1 Readings

Quantum Random Walks: Y. Aharonov et al., PRA 48, 1687 (1993); D. Aharonov et al., qu-ph/0012090; Moore and Russell, qu-ph/0104137; Kempe, qu-ph/0303081 (review)

Nayak and Vishwanath, qu-ph/0010117; Kempe et al. qu-ph/0205083; Shenvi et al. PRA 67, 052307 (2003); Ambainis qu-ph/03110001

Error Correction: Stolze and Suter, Quantum Computing, Ch. 7

Nielsen and Chuang, Quantum Computation and Quantum Information, Ch. 10

2 Classical 1-D Random Walk

Each time step, go one step in a random direction.

If you call the distance travelled in time step i by x_i, then

$$x_i = \begin{cases} +1 & w.p.\ 1/2 \\ -1 & w.p.\ 1/2 \end{cases}$$

and the total distance travelled in n steps is $X = x_1 + \ldots + x_n$. Now, $E(X) = nE(x_i) = 0$ so it is expected that you end up where you started from. However, $var(X) = n(var(x_i)) = nE[(x_i - E(x_i))^2] = nE(x_i^2) = n$, and so in n time steps you have covered a distance of $O(\sqrt{n})$. Alternately, it takes $O(k^2)$ time to go a distance k.

This 1-D walk is a Binomial random walk and in the limit of large n gives a probability density for the net displacement X

$$P_X(y) = \frac{1}{\sqrt{2\pi\Delta^2 n}} exp\left(-\frac{y^2}{2\Delta^2 n}\right)$$

where in this example $\Delta = 1$. This can be rewritten to give the probability that the particle lies in the interval $y \to y + dy$ along the x axis at time t as

$$P(y,t) = \frac{1}{\sqrt{4\pi Dt}} exp\left(-\frac{y^2}{4Dt}\right),$$

where $D = n\Delta^2/2$ is the diffusion coefficient for the random walk and $n = mt$ defines the number of steps per unit time, m. This probability distribution spreads out from a delta function in y at time $t = 0$, in such a way that the area under the curve remains constant and equal to one, while the probability of finding the particle at some distance y along the x-axis increases with time since the standard deviation $\sigma = \sqrt{var(y)} = \sqrt{\Delta^2 n} = \sqrt{2Dt}$ increases as $\sqrt{n}$, or equivalently, as $\sqrt{t}$.

We can construct a probabilistic computational algorithm for this classical 1-D random walk as follows. We have $X \in \mathbf{Z}$ representing the total distance travelled, and a coin $b \in \{0,1\}$. Every step of the walk we update our position depending on the coin, then flip the coin in preparation for the next step. That is,
WALK : $X \leftarrow X + (-1)^b$; pick new b randomly; repeat.

2.1 Quantum 1-D Random Walk

Similar to the probabilistic classical random walk, we have $X \in \mathbf{Z}$ representing the total distance travelled, but now our coin $|b\rangle \in \mathscr{C}^2$ is a quantum bit. The coin flip is implemented as some unitary operator $U = C_0$ (e.g. the Hadamard transform H). That is,
WALK : $|X,b\rangle \leftarrow |X+(-1)^b,b\rangle$; $|b\rangle \leftarrow U|b\rangle$; repeat.

The quantum random walk (QRW) acts on wave states in a Hilbert space $\mathscr{H}^S \otimes \mathscr{H}^c$ where $\mathscr{H}^S$ is the Hilbert space of the position degree of freedom and $\mathscr{H}^c$ that for the coin degree of freedom. The unitary evolution operator on states in this tensor product space is $U = SC$, i.e., the composition of a coin operator and a controlled-shift operator, where

$$\begin{aligned} C &= I \otimes C_0 \\ S &= \sum_b |x+(-1)^b,b\rangle\langle x,b| . \end{aligned}$$

Here is an example. Set $b = 1 \equiv L, b = 0 \equiv R$. Then

$$S = |X-1,L\rangle\langle X,L| + |X+1,R\rangle\langle X,R| ,$$

so S transforms $|X,L\rangle$ to $|X-1,L\rangle$ and $|X,R\rangle$ to $|X+1,R\rangle$. Suppose the coin operator is the Hadamard coin $C_0 = H$. Then C transforms an arbitrary state localized initially at X, $|\psi\rangle = a|X,L\rangle + b|X,R\rangle$, to the state $\frac{1}{\sqrt{2}}(a|X,L\rangle + a|X,R\rangle + b|X,L\rangle - b|X,R\rangle)$. Hence the action of the QRW unitary evolution operator $U = SC$ on this state is to produce the state

$$\frac{a+b}{\sqrt{2}}|X-1,L\rangle + \frac{a-b}{\sqrt{2}}|X+1,R\rangle$$

which has spread out in both directions and has also mixed the components facing in L and R directions.

Quantum walks have very different properties than classical walks. The coin degree of freedom allows non-classical correlations between successive positions to be established, which can be manifested as interferences. Figure 1 shows the probability distribution of the quantum random walk with a Hadamard coin starting in a coin-symmetric initial state $|0,L\rangle + i|0,R\rangle$ after 100 steps. The probability distribution for X after k time steps is small at $X = 0$ with two peaks centered at $\pm ck$ for some constant c. This is clearly very different from the classical binomial (gaussian) distribution which has a maximum at $X = 0$. If one were however to measure the coin degree of freedom after every step, then one regains the classical random walk. One can understand the quantum behavior in Figure 1 qualitatively as follows. There are naturally many different ways to come back to 0 after k time steps, but each of those ways is likely to carry a different phase, so they interfere destructively. Correspondingly, there are fewer ways to get outside some distance away from the start, so here constructive interference is more important.

Some important results from QRW are the following (see review in qu-ph/0303081):

1. Quantum walks do not converge to a stationary distribution, unlike classical walks, since they are unitary and reversible. However one can define a limiting distribution as the average of the probability distributions over time. (qu-ph/0012090)

2. The mixing time, i.e., the time it takes to approach a limiting distribution, is quadratically faster for QRW than for classical walks. (qu-ph/0010117)

3. The 1-D quantum walk takes $O(k)$ time to go a distance k, i.e., it propagates quadratically faster than the classical time $O(k^2)$ (qu-ph/0010117)

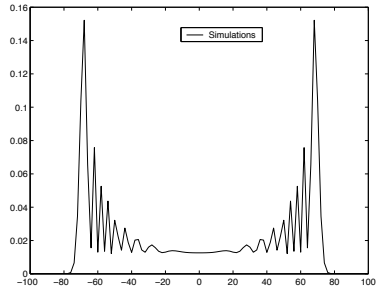

Figure 1: Probability distribution of a 1-D QRW with a Hadamard coin operator after 100 propagation steps, starting from a coin-symmetric initial state located at $X = 0$.

4. The quantum walk can show a faster hitting time than the classical walk, i.e., the time taken to reach a given site. For the 1-D walk this speed-up is also quadratic. For a QRW on a hypercube (an n-dimensional hypercube is a graph with vertex set labelled by n-bit strings $0,1^n$ and connections (edges) existing between vertices that differ in exactly one bit position) the speed-up in hitting time is exponential. (qu-ph/0104137,qu-ph/0205083)

5. A QRW on a hypercube with a coin oracle operator can generate the Grover quantum search algorithm (PRA 67, 052307 (2003)).

6. A QRW on a subset of the hypercube can solve for element distinctness of function values on a finite set in time $O(n^{2/3})$, compared to the classical time $\Omega(n)$ (and the quantum search based time $O(n^{3/4})$. (qu-ph/03110001)

3 Dirac Equation and QRW

First lets recall the basics about the Schrodinger equation. This describes how a quantum state $\left|\psi\right\rangle$ evolves over time. In natural units where $\hbar = c = 1$, Schrodinger's equation is

$$i\frac{d\left|\psi\right\rangle}{dt} = H\left|\psi\right\rangle$$

where H is the Hamiltonian operator. The Hamiltonian is a hermitian operator, and so corresponds to an observable, namely energy. In the case of a 1-D particle, the state $\left|\psi\right\rangle = \psi(x,t)$ is the amplitude of the particle at position x at time t. In this case, the Hamiltonian operator $H = \partial^2/\partial x^2$, so Schrodinger's equation reads

$$i\frac{\partial\psi}{\partial t} = \frac{\partial^2\psi}{\partial x^2},$$

so a state with velocity $\sim k$ is given by $\psi(x) = e^{ikx}$, and this is also an eigenstate of the momentum operator $p = \frac{\hbar}{i}\frac{d}{dx}$.

Schrodinger's equation describes the non-relativistic behavior of a quantum state. In that situation the energy of a particle in 1-D is given by the classical expression $E = p^2/2m$, and by the Hamiltonian operator H above. Relativistically, the energy of a particle is given classically by $E^2 = p^2c^2 + m^2c^4$, so the corresponding relativistic quantum operator should satisfy $\hat{H}^2 = \hat{p}^2c^2 + m^2c^4\hat{I}$. How do we find the square root of this operator? Dirac showed how to do this by expanding the Hilbert space by tensoring it with an additional $\mathscr{C}^{\in}$

space (i.e., with a qubit, and actually with the Hilbert space for the particle spin). This leads to the matrix form we could have

$$\hat{H} = \left[\begin{array}{c|c} \hat{p}c & mc^2\hat{I} \\ \hline mc^2\hat{I} & -\hat{p}c \end{array}\right] = \left[\begin{array}{c|c} \hat{p}c & 0 \\ \hline 0 & -\hat{p}c \end{array}\right] + mc^2 \left[\begin{array}{c|c} \hat{0} & \hat{I} \\ \hline \hat{I} & \hat{0} \end{array}\right]$$

which satisfies the required condition

$$\hat{H}^2 = \left[\begin{array}{c|c} \hat{p}^2c^2 + m^2c^4\hat{I} & 0 \\ \hline 0 & \hat{p}^2c^2 + m^2c^4\hat{I} \end{array}\right].$$

Now we can understand the behavior the particle under this Hamiltonian by recognizing the similarity with a 1-D QRW.

First, consider the solution for $m = 0$. Here the Hamiltonian factors into separate blocks with solutions $\psi_R = f(x - ct)$ and $\psi_L = f(x + ct)$ with e.g., $f(x \pm ct) = e^{i(x-ct)}$. These are solutions to $i\hbar\frac{\partial\psi}{\partial t} = \pm c\frac{\hbar}{i}\frac{d\psi}{dx}$. The solution ψ_R moves to the right at the speed of light c and the solution ψ_L moves to the left with speed c.

Now for the general case when $m \neq 0$. Looking at the Hamiltonian decomposition above into two terms

$$\hat{H} = \left[\begin{array}{c|c} \hat{p}c & 0 \\ \hline 0 & -\hat{p}c \end{array}\right] + mc^2 \left[\begin{array}{c|c} \hat{0} & \hat{I} \\ \hline \hat{I} & \hat{0} \end{array}\right]$$

we see that the second term acts like a coin flip in the additional qubit (spin) space, but with an amplitude m. On exponentiating this Hamiltonian to get the corresponding unitary evolution operator, we arrive at the QRW form $U = SC$ where $C = e^{-\frac{i}{\hbar}mI\otimes\hat{X}} = \cos mI + i\sin mI \otimes \hat{X}$ where $\hat{X}$ is the Pauli X, or bit flip operator on the coin space. What does this mean? Well, when $m = 0, \pi, 2\pi, ...$ there are no coin flips and the evolution will reduce to the evolution under the first term, i.e., free motion to left or right with constant speed c. When $m = \pi/2, 3\pi/2, ...$ the coin flips at each step and we have a 1-D QRW. We saw above that in this situation the particle moves a distance n away from the origin after n steps. This ensures also that the particle moves with constant speed, unlike the classical case where the speed would go to zero as n increases (speed $\propto \sqrt{n}/n$). When m is any other intermediate value, the frequency of coin flips lies inbetween these two cases. Explicit calculation of the actual distance moved after n steps will allow the mass-dependent speed to be evaluated.

4 Mixed state and density matrix

An ensemble (i.e., a collection of quantum systems) can be in a pure or a mixed state. Consider an ensemble (a collection of N) of spins. All N spins can be pointing up (all spins in state $|1\rangle$). This will be an example of a pure state. However, we can also consider a situation where half the spins will be poiting up (spins in state $|1\rangle$) and the other half of the spins will be pointing down (spins in state $|0\rangle$). Thus we know that a particular spin in this ensemble will occupy state $|1\rangle$ with probility $1/2$ and state $|0\rangle$ with probility $1/2$. This is a mixed state.

Now the state of a particular spin in this ensemble can no longer be described with kets (state vectors). We, therefore, resort to the density matrix formalism. Density matrix desribes a general state of a quantum system, in particular density matrix can desribe a state of a spin in an ensemble. Density matrix is written as

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \tag{1}$$

This equation means that our system (ensemble) can occupy states $|\psi_i\rangle$ with the probability p_i.