# A quantum random walk

J. Marbeau and S. Gudder

Department of Mathematics and Computer Science
University of Denver, Denver CO 80208, USA

ABSTRACT. A discrete version of the Feynman path integral formalism is introduced in terms of a quantum random walk. The amplitude $A(p)$ of a discrete path $p$ in phase space is generated by a transition amplitude $A_{jk}$ where $j$ and $k$ are integers. The resulting matrix $A_{jk}$ is called a Dirichlet matrix since it is closely related to a Dirichlet series. It is shown in Section 1 that in order to compute certain probabilities at a discrete time $r$ we must find the entries of the $r$th power of $A_{jk}$. This is accomplished in Section 3 by finding the eigenvalues and eigenvectors of $A_{jk}$. In Section 4 we compute probabilities for the specific example of a square lattice. We observe in Section 3 that the eigenvalues of $A_{jk}$ can be degenerate and in Section 5 we compute their multiplicities.

*RESUME. Nous introduisons, en termes de marche aléatoire, un formalisme qui s'apparente, pour un temps discret, à celui de l'intégrale fonctionnelle de Feynman. L'amplitude $A(p)$ d'une trajectoire à temps discret dans l'espace de phase est générée par une amplitude de transition $A_{jk}$ où $j$ et $k$ sont des entiers. La matrice $A_{jk}$ qui en résulte est appelée matrice de Dirichlet en raison de son étroite relation avec une série de Dirichlet. Nous montrons au paragraphe 1, que pour calculer certaines probabilités au temps discret $r$, il nous faut trouver les coefficients de la r-ième puissance de $A_{jk}$. Cela est accompli au paragraphe 3 où nous trouvons les vecteurs et valeurs propres de $A_{jk}$. Au paragraphe 4, nous calculons les probabilités dans l'exemple particulier d'un réseau carré. Nous observons, au paragraphe 3 que les valeurs propres de $A_{jk}$ peuvent être multiples et nous calculons les multiplicités au paragraphe 5.*

## 1. A random walk

Let $D = \{u_0, u_1, \ldots, u_{n-1}\}$ be a set of unit vectors in $\mathbf{R}^2$ where the angle between $u_i$ and $u_{i+1}$ is $2\pi/n$. A point $x \in \mathbf{R}^2$ is a *lattice point* if $x = \sum_{i=0}^{n-1} a_i u_i$ where $a_i$ is a nonnegative integer, $i = 0, 1, \ldots, n-1$. For example, if $n = 4$ we have a square lattice and if $n = 6$ we have a triangular lattice in $\mathbf{R}^2$. Denoting the lattice points by $L$, we call $S = L \times D$ a *discrete phase space*. Suppose a quantum particle is initially at the origin $0 = (0, 0)$ moving in the direction $v_0 \in D$. After one time step the particle will arrive at the point $v_0 \in L$. The particle will then move in one of the $n$ directions $v_1 \in D$ and after a second time step it will arrive at the point $v_0 + v_1 \in L$. This motion will continue until it arrives at a point $\sum_{i=0}^{r-1} v_i$ after $r$ time steps. Thus the particle moves from one lattice point to an adjacent lattice point in each time step. We call a sequence $(x_0, v_0), \ldots, (x_r, v_r)$ in $S$ where $x_{k+1} = x_k + v_k$, $k = 0, \ldots, r-1$, an *$r$-path*. The $r$-paths give the allowable paths along which a particle can travel.

We are mainly interested in the probability that a particle travels from $(0, v_0)$ to $(x_r, v_r)$ in $S$; that is, the probability that a particle arrives at $x_r$ and then moves in the direction $v_r$ after $r$ time steps given that it was initially at 0 moving in the $v_0$ direction. For a classical random walk we would begin by postulating a probability (or transition probability) that the particle moves from one lattice point to its neighboring lattice points. We would then define the probability that the particle travels along an $r$-path to be the product of the probabilities of the one-step components of the $r$-path. This amounts to assuming that the motion gives a Markov chain. Then the probability that the particle arrives at $x_r$ in $r$ time steps is the sum of the probabilities of all $r$-paths terminating at $x_r$ [2]. But since this is a quantum random walk, we must follow the tenets of quantum mechanics and work with probability amplitudes [5, 7, 11]. Roughly speaking, a probability amplitude is a complex-valued function whose modulus squared is a probability.

Let $a$ be a positive integer such that $a$ and $n$ are relatively prime (it will become clear later why we want this condition). Define the *transition amplitude* $A\colon S \times S \to \mathbf{C}$ by

$$A((x, u_j), (y, u_k)) = \begin{cases} \frac{1}{\sqrt{n}}\, e^{ia\pi(j-k)^2/n} & \text{if } y = x + u_j \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

$j, k = 0, \ldots, n-1$. It will also become clear why we have chosen $A$ to have this form. If

$$p = \{(x_0, v_0), \ldots, (x_r, v_r)\}$$

is an $r$-path with $x_0 = 0$, we define the *amplitude* of $p$ to be

$$A(p) = \prod_{j=0}^{r-1} A((x_j, v_j), (x_{j+1}, v_{j+1})). \tag{2}$$

Let $\mathcal{P}_r((0, v_0), (x_r, v_r))$ be the set of all $r$-paths from $(0, v_0)$ to $(x_r, v_r)$. We define the *$r$-step amplitude* from $(0, v_0)$ to $(x_r, v_r)$ by

$$A_r((0, v_0), (x_r, v_r)) = \sum \{A(p) : p \in \mathcal{P}_r((0, v_0), (x_r, v_r))\} \tag{3}$$

and the *$r$-step probability* from $(0, v_0)$ to $(x_r, v_r)$ is defined as

$$P_r((0, v_0), (x_r, v_r)) = \left|A_r((0, v_0), (x_r, v_r))\right|^2.$$

The computation of $P_r((0, v_0), (x_r, v_r))$ in general appears to be quite difficult. However, if we are only interested in the direction of motion, the problem becomes more tractable. Letting

$$A_r(v_0, v_r) = \sum \{A_r((0, v_0), (x_r, v_r)) : x_r \in L\}$$

we can interpret $A_r(v_0, v_r)$ as the amplitude that a particle moves in direction $v_r$ after $r$ time steps given that it was initially moving in the direction $v_0$. Letting $M$ be the matrix with entries

$$M_{jk} = \frac{1}{\sqrt{n}}\, e^{ia\pi(j-k)^2/n}$$

we have

$$A_r(u_s, u_t) = \sum_{i_1, \ldots, i_{r-1}=0}^{n-1} M_{si_1} M_{i_1 i_2} \ldots M_{i_{r-1} t} = (M^r)_{st} \tag{4}$$

where $M^r$ is the $r$th power of $M$. In particular, $A_1(u_s, u_t) = M_{st}$. The corresponding probability becomes

$$P_r(u_s, u_t) = \left|(M^r)_{st}\right|^2. \tag{5}$$

Letting $H_n$ be the inner product space $\mathbf{C}^n$ with the usual inner product $\langle f, g\rangle = \sum_{i=0}^{n-1} f_i \bar{g}_i$ and norm $\|f\| = \big(\langle f, f\rangle\big)^{1/2}$ we can express (4) and

(5) in a different form. If $\hat{f}_0 = (1,0,\ldots,0),\ldots,\hat{f}_{n-1} = (0,\ldots,0,1)$ denotes the standard basis in $H_n$, then

$$A_r(u_s,u_t) = \left\langle M^r \hat{f}_s, \hat{f}_t \right\rangle \tag{6}$$

and

$$P_r(u_s,u_t) = \left| \left\langle M^r \hat{f}_s, \hat{f}_t \right\rangle \right|^2. \tag{7}$$

Since $P_r(u_s,u_t)$ is supposed to be a probability and since the particle must be moving in one of the $n$ directions after $r$ time steps, we conclude from (7) that we need $M^r$ to satisfy

$$\left\| M^r \hat{f}_s \right\|^2 = \sum_{t=0}^{n-1} \left| \left\langle M^r \hat{f}_s, \hat{f}_t \right\rangle \right|^2 = \sum_{t=0}^{n-1} P_r(u_s,u_t) = 1. \tag{8}$$

In quantum mechanical terminology, we say that the *state* of the system at time $r$ is $M^r \hat{f}_s$ given that the initial state is $\hat{f}_s$. Equation 8 shows that $M^r \hat{f}_s$ is a unit vector. More generally, let $f \in H_n$ be an arbitrary unit vector. Then $f$ is a state of the system for which the probability that the particle is moving in the $t$ direction is $|f_t|^2 = \left|\langle f, \hat{f}_t \rangle\right|^2$. We thus interpret $f$ as giving the amplitude of the probability distribution $|f_t|^2$, $t = 0,\ldots,n-1$. Now suppose that initially we only know the state $f$. Of course, if $f = \hat{f}_s$ we know the initial direction precisely, but in general this may not be possible. Then the state at time $r$ is defined to be $M^r f$. It follows that $\|M^r f\| = 1$ and in particular $\|Mf\| = 1$. We conclude that $M$ preserves norms and hence $M$ is unitary [6].

It will follow from our later work that $M$ is unitary if and only if $a$ and $n$ are relatively prime and this is why we wanted that condition. In order to find the state $M^r f$ or the probability $P_r(u_s,u_t)$ we must compute the $r$th power of the unitary matrix $M$. The only practical way to do this is to diagonalize $M$; that is, find its eigenvalues and eigenvectors. This is what is usually done in the study of classical Markov chains except in that case we have a stochastic matrix to diagonalize instead of a unitary matrix [2].

If $p$ is the $r$-path

$$p = \{(0,u_{i_0}),(x_1,u_{i_1}),\ldots,(x_r,u_{i_r})\}$$

then (1) and (2) give

$$A(p) = \frac{1}{n^{r/2}} \exp\Big[i \sum_{j=1}^{r} a\frac{\pi}{n}(i_j - i_{j-1})^2\Big]. \tag{9}$$

If we interpret $a$ as the mass of the particle, then it can be shown [7] that for large $n$ the summation in (9) is approximately the integral of the kinetic energy $K(t)$ of the particle along the path $p$ minus a positive constant. (If the particle has zero mass, then $a$ is related to its "wavelength".) Such an integral is called the *action* of a free particle.

We thus have for large $n$ that

$$A(p) \sim N \exp\Big[i \int_p K(t)\, dt\Big] \tag{10}$$

where $N$ is a normalization constant. The right hand side of (10) is called the *Feynman amplitude* of a free particle along the continuous path $p$ [5]. We now see that $A(p)$ is a discrete analog of the continuum Feynman amplitude. This is the reason that we chose $A$ to have the form given in (1). Equation 3 is the discrete analog of the Feynman path integral which plays a dominate role in high energy physics [10]. Although the path integral has a physically intuitive appeal, it is subject to various mathematical difficulties. However, this discrete analog is mathematically rigorous and for large $n$ gives a close approximation to the continuum value. Moreover, it can be generalized to the case of a particle moving under the influence of a force by adding a potential energy term [7]. We have thus constructed a discrete quantum mechanics.

Besides the computation of $M^r$ there is another reason for diagonalizing $M$ even for relatively small values of $n$. In elementary particle physics, two important classes of particles are mesons and baryons. Examples of mesons are the pion and kaon, while examples of baryons are the proton and neutron. In the quark model of elementary particles, a meson is composed of one quark and one antiquark while a baryon is composed of three quarks or of three antiquarks. The constituent quarks (or antiquarks) are held together by the strong nuclear force. This force is mediated by an exchange of particles called gluons [3, 11]. In a certain particle model, a meson is represented by a connected multigraph with two vertices (a multigraph can have multiple edges and loops) while a baryon is represented by a connected multigraph with three vertices [8].

The vertices represent quark (or antiquark) constituents and the edges represent gluon paths. In this theory the gluons perform a quantum random walk along the edges of the multigraph. This quantum random walk is governed by a unitary matrix that essentially has the form $M$ given before, where $n$ depends on the number of edges. Since $M$ is unitary, its eigenvalues have the form $e^{i\theta}, \theta \in [0, 2\pi)$. It turns out that the $\theta$'s are closely related to the allowed energy values of the gluons and hence have important physical significance [8]. The multiplicities of the eigenvalues are also important for the calculation of particle masses [8].

## 2. Dirichlet matrices

We now begin a study of the matrices introduced in Section 1. Let $a$ be a positive integer and let $M(n, a)$ be the $n \times n$ matrix whose $jk$ entry is

$$A_{jk} = \frac{1}{\sqrt{n}} e^{i\pi a(j-k)^2/n} \qquad j, k = 0, 1, \ldots, n-1.$$

We call $M(n, a)$ a *Dirichlet matrix*. The reason for this terminology is that $M(n, a)$ is closely related to the *Dirichlet sum*

$$S(n, a) = \sum_{j=0}^{n-1} e^{i\pi a j^2/n}$$

that occurs in various parts of number theory [1,4]. In fact, it follows from Lemma 4 in the next section that the row and column sums of $M(n, a)$ are proportional to a Dirichlet sum. Moreover, Theorem 5 shows that eigenvalues of $M(n, a)$ have a common factor that is a Dirichlet sum. For $a = 2$, we have $S(n, 2) = G(n)$ where $G(n)$ is called *Gauss's sum*. Dirichlet sums satisfy the following Dirichlet reciprocity law [1].

**Theorem 1.** *If $na$ is even, then*

$$S(n, a) = \sqrt{\frac{n}{a}}\, e^{i\pi/4} \overline{S(a, n)}.$$

This reciprocity law is useful for computing $S(n, a)$ for small $a$. For example, as a special case of Theorem 1, if $a = 2$ we have

$$G(n) = \frac{\sqrt{n}}{2}(1 + i)(1 + e^{-i\pi n/2}).$$

As we have shown in Section 1, it is important to know when $M(n,a)$ is unitary. The next theorem gives such a characterization. We shall need the following lemma whose proof is straightforward.

**Lemma 2.** *Two positive integers $n$ and $a$ are relatively prime if and only if $a\ell \neq nm$ for any integers $\ell, m$ with $0 < |\ell| < n$.*

**Theorem 3.** *$M(n,a)$ is unitary if and only if $n$ and $a$ are relatively prime.*

**Proof.** Since

$$\sum_{k=0}^{n-1} |A_{jk}|^2 = 1$$

for $j = 0, \ldots, n-1$, it is clear that $M(n,a)$ is unitary if and only if

$$\sum_{k=0}^{n-1} A_{jk}\bar{A}_{j'k} = 0$$

for $j \neq j'$. For $j \neq j'$ we have

$$\begin{aligned} n\sum_{k=0}^{n-1} A_{jk}\bar{A}_{j'k} &= \sum_{k=0}^{n-1} \exp\left\{ \frac{i\pi a}{n}\left[(j-k)^2 - (j'-k)^2\right]\right\} \\ &= e^{i\pi a(j^2 - j'^2)/n} \sum_{k=0}^{n-1} e^{i2\pi a(j'-j)k/n}. \end{aligned}$$

If $n$ and $a$ are relatively prime, then applying Lemma 2, the geometric series in this last expression satisfies

$$\sum_{k=0}^{n-1}\left[e^{i2\pi a(j'-j)/n}\right]^k = \frac{1 - e^{i2\pi a(j'-j)}}{1 - e^{i2\pi a(j'-j)/n}} = 0$$

and $M(n,a)$ is unitary. If $n$ and $a$ are not relatively prime, then by Lemma 2 there exist $j \neq j'$ such that $a(j-j') = nm$ for some integer $m$. In this case the geometric series has sum $n$ and $M(n,a)$ is not unitary. □

## 3. Diagonalization

We need the following lemma to prove our main result.

**Lemma 4.** *Let $n$ and $a$ be positive integers.*
(a) *If $na$ is even, then*

$$\sum_{k=0}^{n-1} e^{i\pi a(k-j)^2/n} = S(n,a)$$

*for any $0 \leq j \leq 2n-2$.* (b) *If $na$ is odd, then*

$$\sum_{k=0}^{n-1} e^{i\pi a(k-j-\frac{1}{2})^2/n} = \frac{1}{2}S(4n,a)$$

*for any $0 \leq j \leq 2n-2$.*

**Proof.** (a) First suppose $j \leq n-1$. Then

$$S \equiv \sum_{k=0}^{n-1} e^{i\pi a(k-j)^2/n} = \sum_{k=0}^{j-1} e^{i\pi a(k-j)^2/n} + \sum_{k=j}^{n-1} e^{i\pi a(k-j)^2/n}.$$

Letting $r = j-k$ in the first sum and $r = n-k+j$ in the second sum gives

$$S = \sum_{r=1}^{j} e^{i\pi ar^2/n} + \sum_{r=j+1}^{n} e^{i\pi a(n-r)^2/n}.$$

Since $na$ is even, we obtain

$$S = \sum_{r=1}^{n} e^{i\pi ar^2/n} = \sum_{r=0}^{n-1} e^{i\pi ar^2/n} = S(n,a).$$

Next suppose $n \leq j \leq 2n-2$. Then $j = n+r$ for some integer $0 \leq r \leq n-2$. Again, since $na$ is even we have

$$S = \sum_{k=0}^{n-1} e^{i\pi a(k-n-r)^2/n} = \sum_{k=0}^{n-1} e^{i\pi a(k-r)^2/n}.$$

But this last sum equals $S(n,a)$ by the previous result.
(b) Consider the summation

$$T = \sum_{k=0}^{4n-1} e^{i\pi a(k-2j)^2/4n}.$$

Now $T$ is the sum of its odd and even partial sums $T = U + E$ where

$$U = \sum_{k=1}^{2n} e^{i\pi a(2k-1-2j)^2/4n}$$

$$E = \sum_{k=0}^{2n-1} e^{i\pi a(2k-2j)^2/4n}.$$

We can write $E$ as

$$E = \sum_{k=0}^{n-1} e^{i\pi a(k-j)^2/n} + \sum_{k=n}^{2n-1} e^{i\pi a(k-j)^2/n}.$$

Letting $r = k - n$ in the second summation and using the fact that $na$ is odd, we obtain

$$\begin{aligned}\sum_{k=n}^{2n-1} e^{i\pi a(k-j)^2/n} &= \sum_{r=0}^{n-1} e^{i\pi a(r+n-j)^2/n} \\ &= -\sum_{r=0}^{n-1} e^{i\pi a(r-j)^2/n}.\end{aligned}$$

Hence, $E = 0$. Since

$$e^{i\pi a(4n-1-2j)^2/4n} = e^{i\pi a(1+2j)^2/4n}$$

we have

$$U = \sum_{k=0}^{n-1} e^{i\pi a(2k-1-2j)^2/4n} + \sum_{k=n}^{2n-1} e^{i\pi a(2k-1-2j)^2/4n}.$$

Again, letting $r = k - n$ in the second summation and using the fact that $na$ is odd, we obtain

$$\begin{aligned}\sum_{k=n}^{2n-1} e^{i\pi a(2k-1-2j)^2/4n} &= \sum_{r=0}^{n-1} e^{i\pi a(2r+2n-1-2j)^2/4n} \\ &= \sum_{r=0}^{n-1} e^{i\pi a(2r-1-2j)^2/4n}.\end{aligned}$$

It follows that

$$T = U = 2\sum_{k=0}^{n-1} e^{i\pi a(k-j-\frac{1}{2})^2/n}.$$

But since $4na$ is even, it follows from Part a that $T = S(4n, a)$. □

We now come to our main result.

**Theorem 5.** (a) *If $na$ is even, then for $r = 0, 1, \ldots, n-1$, the vector*

$$e_r = \left(e^{-i2\pi ark/n}\right), \quad k = 0, \ldots, n-1$$

*is an eigenvector of $M(n, a)$ with corresponding eigenvalue*

$$\lambda_r = n^{-1/2} S(n, a) e^{-i\pi ar^2/n}.$$

(b) *If $na$ is odd, then for $r = 0, 1, \ldots, n-1$, the vector*

$$e_r = \left(e^{-i2\pi a(r+\frac{1}{2})k/n}\right), \quad k = 0, \ldots, n-1$$

*is an eigenvector of $M(n, a)$ with corresponding eigenvalue*

$$\lambda_r = \frac{n^{-1/2}}{2} S(4n, a) e^{-i\pi a(r+\frac{1}{2})^2/n}.$$

**Proof.** (a) The $j$th coordinate of $M(n, a)e_r$ is

$$[M(n, a)e_r]_j = n^{-1/2} \sum_{k=0}^{n-1} e^{i\pi a(j-k)^2/n} e^{-i2\pi ark/n}.$$

Now the summand may be written

$$e^{-i2\pi arj/n} \exp\left\{i\pi a\left[(j-k)^2 - 2rk + 2rj\right]/n\right\}$$
$$= (e_r)_j e^{-i\pi ar^2/n} e^{i\pi a[k-(j+r)]^2/n}.$$

Applying Lemma 4a gives

$$[M(n, a)e_r]_j = (e_r)_j n^{-1/2} e^{-i\pi ar^2/n} \sum_{k=0}^{n-1} e^{i\pi a[k-(j+r)]^2/n}$$
$$= n^{-1/2} S(n, a) e^{-i\pi ar^2/n} (e_r)_j$$
$$= \lambda_r (e_r)_j.$$

(b) The $j$th coordinate of $M(n,a)e_r$ is

$$[M(n,a)e_r]_j = n^{-1/2}\sum_{k=0}^{n-1} e^{i\pi a(j-k)^2/n} e^{-i\pi a(2r+1)k/n}.$$

Now the summand may be written

$$\begin{aligned} &e^{-i\pi a(2r+1)j/n}\exp\Big\{i\pi a\big[(j-k)^2-(2r+1)k+(2r+1)j\big]/n\Big\} \\ &= (e_r)_j e^{-i\pi a(r+\frac{1}{2})^2/n} e^{i\pi a[k-(j+r+\frac{1}{2})]^2/n}. \end{aligned}$$

Applying Lemma 4b gives

$$\begin{aligned} [M(n,a)e_r]_j &= (e_r)_j n^{-1/2} e^{-i\pi a(r+\frac{1}{2})^2/n}\sum_{k=0}^{n-1} e^{i\pi a[k-(j+r+\frac{1}{2})]^2/n} \\ &= \frac{n^{-1/2}}{2} S(4n,a) e^{-i\pi a(r+\frac{1}{2})^2/n}(e_r)_j \\ &= \lambda_r (e_r)_j. \qquad \square \end{aligned}$$

Applying Theorem 1 with $a=1$ (which is physically important since it corresponds to the smallest mass) we have the following Corollary.

**Corollary 6.** (a) *If $n$ is even, then*

$$\lambda_r = e^{i\pi/4} e^{-i\pi r^2/n}$$

*is an eigenvalue of $M(n,1)$, $r = 0,1,\ldots,n-1$.* (b) *If $n$ is odd, then*

$$\lambda_r = e^{i\pi/4} e^{-i\pi(r+\frac{1}{2})^2/n}$$

*is an eigenvalue of $M(n,1)$, $r = 0,1,\ldots,n-1$.*

It will follow from Theorem 7 that Corollary 6 lists all the eigenvalues of $M(n,1)$. However, in general, Theorem 5 does not determine all the eigenvalues of $M(n,a)$. This is because some of the $\lambda_r$'s may coincide and the corresponding $e_r$'s may be linearly dependent. In this

case, some of the eigenvalues will be missed. The simplest case of this occurs for the matrix

$$M(2,2) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}.$$

We then have $\lambda_0 = \lambda_1 = 0$ and $e_0 = e_1 = (1,1)$. We have missed the eigenvalue $\sqrt{2}$. Notice that $M(2,2)$ is not unitary. Our next result shows that this problem does not occur in the unitary case.

**Theorem 7.** *The vectors $e_r$, $r = 0, \ldots, n-1$, in Theorem 5 are mutually orthogonal if and only if $n$ and $a$ are relatively prime.*

**Proof.** If $na$ is even, then the inner product $\langle e_r, e_s \rangle$ satisfies

$$\langle e_r, e_s \rangle = \sum_{k=0}^{n-1} e^{i2\pi a(s-r)k/n}.$$

The proof now proceeds as in Theorem 3. If $na$ is odd, the proof is similar. □

**Corollary 8.** *The following statements are equivalent.* (a) *$n$ and $a$ are relatively prime.* (b) *$M(n,a)$ is unitary.* (c) *$e_r \perp e_s$ for $r \neq s = 0, \ldots, n-1$.*

**Corollary 9.** *If $n$ and $a$ are relatively prime, then all the eigenvalues of $M(n,a)$ are given in Theorem 5.*

Even in the unitary case, some of the eigenvalues can be degenerate; however, Theorem 5 gives a complete list together with an orthogonal basis of corresponding eigenvectors.

## 4. Probabilities

We now apply the results in Section 3 to compute probabilities. Let $P_r(t)$ be the probability that the particle is moving in direction $u_t$ after $r$ time steps given that it was initially moving in direction $u_0$. Then according to (7) we have

$$P_r(t) = \left| \langle M^r \hat{f}_0, \hat{f}_t \rangle \right|^2, \qquad M = M(n,a). \tag{11}$$

Denoting the normalized eigenvectors and eigenvalues of $M$ by $e_k$, $\lambda_k$, $k = 0, \ldots, n-1$, we have

$$M^r \hat{f}_0 = \sum_k \langle \hat{f}_0, e_k \rangle M^r e_k = \sum_k \langle \hat{f}_0, e_k \rangle \lambda_k^r e_k.$$

Hence,

$$\begin{aligned} \langle M^r \hat{f}_0, \hat{f}_t \rangle &= \sum_k \lambda_k^r \langle \hat{f}_0, e_k \rangle \langle e_k, \hat{f}_t \rangle \\ &= \frac{1}{\sqrt{n}} \sum_k \lambda_k^r (e_k)_t. \end{aligned}$$

Applying Theorem 5 gives for $na$ even

$$\langle M^r \hat{f}_0, \hat{f}_t \rangle = \frac{S(n,a)^r}{n^{\frac{r}{2}+1}} \sum_k e^{-i\pi a r k^2/n} e^{-i2\pi a k t/n}$$

and for $na$ odd

$$\langle M^r \hat{f}_0, \hat{f}_t \rangle = \frac{S(4n,a)^r}{2^r n^{\frac{r}{2}+1}} \sum_k e^{-i\pi a r (k+\frac{1}{2})^2/n} e^{-i2\pi a (k+\frac{1}{2}) t/n}.$$

Since $M$ is unitary, we have $|\lambda_k| = 1$, $k = 0, \ldots, n-1$. It follows from Theorem 5 that

$$|S(n,a)| = \sqrt{n} \quad \text{and} \quad |S(4n,a)| = 2\sqrt{n}.$$

Applying (11) for the case $na$ even, we obtain

$$\begin{aligned} P_r(t) &= \frac{1}{n^2} \Big| \sum_k e^{-i\pi a (rk+t)^2/nr} \Big|^2 \\ &= \frac{1}{n^2} \sum_{k,k'} \exp \frac{i\pi a}{nr} \big[ (rk'+t)^2 - (rk+t)^2 \big] \\ &= \frac{1}{n^2} \sum_{k,k'} \exp \frac{i\pi a}{n} (k'-k) \big[ r(k'+k) + 2t \big] \\ &= \frac{1}{n} + \frac{2}{n^2} \sum_{k=0}^{k'-1} \sum_{k'=1}^{n-1} \cos \left[ \frac{\pi a}{n} (k'-k)(r(k'+k)+2t) \right]. \end{aligned}$$

In a similar way, for $na$ odd we have

$$P_r(t) = \frac{1}{n} + \frac{2}{n^2} \sum_{k=0}^{k'-1} \sum_{k'=1}^{n-1} \cos\left[\frac{\pi a}{n}(k'-k)(r(k'+k+1)+2t)\right].$$

For example, in the simple case $n = 4$, $a = 1$, we have

$$P_r(t) = \frac{1}{4} + \frac{1}{8}\left[\cos\frac{\pi}{4}(r+2t) + \cos\pi(r+t) + \cos\frac{\pi}{4}(3r+2t) + \cos\frac{3\pi}{4}(3r+2t) + \cos\pi(2r+t) + \cos\frac{\pi}{4}(5r+2t)\right].$$

This last expression can be simplified as

$$P_r(t) = \frac{1}{8}\left[(1+(-1)^{r+t})\left(1+2\cos\frac{\pi t}{2}\cos\frac{\pi r}{4}\right) + 2\cos^2\frac{\pi t}{2}\right]. \qquad (12)$$

In this case, one can see from the form of the eigenvalues that the motion has period 8. Applying (12), the probabilities are tabulated in Table 1. Of course, for larger values of n the probabilities are much more complicated.

| $r$ | $P_r(0)$ | $P_r(1)$ | $P_r(2)$ | $P_r(3)$ |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 |
| 1 | 1/4 | 1/4 | 1/4 | 1/4 |
| 2 | 1/2 | 0 | 1/2 | 0 |
| 3 | 1/4 | 1/4 | 1/4 | 1/4 |
| 4 | 0 | 0 | 1 | 0 |
| 5 | 1/4 | 1/4 | 1/4 | 1/4 |
| 6 | 1/2 | 0 | 1/2 | 0 |
| 7 | 1/4 | 1/4 | 1/4 | 1/4 |
| 8 | 1 | 0 | 0 | 0 |
| ⋮ | | | | |

Table 1 (Probabilities $P_r(t)$)

## 5. Multiplicities

It was mentioned in Section 1 that the eigenvalue multiplicities for $M(n,a)$ were needed for certain elementary particle studies. There is also a mathematical reason for finding these multiplicities. By the spectral theorem [6] $M(n,a)$ has a unique representation of the form

$$M(n,a) = \sum_{j=1}^{m} \mu_j P_j$$

where $\mu_j$, $j = 1, \ldots, m$, are the distinct eigenvalues of $M(n,a)$ and $P_j$ is the orthogonal projection onto the eigenspace of $\mu_j$. Now the dimension of $P_j$ is the multiplicity $m_j$ of $\mu_j$. Moreover, since we have found the eigenvectors corresponding to $\mu_j$ in Theorem 5, this may enable us to compute $P_j$ by adding the $m_j$ one-dimensional projections corresponding to these eigenvectors.

We shall use the notation $(n,m)$ for the greatest common divisor of two integers $n, m$. In the sequel we shall assume that $M(n,a)$ is unitary and hence $(n,a) = 1$. We first consider the case in which $na$ is even. Let $\lambda_r$ be the (possibly repeated) eigenvalues of $M(n,a)$ as given in Theorem 5a, $r = 0, 1, \ldots, n-1$.

**Lemma 10.** *Let $na$ be even and let $0 \leq x < n$ be an integer. Then $\lambda_x = \lambda_r$ if and only if $x^2 = r^2 \pmod{n}$ for $n$ odd and $x^2 = r^2 \pmod{2n}$ for $n$ even.*

**Proof.** Applying Theorem 5a, $\lambda_x = \lambda_r$ if and only if

$$\frac{\pi a x^2}{n} = \frac{\pi a r^2}{n} \pmod{2\pi}$$

and the latter is equivalent to

$$a(x^2 - r^2) = 0 \pmod{2n}. \tag{13}$$

If $n$ is odd, then $a$ is even so $(n,a) = 1$ and (13) imply $x^2 - r^2 = 0 \pmod{n}$. □

To solve the congruence relation in Lemma 10 we shall need some results from elementary number theory. The next two lemmas appear as exercises 16, 18 (slightly modified) in [9; p. 301]. In the sequel, all numbers that we consider are integers.

**Lemma 11.** *Let $p$ be an odd prime, $e > 0$ and $0 \leq r < p^e$ with $r \neq 0 \pmod{p}$. The congruence*

$$x^2 = r^2 \pmod{p^e}, \quad 0 \leq x < p^e$$

*has exactly two solutions $x = r$ and $x = p^e - r$.*

**Proof.** If $x^2 = r^2 \pmod{p^e}$, then $p^e \mid (x - r)(x + r)$. But

$$(x + r) - (x - r) = 2r$$

so that $(x + r, x - r) \mid 2r$. Since $p$ is odd and $r \neq 0 \pmod{p}$ we have $(p, r) = 1$ and $(p, 2) = 1$. Hence, $(p, 2r) = 1$ and any distinct divisors of $2r$ and $p$ are relatively prime. We conclude that

$$((x + r, x - r), p) = 1.$$

It follows that either $p^e \mid (x + r)$ or $p^e \mid (x - r)$. The first case gives $x = p^e - r$ and the second case gives $x = r$. Conversely, both $r$ and $p^e - r$ are solutions to the congruence. They are distinct since $p^e - r = r$ would imply $p$ even. □

**Lemma 12.** *For $e > 0$, let $r$ be odd with $0 \leq r < 2^e$. The congruence*

$$x^2 = r^2 \pmod{2^e}, \quad 0 \leq x < 2^e$$

*has exactly four solutions if $e \geq 3$, exactly two solutions if $e = 2$ and exactly one solution if $e = 1$.*

**Proof.** If $x^2 = r^2 \pmod{2^e}$, then as in the proof of Lemma 11, $(x + r, x - r) \mid 2r$. Since $r$ is odd, $(x + r, x - r)$ contains at most one factor 2. Hence, one of the following possibilities holds

$$\begin{array}{lll} 2^e \mid x + r & \text{with} & 0 \leq x + r < 2^{e+1} \\ 2^e \mid x - r & \text{with} & -2^e < x - r < 2^e \\ 2^{e-1} \mid x - r & \text{with} & -2^e < x - r < 2^e \\ 2^{e-1} \mid x + r & \text{with} & 0 \leq x + r < 2^{e+1}. \end{array}$$

These give the possible solutions $x = 2^e - r$, $x = r$, $x = 2^{e-1} + r$, $x = 2^{e-1} - r$. Conversely, these numbers clearly satisfy the given congruence. If $e \geq 3$, the solutions are distinct. Indeed, otherwise we obtain one of the following contradictions.

$$\begin{aligned}
2^e - r &= r &\Rightarrow \quad r &= 2^{e-1} \\
2^e - r &= 2^{e-1} + r \Rightarrow \quad r &= 2(2^{e-2} - 2^{e-3}) \\
2^e - r &= 2^{e-1} - r \Rightarrow \quad 2^e &= 2^{e-1} \\
r &= 2^{e-1} + r \Rightarrow \quad 2^{e-1} &= 0 \\
r &= 2^{e-1} - r \Rightarrow \quad r &= 2^{e-2} \\
2^{e-1} + r &= 2^{e-1} - r \Rightarrow \quad r &= 0.
\end{aligned}$$

If $e = 2$, then the congruence becomes $x^2 = r^2 \pmod 4$, $0 \le x < 4$. Since $1^2 = 1 \pmod 4$, $3^2 = 1 \pmod 4$, there are two distinct solutions $x = r$, $x = 4 - r$. If $e = 1$, there is only one solution $x = r = 1$. □

Notice that Lemmas 11 and 12 solve our desired congruence relation for the case in which $n$ has only one prime factor and $(r, n) = 1$. The next lemma extends this to the case $(r, n) = 1$ for general $n$.

**Lemma 13.** *Let $0 \le r < n$ with $(r, n) = 1$ and let $k$ be the number of distinct prime divisors of $n$. The congruence*

$$x^2 = r^2 \pmod n, \quad 0 \le x < n$$

*has exactly* (a) $2^k$ *solutions if $n$ is odd,* (b) $2^{k-1}$ *solutions if $n$ is even, $n \neq 0 \pmod 4$,* (c) $2^k$ *solutions if $n = 0 \pmod 4$, $n \neq 0 \pmod 8$,* (d) $2^{k+1}$ *solutions if $n = 0 \pmod 8$.*

**Proof.** Let $n$ have the prime factorization

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}.$$

First suppose that $n$ is odd. Then $x^2 = r^2 \pmod n$ if and only if $x^2 = r^2 \pmod{p_i^{e_i}}$, $i = 1, \dots, k$. Let $r_i$ be the residue of $r$ modulo $p_i^{e_i}$. Then $x^2 = r^2 \pmod n$ if and only if $x^2 = r_i^2 \pmod{p_i^{e_i}}$, $i = 1, \dots, k$. From Lemma 11, each congruence $x^2 = r_i^2 \pmod{p_i^{e_i}}$ has exactly two solutions, $r_i$ and $p_i^{e_i} - r_i$. Hence, $x = \pm r_i \pmod{p_i^{e_i}}$, $i = 1, \dots, k$, and this gives $2^k$ systems of congruence relations. By the Chinese Remainder Theorem [9] each system has a unique solution modulo $n$. Moreover, the solutions cannot overlap since $(r, n) = 1$. Hence, there are $2^k$ distinct solutions. Now suppose that $n$ is even and that $n$ has the above prime decomposition with $p_1 = 2$. As before, $x^2 = r^2 \pmod n$ if and only if $x^2 = r_i^2 \pmod{p_i^{e_i}}$, $i = 1, \dots, k$. For $i \ge 2$, we have $x = \pm r_i \pmod{p_i^{e_i}}$. For $i = 1$, we have $x^2 = r_1^2 \pmod{2^{e_1}}$. Applying Lemma 12, this latter congruence has one solution if $e_1 = 1$ ($n \neq 0 \pmod 4$), two

solutions if $e_1 = 2$ ($n = 0 \pmod 4$, $n \neq 0 \pmod 8$) and four solutions if $e_1 = 3$ ($n = 0 \pmod 8$). Proceeding as before, the result is obtained. □

It follows from Lemma 13 that the number of distinct solutions of $x^2 = r^2 \pmod n$, $0 \leq x < n$, is independent of $r$ if $(r, n) = 1$. We denote this number of solutions by $\psi(n)$. That is, $\psi(n) = 2^j$ where $j$ equals $k-1$, or $k$, or $k+1$ depending on the value of $n$. For an arbitrary $0 \leq r < n$, define the function or two variables $d = d(r, n) = (r^2, n)$, let $\delta^2 = \delta^2(r, n)$ be the smallest positive square multiple of $d$ and let $\Delta = \Delta(r, n) = d/\delta$. The next theorem extends Lemma 13 to the general case.

**Theorem 14.** *If $0 \leq r < n$, then the congruence*

$$x^2 = r^2 \pmod n, \quad 0 \leq x < n \tag{14}$$

*has $\Delta\psi(n/d)$ distinct solutions.*

**Proof.** If $x$ is a solution to (14), then $x^2$ is a multiple of $d$. Hence, $x^2$ is a multiple of $\delta^2$. It follows that $x$ is a multiple of $\delta$. It is clear that $\delta^2 = dd'$ where $d'$ is the product of the prime divisors of $d$ that have odd exponents in the prime factorization of $d$. For $0 \leq x < n$, (14) is equivalent to

$$\delta^2\left[\frac{x^2}{\delta^2} - \frac{r^2}{\delta^2}\right] = 0 \pmod n$$

which is equivalent to

$$d'\left[\frac{x^2}{\delta^2} - \frac{r^2}{\delta^2}\right] = 0 \pmod{n/d}. \tag{15}$$

We now show that $(d', n/d) = 1$. Let $\alpha$ be a positive integer. If $\alpha \mid (d', n/d)$ then $\alpha d \mid (\delta^2, n)$. But $\delta^2 \mid r^2$ so $\alpha d \mid (r^2, n)$. But $(r^2, n) = d$ so $\alpha = 1$. We next show that $(r/\delta, n/d) = 1$. If $\alpha \mid (r/\delta, n/d)$ then $\alpha\delta^2 \mid r^2$ and $\alpha d \mid n$. But $\alpha d \mid \alpha\delta^2$ so $\alpha d \mid (r^2, n)$. Again, we have $\alpha = 1$. It now follows from (15) that $x^2 = r^2 \pmod n$ if and only if

$$\left(\frac{x}{\delta}\right)^2 = \left(\frac{r}{\delta}\right)^2 \pmod{n/d}$$

where $(r/\delta, n/d) = 1$. Applying Lemma 13, the number of solutions modulo $n/d$ to

$$x^2 = \left(\frac{r}{\delta}\right)^2 \pmod{n/d} \tag{16}$$

is $\psi(n/d)$. Let $x_0$ be a solution to (16). Then $x/\delta = x_0 \pmod{n/d}$ if and only if

$$x = \delta x_0 + m\frac{\delta}{d}n, \quad 0 \le m < \frac{d}{\delta}.$$

Hence, for each solution of (16) we have $\Delta = d/\delta$ distinct solutions to (14). Also, two different solutions to (16) cannot yield the same solution to (14). Indeed, if

$$\delta x_0 + m\frac{\delta}{d}n = \delta x_1 + m'\frac{\delta}{d}n$$

then $x_0 - x_1 = (m' - m)n/d$. But $0 \le x_0,\ x_1 < n/d$. Hence $m = m'$ which implies $x_0 = x_1$. Hence, (14) has $\Delta\psi(n/d)$ distinct solutions. □

Lemma 10 and Theorem 14 together now give the multiplicities for the case $na$ even. But as we shall see in the proof of the next theorem, the case $na$ odd can be reduced to the $na$ even case giving a complete solution. We continue to assume that $(n, a) = 1$ and that $\lambda_r$, $r = 0, \ldots, n-1$ are the (possibly repeated) eigenvalues of $M(n, a)$ given in Theorem 5. We use the notation $\psi(r, n) = \psi(n/d(r, n))$.

**Theorem 15.** *The multiplicity of $\lambda_r$ is*

(a) $\Delta(r, n)\psi(r, n)$ *if $a$ is even*
(b) $\frac{\Delta(r,2n)}{2}\psi(r, 2n)$ *if $n$ is even*
(c) $\Delta(2r + 1, n)\psi(2r + 1, n)$ *otherwise.*

**Proof.** (a) In this case $na$ is even and $n$ is odd. Applying Lemma 10 and Theorem 14 gives the result. (b) Again $na$ is even. By Lemma 10, $\lambda_x = \lambda_r$ if and only if $x^2 = r^2 \pmod{2n}$. But we are only concerned with the solutions modulo $n$. By Theorem 14, $x^2 = r^2 \pmod{2n}$ has

$$\Delta(r, 2n)\psi\left[\frac{2n}{d(r, 2n)}\right] = \Delta(r, 2n)\psi(r, 2n)$$

solutions modulo $2n$. However, since $n$ is even, for every $0 \le x < n$, $(x + n)^2 = x^2 \pmod{2n}$. Hence, there are twice as many solutions modulo $2n$ as there are modulo $n$. This completes the proof of (b).

(c) In this case $na$ is odd and the eigenvalues $\lambda_r$, $0 \leq r < n$, of $M(n,a)$ are given in Theorem 5b. Let $\mu_{2r+1}$ be the $(2r+1)$th eigenvalue listed for $M(4n,a)$. Applying Theorem 5, we have $\lambda_r = \mu_{2r+1}$, $0 \leq r < n$. The multiplicity of $\mu_{2r+1}$ is twice the multiplicity of $\lambda_r$. Indeed, we are only concerned with finding the numbers $0 \leq x < 2n$ such that $\mu_x = \mu_{2r+1}$ and for such $x$, $\mu_{4n-x} = \mu_x$ since

$$(4n - x)^2 = x^2 \pmod{8n}.$$

Applying Part b of this theorem, the multiplicity $m_r$ of $\lambda_r$ becomes

$$m_r = \frac{\Delta(2r+1, 8n)}{4}\psi(2r+1, 8n).$$

Since $2r+1$ is odd we have

$$d(2r+1, 8n) = ((2r+1)^2, 8n) = ((2r+1)^2, n) = d(2r+1, n).$$

Hence,

$$\Delta(2r+1, 8n) = \Delta(2r+1, n)$$

and

$$m_r = \frac{\Delta(2r+1, n)}{4}\psi(2r+1, 8n).$$

Since $n/d(2r+1, n)$ is odd, applying Lemma 13a we have $\psi(2r+1, n) = 2^k$ where $k$ is the number of distinct prime divisors of $n/d(2r+1, n)$. Since

$$8n/d(2r+1, n) = 0 \pmod{8}$$

and $8n/d(2r+1, n)$ has $k+1$ distinct prime divisors, applying Lemma 13d we have $\psi(2r+1, 8n) = 2^{k+2}$. Hence,

$$\psi(2r+1, 8n) = 4\psi(2r+1, n).$$

The result now follows. □

**Acknowledgement**

We would like to thank Professor Paul Pedersen for pointing out some relevant references and theorems in number theory.

## Références

[1] T. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
[2] E. Cinlar, *Introduction to Stochastic Processes*, Prentice Hall, Englewood Cliffs, NJ, 1975.
[3] F. Close, *An Introduction to Quarks and Partons*, Academic Press, London, 1979.
[4] L. Dickson, *Studies in the Theory of Numbers*, University of Chicago Press, Chicago, 1930.
[5] R. Feynman and A. Hibbs, *Quantum Mechanics and Path Integrals*, McGraw-Hill, New York, 1965.
[6] S. Friedberg, A. Insel, and L. Spence, *Linear Algebra*, Prentice Hall, Englewood Cliffs, NJ, 1979.
[7] S. Gudder, *Quantum Probability*, Academic Press, Orlando, 1988.
[8] _____, "Finite model for particles", *Hadronic J.* (to appear).
[9] K. Rosen, *Elementary Number Theory and its Applications*, Addison Wesley, Reading, MA, 1984.
[10] L. Schulman, *Techniques and Aplications of Path Integration*, Wiley (Interscience), New York, 1981.
[11] A. Sudbery, *Quantum Mechanics and the Particles of Nature*, Cambridge University Press, Cambridge, England, 1986.

*(Manuscrit reçu le 11 janvier 1989)*