A new type of limit theorems for the one-dimensional quantum random walk

By Norio KONNO

Abstract. In this paper we consider the one-dimensional quantum random walk X_n^{φ} at time n starting from initial qubit state φ determined by 2×2 unitary matrix U. We give a combinatorial expression for the characteristic function of X_n^{φ}. The expression clarifies the dependence of it on components of unitary matrix U and initial qubit state φ. As a consequence, we present a new type of limit theorems for the quantum random walk. In contrast with the de Moivre-Laplace limit theorem, our symmetric case implies that X_n^{φ}/n converges weakly to a limit Z^{φ} as $n \to \infty$, where Z^{φ} has a density $1/\pi(1-x^2)\sqrt{1-2x^2}$ for $x \in (-1/\sqrt{2}, 1/\sqrt{2})$. Moreover we discuss some known simulation results based on our limit theorems.

1 Introduction.

The classical random walk on the line is the motion of a particle which inhabits the set of integers. The particle moves at each time step either one unit to the left with probability p or one unit to the right with probability $q = 1 - p$. The directions of different steps are independent of each other. This classical random walk is often called the simple random walk. For general random walks on a countable space, there is a beautiful theory (see Spitzer [12]). In the presnet paper, we consider quantum variations of the classical random walk and refer to such processes as quantum random walks.

Very recently quantum random walks have been widely investigated by a number of groups in connection with the quantum computing, for exmples, [1, 3, 4, 5, 6, 8, 9, 13, 14]. For more general setting including quantum cellular automata, see Meyer [7]. This paper is an extended version of our previous short letter with no proof (Konno [4]).

In Ambainis *et al.* [1], they gave two general ideas for analyzing quantum random walks. One is the path integral approach, the other is the Schrödinger approach. In this paper, we take the path integral approach, that is, the probability amplitude of a state for the quantum random walk is given as a combinatorial sum over all possible paths leading to that state.

The quantum random walk considered here is determined by 2×2 unitary matrix U stated in the next section. The new points of this paper is to introduce 4 matrices, P, Q, R and S

2000 Mathematics Subject Classification. Primary 60F05; Secondary 60G50, 82B41, 81Q99.

Key Words and Phrases. Quantum random walk, the Hadamard walk, limit theorems.

This work was partially supported by the Grant-in-Aid for Scientific Research (B) (No.12440024) of Japan Society of the Promotion of Science.

given by the unitary matrix U, to obtain a combinatorial expression for the characteristic function by using them, and to clarify the dependence of the mth moment and symmetry of distribution for the quantum random walk on the unitary matrix U and initial *qubit* (quantum bit) state φ. Furthermore we give a new type of limit theorems for the quantum random walk by using our results. Our limit theorem shows that the behavior of quantum random walk is remarkably different from that of the classical ramdom walk. As a corollary, it reveals whether some simulation results already known are accurate or not.

The rest of the paper is organized as follows. In Section 2, we introduce a definition of the quantum random walk and explain our results. Section 3 gives the characteristic function. In Section 4, we present a condition for symmetry of the distribution. Section 5 is devoted to a proof of the limit theorem. In Section 6, we consider the Hadamard walk case.

2 Definition and results.

The time evolution of the one-dimensional quantum random walk studied here is given by the following unitary matrix:

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

where $a, b, c, d \in \mathbf{C}$ and $\mathbf{C}$ is the set of the complex numbers. So we have $|a|^2 + |c|^2 = |b|^2 + |d|^2 = 1$, $a\overline{c} + b\overline{d} = 0$, $c = -\triangle\overline{b}$, and $d = \triangle\overline{a}$, where $\overline{z}$ is the complex conjugate of $z \in \mathbf{C}$ and $\triangle = \det U = ad - bc$. We note that the unitarity of U gives $|\triangle| = 1$.

The quantum random walk is a quantum generalization of the classical random walk in one dimension with an additional degree of freedom called the chirality. The chirality takes values *left* and *right*, and means the direction of the motion of the particle. The evolution of the quantum random walk is given by the following way. At each time step, if the particle has the left chirality, it moves one unit to the left, and if it has the right chirality, it moves one unit to the right. More precisely, we present the left and right chirality states as $|L\rangle = {}^t[1, 0]$ and $|R\rangle = {}^t[0, 1]$, where t indicates the transposed operator. So the unitary matrix U acts on two chirality states $|L\rangle$ and $|R\rangle$ as

$$U|L\rangle = a|L\rangle + c|R\rangle, \qquad U|R\rangle = b|L\rangle + d|R\rangle.$$

The study on the dependence of some important quantities (e.g., characteristic function, the mth moment, limit density) on initial qubit state is one of the essential parts, so we define the set of initial qubit states as follows:

$$\Phi = \left\{ \varphi = {}^t[\alpha, \beta] \in \mathbf{C}^2 : |\alpha|^2 + |\beta|^2 = 1 \right\}.$$

From now on, we will give a precise definition of the quantum random walk X_n^{φ} at time n starting from initial qubit state $\varphi \in \Phi$. First we decompose $U = P + Q$, where

$$P = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, \quad Q = \begin{bmatrix} 0 & 0 \\ c & d \end{bmatrix}.$$

The important point is that P (resp. Q) represents that the particle moves to the left (resp. right). We define the $(4N+2)\times(4N+2)$ matrix by

$$\overline{U}_N = \begin{bmatrix} 0 & P & 0 & \dots & \dots & 0 & Q \\ Q & 0 & P & 0 & \dots & \dots & 0 \\ 0 & Q & 0 & P & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & Q & 0 & P & 0 \\ 0 & \dots & \dots & 0 & Q & 0 & P \\ P & 0 & \dots & \dots & 0 & Q & 0 \end{bmatrix}, \qquad \text{with} \qquad 0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Then we see that $\overline{U}_N$ becomes also unitary matrix, since P and Q satisfy

$$PP^* + QQ^* = P^*P + Q^*Q = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad PQ^* = QP^* = Q^*P = P^*Q = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

where $*$ means the adjoint operator. Here an initial qubit state is given by

$$\Psi^{(0)}(\varphi) = \begin{bmatrix} 0_N \\ \varphi \\ 0_N \end{bmatrix} \in \mathbf{C}^{4N+2},$$

where $0_N = {}^t[0,\dots,0] \in \mathbf{C}^{2N}$ is the zero vector and $\varphi = {}^t[\alpha,\beta]$. The qubit state at time n, $\Psi^{(n)}(\varphi)$, is determined by

$$\Psi^{(n)}(\varphi) = (\overline{U}_N)^n \Psi^{(0)}(\varphi). \tag{2.1}$$

We write

$$\Psi^{(n)}(\varphi) = {}^t[\Psi^{(n)}_{-N}(\varphi), \Psi^{(n)}_{-(N-1)}(\varphi), \dots, \Psi^{(n)}_{N}(\varphi)],$$
$$\Psi^{(n)}_k(\varphi) = \begin{bmatrix} \Psi^{(n)}_{L,k}(\varphi) \\ \Psi^{(n)}_{R,k}(\varphi) \end{bmatrix} = \Psi^{(n)}_{L,k}(\varphi)|L\rangle + \Psi^{(n)}_{R,k}(\varphi)|R\rangle \in \mathbf{C}^2.$$

Then $\Psi^{(n)}_k(\varphi)$ is the two component vector of amplitudes of the particle being at site k and at time n with the chirality being left (upper component) and right (lower component). We see that (2.1) implies

$$\Psi^{(n+1)}_k(\varphi) = (\overline{U}_N\Psi^{(n)}(\varphi))_k = Q\Psi^{(n)}_{k-1}(\varphi) + P\Psi^{(n)}_{k+1}(\varphi). \tag{2.2}$$

We define the quantum random walk X^{φ}_n with state space $\{-N,\dots,N\}$ by

$$P(X^{\varphi}_n = k) = \|\Psi^{(n)}_k(\varphi)\|^2.$$

By construction $P(X^{\varphi}_0 = 0) = 1$. We remark $P(X^{\varphi}_n = k)$ is independent of N as far as $n \le N$. Hence we naturally regard X^{φ}_n as a $\mathbf{Z}$-valued random variable, where $\mathbf{Z}$ is the set of the integers, and denote by the same symbol X^{φ}_n.

In contrast with classical random walks, X_n^{φ} can not be written as $X_n^{\varphi} = Y_1 + \cdots + Y_n$, where $Y_1, Y_2, \dots$ are independent and identically distributed random variables. It is also noted that the quantum random walk is not a stochastic process. It is a sequence of distributions arising from products of the unitary matrix $\overline{U}_N$. The unitarity of $\overline{U}_N$ ensures

$$\sum_{k \in \mathbf{Z}} P(X_n^{\varphi} = k) = \|(\overline{U}_N)^n \overline{\varphi}\|^2 = \|\overline{\varphi}\|^2 = |\alpha|^2 + |\beta|^2 = 1,$$

for any $1 \le n \le N$ and initial state $\overline{\varphi} = {}^t[0_N, \varphi, 0_N]$. That is, the amplitude always defines a probability distribution for the location. For initial state $\overline{\varphi} = {}^t[0_N, \varphi, 0_N]$, we have

$$\begin{aligned}
&\overline{U}_N \overline{\varphi} = {}^t[0_{N-1}, P\varphi, 0, Q\varphi, 0_{N-1}], \\
&\overline{U}_N^2 \overline{\varphi} = {}^t[0_{N-2}, P^2\varphi, 0, (PQ+QP)\varphi, 0, Q^2\varphi, 0_{N-2}], \\
&\overline{U}_N^3 \overline{\varphi} = {}^t[0_{N-3}, P^3\varphi, 0, (P^2Q + PQP + QP^2)\varphi, 0, (Q^2P + QPQ + PQ^2)\varphi, 0, Q^3\varphi, 0_{N-3}].
\end{aligned}$$

This shows that expansion of $U^n = (P+Q)^n$ for the quantum random walk corresponds to that of $1^n = (p+q)^n$ for the classical random walk.

We now explain our results briefly. Using an explicit form of $P(X_n^{\varphi} = k)$ (Lemma 3), we obtain the characteristic function of X_n^{φ} (Theorem 4) and the mth moment of it (Corollary 5). One of the interesting facts is that, when m is even, the mth moment of X_n^{φ} is independent of the initial qubit state $\varphi \in \Phi$. On the other hand, when m is odd, the mth moment depends on the initial qubit state. So the standard deviation of X_n^{φ} depends on the initial qubit state $\varphi \in \Phi$. Our main theorem is as follows:

THEOREM 1. *Suppose $abcd \neq 0$. Then we have*

$$\lim_{n\to\infty} \frac{X_n^{\varphi}}{n} = Z^{\varphi} \qquad \textit{in law},$$

where Z^{φ} is a random variable whose distribution has a density $f_{\alpha,\beta}(x)dx$ such that

$$f_{\alpha,\beta}(x) = \frac{\sqrt{1-|a|^2}\,(1-\lambda_{\alpha,\beta}x)}{\pi(1-x^2)\sqrt{|a|^2 - x^2}}, \qquad \textit{with} \;\; \lambda_{\alpha,\beta} = |\alpha|^2 - |\beta|^2 + \frac{a\alpha\overline{b\beta} + \overline{a\alpha}b\beta}{|a|^2},$$

for $x \in (-|a|, |a|)$, and $f_{\alpha,\beta}(x) = 0$ for $|x| \ge |a|$. Here $\varphi = {}^t[\alpha, \beta]$ as before.

It can be confirmed that $f_{\alpha,\beta}(x)$ satisfies the property of a density function. Indeed, we see that $f_{\alpha,\beta}(x) \ge 0$ since $1 \pm \lambda_{\alpha,\beta}|a| \ge 0$, and that

$$\begin{aligned}
\int_{-|a|}^{|a|} f_{\alpha,\beta}(x)\,dx &= \frac{\sqrt{1-|a|^2}}{\pi} \int_0^1 t^{-1/2}(1-t)^{-1/2}(1-|a|^2t)^{-1}\,dt \\
&= \frac{\sqrt{1-|a|^2}}{\pi} \Gamma(1/2)^2 {}_2F_1(1/2, 1; 1; |a|^2) \\
&= 1.
\end{aligned}$$

Here ${}_2F_1(a, b; c; z)$ is the hypergeometric function (see Sect. 5). The last equality comes from $\Gamma(1/2) = \sqrt{\pi}$ and ${}_2F_1(1/2, 1; 1; |a|^2) = 1/\sqrt{1-|a|^2}$. Remark that

$$E(Z^{\varphi}) = -(1 - \sqrt{1-|a|^2})\,\lambda_{\alpha,\beta}, \quad E((Z^{\varphi})^2) = 1 - \sqrt{1-|a|^2}.$$

Moreover, an easy computation shows that $|E((Z^{\varphi})^m)| \le 2|a|^m$ for any $m \ge 1$.

It should be noted that, if $|a| = 1$, then $b = c = 0$ and $|d| = 1$. So this case is trivial. In fact, Corollary 5 (ii) implies that $\lim_{n\to\infty} X_n^{\varphi}/n = W^{\varphi}$, in law, where W^{φ} is determined by $P(W^{\varphi} = -1) = |\alpha|^2$ and $P(W^{\varphi} = 1) = |\beta|^2$. Theorem 1 suggests the following result on symmetry of distribution for the quantum random walk (Theorem 6). Define

$$\begin{aligned}
\Phi_s &= \{\varphi \in \Phi : \ P(X_n^{\varphi} = k) = P(X_n^{\varphi} = -k) \ \text{for any } n \in \mathbf{Z}_+ \text{ and } k \in \mathbf{Z}\}, \\
\Phi_0 &= \{\varphi \in \Phi : \ E(X_n^{\varphi}) = 0 \ \text{for any } n \in \mathbf{Z}_+\}, \\
\Phi_\perp &= \left\{\varphi = {}^t[\alpha, \beta] \in \Phi : |\alpha| = |\beta| = 1/\sqrt{2}, \ a\alpha\overline{b\beta} + \overline{a\alpha}b\beta = 0\right\},
\end{aligned}$$

where $\mathbf{Z}_+$ is the set of the positive integers. For $\varphi \in \Phi_s$, the probability distribution of X_n^{φ} is symmetric for any $n \in \mathbf{Z}_+$. Using explicit forms of distribution of X_n^{φ} (Lemma 3) and $E(X_n^{\varphi})$ (Corollary 5 (i) for $m = 1$ case), we have $\Phi_s = \Phi_0 = \Phi_\perp$.

3 Characteristic function.

This section gives a combinatorial expression of the characteristic function of the quantum random walk X_n^{φ}. As a corollary, we obtain the mth moment of X_n^{φ}. For fixed l and m, we consider

$$\Xi(l, m) = \sum_{l_j, m_j \ge 0: l_1 + \cdots + l_n = l, m_1 + \cdots + m_n = m} P^{l_1} Q^{m_1} P^{l_2} Q^{m_2} \cdots P^{l_n} Q^{m_n}.$$

It should be noted that for $l + m = n$ and $-l + m = k$, we see that $\Psi_k^{(n)}(\varphi) = \Xi(l, m)\varphi$, since $\Psi_k^{(n)}(\varphi) = {}^t[\Psi_{L,k}^{(n)}(\varphi), \Psi_{R,k}^{(n)}(\varphi)] (\in \mathbf{C}^2)$ is a two component vector of amplitudes of the particle being at site k at time n for initial qubit state $\varphi \in \Phi$ and $\Xi(l, m)$ is the sum of all possible paths in the trajectory consisting of l steps left and m steps right with $l = (n - k)/2$ and $m = (n + k)/2$ (see (2.2)). For example, in the case of $P(X_4^{\varphi} = -2)$, we have the following expression:

$$\Xi(3, 1) = QP^3 + PQP^2 + P^2QP + P^3Q.$$

Here we find a nice relation: $P^2 = aP$. By using this, we have $\Xi(3, 1) = a^2QP + aPQP + aPQP + a^2PQ$. Moreover, to compute general $\Xi(l, m)$, it is convenient to introduce

$$R = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}, \quad S = \begin{bmatrix} 0 & 0 \\ a & b \end{bmatrix}.$$

Then we obtain the following table of products of the matrices P, Q, R and S:

	P	Q	R	S
P	aP	bR	aR	bP
Q	cS	dQ	cQ	dS
R	cP	dR	cR	dP
S	aS	bQ	aQ	bS

Table 1

where $PQ = bR$, for example. Since P, Q, R and S form an orthonormal basis of the vector space of complex 2×2 matrices with respect to the trace inner product $\langle A|B\rangle = \mathrm{tr}(A^*B)$, $\Xi(l,m)$ has the following form:

$$\Xi(l,m) = p_n(l,m)P + q_n(l,m)Q + r_n(l,m)R + s_n(l,m)S.$$

Next problem is to obtain explicit forms of $p_n(l,m), q_n(l,m), r_n(l,m)$, and $s_n(l,m)$. The above example of $n = l + m = 4$ case, we have

$$\begin{aligned}
&\Xi(4,0) = a^3P, \quad \Xi(3,1) = 2abcP + a^2bR + a^2cS, \\
&\Xi(2,2) = bcdP + abcQ + b(ad+bc)R + c(ad+bc)S, \\
&\Xi(1,3) = 2bcdQ + bd^2R + cd^2S, \quad \Xi(2,2) = d^3Q.
\end{aligned}$$

So, for example, $p_4(3,1) = 2abc$, $q_4(3,1) = 0$, $r_4(3,1) = a^2b$, and $s_4(3,1) = a^2c$. The following holds in general.

LEMMA 2. *We write $l \wedge m = \min\{l,m\}$. Suppose $abcd \neq 0$. Then*
(i) for $l \wedge m \geq 1$, we have

$$\Xi(l,m) = a^l \overline{a}^m \triangle^m \sum_{\gamma=1}^{l\wedge m} \left(-\frac{|b|^2}{|a|^2}\right)^\gamma \binom{l-1}{\gamma-1}\binom{m-1}{\gamma-1} \left[\frac{l-\gamma}{a\gamma}P + \frac{m-\gamma}{\triangle\overline{a}\gamma}Q - \frac{1}{\triangle\overline{b}}R + \frac{1}{b}S\right],$$

(ii) for $l \geq 1$ and $m = 0$, we have $\Xi(l,0) = a^{l-1}P$,
(iii) for $l = 0$ and $m \geq 1$, we have $\Xi(0,m) = \triangle^{m-1}\overline{a}^{m-1}Q$.

Proof. We first calculate explicit forms of $p_n(l,m)$. To begin, we assume $l \geq 2$ and $m \geq 1$. From Table 1, it is sufficient to consider only the following case:

$$C(w)_{\gamma,l,m} = P^{w_1}Q^{w_2}P^{w_3}\cdots Q^{w_{2\gamma}}P^{w_{2\gamma+1}},$$

where $w = (w_i) \in \mathbf{Z}_+^{2\gamma+1}$, with $l = \sum_{k=0}^{\gamma} w_{2k+1}$ and $m = \sum_{k=1}^{\gamma} w_{2k}$. For example, we take $w_1 = w_2 = w_3 = 1$ and $\gamma = 1$ as PQP. We remark that $2\gamma+1$ is the number of clusters of P's and Q's. Next we consider the range of γ. The minimum is $\gamma = 1$, that is, 3 clusters. This case is $P\cdots PQ\cdots QP\cdots P$. The maximum is $\gamma = (l-1)\wedge m$. This case includes the patterns for example:

$$PQPQPQ\cdots PQPQPP\cdots PP\ (l-1 \geq m), \quad PQPQPQ\cdots PQPQQ\cdots QQP\ (l-1 \leq m).$$

We introduce a set of sequences with $2\gamma+1$ components: for fixed $\gamma \in [1, (l-1)\wedge m]$,

$$W_{\gamma,l,m} = \{w = (w_i) \in \mathbf{Z}_+^{2\gamma+1} : \sum_{k=0}^{\gamma} w_{2k+1} = l,\ \sum_{k=1}^{\gamma} w_{2k} = m\}.$$

By a standard combinatorial argument, we have

$$|W_{\gamma,l,m}| = \binom{l-1}{\gamma}\binom{m-1}{\gamma-1}. \tag{3.1}$$

Let $w \in W_{\gamma,l,m}$. Then by using Table 1, we have

$$\begin{aligned} C(w)_{\gamma,l,m} &= a^{w_1-1}Pd^{w_2-1}Qa^{w_3-1}P\cdots d^{w_{2\gamma}-1}Qa^{w_{2\gamma+1}-1}P \\ &= a^{l-(\gamma+1)}d^{m-\gamma}(PQ)^{\gamma}P \\ &= a^{l-(\gamma+1)}d^{m-\gamma}b^{\gamma}c^{\gamma}P. \end{aligned} \tag{3.2}$$

Combining (3.1) and (3.2), we obtain

$$\begin{aligned} p_n(l,m)P &= \sum_{\gamma=1}^{(l-1)\wedge m}\sum_{w\in W_{\gamma,l,m}} C(w)_{\gamma,l,m} \\ &= \sum_{\gamma=1}^{(l-1)\wedge m}\binom{l-1}{\gamma}\binom{m-1}{\gamma-1}a^{l-(\gamma+1)}b^{\gamma}c^{\gamma}d^{m-\gamma}P. \end{aligned}$$

When $l \geq 1$ and $m = 0$, it is easy to see that $p_n(l,0)P = P^l = a^{l-1}P$. Furthermore, when $l = 1, m \geq 1$ and $l = 0, m \geq 0$, it is clear that $p_n(l,m) = 0$.

As in the case of $p_n(l,m)$, we compute $q_n(l,m), r_n(l,m)$, and $s_n(l,m)$ by considering the patterns $Q^{w_1}P^{w_2}Q^{w_3}\cdots P^{w_{2\gamma}}Q^{w_{2\gamma+1}}$, $P^{w_1}Q^{w_2}P^{w_3}\cdots Q^{w_{2\gamma}}$, and $Q^{w_1}P^{w_2}Q^{w_3}\cdots P^{w_{2\gamma}}$, respectively. Then we obtain

$$q_n(l,m) = \begin{cases} \sum_{\gamma=1}^{l\wedge(m-1)}\binom{l-1}{\gamma-1}\binom{m-1}{\gamma}a^{l-\gamma}b^{\gamma}c^{\gamma}d^{m-(\gamma+1)} & \text{for } l \geq 1, m \geq 2, \\ d^{m-1} & \text{for } l = 0, m \geq 1, \\ 0 & \text{for } m = 1, l \geq 1 \text{ and } m = 0, l \geq 0, \end{cases}$$

$$r_n(l,m) = \begin{cases} \sum_{\gamma=1}^{l\wedge m}\binom{l-1}{\gamma-1}\binom{m-1}{\gamma-1}a^{l-\gamma}b^{\gamma}c^{\gamma-1}d^{m-\gamma} & \text{for } l,m \geq 1, \\ 0 & \text{for } l\wedge m = 0, \end{cases}$$

$$s_n(l,m) = \begin{cases} \sum_{\gamma=1}^{l\wedge m}\binom{l-1}{\gamma-1}\binom{m-1}{\gamma-1}a^{l-\gamma}b^{\gamma-1}c^{\gamma}d^{m-\gamma} & \text{for } l,m \geq 1, \\ 0 & \text{for } l\wedge m = 0. \end{cases}$$

For $l \wedge m \geq 1$, the above explicit forms of $p(l,m), q_n(l,m), r_n(l,m)$, and $s_n(l,m)$ imply

$$\Xi(l,m) = a^l d^m \sum_{\gamma=1}^{l\wedge m}\left(\frac{bc}{ad}\right)^{\gamma}\binom{l-1}{\gamma-1}\binom{m-1}{\gamma-1}\left[\frac{l-\gamma}{a\gamma}P + \frac{m-\gamma}{d\gamma}Q + \frac{1}{c}R + \frac{1}{b}S\right].$$

From $c = -\triangle\overline{b}$ and $d = \triangle\overline{a}$, the proof of Lemma 2 (i) is complete. Furthermore, parts (ii) and (iii) are easily shown, so we will omit the proofs of them. □

The distribution of X_n^{φ} can be derived from Lemma 2 by direct computation. Let $[x]$ denote the maximal integer smaller than or equal to x. Let

$$\kappa_{\gamma,\delta,n,k} = \binom{k-1}{\gamma-1}\binom{k-1}{\delta-1}\binom{n-k-1}{\gamma-1}\binom{n-k-1}{\delta-1}.$$

LEMMA 3. *For $k = 1, 2, \ldots, [n/2]$, we have*

$$
\begin{aligned}
&P(X_n^{\varphi} = n-2k) \\
&= |a|^{2(n-1)} \sum_{\gamma=1}^{k} \sum_{\delta=1}^{k} \left(-\frac{|b|^2}{|a|^2}\right)^{\gamma+\delta} \left(\frac{\kappa_{\gamma,\delta,n,k}}{\gamma\delta}\right) \Big[\{k^2|a|^2 + (n-k)^2|b|^2 - (\gamma+\delta)(n-k)\}|\alpha|^2 \\
&\qquad + \{k^2|b|^2 + (n-k)^2|a|^2 - (\gamma+\delta)k\}|\beta|^2 \\
&\qquad + \frac{1}{|b|^2}\Big[\{(n-k)\gamma - k\delta + n(2k-n)|b|^2\}a\alpha\overline{b\beta} \\
&\qquad\qquad + \{-k\gamma + (n-k)\delta + n(2k-n)|b|^2\}\overline{a\alpha}b\beta + \gamma\delta\Big]\Big],
\end{aligned}
$$

$$
\begin{aligned}
&P(X_n^{\varphi} = -(n-2k)) \\
&= |a|^{2(n-1)} \sum_{\gamma=1}^{k} \sum_{\delta=1}^{k} \left(-\frac{|b|^2}{|a|^2}\right)^{\gamma+\delta} \left(\frac{\kappa_{\gamma,\delta,n,k}}{\gamma\delta}\right) \Big[\{k^2|b|^2 + (n-k)^2|a|^2 - (\gamma+\delta)k\}|\alpha|^2 \\
&\qquad + \{k^2|a|^2 + (n-k)^2|b|^2 - (\gamma+\delta)(n-k)\}|\beta|^2 \\
&\qquad + \frac{1}{|b|^2}\Big[\{k\gamma - (n-k)\delta - n(2k-n)|b|^2\}a\alpha\overline{b\beta} \\
&\qquad\qquad + \{-(n-k)\gamma + k\delta - n(2k-n)|b|^2\}\overline{a\alpha}b\beta + \gamma\delta\Big]\Big],
\end{aligned}
$$

$$P(X_n^{\varphi} = n) = |a|^{2(n-1)}\{|b|^2|\alpha|^2 + |a|^2|\beta|^2 - (a\alpha\overline{b\beta} + \overline{a\alpha}b\beta)\},$$
$$P(X_n^{\varphi} = -n) = |a|^{2(n-1)}\{|a|^2|\alpha|^2 + |b|^2|\beta|^2 + (a\alpha\overline{b\beta} + \overline{a\alpha}b\beta)\}.$$

By using Lemma 3, we obtain a combinatorial expression for the characteristic function of X_n^{φ} as follows. This result will be used in order to obtain a limit theorem of X_n^{φ}. Let $\mu_{\alpha,\beta} = (|a|^2 - |b|^2)(|\alpha|^2 - |\beta|^2) + 2(a\alpha\overline{b\beta} + \overline{a\alpha}b\beta)$ and $\nu_{\gamma,\delta,n,k} = (n-k)^2 + k^2 - n(\gamma+\delta) + 2\gamma\delta/|b|^2$.

THEOREM 4. *(i) Suppose $abcd \neq 0$. Then we have*

$$
\begin{aligned}
E(e^{i\xi X_n^{\varphi}}) &= |a|^{2(n-1)} \Big[\cos(n\xi) - i\mu_{\alpha,\beta}\sin(n\xi) \\
&\quad + \sum_{k=1}^{\left[\frac{n-1}{2}\right]} \sum_{\gamma=1}^{k} \sum_{\delta=1}^{k} \left(-\frac{|b|^2}{|a|^2}\right)^{\gamma+\delta} \left(\frac{\kappa_{\gamma,\delta,n,k}}{\gamma\delta}\right) \Big[\nu_{\gamma,\delta,n,k} \cos((n-2k)\xi) \\
&\qquad - (n-2k)\Big\{\mu_{\alpha,\beta}\, n + \frac{\gamma+\delta}{2|b|^2}(|\alpha|^2 - |\beta|^2 - \mu_{\alpha,\beta})\Big\} i\sin((n-2k)\xi)\Big] \\
&\quad + I\left(\frac{n}{2} - \left[\frac{n}{2}\right]\right) \times \sum_{\gamma=1}^{\frac{n}{2}} \sum_{\delta=1}^{\frac{n}{2}} \left(-\frac{|b|^2}{|a|^2}\right)^{\gamma+\delta} \left(\frac{\kappa_{\gamma,\delta,n,n/2}}{2\gamma\delta}\right) \nu_{\gamma,\delta,n,n/2} \Big],
\end{aligned}
$$

where $I(x) = 1$ (resp. $= 0$) if $x = 0$ (resp. $x \neq 0$).
(ii) Let $b = 0$. Then we have

$$E(e^{i\xi X_n^{\varphi}}) = \cos(n\xi) + i(|\beta|^2 - |\alpha|^2)\sin(n\xi).$$

(iii) Let $a = 0$. Then we have

$$E(e^{i\xi X_n^\varphi}) = \begin{cases} \cos\xi + i(|\alpha|^2 - |\beta|^2)\sin\xi & \text{if } n \text{ is odd,} \\ 1 & \text{if } n \text{ is even.} \end{cases}$$

We should remark that the above expression of the characteristic function in part (i) is not uniquely determined. From this theorem, we have the mth moment of X_n^φ in the standard fashion. The following result can be used in order to study symmetry of distribution of X_n^φ.

COROLLARY 5. *(i) Suppose $abcd \neq 0$. When m is odd, we have*

$$\begin{aligned} E((X_n^\varphi)^m) &= -|a|^{2(n-1)} \Bigg[\mu_{\alpha,\beta}\, n^m + \sum_{k=1}^{\left[\frac{n-1}{2}\right]} \sum_{\gamma=1}^{k} \sum_{\delta=1}^{k} \left(-\frac{|b|^2}{|a|^2} \right)^{\gamma+\delta} \frac{(n-2k)^{m+1}\, \kappa_{\gamma,\delta,n,k}}{\gamma\delta} \\ &\qquad \times \left\{ \mu_{\alpha,\beta}\, n + \frac{\gamma+\delta}{2|b|^2} (|\alpha|^2 - |\beta|^2 - \mu_{\alpha,\beta}) \right\} \Bigg]. \end{aligned}$$

When m is even, we have

$$E((X_n^\varphi)^m) = |a|^{2(n-1)} \left\{ n^m + \sum_{k=1}^{\left[\frac{n-1}{2}\right]} \sum_{\gamma=1}^{k} \sum_{\delta=1}^{k} \left(-\frac{|b|^2}{|a|^2} \right)^{\gamma+\delta} \frac{(n-2k)^m \kappa_{\gamma,\delta,n,k}\, \nu_{\gamma,\delta,n,k}}{\gamma\delta} \right\}.$$

(ii) Let $b = 0$. Then we have

$$E((X_n^\varphi)^m) = \begin{cases} n^m(|\beta|^2 - |\alpha|^2) & \text{if } m \text{ is odd,} \\ n^m & \text{if } m \text{ is even.} \end{cases}$$

(iii) Let $a = 0$. Then we have

$$E((X_n^\varphi)^m) = \begin{cases} |\alpha|^2 - |\beta|^2 & \text{if } n \text{ and } m \text{ are odd,} \\ 1 & \text{if } n \text{ is odd and } m \text{ is even,} \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

For any case, when m is even, $E((X_n^\varphi)^m)$ is independent of initial qubit state φ. Therefore a parity law of the mth moment can be derived from the above result.

4 Symmetry of distribution.

In this section, we give a necessary and sufficient condition for the symmetry of the distribution of X_n^φ.

THEOREM 6. *Let Φ_s, Φ_0, and $\Phi_\perp$ be as in Section 2. Suppose $abcd \neq 0$. Then we have $\Phi_s = \Phi_0 = \Phi_\perp$.*

This is a generalization of the result given by [5] for the Hadamard walk introduced in Section 6. Nayak and Vishwanath [9] discussed the symmetry of distribution and showed that ${}^t[1/\sqrt{2},\ \pm i/\sqrt{2}] \in \Phi_s$ for the Hadamard walk.

Proof. (i) $\Phi_s \subset \Phi_0$. This is obvious by definition.
(ii) $\Phi_0 \subset \Phi_\perp$. By Corollary 5 (i) with $m=1$, we see that $E(X_1^\varphi) = E(X_2^\varphi) = 0$ if and only if $\mu_{\alpha,\beta} = 0$. Then this implies that for $n \geq 3$, Corollary 5 (i) with $m=1$ can be rewritten as

$$E(X_n^\varphi) = -\frac{|a|^{2(n-1)}(|\alpha|^2 - |\beta|^2)}{2|b|^2} \sum_{k=1}^{\left[\frac{n-1}{2}\right]} \sum_{\gamma=1}^{k} \sum_{\delta=1}^{k} \left(-\frac{|b|^2}{|a|^2}\right)^{\gamma+\delta} \frac{(n-2k)^2(\gamma+\delta)\,\kappa_{\gamma,\delta,n,k}}{\gamma\delta}.$$

Therefore $E(X_n^\varphi) = 0$ $(n \geq 3)$ gives $|\alpha| = |\beta|$. Combining $|\alpha| = |\beta|$ with $\mu_{\alpha,\beta} = 0$, we have the desired result.
(iii) $\Phi_\perp \subset \Phi_s$. We assume that $|\alpha| = |\beta| = 1/\sqrt{2}$ and $a\alpha\overline{b\beta} + \overline{a\alpha}b\beta = 0$. By using these and Lemma 3, we see that for $k = 1, 2, \ldots, [n/2]$,

$$P(X_n^\varphi = n-2k) = P(X_n^\varphi = -(n-2k)) = \frac{|a|^{2(n-1)}}{2} \sum_{\gamma=1}^{k} \sum_{\delta=1}^{k} \left(-\frac{|b|^2}{|a|^2}\right)^{\gamma+\delta} \frac{\kappa_{\gamma,\delta,n,k}\,\nu_{\gamma,\delta,n,k}}{\gamma\delta},$$

and $P(X_n^\varphi = n) = P(X_n^\varphi = -n) = |a|^{2(n-1)}|\alpha|^2$. So the desired conclusion is obtained. $\square$

5 Proof of Theorem 1.

Let $P_n^{\nu,\mu}(x)$ denote the Jacobi polynomial. Then it is well known that $P_n^{\nu,\mu}(x)$ is orthogonal on $[-1,1]$ with respect to $(1-x)^\nu(1+x)^\mu$ with $\nu, \mu > -1$, and that the following relation holds:

$$P_n^{\nu,\mu}(x) = \frac{\Gamma(n+\nu+1)}{\Gamma(n+1)\Gamma(\nu+1)}\,{}_2F_1(-n, n+\nu+\mu+1; \nu+1; (1-x)/2), \tag{5.1}$$

where $\Gamma(z)$ is the gamma function and ${}_2F_1(a,b;c;z)$ is the hypergeometric function:

$${}_2F_1(a,b;c;z) = \sum_{n=0}^{\infty} \frac{\Gamma(a+n)}{\Gamma(a)} \frac{\Gamma(b+n)}{\Gamma(b)} \frac{\Gamma(c)}{\Gamma(c+n)} \cdot \frac{z^n}{n!}.$$

Let $\rho_{n,k,i} = P_{k-1}^{i,n-2k}(2|a|^2 - 1)$ for $i = 0, 1$. Then we see that

$$\begin{aligned}
\sum_{\gamma=1}^{k} \left(-\frac{|b|^2}{|a|^2}\right)^{\gamma-1} \frac{1}{\gamma} \binom{k-1}{\gamma-1} \binom{n-k-1}{\gamma-1} &= {}_2F_1(-(k-1), -\{(n-k)-1\}; 2; -|b|^2/|a|^2) \\
&= |a|^{-2(k-1)}{}_2F_1(-(k-1), n-k+1; 2; 1-|a|^2) \\
&= \frac{1}{k}|a|^{-2(k-1)}\rho_{n,k,1}.
\end{aligned}$$

The first equality is given by the definition of the hypergeometric function (see p.35 in [11]). The second equality comes from the relation: ${}_2F_1(a,b;c;z) = (1-z)^{-a}{}_2F_1(a, c-b; c; z/(z-1))$. The last equality follows from (5.1). In a similar way, we have

$$\sum_{\gamma=1}^{k} \left(-\frac{|b|^2}{|a|^2}\right)^{\gamma-1} \binom{k-1}{\gamma-1} \binom{n-k-1}{\gamma-1} = |a|^{-2(k-1)}\rho_{n,k,0}.$$

By using the above relations and Theorem 4, we obtain the following asymptotics of characteristic function $E(e^{i\xi X_n^\varphi/n})$:

LEMMA 7. *If $n \to \infty$ with $k/n = x \in (-(1-|a|)/2, (1+|a|)/2)$, then*

$$E(e^{i\xi X_n^\varphi/n}) \sim \sum_{k=1}^{\left[\frac{n-1}{2}\right]} |a|^{2n-4k-2}|b|^4$$
$$\times \left[\left\{ \frac{2x^2-2x+1}{x^2}\,\rho_{n,k,1}^2 - \frac{2}{x}\,\rho_{n,k,0}\rho_{n,k,1} + \frac{2}{|b|^2}\,\rho_{n,k,0}^2 \right\} \cos((1-2x)\xi) \right.$$
$$\left. - \left(\frac{1-2x}{x}\right)\left\{ \frac{\mu_{\alpha,\beta}}{x}\,\rho_{n,k,1}^2 + \frac{|\alpha|^2-|\beta|^2-\mu_{\alpha,\beta}}{|b|^2}\,\rho_{n,k,0}\,\rho_{n,k,1} \right\} i\sin((1-2x)\xi) \right],$$

where $f(n) \sim g(n)$ means $f(n)/g(n) \to 1$ $(n \to \infty)$.

Next we use an asymptotic result on the Jacobi polynomial $P_n^{\alpha+an,\beta+bn}(x)$ derived by Chen and Ismail [2]. By using (2.16) in their paper with $\alpha \to 0$ or $1, a \to 0, \beta = b \to (1-2x)/x, x \to 2|a|^2-1$ and $\triangle \to 4(1-|a|^2)\{(2x-1)^2-|a|^2\}/x^2$, we have the following lemma. It should be noted that there are some minor errors in (2.16) in that paper, for example, $\sqrt{(-\triangle)} \to \sqrt{(-\triangle)}^{-1}$.

LEMMA 8. *If $n \to \infty$ with $k/n = x \in (-(1-|a|)/2, (1+|a|)/2)$, then*

$$\rho_{n,k,0} \sim \frac{2|a|^{2k-n}}{\sqrt{\pi n\sqrt{-\Lambda}}}\cos(An+B),$$
$$\rho_{n,k,1} \sim \frac{2|a|^{2k-n}}{\sqrt{\pi n\sqrt{-\Lambda}}}\sqrt{\frac{x}{(1-x)(1-|a|^2)}}\cos(An+B+\theta),$$

where $\Lambda = (1-|a|^2)\{(2x-1)^2-|a|^2\}$, A and B are some constants (which are independent of n), and $\theta \in [0,\pi/2]$ is determined by $\cos\theta = \sqrt{(1-|a|^2)/4x(1-x)}$.

Proof of Theorem 1. From the Riemann-Lebesgue lemma and Lemmas 7 and 8, we see that

$$\begin{aligned}
\lim_{n\to\infty} E(e^{i\xi\frac{X_n^\varphi}{n}}) &= \frac{1-|a|^2}{\pi}\int_{\frac{1-|a|}{2}}^{\frac{1}{2}} \frac{\cos((1-2x)\xi) - i\lambda_{\alpha,\beta}(1-2x)\ \sin((1-2x)\xi)}{x(1-x)\sqrt{(|a|^2-1)(4x^2-4x+1-|a|^2)}}\,dx \\
&= \frac{\sqrt{1-|a|^2}}{\pi}\int_{-|a|}^{|a|} \frac{\cos(x\xi) - i\lambda_{\alpha,\beta}\,x\ \sin(x\xi)}{(1-x^2)\sqrt{|a|^2-x^2}}\,dx \\
&= \int_{-|a|}^{|a|} \frac{\sqrt{1-|a|^2}\,(1-\lambda_{\alpha,\beta}x)}{\pi(1-x^2)\sqrt{|a|^2-x^2}}e^{i\xi x}\,dx.
\end{aligned}$$

Hence X_n^φ/n converges weakly to the limit Z^φ. $\square$

6 Hadamard walk case.

In this section, we focus on the Hadamard walk, which has been extensively investigated in the study of quantum random walks. The unitary matrix U of the Hadamard walk is defined by the following Hadamard gate (see Nielsen and Chuang [10]):

$$U = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

The dynamics of this walk corresponds to that of the symmetric random walk in the classical case. However the symmetry of the walk depends heavily on initial qubit state, see [5].

For example, in the case of the Hadamard walk with initial qubit state $\varphi = {}^t[1/\sqrt{2}, i/\sqrt{2}]$ (symmetric case), direct computation gives

$$\begin{aligned} &P(X_4^\varphi = -4) = P(X_4^\varphi = 4) = 1/16, \\ &P(X_4^\varphi = -2) = P(X_4^\varphi = 2) = 6/16, \quad P(X_4^\varphi = 0) = 2/16. \end{aligned}$$

In contrast with the above result, as for the classical symmetric random walk Y_n^o starting from the origin, we see that

$$\begin{aligned} &P(Y_4^o = -4) = P(Y_4^o = 4) = 1/16, \\ &P(Y_4^o = -2) = P(Y_4^o = 2) = 4/16, \quad P(Y_4^o = 0) = 6/16. \end{aligned}$$

In fact, quantum random walks behave quite differently from classical random walks. For the classical walk, the probability distribution is a binomial distribution. On the other hand, the probability distribution in the quantum random walk has a complicated and oscillatory form.

Now we compare our analytical result (Theorem 1) with the numerical ones given by Mackay *et al.* [6], Travaglione and Milburn [13] for the Hadamard walk. In this case, Theorem 1 implies that for any initial qubit state $\varphi = {}^t[\alpha, \beta]$,

$$\lim_{n\to\infty} P(a \le X_n^\varphi/n \le b) = \int_a^b \frac{1 - (|\alpha|^2 - |\beta|^2 + \alpha\overline{\beta} + \overline{\alpha}\beta)x}{\pi(1-x^2)\sqrt{1-2x^2}} \, 1_{(-1/\sqrt{2}, 1/\sqrt{2})}(x)\, dx,$$

where $1_{(u,v)}(x)$ is the indicator function, that is, $1_{(u,v)}(x) = 1$, if $x \in (u,v)$, $= 0$, if $x \notin (u,v)$. For the classical symmetric random walk Y_n^o starting from the origin, the de Moivre-Laplace theorem shows

$$\lim_{n\to\infty} P(a \le Y_n^o/\sqrt{n} \le b) = \int_a^b \frac{e^{-x^2/2}}{\sqrt{2\pi}} dx.$$

If we take $\varphi = {}^t[1/\sqrt{2}, i/\sqrt{2}]$ (symmetric case), then we have the following quantum version of the de Moivre-Laplace theorem:

$$\lim_{n\to\infty} P(a \le X_n^\varphi/n \le b) = \int_a^b \frac{1}{\pi(1-x^2)\sqrt{1-2x^2}} \, 1_{(-1/\sqrt{2}, 1/\sqrt{2})}(x)\, dx.$$

So there is a remarkable difference between the quantum random walk X_n^φ and the classical one Y_n^o even in a symmetric case. Noting that $E(X_n^\varphi) = 0$ $(n \ge 0)$ for any $\varphi \in \Phi_s$, we have

$$\lim_{n\to\infty} sd(X_n^\varphi)/n = \sqrt{(2-\sqrt{2})/2} = 0.54119\ldots,$$

where $sd(X)$ is the standard deviation of X. This rigorous result reveals that numerical simulation result $3/5 = 0.6$ given by [13] is not so accurate.

As in a similar way, if we take $\varphi = {}^t[0, e^{i\theta}]$ with $\theta \in [0, 2\pi)$ (asymmetric case), then we see

$$\lim_{n\to\infty} P(a \le X_n^\varphi/n \le b) = \int_a^b \frac{1}{\pi(1-x)\sqrt{1-2x^2}} 1_{(-1/\sqrt{2},1/\sqrt{2})}(x)\, dx.$$

So we have

$$\lim_{n\to\infty} E(X_n^\varphi)/n = (2-\sqrt{2})/2 = 0.29289\ldots, \quad \lim_{n\to\infty} sd(X_n^\varphi)/n = \sqrt{(\sqrt{2}-1)/2} = 0.45508\ldots.$$

When $\varphi = {}^t[0, 1]$ ($\theta = 0$), Nayak and Vishwanath [9] and Ambainis *et al.* [1] gave a similar result, but both papers did not treat weak convergence. The former paper took the Schrödinger approach, and the latter paper took two approaches, that is, the Schrödinger approach and the path integral approach. However both their results come mainly from the Schrödinger approach by using a Fourier analysis. The details on the derivation based on the path integral approach in [1] are not so clear compared with this paper.

In another asymmetric case $\varphi = {}^t[e^{i\theta}, 0]$ with $\theta \in [0, 2\pi)$, a similar argument implies

$$\lim_{n\to\infty} P(a \le X_n^\varphi/n \le b) = \int_a^b \frac{1}{\pi(1+x)\sqrt{1-2x^2}} 1_{(-1/\sqrt{2},1/\sqrt{2})}(x)\, dx.$$

The symmetry of distribution gives the following same result as in the previous case $\varphi = {}^t[0, e^{i\theta}]$. So the standard deviation of the limit distribution Z^φ is given by $\sqrt{(\sqrt{2}-1)/2} = 0.45508\ldots$. Simulation result 0.4544 ± 0.0012 in [6] (their case is $\theta = 0$) is consistent with our rigorous result.

Acknowledgment. The author would like to thank the referee for the careful reading and useful suggestions which improve the paper.

References

[1] A. Ambainis, E. Bach, A. Nayak, A. Vishwanath and J. Watrous, One-dimensional quantum walks. In Proceedings of the 33rd Annual ACM Symposium on Theory of Computing, (2001), 37-49.

[2] L.-C. Chen and M. E. H. Ismail, On asymptotics of Jacobi polynomials, SIAM J. Math. Anal., **22** (1991), 1442-1449.

[3] A. M. Childs, E. Farhi and S. Gutmann, An example of the difference between quantum and classical random walks, Quantum Information Processing, **1** (2002), 35-43, quant-ph/0103020.

[4] N. Konno, Quantum random walks in one dimension, Quantum Information Processing, **1** (2002), 345-354, quant-ph/0206053.

[5] N. Konno, T. Namiki and T. Soshi, Symmetry of distribution for the one-dimensional Hadamard walk, Interdisciplinary Information Sciences, **10** (2004), 11-22, quant-ph/0205065.

[6] T. D. Mackay, S. D. Bartlett, L. T. Stephanson and B. C. Sanders, Quantum walks in higher dimensions, J. Phys. A: Math. Gen., **35** (2002), 2745-2753, quant-ph/0108004.

[7] D. A. Meyer, From quantum cellular automata to quantum lattice gases, J. Stat. Phys., **85** (1996), 551-574, quant-ph/9604003.

[8] C. Moore and A. Russell, Quantum walks on the hypercubes, (2001), quant-ph/0104137.

[9] A. Nayak and A. Vishwanath, Quantum walk on the line, (2000), quant-ph/0010117.

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

[11] M. Petkovšek, H. S. Wilf and D. Zeilberger, $A = B$, A K Peters, Ltd., 1996.

[12] F. Spitzer, Principals of Random Walks, 2nd edition, Springer-Verlag, 1976.

[13] B. C. Travaglione and G. J. Milburn, Implementing the quantum random walk, Phys. Rev. A, **65** (2002) 032310, quant-ph/0109076.

[14] T. Yamasaki, H. Kobayashi and H. Imai, Analysis of absorbing times of quantum walks, Phys. Rev. A, **68** (2003) 012302, quant-ph/0205045.

Norio KONNO
Department of Applied Mathematics
Faculty of Engineering
Yokohama National University
Hodogaya-ku, Yokohama 240-8501
Japan
E-mail: norio@mathlab.sci.ynu.ac.jp