Scattering model for quantum random walks on a hypercube

Jozef Košík[1] and Vladimír Bužek[1,2]
[1]*Research Center for Quantum Information, Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 845 11 Bratislava, Slovakia*
[2]*Faculty of Informatics, Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic*
(Received 22 March 2004; published 4 January 2005)

Following a recent work by Hillery *et al.* [Phys. Rev. A **68**, 032314 (2003)], we introduce a scattering model of a quantum random walk (SQRW) on a hybercube. We show that this type of quantum random walk can be reduced to the quantum random walk on the line and we derive the corresponding hitting amplitudes. We investigate the scattering properties of the hypercube, connected to the semi-infinite tails. We prove that the SQRW is a generalized version of the coined quantum random walk. We show how to implement the SQRW efficiently using a quantum circuit with standard gates. We discuss one possible version of a quantum search algorithm using the SQRW. Finally, we analyze symmetries that underlie the SQRW and may simplify its solution considerably.

DOI: 10.1103/PhysRevA.71.012306 PACS number(s): 03.67.Lx, 05.40.Fb

I. INTRODUCTION

Quantum random walk is a theoretical concept conceived to simulate certain algorithms using quantum-mechanical elements, i.e., unitary operators and measurements [1]. In particular, it has been shown recently that it is possible to use a quantum random walk to perform a search in a database with the topology of the hypercube faster than it can be done classically [2]. It is an oracle-based algorithm, which is optimal in its speed. Another successful application of quantum random walks has been demonstrated by Childs *et al.* [3], who have also constructed an oracle problem that can be solved by a quantum algorithm exploiting a quantum random walk exponentially faster than any classical algorithm.

These two examples justify the general hope that quantum random walks might be able to solve some problems, based on random processes [4] (e.g., Monte Carlo methods, 2-SAT, graph connectivity, etc.) faster than corresponding classical algorithms.

In general, there are essentially three types of quantum random walks. First, let us mention the so-called coined quantum random walk (CQRW), which is a discrete time walk which makes use of an additional quantum system, the coin [5]. The second type of quantum random walks is described by a continuous (Hamiltonian) dynamics of a quantum system [6]. Quantum random walks on regular graphs have been first discussed by Watrous [7]. The third type of quantum random walks based on physical model of optical multiports has recently been introduced by Hillery *et al.* [8,9].

Before we proceed, we note that a quantum random walk as discussed by Aharonov *et al.* [10] is basically a mapping $\psi:\mathcal{G}_{\mathcal{V}}\to\mathbb{C}^d$, which is updated at each step by a function $\psi(x)\mapsto F[\psi(y):(xy)\in\mathcal{G}_{\mathcal{E}}]$, where $\mathcal{G}=(\mathcal{G}_{\mathcal{V}},\mathcal{G}_{\mathcal{E}})$ is a graph with vertices $\mathcal{G}_{\mathcal{V}}$ and edges $\mathcal{G}_{\mathcal{E}}$.

We therefore can say that the quantum random walk is a special instance of the quantum cellular automaton [11,12]. The classical cellular automaton is a concept general enough to accommodate virtually any algorithm; more precisely, any Turing machine can be simulated using a cellular automaton.

The CQRW is usually defined on regular graphs (each vertex having the same number of outgoing edges). The definition on nonregular graphs is also possible, and some interesting algorithms are based on this version [13]. However, the latter version does not possess the symmetries of the former one, nor its neat tensor product structure (the unitary evolution operator CQRW on the regular Cayley graph commutes with generators of the underlying group). Instead, the whole graph must be addressed, by means of an oracle which tells us whether any two vertices are connected by an edge [14], which causes a considerable growth of the resources.

In this paper, we will focus our attention on a quantum-optical model of multiports [8,9] which describes a possible physical realization of specific quantum random walks. In this scheme, we have an array of multiports (see, e.g., [15] and references therein), interconnected with optical paths. A photon is launched into one path and is transformed by the action of the multiports. This action can be described as a scattering process, therefore we will refer to this scheme as the scattering quantum random walk (SQRW).

The SQRW is more viable from the experimental point of view, can be extended to nonregular graphs, and is equivalent to CQRW on the regular graphs.

We will investigate a particular arrangement of the multiports when are localized at the vertices of a hypercube. The array of multiports effectively acts as a scattering potential, when connected to semi-infinite tails. It can be endowed with two characteristic values, namely the reflection and transmission amplitude for photons. This was done in Refs. [8,9] for a special two-dimensional hypercube.

Our paper is organized as follows. In Sec. II we define the SQRW on the hypercube. In Sec. III, we show how the SQRW on the hypercube may be reduced to the cellular automaton on the line. In addition, we will compute the hitting amplitude and we will make some other simulations. In Sec. IV, we will investigate scattering properties of the hypercube connected to semi-infinite tails. Section VII contains the proof that the SQRW is equivalent to a generalized version of the coined quantum random walk. In Sec. VI, we show

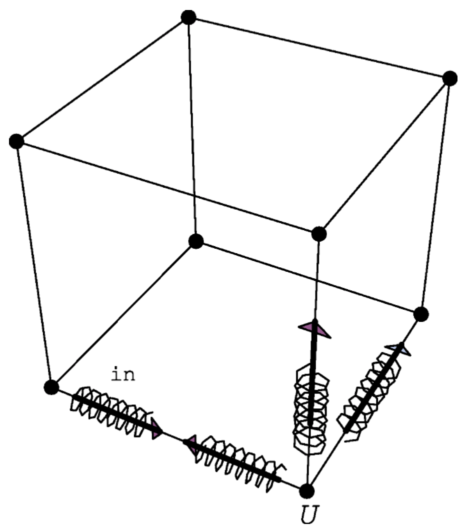

FIG. 1. Action of the multiport (U) on the ingoing photon (in) on the dim 3 hypercube. Coherent superposition of three photonic excitations is created.

how to implement the SQRW efficiently on the quantum circuit. In Sec. VIII, we discuss one possible version of a search algorithm using the SQRW. Finally, in Sec. IX, we will analyze symmetries that underlie the SQRW and which may considerably simplify the solution of the model.

II. THE DEFINITION OF SQRW

The SQRW was first presented in Ref. [8]. The technique behind its implementation is the multiports [15]: linear optical elements, interconnected with optical paths. Each multiport has in general a different number of *inputs* (which at the same time serve also as outputs). A coherent superposition of photons entering the multiport is transformed into another coherent superposition of photons outgoing from the multiport. The multiports are the vertices of a graph $\mathcal{G}_{\mathcal{V}}$, and the optical paths are its edges.

The photon traveling between the multiports x,y is denoted $|xy\rangle$. The Hilbert space on which the state of the photon is defined is spanned by vectors $|xy\rangle$, $(xy)\in\mathcal{G}_{\mathcal{E}}$ and can be decomposed into a direct sum of Hilbert subspaces $\mathcal{H}=\oplus_{x\in\mathcal{G}_{\mathcal{V}}}\mathcal{H}_x$, where $\mathcal{H}_x=\text{span}\{|yx\rangle:(yx)\in\mathcal{G}_{\mathcal{E}}\}$. That is, the basis of $\mathcal{H}_x$ is composed of the states of photons ingoing into the multiport at x. For convenience, we introduce the Hilbert subspace spanned by the states of photons outgoing from the vertex at x: $\hat{\mathcal{H}}_x=\text{span}\{|xy\rangle:(xy)\in\mathcal{G}_{\mathcal{E}}\}$.

The evolution operator of states in $\mathcal{H}$ is $U=\oplus_{x\in\mathcal{G}_{\mathcal{V}}}U_x$, where U_x is isometry $\mathcal{H}_x\to\hat{\mathcal{H}}_x$ (onto, hence linear, hence unitary). Since the subspaces are orthogonal, U is unitary.

The concrete realization of the unitary operator U_x reflects the fact that the multiport partially reflects and partially transmits the ingoing photon (see Fig. 1). Denoting the reflection and transmission coefficients r and t, respectively, we have

$$U_x|yx\rangle = r|xy\rangle + t\sum_{(xz)\in\mathcal{G}_E}|xz\rangle, \tag{2.1}$$

where $(xy)\in\mathcal{G}_{\mathcal{E}}$. For U to be unitary, these coefficients must satisfy the relations [8]

$$|r|^2+(d-1)|t|^2=1, \tag{2.2}$$

$$(d-2)|t|^2+r^*t+rt^*=0. \tag{2.3}$$

The operator U_x (for any x) has in the natural basis the matrix of the form $(U_x)_{ij}=r\delta_{ij}+t(1-\delta_{ij})$. The relations (2.2) may be satisfied by using the Grover coefficients $r=(2/d)-1$, $t=2/d$ (in what follows, we will call this setup the Grover multiport; for more details, see Ref. [16]).

The pseudo-eigensystem of any such U_x can be readily computed ("pseudo" means that we set an isomorphism between $\mathcal{H}_x$ and $\hat{\mathcal{H}}_x$ such that $|yx\rangle\equiv|xy\rangle$). Since $U_x=2|s\rangle\langle s|-1$ ($|s\rangle$ is the complete superposition over the basis of the domain of U_x, which we denote $|1\rangle,\ldots,|d\rangle$), the eigenvectors are $|s\rangle$ (with pseudo-eigenvalue 1) and linearly independent (but not orthogonal) set $\{|1\rangle-|k\rangle:k=2,\ldots,d\}$ [with $(d-1)$-degenerate pseudo-eigenvalue -1]. Performing the direct sum of these eigenvectors leads us to a pseudo-eigensystem of U, with pseudo-eigenvalues ±1.

There are many other choices of the reflection and the transmission coefficients. One set of them is the following (we will use it when necessary):

$$t=\frac{1}{d^p},$$

$$r=\sqrt{1-\frac{d-1}{d^{2p}}}e^{i\theta}, \tag{2.4}$$

where $\cos\theta=(1-d/2)/\sqrt{d^{2p}-d+1}$ with $p>1/2$. If we set $p=1$, then the reflection amplitude goes to $\lim_{d\to\infty}r=-\frac{1}{2}+i(\sqrt{3}/2)$. Obviously, for large dimensions, almost all of the photons will be reflected. The multiports with these coefficients will be the so-called *symmetric* multiports. We will later compare both sets of coefficients with respect to their mixing properties.

From now on, we will be dealing with the multiports arranged into the form of the d-dimensional hypercube. The edges of the hypercube will form two-way optical paths.

The d-dimensional hypercube is the Cayley graph $\mathcal{G}=(\mathbb{Z}_2^d,[d])$, where $[d]=\{0,\ldots,d\}$ is the set of generators of the additive (mod 2) group $\mathbb{Z}_2^d$ (the binary strings with only one 1). For any $x,y\in\mathbb{Z}_2^d$, we set the scalar product $xy=x_1y_1+\ldots+x_dy_d$ (mod 2). The norm $|x|=\sqrt{xx}$ is the Hamming weight (the number of 1s in x). The set $\ell_w=\{x:|x|=w\}$ is called the *layer* of the hypercube.

For simplicity, we will denote the basis states of $\mathcal{H}$ for the d-hypercube $|xy\rangle$ as $|x;a\rangle$, where x is the vertex and $a=1,\ldots,d$ is the generator such that $x+a=y$.

III. THE TOPOLOGY OF THE HYPERCUBE

The hypercube may be "broken up" in individual layers ℓ_w, i.e., sets of vertices with equal Hamming weight. There is a special class of vectors from $\mathcal{H}$, which is closed with respect to U and whose members may be described by a smaller number of coefficients, thus simplifying the evolution equations. Namely, these are the vectors $|\psi\rangle$ such that

$\langle x;a|\psi\rangle$ is the same for all $|x|=w$ and for all a. Under this assumption, the vectors are specified by coefficients $\{\psi_{w,\pm}\}$ where $\psi_{w,\pm}=\langle x;a|\psi\rangle$ with $|x|=w$, $|x+a|=w\pm 1$.

The reduced equations for evolution of the coefficients $\psi_{w,\pm}$ are given from the assumptions that each vertex from ℓ_w has a fixed number of edges which connect it to the previous and next layer (with Hamming weight having $w\pm 1$). We note that a vertex $|x|=w$ is connected with w edges from the previous layer and with $d-w$ edges with the next layer. Since the coefficients assigned to the projection $|\psi\rangle$ to a given layer are fixed, we obtain the recursive relations,

$$(U\psi)_{w,+} = tw\psi_{w-1,+} + [t(d-w-1)+r]\psi_{w+1,-},$$

$$(U\psi)_{w,-} = t(d-w)\psi_{w+1,-} + [t(w-1)+r]\psi_{w-1,+}. \quad (3.1)$$

For $w=0$ and $w=d$, these equations still hold wherever it makes sense, i.e., for $\psi_{0,+},\psi_{d,-}$. The coefficients $\psi_{-1,\cdot},\psi_{d+1,\cdot}$ are neglected as long as they are multiplied by zero in the equation.

The evolution which is governed by these equations is called the symmetric SQRW.

If the initial state is $\psi_{0,+}=1/\sqrt{d}$, then we immediately obtain the expression for the hitting amplitude

$$\psi_{d,-}(d) = [t(d-1)+r](d-1)!\frac{t^{d-1}}{\sqrt{d}}. \quad (3.2)$$

Using the Grover parameters ($r=2/d-1$ and $t=2/d$), we find for the quantum probability p_q to get from the vertex $|x|=0$ to the vertex $|x|=d$ in d steps the expression

$$p_q = |\psi_{d,-}(d)|^2 = \left(\frac{d!}{d^d}\right)^2 \frac{4^{d-1}}{d}. \quad (3.3)$$

Classically, the probability that we are at a given vertex from ℓ_w is p_w, for which holds $(Wp)_w=(1/d)wp_{w-1}+(1/d)\times(d-w)p_{w+1}-1$. From this we obtain the hitting probability $(W^d p_0)=(1/d^d)d!$. The classical probability to get from the vertex $|x|=0$ to vertex $|x|=d$ in d steps reads

$$p_c = \frac{d!}{d^d}. \quad (3.4)$$

Using the previous expression, we find that the classical and quantum hitting probabilities are related like

$$p_q = p_c^2 \frac{4^{d-1}}{d}. \quad (3.5)$$

The ratio p_q/p_c as a function of the dimension d of the hypercube is given by the expression

$$\frac{p_q}{p_c} = \frac{d!}{d^d}\frac{4^{d-1}}{d}, \quad (3.6)$$

and is plotted in Fig. 2. The whole model can be used to simulate the coined quantum random walk on the line segment with the position-dependent coin. The state of the coin is described by a vector $[\psi_{w,+},\psi_{w,-}]$, $w=0,\ldots,d$ and is updated at each step with the update rules given by Eq. (3.1). We might be troubled by the fact that the update rule is not unitary. But we need the unitarity only to conserve the inner product $\langle\vec{\alpha}|\vec{\alpha}\rangle$. Actually, the inner product

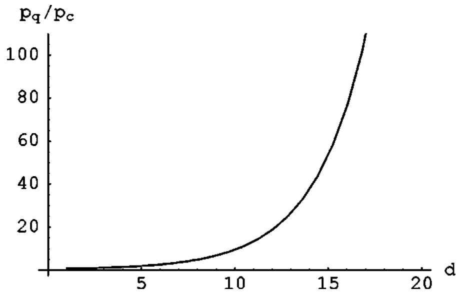

FIG. 2. The ratio p_q/p_c of hitting probability for classical (p_c) and quantum (p_q) random walk on the hypercube, related to the dimension d.

$$\langle\vec{\psi}|\vec{\psi}\rangle = \sum_{w=0}^{d}\binom{d}{w}^2(|\psi_{w,+}|^2+|\psi_{w,-}|^2) \quad (3.7)$$

is conserved.

Though we have simplified the problem by the assumption of symmetric initial values, we are still far from its explicit solution. The solution would rely on the path integration along different paths by which two sites can be connected in a presupposed number of steps. Each path would be assigned a complex amplitude (basically some product of r,t), and by adding all the relevant paths together, we would get the amplitude distribution over the hypercube. This normally gives us enormous combinatorial expressions, which are difficult to interpret.

Since the SQRW on the hypercube with symmetric initial states is equivalent to the nonunitary one-dimensional (quantum) random walk on the finite sequence of layers ℓ_w, we may explore the probability distribution $p_n(w)$ over the layers for an initial state $|\psi_0\rangle=\Sigma_a(1/\sqrt{d})|0\cdots 0;a\rangle$, where $p_n(w)$ is the expectation value of the operator

$$M_w := \sum_{x\in\ell_w,a}|x;a\rangle\langle x;a|, \quad (3.8)$$

i.e., $p_n(w)=\langle\psi_0|(U^\dagger)^n M_w U^n|\psi_0\rangle$. In Fig. 3, we present a result of simulation of the evolution of $p_n(w)$.

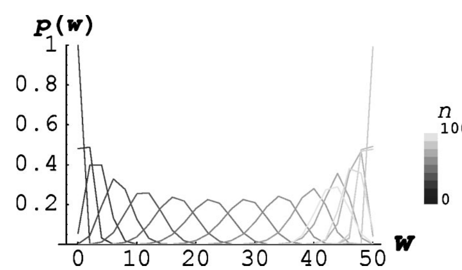

FIG. 3. The probability distribution of the SQRW, $p_n(w)$, for the hypercube of the dimension $d=50$, with a symmetric initial state localized at the vertex $0\cdots 0$, and steps $n=1,\cdots,100$. We consider Grover multiports.

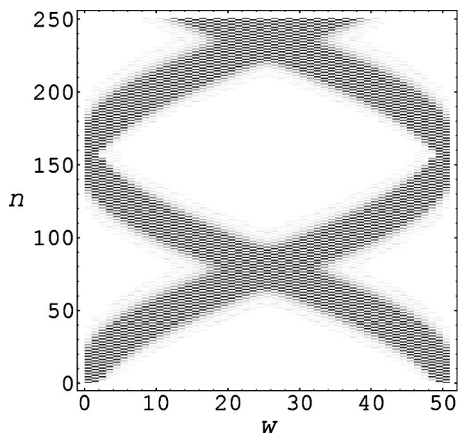

FIG. 4. The probability distribution of the symmetric SQRW on the hypercube of dim 50, for steps n 0 to 250, with the initial state $\psi_{0,+}=\psi_{d,-}=1/\sqrt{2d}$ (other ψ's$=0$) and symmetric multiports.

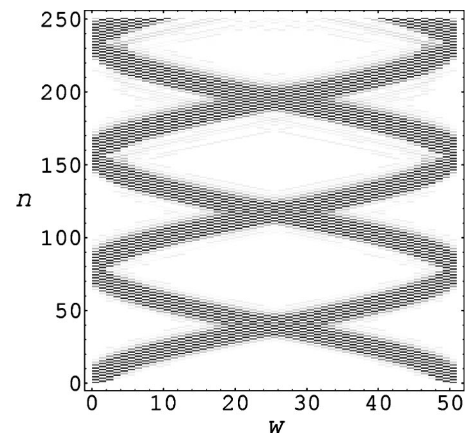

FIG. 6. The probability distribution of the symmetric SQRW on the hypercube of dim 50, for steps n 0 to 250, with the initial state $\psi_{0,+}=\psi_{d,-}=1/\sqrt{2d}$ (other ψ's$=0$) and Grover multiports.

We see that the SQRW on the hypercube is effectively isomorphic to a dynamics of a resonator: We start with one excited site, and the excitation propagates as a Gaussian packet along the resonator. As the packet hits the boundary, the corresponding site is excited, and the packet is reflected in the opposite direction.

From Fig. 3, we see that the hypercube acts as a resonator when it comes to the evolution of the probability distribution over the layers.

We have performed detailed simulations for the symmetric SQRW with initial conditions such that either only the coefficients $\psi_{0,+};\psi_{d,-}$ are nonzero, or $\psi_{d/2,\pm}\neq 0$. There are two choices of the multiports: the Grover and the symmetric multiports. We make the simulations for both of them, and for both initial conditions (see Figs. 4–7). We see the periodicity of the evolution, another feature akin to the resonant behavior. Note that the Grover multiport has much better mixing properties than the symmetric multiport, owing to the fact that it is more distant from unity.

IV. HYPERCUBE AS A SCATTERING POTENTIAL

In Ref. [8], a model of a two-dimensional hypercube with semi-infinite tails attached to the vertices with the Hamming weights 0 and 2 has been studied. Each tail has been supposed to be a one-dimesional lattice with perfectly transmitting multiports. Along one tail, a photon enters the hypercube, and emerges on the other side. It is possible to calculate explicitly the transmission coefficient of the whole structure. In the present section, we will study an analogous problem for an arbitrary-dimensional hypercube. We will utilize some symmetry assumptions, which allows us to perform the calculation (or at least the simulation) for arbitrary dimensions. The scheme we consider is shown in Fig. 8.

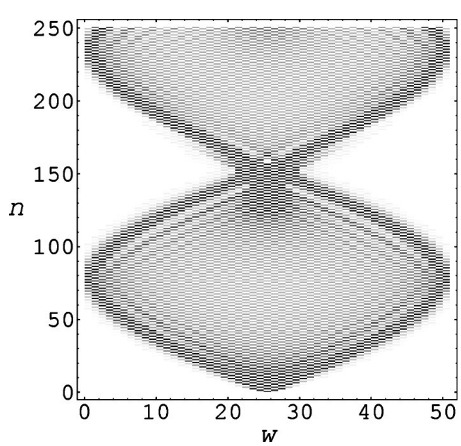

FIG. 5. The probability distribution of the symmetric SQRW on the hypercube of dim 50, for steps n 0 to 250, with the initial state $\psi_{d/2+1,\pm}=1/\sqrt{2\binom{d}{d/2+1}}$ (other ψ's$=0$) and symmetric multiports.

Now everything is as before, except that the multiports at the vertices with Hamming weight 0 and d have reflection and transmission coefficients given by expressions $\tilde{r}=[2/(d+1)]-1$ and $\tilde{t}=2/(d+1)$, respectively. The multiports outside the hypercube are perfectly transmitting. The initial state is a photon traveling from the vertex -1 to the vertex $|x|=0$ of the hypercube. The state of the whole system is described by complex numbers $\alpha_{w,\pm}$ which represent the amplitude that the photon travels from a vertex $|x|=w$ and is directed to the next or previous layer $\ell_{w\pm1}$. Now we let w run through $\mathbb{Z}$. The resulting relations are

$$(U\psi)_{0,+}=\tilde{t}\psi_{-1,+}+[(d-1)\tilde{t}+\tilde{r}]\psi_{1,-},$$

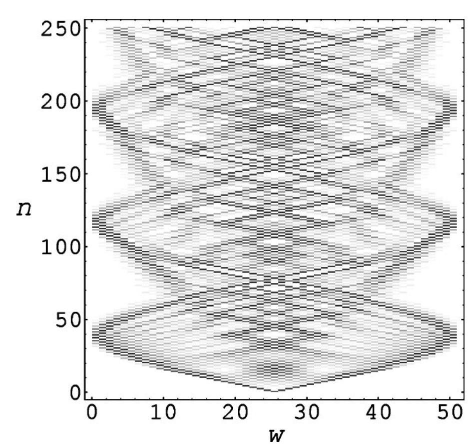

FIG. 7. The probability distribution of the symmetric SQRW on the hypercube of dim 50, for steps n 0 to 250, with the initial state $\psi_{d/2+1,\pm}=1/\sqrt{2\binom{d}{d/2+1}}$ (other ψ's$=0$) and Grover multiports.

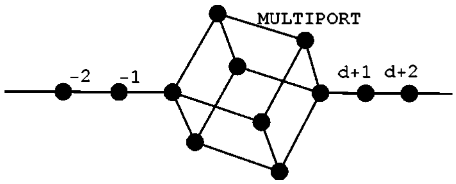

FIG. 8. The scattering potential (three-dimensional hypercube). The vertices outside the hypercube are denoted $-\infty,\ldots,-2$ and $d+1,\ldots$ for the hypercube of dimension d.

$$(U\psi)_{0,-} = \tilde{r}\psi_{-1,+} + d\tilde{t}\psi_{1,-},$$

$$(U\psi)_{d,+} = d\tilde{t}\psi_{d-1,+},$$

$$(U\psi)_{d,-} = [(d-1)\tilde{t} + \tilde{r}]\psi_{d-1,+},$$

$$(U\psi)_{w,+} = tw\psi_{w-1,+} + [r + (d-w-1)t]\psi_{w+1,-},$$

$$(U\psi)_{w,-} = t(d-w)\psi_{w+1,-} + [t(w-1) + r]\psi_{w-1,+}. \quad (4.1)$$

We begin with the particle in the state $|-1,0\rangle$, i.e., a particle localized at the vertex just left of the hypercube on the tail, and pointing to the right (see Fig. 8).

We have simulated the probability that a particle incoming from the left will be absorbed by the detector after n steps (see Fig. 9). This means that the system evolves for n steps, and then a projection on the vector $|d;d+1\rangle$ is performed. The result shows periodic beats of the probability of the absorption of the photon by the detector.

V. NONSYMMETRIC INITIAL STATE

When we impose a symmetry condition on initial states, the whole problem becomes linear in the dimension of the hypercube (normally its complexity is exponential in d). But we also may be interested in the behavior that appears as a result of phase differences between the components of the initial state. Given the d-dimensional hypercube with semi-infinite tails attached to the vertices $0\cdots 0$ and $1\cdots 1$, we consider the initial state

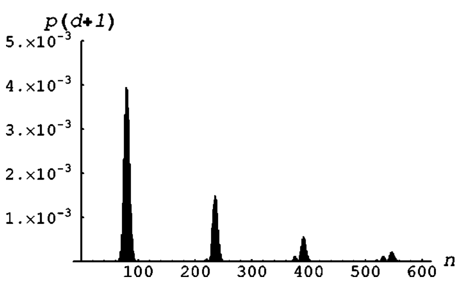

FIG. 9. The scattering probability of a 10-dimensional hypercube, for a photon incoming from the source (S) (n is the number of steps). The multiports are symmetric.

$$|\psi_0\rangle = \sum_{j=1}^{d} \gamma_j |0\cdots 0;j\rangle. \quad (5.1)$$

Now the amplitude of $U^d|\psi_0\rangle$ to project onto the state $|1\cdots 1;+\rangle$ is given by the sum of amplitudes to traverse from $\cdot 0$ to $1\cdots 1$ in d steps, which is $t^{(d-1)}\tilde{t}$. In particular, for the initial state $|0\cdot;j\rangle$ we have $(d-1)!$ such paths. The situation is analogous for all j, with each initial direction j contributing the factor γ_j of the amplitude. The overall amplitude is

$$\langle 1\cdots 1;+|U^d|\psi_0\rangle = \sum_{j=1}^{d} \gamma_j (d-1)!\, t^{(d-1)}\tilde{t}. \quad (5.2)$$

The probability of detecting the particle at the state $|1\cdots 1;+\rangle$ depends only on $\Sigma_{j=1}^{d}\gamma_j$. In this sense, the hypercube with tails attached behaves like a Mach-Zehnder interferometer.

VI. IMPLEMENTING THE SQRW

Until now, we have not discussed the question whether it is feasible to implement the SQRW. To build a whole network of multiports, we need exponentially growing resources (the number of vertices grows exponentially). However, to encode the states under consideration, we need only $d\lceil \log d\rceil$ qubits. So we can ask a question: Is it possible to build a network of quantum gates operating on the qubit register of this size? This is most easily done only on the hypercube without the semi-infinite tails attached; however, it is also possible to implement this scheme by adding some overhead of gates to the network. We need d qubits for the position register $|x\rangle$ and at least $\lceil \log d\rceil$ qubits for the direction register $|\varphi\rangle$. The first part of one application of the unitary operator U is controlled negation of each bit of x depending on $|\varphi\rangle$. The second part is the transformation of the state $|\varphi\rangle$, so that the action of the multiports is accounted. More precisely, the first part is

$$|x\rangle|\varphi\rangle \to \sum_a |x+a\rangle\langle a|\varphi\rangle|a\rangle, \quad (6.1)$$

and the second part reads

$$|x\rangle|a\rangle \to |x\rangle\left[r|a\rangle + \sum_{b\neq a} t|b\rangle\right], \quad (6.2)$$

for each $a=1,\ldots,d$. The first part described by Eq. (6.1) can be implemented using a variant of the controlled-NOT (CNOT) gate. The CNOT gate operates on two qubits such that it negates the first (target) qubit, iff the second (control) qubit is nonzero. The action of the CNOT gate is described by the two-qubit operator $C_{\mathrm{CNOT}} = \sigma_x \otimes |1\rangle\langle 1| + \mathbb{1}\otimes|0\rangle\langle 0|$. We employ the ϕ_{CNOT} gate, which differs from the CNOT gate in that it has a d-dimensional control state, unlike a single qubit. If the control state is $|\phi\rangle$ (the accepting control state), then the target qubit is negated, otherwise it is kept in the original state. The operational form of the ϕ_{CNOT} gate is

$$\phi_{\mathrm{CNOT}} = \sigma_x \otimes |\phi\rangle\langle\phi| + 1 \otimes (1 - |\phi\rangle\langle\phi|). \quad (6.3)$$

Obviously, the ϕ_{CNOT} is unitary.

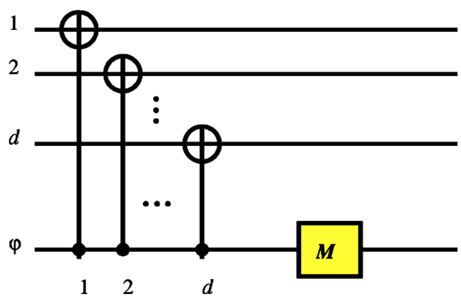

FIG. 10. The gate which implements the SQRW on the d-dimensional hypercube. The input state is the position register (d qubits labeled as $1,\ldots,d$) and the direction register $|\varphi\rangle$. There are d ϕ_{CNOT} gates stacked together, with accepting states $|1\rangle,\ldots,|d\rangle$, which change the position register, and the gate M which changes the direction register.

The operation (6.1) can be implemented by using d ϕ_{CNOT} gates (see Fig. 10). Each gate operates on a different qubit from the position register. If the gate operates on the ath qubit, the accepting control state is chosen to be $|a\rangle$ (see Fig. 10).

The operations (6.1) and (6.2) are implemented by using a single unitary operation M operating on the direction register. It corresponds to the transformation of the state due to the multiports. It reads

$$M = \sum_a \left[r|a\rangle\langle a| + t\sum_{b\neq a} |b\rangle\langle b| \right]. \tag{6.4}$$

The $d\times d$ matrix form of M is

$$M = \begin{pmatrix} r & t & \cdots & t \\ t & r & \cdots & \\ \vdots & & \ddots & \\ t & \cdots & t & r \end{pmatrix}. \tag{6.5}$$

Consequently, the unitary evolution operator U of the SQRW on the hypercube may be decomposed as $U=G_2G_1=(1\otimes M)C_1\cdots C_d$, where $C_a=\sigma_x\otimes|a\rangle\langle a|+1\otimes(1-|a\rangle\langle a|)$ is the ϕ_{CNOT} operator with the target qubit being the ath qubit from the position register, and accepting the state $|\phi\rangle=|a\rangle$, with $a=1,\ldots,d$. The operators C_a are mutually commuting, and have common eigenvectors. To find them, we decompose the eigenvectors into the product of $(2\times d)$-dimensional vectors $|\psi\rangle\otimes|\chi\rangle$. Applying C_a on $|\psi\rangle|\chi\rangle$, we obtain (providing that $\sigma_x|\psi\rangle=\lambda|\psi\rangle$)

$$\begin{aligned} C_a|\psi\rangle|\chi\rangle &= \sigma_x|\psi\rangle|a\rangle\langle a|\chi\rangle + |\psi\rangle\otimes(|\chi\rangle - |a\rangle\langle a|\chi\rangle) \\ &= |\psi\rangle\otimes[(\lambda-1)\langle a|\chi\rangle|a\rangle + |\chi\rangle] \\ &= \begin{cases} |\psi\rangle|\chi\rangle, & \lambda = 1, \\ |\psi\rangle\otimes[|\chi\rangle - 2\langle a|\chi\rangle|a\rangle], & \lambda = -1. \end{cases} \end{aligned} \tag{6.6}$$

The case with $\lambda=-1$ has to be dealt with separately. If $|\chi\rangle=|a\rangle$, then we get $C_a|\psi\rangle|a\rangle=-|\psi\rangle|a\rangle$, and if $|\chi\rangle=|b\rangle, b\neq a$, then $C_a|\psi\rangle|b\rangle=|\psi\rangle|b\rangle$. We arrive at the conclusion that the eigensystem of C_a is the set of vectors $|\psi\rangle|\chi\rangle$, where $|\psi\rangle$ is the eigenvector of σ_x and $\chi=|a\rangle$, $a=1,\ldots,d$. What about the eigensystem of G_2? The matrix M can be diagonalized, since it is translationally invariant. We search for the eigenvectors in the form $\psi_k=\Sigma_{a=1,d}e^{2\pi ika/d}e_a$, which yields

$$\begin{aligned} M\psi_k &= \sum_{a=1,d}\left(re^{2\pi ika/d} + \sum_{b=1,d-1} te^{2\pi ik(a\Theta b)/d}\right)e_a \\ &= \underbrace{\left(r + t\sum_{b=1,d-1} e^{-2\pi ikb/d}\right)}_{\lambda_k}\sum_{a=1,d} e^{2\pi ika/d}e_a, \end{aligned} \tag{6.7}$$

where $\lambda_k=r-t$ if $k\neq 0$, and $\lambda_k=r-t+td$.

VII. SQRW IS SUPERSET OF COINED QUANTUM RANDOM WALK

In this section, we will discuss the connection between the scattering and the coined quantum random walks. The SQRW reduces to the coined quantum random walk on a regular graph (having all vertices with the same degree), and conversely, the SQRW is the generalization of the coined quantum random walk on general graphs.

There is an isomorphism between the coined quantum random walk (CQRW) and the SQRW on the same Cayley graph over the Abelian group, $\mathcal{G}$. We recall that the CQRW is defined by a unitary operator E on the Hilbert space $\mathcal{H}_E=\mathcal{H}_X\otimes\mathcal{H}_A$, where $\mathcal{H}_X$ is spanned by vectors $|x\rangle, x\in\mathcal{G}_{\mathcal{V}}$, and $\mathcal{H}_A$ is spanned by the generators of $\mathcal{G}$, the basis vectors $|a\rangle$. One step of the CQRW is given by $E=SC$, where $S=\Sigma_aT_a\otimes\pi_a$ and $C=1\otimes M$. Here $T_a|x\rangle=|x+a\rangle$ is the translation, π_a is the projection to $|a\rangle$, and M is any unitary operator. The isometry is given by one-to-one mapping of basis vectors of both $\mathcal{H}$ and $\mathcal{H}_E$ like $|x(x+a)\rangle_{\mathcal{H}}\equiv|x\rangle|a\rangle_{\mathcal{H}_E}$. The correspondence between operators U and E is $U_x|yx\rangle$, where $y+a=x$ is the same as applying the translation S on $|x-a\rangle|a\rangle$ and then applying the coin M on $|a\rangle$ such that matrix representations of U_x in the natural basis of $\mathcal{H}_x,\widetilde{\mathcal{H}}_x$ and M in the natural basis of $\mathcal{H}_A$ are the same.

For regular graphs, we can decompose $\mathcal{H}_E$ into the direct product of $\mathcal{H}_{Ex}$ such that $\mathcal{H}_{Ex}=\mathrm{span}\{|x-a\rangle|a\rangle : a \text{ is gen.}\mathcal{G}\}$.

The scheme for generalizing the coined quantum random walk on general graphs was proposed in Ref. [14], but this has required an oracle which operates on the set of all edges of the graph. Our scheme is based on local operations done by multiports, so it is more reasonable and easier to implement physically. This was actually proposed in Ref. [17]. Algorithms based on coined quantum random walks were proposed in Ref. [13].

VIII. SEARCHING WITH SQRW

In this section, we will address a question whether it is possible to use the SQRW for a database search or a similar task. To answer this question, we need to formulate what a quantum database is and how we can move around its entries using the SQRW.

The database we are searching in is the so-called quantum dictionary. The classical dictionary is a set of pairs (key, value). The set of all keys is given by the topology of a graph, yielding the adjacency relations among all the keys.

Random walk (classical) in the dictionary is bound to the edges of this graph.

The searching problem in the dictionary is given as follows: given a value, find a key, such that (key,value) is in the dictionary. For N keys, this is an $O(N)$ problem. To obtain a quantum version of this scheme, we have to "quantize" (noncanonically) the problem. Due to the fact that the graph is not regular, we cannot factorize the complete Hilbert space, but we need to label the states in the most general fashion: $|xy\rangle$, where (xy) is an edge. The searching procedure consists of applying one step of the SQRW, and then by querying the database. The query corresponds to an application of a unitary operator (the oracle) [18], which flips some auxiliary qubit, depending on whether the value assigned to the key is the one we are searching for. That is, the oracle is the transformation $\mathcal{O}|xy\rangle|q\rangle \mapsto |xy\rangle|q\oplus f(x,y)\rangle$, where $f(x,y)$ gives the value 1 if any of the vertices x,y satisfy the query, and 0 otherwise. It is clear that the oracle $\mathcal{O}$ is unitary. Now the searching algorithm is based on the sequence of operations $(\mathcal{O}U)^n$, where U makes one step of the SQRW and $\mathcal{O}$ is the oracle query (equivalent to the action of the multiports). One such algorithm has been presented in Ref. [2]. In our terms it is the SQRW on the hypercube, where the multiport assigned to one marked key has trivial coefficients r,t (they only change the phase), while the other multiports have coefficients corresponding to the action of the Grover operator to the direction states. In Ref. [2], it has been shown that the marked key can be found in $O(\sqrt{N})$ steps with probability $O(1)$, where N is the number of vertices of the hypercube.

IX. SYMMETRIES OF THE EVOLUTION OPERATOR U

The basic relation $U\psi=\lambda\psi$, where $\psi=\Sigma_{xa}\gamma_{xa}|xa\rangle$ yields the following recurrence relation:

$$r\gamma_{x,-a} + t\sum_{b\neq a}\gamma_{xb} = \lambda\gamma_{x+a,a}. \tag{9.1}$$

Finding the symmetries of this operator helps us to find its eigensystem. We can Fourier transform the states of $\mathcal{H}$ to another basis, in which solutions can be found more easily. The operator U has many symmetries, one of which is the translation $T_b: x\mapsto x+b$. The eigenvectors of T_b are (for details, see Ref. [16])

$$|\widetilde{ka}\rangle = \sum_x (-1)^{kx}|x;a\rangle, \tag{9.2}$$

with eigenvalues $(-1)^{k_b}$, $k\in\mathbb{Z}_2^d$. The action of U on $|\widetilde{ka}\rangle$ is

$$U|\widetilde{ka}\rangle = (-1)^{k_a}\left(r|\widetilde{ka}\rangle + \sum_{b\neq a}|\widetilde{kb}\rangle\right), \tag{9.3}$$

and in the basis $|\widetilde{ka}\rangle$, U has the form $\widetilde{U}=\mathrm{diag}(\{\widetilde{V}_k\})$, where

$$\widetilde{V}_k = \begin{pmatrix} r(-1)^{k_1} & t(-1)^{k_2} & \cdots & t(-1)^{k_d} \\ t(-1)^{k_1} & r(-1)^{k_2} & t(-1)^{k_3} & \cdots \\ & \vdots & \ddots & \cdots \\ t(-1)^{k_1} & \cdots & & r(-1)^{k_d} \end{pmatrix}. \tag{9.4}$$

Now we only need to find the eigensystem of this comparatively small matrix. It is obvious that $\widetilde{V}_k$ is translationally symmetric. The eigensystem of Eq. (9.4) can be found in Ref. [16].

In what follows, we will find another symmetry. Unlike the previous case, now we will be changing both the elements of the position and the direction Hilbert spaces. This transformation R will change the vector $|x,a\rangle$ such that the binary string x is cyclically shifted right by one place and a is set to $a\oplus 1$ modulo d. Since a is unambiguously defined by the position in the binary string at which x differs from $x+a$, this transformation is a symmetry. This can be viewed as a rotation along the line segment connecting two opposite vertices $0\cdots 0$ and $1\cdots 1$. We can choose any other two vertices x,y such that $|x-y|=d$, and get a symmetry operator $R_{xy}=B_x^\dagger RB_x$, where B_x changes the role of 0 to x and 1 to $1+x$. More precisely, $B_x|z,a\rangle=|z+x,a\rangle$ (hence $B^\dagger=B$). Two transformations R_x,R_y generally do not commute, but they both commute with U.

X. CONCLUSION

We have proved that the SQRW is in fact a version of the coined quantum random walk. We can use this observation to extend the coined quantum random walk to the cases of nonregular graphs. While it is in principle easy to construct the SQRW on any graph, it is still a question whether we also can simulate it efficiently (e.g., like in Sec. VI). This point is crucial for further development of quantum algorithms based on the SQRW in higher dimensions (where the speedup may become noticeable). The class of algorithms based on the SQRW is the database searching, using the oracle queries along with the "random" steps. We already know at least one such algorithm (see Ref. [2]) and we know that it is optimal. We cannot expect that the complexity drops below $O(\sqrt{N})$ for N database keys, but the new algorithms may be more general in their inputs, and may be easier to implement.

We have found the connection between mixing properties of the multiport (or the coin) and the distance of the respective operator from unity. It might be interesting to find an exact function of this distance, which yields the measure of mixing for the SQRW.

ACKNOWLEDGMENT

This work was supported by the European Union projects QUPRODIS, QGATES, and CONQUEST.

[1] J. Kempe, Contemp. Phys. **44**, 307 (2003).
[2] N. Shenvi, J. Kempe, and K. B. Whaley, Phys. Rev. A **67**, 052307 (2003).
[3] A. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman, in *Proceedings of the 35th ACM Symposium on Theory of Computing (STOC'03)* (ACM Press, New York, 2003), pp. 59–68.
[4] We should note that there is nothing really *random* (in a classical sense) about quantum random walk: the quantum evolution is always unitary (deterministic), and the only randomness involved in the scheme is the random outcomes of the measurements.
[5] Y. Aharonov, L. Davidovich, and N. Zagury, Phys. Rev. A **48**, 1687 (1993).
[6] A. M. Childs, E. Farhi, and S. Gutmann, Quantum Inf. Process. **1**, 35 (2002).
[7] J. Watrous, J. Comput. Syst. Sci. **62**, 376 (2001).
[8] M. Hillery, J. Bergou, and E. Feldman, Phys. Rev. A **68**, 032314 (2003).
[9] E. Feldman and M. Hillery, e-print quant-ph/0403066.
[10] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani, in *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing (STOC'01)* (ACM Press, New York, 2001), pp. 50–59.
[11] D. A. Meyer, J. Stat. Phys. **85**, 551 (1996).
[12] B. Schumacher and R. F. Werner, e-print quant-ph/0405174.
[13] A. M. Childs and J. M. Eisenberg, e-print quant-ph/0311038; see also A. Ambainis, e-print quant-ph/0311001.
[14] V. Kendon, e-print quant-ph/0306140; V. Kendon and B. Sanders, e-print quant-ph/0404043.
[15] I. Jex, S. Stenholm, and A. Zeilinger, Opt. Commun. **117**, 95 (1995).
[16] C. Moore and A. Russel, e-print quant-ph/0104137.
[17] A. Ambainis, e-print quant-ph/0403120.
[18] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).