{k=0}^{n/2}\binom{n}{2k}(-1)^k\int_0^{\pi/2}d\theta\left(2-\sin^2\theta\right)^{(n-2k)/2}\sin^{2k}\theta \\ &= \frac{2^{1-n/2}}{\pi}\sum_{k=0}^{n/2}\binom{n}{2k}(-1)^k\int_0^{\pi/2}d\theta\sum_{j=0}^{n/2-k}\binom{\frac{n}{2}-k}{j}2^{n/2-k-j}\sin^{2j}\theta\,(-1)^j\sin^{2k}\theta \\ &= \frac{2}{\pi}\sum_{k=0}^{n/2}\sum_{j=0}^{n/2-k}\binom{n}{2k}\binom{\frac{n}{2}-k}{j}\frac{(-1)^{k+j}}{2^{k+j}}\frac{[2(k+j)-1]!!}{[2(k+j)]!!}\frac{\pi}{2}\,, \end{aligned} \tag{14}$$

where we have used the fact that

$$\int_0^{\pi/2}\sin^{2m}\theta\,d\theta = \frac{(2m-1)!!}{(2m)!!}\frac{\pi}{2} \tag{15}$$

The reduction of formula (9) is analogous:

$$\sin(n\arctan x)x = \frac{\frac{i}{2}\left((1-i\,x)^n-(1+i\,x)^n\right)x}{(1+x^2)^{\frac{n}{2}}}\,. \tag{16}$$

Setting $x \to \frac{\sin\theta}{\sqrt{1+\cos^2\theta}}$ we get

$$\begin{aligned} R_B &= i2^{-1-n/2}\frac{\sin\theta}{\sqrt{2-\sin^2\theta}}\left\{\left(\sqrt{2-\sin^2\theta}-i\sin\theta\right)^n-\left(\sqrt{2-\sin^2\theta}+i\sin\theta\right)^n\right\} \\ &= 2^{-n/2}\frac{\sin\theta}{\sqrt{2-\sin^2\theta}}\sum_{k=0}^{n/2}\binom{n}{2k+1}(-1)^k\left(2-\sin^2\theta\right)^{(n-2k-1)/2}\sin^{2k+1}\theta \\ &= 2^{-n/2}\sum_{k=0}^{n/2}\binom{n}{2k+1}(-1)^k(2-\sin^2\theta)^{(n-2k-2)/2}\sin^{2k+2}\theta\,. \end{aligned} \tag{17}$$

Then we obtain upon integration

$$
\begin{aligned}
\alpha_2'(e) &= \frac{1}{2\pi}\int_{-\pi}^{\pi} R_B\, d\theta \\
&= \frac{2^{1-n/2}}{\pi}\sum_{k=0}^{n/2}\binom{n}{2k+1}(-1)^k\int_0^{\pi/2} d\theta(2-\sin^2\theta)^{(n-2k-2)/2}\sin^{2k+2}\theta \\
&= \frac{2^{1-n/2}}{\pi}\sum_{k=0}^{n/2}\binom{n}{2k+1}(-1)^k\int_0^{\pi/2} d\theta \\
&\quad\times\sum_{j=0}^{n/2-k-1}\binom{\frac{n}{2}-k-1}{j}2^{n/2-k-j-1}\sin^{2j}\theta(-1)^j\sin^{2k+2}\theta \\
&= \frac{1}{\pi}\sum_{k=0}^{n/2}\sum_{j=0}^{n/2-k-1}\binom{n}{2k+1}\binom{\frac{n}{2}-k-1}{j}\frac{(-1)^{k+j}}{2^{k+j}}\frac{[2(k+j)+1]!!}{[2(k+j)+2]!!}\frac{\pi}{2}\,.
\end{aligned}
\tag{18}
$$

The coefficients

$$
\left.
\begin{aligned}
&\alpha_1'(e) \\
&\alpha_2'(e) \\
&\alpha_3'(e) = -\alpha_2'(e) \\
&\alpha_4'(e) = \ \ \alpha_1'(e)
\end{aligned}
\right\}
\tag{19}
$$

are the elements of the matrix M, which transform the initial chirality of the particle at the 0-th vertex in n steps of Hadamard walk, where n is even number. Now the probability distribution $p(n,x)$ of the quantum random walk on the line with coin (1), and initial chirality $(\gamma_L,\gamma_R)^T$ is

$$
p(n,0) = \begin{cases}
\left\| \begin{pmatrix} \alpha_1'(e) & \alpha_2'(e) \\ \alpha_3'(e) & \alpha_4'(e) \end{pmatrix} \begin{pmatrix} \gamma_L \\ \gamma_R \end{pmatrix} \right\|^2 & : \quad n \text{ even} \\
0 & : \quad n \text{ odd}
\end{cases}
\tag{20}
$$

where the respective coefficients are from the equations (14), (18) and (19). This is the main result in this section.

Conclusion

We have given the explicit solution for the probability, that the zeroth vertex is occupied after n steps of the discrete quantum random walk on the line with Hadamard coin, when the initial state is of $|0\rangle|\chi\rangle$ (the particle is initially localized at the 0-th vertex, with any chirality $|\chi\rangle$). The formula $p(n,0)$ is that of (20).

2.1 Path integral and discrete quantum random walk

The above method of computing the relevant amplitudes of quantum random walk is too cumbersome to generalize to other graphs and other coins. In [11] the formulas which resulted from the Fourier transform (such as in (6)) have been approximately integrated using the method of stationary phase, which gave some asymptotic results for large n. In particular, it revealed the existence of peaks in the probability distribution shifted towards the boundaries of the probability distribution (the vertices $\pm n$ for the n^{th} step). Other authors ([6, 3], also [8] in a different context) have also used the path integral method to derive similar results. While their methods have presupposed concrete graphs (the line) and 2-dimensional coin, we now give the general formula for the path integral of the discrete quantum random walk on any d-regular graph, with any unitary coin.

The path integral formula

Let $\mathcal{G}$ be a Cayley graph on an additive commutative group $(G, +)$, which is generated by a subset $A \subset G$. That is, G is the set of vertices of $\mathcal{G}$ and there is an edge between the vertices x_1, x_2, if and only if there is $a \in A$ such that $x_2 = ax_1$. Let the initial state of discrete quantum random walk on this graph be $|x_0\rangle|a_0\rangle$, and the coin be an unitary operator C. The coin space is $\mathcal{H}_A = \text{span}\{|a\rangle : a \in A\}$. Now we resort to intuitive reasoning: Consider the particle in the state $|\psi\rangle = |xa\rangle$. Backtracking $|\psi\rangle$ to the previous step we see that $S^{-1}|\psi\rangle = |x-a\rangle|a\rangle$. By another backtrack step we get $(I\otimes C)^{-1}S^{-1}|\psi\rangle = \sum_{a'} |x-a\rangle\langle a|C|a'\rangle|a\rangle$ Finally, the amplitude corresponding to the random walk starting at $|x_0\rangle|a_0\rangle$ and following the sequence of edges $(a_0a_1), (a_1a_2), \ldots, (a_{n-1}a_n)$ in n steps, is

$$\Gamma(a_0, a_1, \ldots, a_n) = \langle a_n|C|a_{n-1}\rangle\langle a_{n-1}|C|a_{n-2}\rangle \ldots \langle a_1|C|a_0\rangle \tag{21}$$

whence the particle moves from the vertex x_0 to the vertex $x = x_0 + a_1 + a_2 + \cdots + a_n$ and ends up with the chirality $|a_n\rangle$. The overall amplitude that the particle will move from x_0 to x is given by the sum along all the paths, which connect x_0 and x, weighed by (21), i.e. if U is the operator of one step of the random walk, then

$$(|x\rangle\langle x| \otimes I)U^n|x_0\rangle|a_0\rangle = |x\rangle \otimes \sum_{\substack{\text{paths } x_0 \to x \\ \text{in } n \text{ steps} \\ x = x_0 + a_1 + \cdots + a_n}} \Gamma(a_0, a_1, \ldots, a_n)|a_n\rangle \tag{22}$$

Of course, the probability distribution is $p(n, x) = \|\langle x|\psi_n\rangle\|^2$, where $\langle x|\psi_n\rangle$ is the projection of $|\psi_n\rangle$ on $|x\rangle\langle x| \otimes I$. We show an example of how this sum can be evaluated for a simple (non-unitary) coin.

The example: Hypercube

The hypercube of dimension d is the graph, where each vertex is connected with d adjacent vertices. In mathematical terms, it is the Cayley graph on the additive group $\{0, 1\}^d =$

$\mathbb{Z}_{2^d}$, with the generating set $A = \{e_a : e_a = 2^a, a = 1, \dots d\}$. The vertices may be conceived as the bit strings x with length d, and the generators as the bit strings e_a with length d, which have zeros everywhere but at the a-th position, $a = 1, \dots, d$. Each vertex x has its Hamming weight $w_H(x)$ (the number of ones in the bit string) and each two vertices have Hamming distance $d_H(x, y)$ (the minimum number of bits we need to flip to change x to y). Let the discrete quantum random walk start at the position $x_0 = 0^d$. Then every other vertex x has Hamming distance from x_0 equal to its Hamming weight. How many paths of length n are there between x_0 and x? It is easier to consider only the recurring paths (which start and end at the same vertex) and hitting paths (which reach some fixed vertex with $w_H = n$ from vertex with $w_H = 0$ in n steps). The number of hitting paths (length n) is clearly $W^{\text{hit}}(n) = n!$. For the number of recurring paths starting at vertex 0^d we are free to apply $2k_j$ flips on each j^{th} bit ($k_j = 0, 1, \dots$) , such that $k_1 + \cdots + k_d = \frac{n}{2}$. An elementary combinatorial result states that given d non-negative integers, which sum up to m, we can assign values to the integers in $\binom{m+d-1}{d-1}$ ways, if the order of the integers matters. Applying this result to our problem, we determine that there are

$$W^{\text{recur}}(n) = \binom{n/2 + d - 1}{d - 1} \tag{23}$$

ways to get from $x_0 = 0^d$ back to x_0 in n steps. For the classical random walk on the hypercube, where the probability of moving from a given vertex to an adjacent one is $\frac{1}{d}$, the factor associated with each path of length n is $\frac{1}{d^n}$. For the quantum random walk, the phase associated with each of the paths may differ, due to the mixing properties of the coin matrix C. Quantum random walks on the hypercube have been analyzed in [5, 7] for a special coin, the Grover coin:

$$G_d = \begin{pmatrix} \frac{2}{d} - 1 & \frac{2}{d} & \dots & \dots \\ \frac{2}{d} & \frac{2}{d} - 1 & \frac{2}{d} & \dots \\ \vdots & \vdots & \ddots & \dots \end{pmatrix} \tag{24}$$

and the eigenstate of the evolution operator was found. In the following, a shall denote the diagonal terms, and b the non-diagonal ones. Using the path integral method, we may obtain a direct insight into the structure of the walk: let the initial state be $|\psi_0\rangle = |0^d\rangle \otimes \frac{1}{\sqrt{d}}(|e_1\rangle + \cdots + |e_d\rangle)$, where $e_j, j = 1, \dots, d$ are the vertices with Hamming weight unity. The walk will be symmetric over the layers $\ell_1, \dots, \ell_d$, where ℓ_j is the set of all vertices with Hamming weight j. The first step of quantum random walk will transform the initial state $|\psi_0\rangle = |0^d\rangle|\chi_0\rangle$, where $|\chi_0\rangle = \frac{1}{\sqrt{d}}(1, \dots, 1)$ in the basis $(|e_1\rangle, \dots, |e_d\rangle)$:

$$|\psi_0\rangle \to \sum_{k=1}^{d} |e_k\rangle\langle e_k|G_d|\chi_0\rangle|e_k\rangle \tag{25}$$

$$= \sum_{k=1}^{d} |e_k\rangle \frac{1}{\sqrt{d}}(a + (d-1)b)|e_k\rangle\,. \tag{26}$$

Now the particle occupies each vertex with Hamming weight unity (in coherent superposition); its chirality is $|e_k\rangle$, where e_k is the respective vertex; its amplitude is $\frac{1}{\sqrt{d}}(a+b(d-1))$. We will investigate the probability that the particle will hit the farthest vertex of the hypercube (Hamming weight d) in d steps. After the first step, every other step in the "correct" direction (increasing the Hamming weight by one) will add the factor b to the path integral (total factor of b^{d-1}). The number of possible paths from a fixed vertex with $w_H = 1$ to a fixed vertex with $w_H = d$ in $(d-1)$ steps is $(d-1)!$. From symmetry we see that, after d steps the state of the particle projected on the vertex with Hamming weight d will be

$$\langle x \upharpoonright_{w_H=d} |\psi_d\rangle = \sum_{k=1}^{d} \frac{1}{\sqrt{d}}(a+(d-1)b)b^{d-1}(d-1)!|e_k\rangle \,. \tag{27}$$

Now the probability that the particle is localized at the farthest vertex after d steps of quantum random walk driven by the Grover coin, with initial state $|0^d\rangle\frac{1}{\sqrt{d}}(1,\ldots,1)$ is $p^{\mathrm{quant,Grov,hit}}(d) = b^{2d}\,[(d-1)!]^2\,(\frac{a}{b}+d-1)^2$. Compare this to the hitting probability of the classical random walk on the hypercube: $p^{\mathrm{clas,hit}}(d) = \frac{d!}{d^d}$. We get a striking result: the hitting probability of quantum random walk on the hypercube driven by the Grover coin is exponentially greater than in classical case, the ratio $(d \to \infty)$ being‡: $r = \frac{p^{\mathrm{quant,Grov,hit}}(d)}{p^{\mathrm{clas,hit}}(d)} \sim e^{\alpha d}\sqrt{d}$, with $\alpha \approx 0.386$ A similar result on the same theme was already derived in [5], but our method is much simpler.

Conclusion

We have shown that discrete quantum random walk on the hypercube driven by Grover coin traverses the hypercube exponentially faster then in the classical case. It can also be shown, that its recurring properties are stronger than for the classical counterpart: namely, the probability that a localized particle with chirality $\frac{1}{\sqrt{d}}(1,\ldots,1)$ will return to the original position after two steps will be $4(1-\frac{1}{d^2})$ times the classical probability. This two-fold speedup is a paradoxical feature of quantum random walk.

3 Spin model of quantum random walk

3.1 Introduction

Randomized algorithms provide an effective way of exploring large combinatorial structures, using only limited computational resources. Examples of these algorithms are various Monte Carlo methods and random walks. Random walks are put to use whenever the task is to check a vast number of paths to give a definite result. For instance, the travelling salesman problem (the problem of finding the shortest route between two points, given all the possible routes) is superpolynomial in its complexity, thus hardly solvable using brute force.

‡ We have used the Stirling approximation $n! \approx \sqrt{2\pi n}\, n^n\, e^{-n}$.

Since the advent of quantum computing, it has been shown that some problems which have exponential complexity with respect to classical methods of solving, can be effectively computed on quantum computers. Shor's celebrated algorithm for factorizing integers and Grover's search algorithm are the best known. More recently, quantum random walks have been proposed as new means of implementing new algorithms. There are two basic approaches, sketched in [2, 11, 13]. In both cases the states of Hilbert space are identified with vertices of a graph, which underlies a combinatorial problem. We may traverse the graph using discrete sequence of unitary transformations, which apply on the whole graph, or setting an interaction between adjacent vertices and evolving the state vector using a suitable chosen Hamiltonian. In the first case, we need an additional Hilbert space (the coin space), which gives additional information on the direction of the walk. We shuffle the amplitudes of the coin belonging to different vertices at each step, to simulate random choice of path (without this modification, the walk would reduce to a trivial process, see [8] and the No-go Lemma therein). These walks have proved to lead to quadratic to exponential speedup with respect to various measures, compared to their classical counterparts [2, 5], and an oracle-based search algorithm on the hypercube has been proposed [10]. The second approach is based on the evolution which is continuous in time, governed be the Hamiltonian which is effectively the adjacency matrix of the graph [13, 9]. In some cases it has turned out that the quantum random walk penetrates the graph exponentially faster than in the classical case. We will discuss a model which is somewhat similar to this one.

We propose a model which is composed of qubits conceived as spin $\frac{1}{2}$-particles arranged on a lattice, which interact locally; the interaction flips the orientations of two neighboring qubits whenever they are antiparalell. This interaction is somewhat similar to the Ising model interaction,

$$H_{\text{Ising}} = \sum_a \sigma_x^{(a)} \otimes \sigma_x^{(a+1)}$$

where a runs through the vertices of a 1-dimensional lattice. In our case, we will be working in the basis of eigenstates of σ_z, $\sigma_z|j\rangle = (-1)^j|j\rangle, j = 0, 1,$ If we prepare the system on an n-cycle in the state $|10\dots0\rangle$, it will evolve in an oscillatory manner, relaxing to the state $|00\dots0\rangle$ in time average. There is approximately twice as great average probability for the first qubit to be in the state $|1\rangle$ than for the rest of the qubits, which initially were polarized in the state $|0\rangle$. The residual polarization in the state $|1\rangle$ drops to zero as time $T \to \infty$, with upper bound $O(\frac{n^2}{T})$.

3.2 The model

Let the Hilbert space $\mathcal{H} = [|0\rangle, |1\rangle]^{\otimes n}$ be spanned by linear combination of vectors $|x\rangle, x = 0, \dots, 2^n - 1$. The vectors of $\mathcal{H}$ represent the states of arrangements of n qubits on a n-cycle. The Hamiltonian for the evolution is

$$H = \sum_{a=1}^{n} |0\rangle\langle 1|_a \otimes |1\rangle\langle 0|_{a\oplus 1} + \text{h.c.} \tag{28}$$

where $\oplus$ is modulo n and h.c. stands for Hermitian conjugate. That is, the neighboring qubits interact, by flipping their polarizations (in $\{|0\rangle, |1\rangle\}$ basis). We say that the position of the walk is at the a-th vertex, if there is a nonzero probability to find the qubit at the a-th vertex in state $|1\rangle$. If the initial state is $|\psi(0)\rangle = |10\ldots0\rangle$, then

$$|\psi(t)\rangle := e^{-iHt}|\psi(0)\rangle = \sum_{a=1}^{n} c_a|e_a\rangle \tag{29}$$

is the state at time t, where $|e_a\rangle = |0\ldots1\ldots0\rangle$ with 1 but at the a-th position. The state $|\psi(t)\rangle$ is the coherent sum of the states, where the walk is positioned exactly at the a-th vertex. The whole evolution thus lives only on the subspace $\mathcal{H}_1 \subset \mathcal{H}$, where $\mathcal{H}_1 := [e_1, \ldots, e_n] =$. Then a-th qubit alone will be in the state

$$\rho^{(a)} = |c_a|^2|1\rangle\langle1| + (1-|c_a|^2)|0\rangle\langle0| \tag{30}$$

where $\rho^{(a)} := \mathrm{Tr}_S(|\psi(t)\rangle\langle\psi(t)|), S = [|e_a\rangle]^\perp$ is the density matrix of the a-th qubit, obtained by tracing over the Hilbert subspace of $\mathcal{H}_1$, attributed to the remaining qubits. We see that the vector on the Bloch sphere of $\rho^{(a)}$ is parallel to the chord connecting the extremal points $|0\rangle, |1\rangle$.

The measure $p_a := |c_a|^2$ is the measure of polarization of the a-th qubit, and may be thought of as the probability that the walk is positioned at the a-th vertex. The coefficients c_a are easy to compute from the Schrődinger equation:

$$i\dot{c}_a = c_{a\ominus1} + c_{a\oplus1}\,. \tag{31}$$

Now from the translational invariance of the Hamiltonian, $HD - DH = 0$, where $D|e_a\rangle = |e_{a\oplus1}\rangle$. We may use the Fourier transform:

$$c_a = \sum_{k=1}^{n} v_k e^{i2\pi ka/n} \tag{32}$$

$$v_k = \frac{1}{n}\sum_{a=1}^{n} c_a e^{-i2\pi ka/n}\,. \tag{33}$$

Substituting in (31) we obtain

$$c_a(t) = \frac{1}{n}\sum_{k=1}^{n} e^{-i\lambda_k t} e^{i2\pi ka/n} \tag{34}$$

where $\lambda_k = 2\cos\frac{2\pi k}{n}$ is the eigenvalue of the reduced Hamiltonian $H' := PHP$, where P is the projection on the space $[|e_1\rangle, \ldots, |e_n\rangle]$. The evolution of $p_a(t) := |c_a(t)|^2$ is oscillatory, as we see in FIG. 1 to FIG. 3. Obviously, the first qubit (initially in the state $|1\rangle$) relaxes to the opposite polarization, but after some time its original polarization is partially restored. It is when the phase waves propagating in the opposite direction form the first vertex start to interfere. In the long run, however, the evolution always returns to the vicinity of the initial state, see FIG. 4 Interpreting p_a as the probability

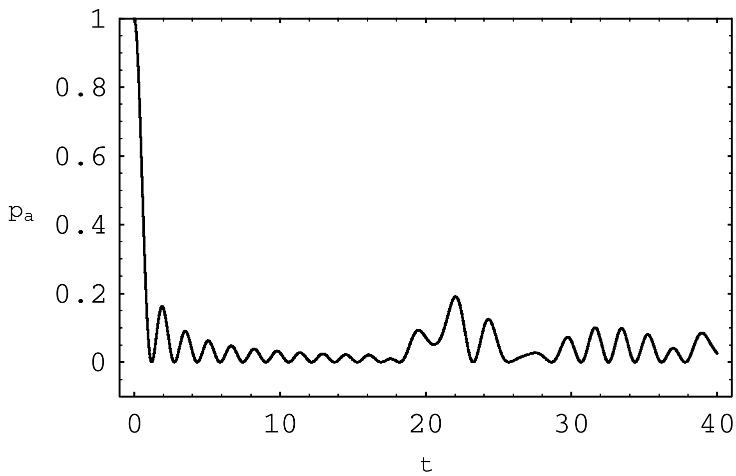

Fig. 1 Evolution of the first qubit, with $n = 40$.

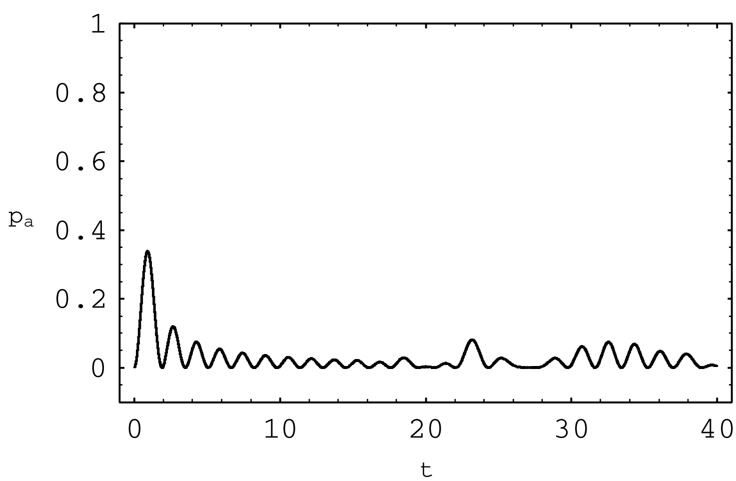

Fig. 2 Evolution of the second qubit, with $n = 40$.

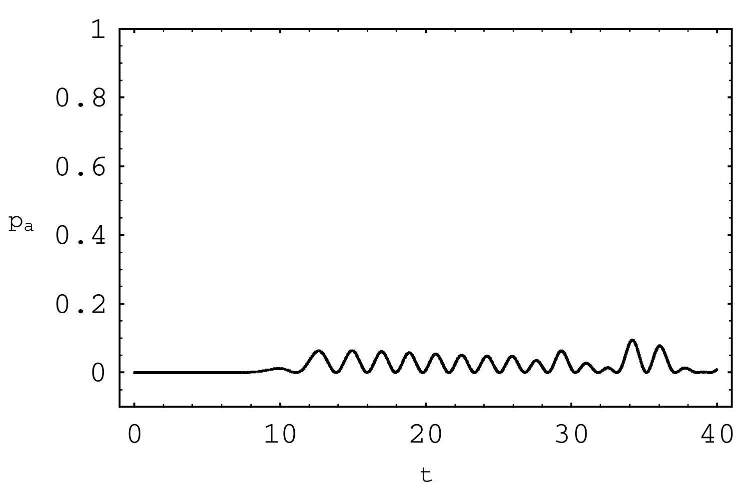

Fig. 3 Evolution of the 20-th qubit, with $n = 40$.

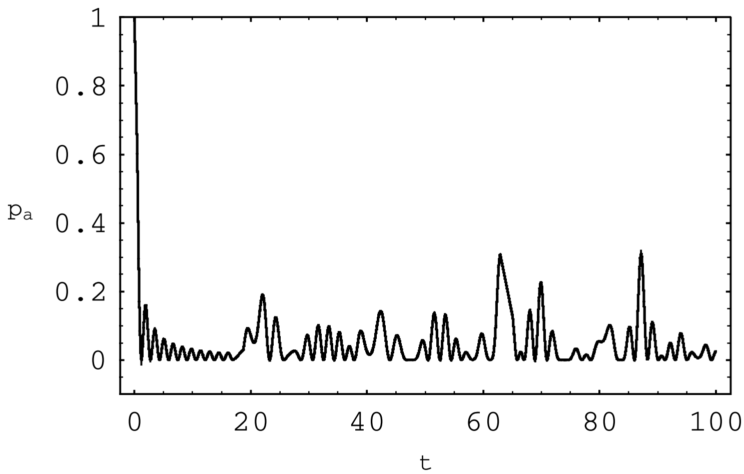

Fig. 4 Evolution of the first qubit, for $n = 40$ and longer times.

that in the random walk the a-th vertex is occupied, we see a sharp contrast with classical behavior of the random walk, when we allow at each instant to move to the left or right on the cycle. The generator matrix of this walk is

$$M = \begin{pmatrix} -2 & 1 & \cdots & 1 \\ 1 & -2 & 1 & \cdots \\ & \vdots & \ddots & \cdots \\ 1 & \cdots & 1 & -2 \end{pmatrix}. \tag{35}$$

Let the probability that the a-th vertex is occupied be denoted $\tilde{p}_a(t)$ and the probability distribution over the vertices be denoted $\tilde{p}(t) = (\tilde{p}_1(t), \ldots, \tilde{p}_n(t))^T$. Then the equation of motion for the classical random walk is

$$\tilde{p}(t) = e^{tM} \cdot \tilde{p}(0) \tag{36}$$

where $e^{tM} = \sum_{k=0}^{\infty} \frac{t^k}{k!} M^k$ is the exponential of the matrix. The matrix M is virtually identical with the reduced Hamiltonian H' which governs the evolution of quantum random walk. The diagonal elements (which we need in the classical random walk because of the normalization of the vector $\tilde{p}$) would only contribute to the evolution of $|\psi(t)\rangle$ with an overall phase, and would not change the evolution of $p(t)$. By means similar to what we have used for the quantum random walk, we compute $\tilde{p}$:

$$\tilde{p}_a(t) = \frac{1}{n} \sum_{k=1}^{n} e^{-\mu_k t} e^{i2\pi ka/n} \tag{37}$$

where $\mu_k = 4\sin^2 \frac{k\pi}{n}$. Obviously, $\lim_{t\to\infty} \tilde{p}_a(t) = \frac{1}{n}$, which is the stationary distribution of the classical random walk on the cycle. Since $p_a(t)$ is oscillatory, it makes no sense to define its stationary distribution. Various alternative definitions of the stationary distribution have been proposed, one of them being the average distribution

$$\pi_a(T) := \frac{1}{T}\int_0^T p_a(t)\,dt\,. \tag{38}$$

We show that there exists $\lim_{T\to\infty}\pi_a(T)$, which differs from $1/n$ as expected from the classical random walk.

Assuming n is odd, we have

$$\begin{aligned} p_a(t) &= \frac{1}{n^2}\sum_{k,j=1}^{n} e^{-i(\lambda_k-\lambda_j)t}e^{i2\pi(k-j)a/n} \\ &= \sum_{\lambda_k=\lambda_j} + \sum_{\lambda_k\neq\lambda_j} \\ &:= \sum_{k=j} + \sum_{\substack{k=n-j\\ j\neq n}} + R(t) \\ &= \frac{1}{n} + \begin{cases} \frac{n-1}{n^2} & : a=n \\ -\frac{1}{n^2} & : a\neq n \end{cases} \end{aligned}$$

using the identity $\lambda_k-\lambda_j \sim \sin(\frac{(k-j)\pi}{n})\sin(\frac{(k+j)\pi}{n})$ and the fact that the terms in both sums are different, since n is odd. The term $R(t)$ is the residual part of $p_a(t)$. Integrating $R(t)$ as in (38) we obtain

$$\pi_a(T) = \begin{cases} \frac{2}{n}-\frac{1}{n^2} & : a=n \\ -\frac{1}{n}-\frac{1}{n^2} & : a\neq n \end{cases} + \underbrace{\frac{1}{T}\int_0^T R(t)\,dt}_{I(T)}$$

On integrating $I(T)$ we get

$$I(T) = \sum_{\lambda_k\neq\lambda_j}\frac{1}{n^2}e^{i2\pi(k-j)a/n}\frac{e^{-i(\lambda_k-\lambda_j)T}-1}{-iT(\lambda_k-\lambda_j)}.\,.$$

Obviously, the following inequality holds:

$$|I(T)| \leq \sum_{\lambda_k\neq\lambda_j}\frac{1}{n^2}\frac{2}{T|\lambda_k-\lambda_j|} \tag{39}$$

and for $T\to\infty$ the term $I(T)$ vanishes. This proves the existence of the stationary distribution in time average probability. Giving the bound on the difference $|\lambda_k-\lambda_j| \geq |\cos\frac{2\pi}{n}-\cos 0|$ we have from the intermediate value theorem $|\lambda_k-\lambda_j| \geq |\sin\vartheta|\frac{2\pi}{n}, \vartheta \in (0,\frac{2\pi}{n})$. From the convexity of sin, for large n, we have $|\sin\vartheta| \geq \frac{2}{\pi}\vartheta$. The monotonicity of $\sin\vartheta, \vartheta\in(0,\frac{\pi}{2})$ implies $|\lambda_k-\lambda_j| \geq \frac{2}{\pi}(\frac{2\pi}{n})^2$. Substituting back in (39) we obtain the result $|I(T)| \leq O(\frac{n^2}{T})$. The rate of convergence of π_a to the stationary distribution is linear in time. By a similar argument we can show from (37) that $\tilde{\pi}_a(T)$, the time average of $\tilde{p}_a(t)$, converges to $\frac{1}{n}$ as $O(\frac{n^2}{T})$.

The quantum and classical random walks do not differ significantly in their speed of convergence to the stationary distribution.

3.3 Quantum walk on the line

Replacing the periodic boundary conditions with open boundary conditions, we may transfer from the model of quantum random walk on the cycle to the quantum random walk on the line. The equations (34) and (37) now take the form

$$c_a^{(\text{line})}(t) = \frac{1}{2\pi}\int_0^{2\pi} e^{-i2t\cos k} e^{ika}\, dk \tag{40}$$

and

$$\tilde{p}_a^{(\text{line})}(t) = \frac{1}{2\pi}\int_0^{2\pi} e^{-2t\sin^2(k/2)} e^{ika}\, dk\,. \tag{41}$$

These integrals can be explicitly evaluated in the form of Bessel functions:

$$c_a^{(\text{line})}(t) = (-i)^a \mathrm{J}_a(2t) \tag{42}$$

$$\tilde{p}_a^{(\text{line})}(t) = e^{-2t}\mathrm{I}_a(2t)\,. \tag{43}$$

Both (42) and (43) are properly normalized (see [1], (9.1.76), (9.6.33)). From the asymptotic forms of Bessel functions for $t \Longrightarrow \infty$, $\mathrm{J}_a(t) \sim \sqrt{\frac{2}{\pi t}}\cos(t - \frac{1}{2}a\pi - \frac{\pi}{4})$ and $\mathrm{I}_a(t) \sim \frac{e^t}{\sqrt{2\pi t}}(1 - \frac{4a^2-1}{8t} + \cdots)$, we see that that in the limit of large t, the quantum random walk relaxes to the state $|0\ldots 0\rangle$, while classical random walk approaches the state when there is negligible probability at each vertex to be occupied.

3.4 Generalization of the model and conclusion

We may generalize the model for an arbitrary interaction between adjacent vertices of a lattice (or conveniently, a graph). Consider an unoriented graph with (vertices, edges), $G = (G^v, G^e)$, and a Hamiltonian

$$H = \sum_{a\in G^v}\sum_{a'\in E(a)} (\omega_a \otimes \omega_{a'}^* + \omega_a^* \otimes \omega_{a'}) \tag{44}$$

where $E(a)$ is the set of vertices adjacent to a, such that $(aa') \in G^e$. The operator ω_a acts on the qubit at the a-th vertex. Setting $\omega_a := |0\rangle\langle 1|_a$ we get precisely the quantum random walk we have discussed before. We may immediately translate the results from the classical theory of random walks on graphs to the quantum domain, if we take the Hamiltonian H as the generator of the walk, for complex valued time $-it$.

Our model of quantum random walk on the cycle does not exhibit any significant difference from the classical case in the speed of convergence (both are $O(\frac{n^2}{T})$, though there is a qualitative difference between the two cases in their limiting distributions. In the case of random walk on the line, the quantum walk converges quadratically faster to the limiting distribution than classical one (see the asymptotical expansion of the Bessel functions). This walk could in principle be easy to implement if the ω_a operator can be decomposed using the spin-flip operators $|0\rangle\langle 1|, |1\rangle\langle 0|$, which can be done for the Ising model, for example.

Acknowledgements

I thank Prof. Vladimír Bužek for the original proposal of the model and useful discussions.

References

[1] Milton Abramowitz and Irene A. Stegun: *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tools*, U.S. Department of Commerce, National Bureau of Standards, Applied Mathematical Series, 1964–1972.

[2] D. Aharonov, A. Ambainis, J. Kempe, U. Vazirani: *Quantum Walks On Graphs*, quant-ph/0012090 v1.

[3] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, J. Watrous: "One-dimensional quantum walks", In: *Proc. of* 33^{rd} *Ann. ACM Symp. on Theory of Computing*, pp. 37–49.

[4] P.W. Shor: In *Proc. of the 35th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos CA, 1994, pp. 124.

[5] J. Kempe: *Quantum random walk hit exponentially faster*, quant-ph/0205083 v1.

[6] Norio Konno: *A new type of limit theorems for the one-dimensional quantum random walk*, quant-ph/0206103.

[7] C. Moore and A. Russel: *Quantum walks on the hypercube*, quant-ph0104137.

[8] David A. Meyer: *From quantum Cellular Automata to Quantum Lattice Gases*, quant-ph/9604003v2.

[9] A.M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, D.A. Spielman: *Exponential algorithmic speedup by quantum walk*, quant-ph/0209131.

[10] N. Shenvi, J. Kempe, K.B. Whaley: *A quantum random walk search algorithm*, quant-ph/0210064.

[11] A. Nayak and A. Vishwanath: *Quantum Walk on the Line*, quant-ph/0010117 v1.

[12] Michael A. Nielsen and Isaac L. Chuang: *Quantum Computation and Quantum Information*, Cambridge University Press, 2000, ISBN 0-52163503-9.

[13] A.M. Childs, E. Farhi, S. Gutman: *An example of the difference between quantum and classical random walks*, quant-ph/0103020.