Controllability of quantum walks on graphs

Francesca Albertini · Domenico D’Alessandro

Received: 17 June 2010 / Accepted: 6 March 2012 / Published online: 23 March 2012
© Springer-Verlag London Limited 2012

Abstract In this paper, we consider discrete time quantum walks on graphs with coin, focusing on the decentralized model, where the coin operation is allowed to change with the vertex of the graph. When the coin operations can be modified at every time step, these systems can be looked at as control systems and techniques of geometric control theory can be applied. In particular, the set of states that one can achieve can be described by studying controllability. Extending previous results, we give a characterization of the set of reachable states in terms of an appropriate Lie algebra. Controllability is verified when any unitary operation between two states can be implemented as a result of the evolution of the quantum walk. We prove general results and criteria relating controllability to the combinatorial and topological properties of the walk. In particular, controllability is verified if and only if the underlying graph is not a bipartite graph and therefore it depends only on the graph and not on the particular quantum walk defined on it. We also provide explicit algorithms for control and quantify the number of steps needed for an arbitrary state transfer. The results of the paper are of interest in quantum information theory where quantum walks are used and analyzed in the development of quantum algorithms.

Keywords Control theory methods in quantum information · Quantum walks · Lie algebras and lie groups

F. Albertini (✉)
Dipartimento di Matematica Pura ed Applicata, Università di Padova, Via Trieste 63, 35121 Padua, Italy
e-mail: albertin@math.unipd.it

D. D’Alessandro
Department of Mathematics, Iowa State University, 440 Carver Hall, Ames, 5001 IA, USA
e-mail: daless@iastate.edu
1 Introduction

In recent years, quantum walks on graphs have emerged as one of the most useful protocols to design quantum algorithms. This concerns, in particular, problems that are naturally formulated on graphs, such as search problems where one is allowed to visit one location at a time moving between neighboring vertices (see, e.g., [4, 19]). The study of these systems has now developed in a new, rich, area of quantum information and mathematics. There are several aspects that are worth studying, all interconnected: the design of quantum algorithms with better performances than the classical ones, and, in particular, than the randomized algorithms based on classical random walks; the complexity theory of these algorithms; the dynamics of these systems; their physical implementation. Reviews on quantum walks and their algorithmic applications can be found in [3, 12, 13]. Moreover, quantum walks are often used as models in the study of natural phenomena (see, e.g., [14] for an application to energy transfer in photosynthesis).

There are two different versions of quantum walks: continuous and discrete time. In its simplest form, a continuous time quantum walk on a graph is a quantum system with state $|\psi\rangle$ varying in a finite dimensional Hilbert space. We will follow Dirac notation of quantum mechanics in denoting by $|\psi\rangle$ a general vector, so that $\langle\psi|\phi\rangle$ denotes the inner product of two vectors $|\psi\rangle$ and $|\phi\rangle$ and $|\psi\rangle\langle\phi|$ the outer product (column by row). The state $|\psi\rangle$ evolves according to the Schrödinger equation

$$i\dot{|\psi\rangle} = H|\psi\rangle,$$

where the linear operator $H$, called the Hamiltonian, is constrained by the underlying graph, i.e., $H_{jk} \neq 0$ if and only if there is an edge connecting the $j$th and $k$th vertex of the graph. One important case is when $H$ is the adjacency matrix of the graph. Discrete time quantum walks come in different forms. One may use a quantum system, whose basis states represent the edges of the graph and define the evolution on the corresponding Hilbert space (see, e.g., [11] and the references therein) or one may use two quantum systems, called the coin and the walker, the coin having dimension equal to the degree $d$ of the graph, assumed regular (see definitions at the beginning of Sect. 2), and the walker having dimension equal to the number of vertices $N$. This second model, although restricted to regular graphs, has the advantage of making the role of the coin more transparent and intuitive and requiring a Hilbert space whose dimension $(dN)$ may be significantly smaller than the one ($N^2$) for the walk defined on the edges of the graph. There are some known relations among the various types of quantum walks. Some of them are discussed in [5, 7]. Related models are considered in the context of quantum cellular automata and quantum robots (see, e.g., [21, 22] and references therein).

In this paper, we consider discrete time quantum walks with coin on regular graphs. The evolution of these systems at every step is the sequence of two operations; one operation on the coin system, called coin tossing, and one operation on the walker system, called the conditional shift, which changes the state of the walker according to the state of the coin. We assume that, at every step, one can change the coin tossing transformation and we adopt a decentralized model where the coin transformation
may depend on the current state of the walker system. The main topic of this paper is to characterize the set of states that can be obtained with these models, that is, their controllability.

The paper is organized as follows. In Sect. 2, we describe in mathematical terms the models we want to study. In Sect. 3, we define the controllability of these models and give criteria to describe the set of reachable states. In particular, by modifying the proof that was given in [2,8] we extend and strengthen a result which describes the set of admissible evolutions of these systems as a Lie group (Theorems 1 and 2). This Lie group might have one or more connected components and its Lie algebra is generated by an appropriate set of matrices. An important problem, in this context, is to characterize explicitly this Lie algebra for various quantum walks. In Sect. 4, we relate the Lie algebraic controllability criterion described in Sect. 3 with the orbits of the permutations associated with the walk. This correspondence will allow us to infer further controllability properties of these systems and, in particular, to solve the Lie algebra characterization problem above mentioned (Theorem 6). As a consequence of this general result, we obtain several strong statements in special cases. In particular, quantum walks with a graph of degree $d$ greater than $\frac{N}{2}$, where $N$ is the number of vertices, are always completely controllable (Proposition 4.1). Here, complete controllability means that every unitary evolution can be obtained with the dynamics of the system. In Sect. 5, we adopt a more direct approach to the study of controllability, by giving explicit constructive algorithms for state transfer. In doing so, we obtain an upper bound on the worst case number of steps needed for an arbitrary state transfer. A byproduct of this method of control is another condition of controllability which is expressed in terms of the properties of the graph underlying the quantum walk (Theorem 7). Sect. 6 relates the results obtained with this constructive approach, with the ones obtained in the previous sections. We do this in Theorem 8 and we add a purely graph theoretic criterion of controllability (point 4 of Theorem 8). In particular, controllability is verified if and only if the underlying graph is not a bipartite graph. We notice that controllability only depends on the graph and not on the walk defined on it and that even purely graph theoretic questions can be answered using the concept of quantum walk (cf. Theorem 9). Section 7 contains some examples including a full treatment for graphs of degree two (i.e., cycles).

## 2 Model definition

Let $G := \{ V, E \}$ be an undirected graph, where $V$ denotes the associated set of vertices and $E$ the associated set of edges. We shall denote by $N$ the number of elements in $V$. We assume that

H1) $G$ is a regular graph, that is, all the vertices have the same number $d$ of adjacent vertices. The number $d$ is referred to as the degree of the graph $G$.

H2) $G$ is connected, without self loops (i.e., edges connecting a vertex to itself) and without multiple edges (i.e., two or more edges connecting the same pair of vertices).

Given the graph $G$, a quantum walk on $G$ is a quantum mechanical system defined as follows. The state of this system varies on a Hilbert space $\mathcal{C} \otimes \mathcal{W}$. The space $\mathcal{W}$ is
called the walker space and an orthonormal basis for $W$ is given by $\{|0\}, \ldots, |N-1\}$, where $\{0, \ldots, N-1\}$ are the labels of the vertices in $V$. The space $C$ is called the coin space and an orthonormal basis for $C$ is given by $|c_1\rangle, \ldots, |c_d\rangle$, where $d$ is the degree of the graph. The states $\{|c_1\}, \ldots, |c_d\}$ are in one to one correspondence with possible ‘directions’ of motion on the graph. More precisely, with every value $c_l$ it is associated a permutation $\pi_l$ of the vertices in $V$. The permutation $\pi_l$ is such that $\pi_l i = j$ implies that there is an edge in $E$ connecting the vertices $i$ and $j$ and for an edge connecting $i$ and $j$ there exists a unique value $c_l$ and associated permutation $\pi_l$ such that $\pi_l i = j$. A quantum mechanical system with state varying on $W$ will be referred to as a walker system and a system varying on $C$ will be referred to as a coin system.

The state of the quantum walk is described by a unit vector $|\psi\rangle$ in $C \otimes W$, i.e.,

$$|\psi\rangle := \sum_{k=0}^{N-1} \sum_{j=0}^{d} \alpha_{kj} |c_k\rangle \otimes |j\rangle. \quad (2)$$

According to the measurement postulate of quantum mechanics (see, e.g., [16]), the meaning of the state $|j\rangle \in W$ is that if we measure the position of the walker we find the position $j$ with certainty. More in general, from (2), the probability $p_j$ of finding the walker in position $j$ is obtained by tracing out the coin degrees of freedom, that is, $p_j = \sum_{k=1}^{d} |\alpha_{kj}|^2$.

We will denote by $U(n)(SU(n))$ the Lie group of $n \times n$ unitary matrices ($n \times n$ unitary matrices with determinant equal to one), while $u(n)(su(n))$ denotes the corresponding Lie algebra of skew-Hermitian $n \times n$ matrices (skew-Hermitian $n \times n$ matrices with zero trace). There are several introductory books on Lie algebras and Lie groups (see e.g., [10,15,17]). The book [6] presents introductory notions with a view to applications to the control of quantum systems.

As a simple example of a quantum walk on a graph $G$ consider for $G$ the cycle with four vertices in Fig. 1. The coin state $|c_1\rangle$ is associated with a permutation $\pi_1 := (0 \ 1 \ 2 \ 3)$ while the coin state $|c_2\rangle$ is associated with a permutation $\pi_2 := (0 \ 3 \ 2 \ 1)$.

The dynamics of a quantum walk system is a sequence of two types of operations which we now define. A coin tossing operation on $C \otimes W$ is an operation of the type...
with $Q_j \in U(d)$. This operation applies a unitary evolution to the coin state and this operation is allowed to depend on the current walker state. The second operator we define is the conditional shift, which is an operator of the form

$$S := \sum_{k=1}^{d} |c_k\rangle\langle c_k| \otimes P_k. \quad (4)$$

This operator applies to a state in $\mathcal{W}$ a permutation $P_k$ depending on the current value of the coin system. The permutation operator $P_k$ is the one corresponding to the permutation $\pi_k$ in that $|j\rangle = P_k|l\rangle \leftrightarrow j = \pi_k l$. In the basis

$$e_{kj} := |c_k\rangle \otimes |j\rangle \quad k = 1, \ldots, d, \quad j = 0, \ldots, N - 1, \quad (5)$$

$S$ has the matrix representation

$$S = \begin{pmatrix}
P_1 & 0 & \cdots & 0 \\
0 & P_2 & \cdots & 0 \\
0 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & P_d
\end{pmatrix}, \quad (6)$$

where, with minor abuse of notation, we denote by the same symbol $P_k$ the permutation operator and the matrix that represents it in the standard basis.

For the example given in Fig. 1, we have:

$$C = \sum_{j=0}^{3} Q_j \otimes |j\rangle\langle j|, \quad \text{with } Q_j \in U(2)$$

and

$$S = \begin{pmatrix}
P_1 & 0 \\
0 & P_2
\end{pmatrix}, \quad \text{where } P_1 = \begin{pmatrix}
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0
\end{pmatrix} \quad \text{and } P_2 = P_1^{-1}.$$

Summarizing, the action of the coin tossing operation and conditional shift on the vector space $C \otimes \mathcal{W}$ is given, for $k = 1, \ldots, d$, and $j = 0, \ldots, N - 1$, by

$$Ce_{kj} = (Q_j|c_k\rangle) \otimes |j\rangle, \quad (7)$$

$$Se_{kj} = |c_k\rangle \otimes (P_k|j\rangle) = |c_k\rangle \otimes |\pi_k j\rangle.$$
The dynamics of the quantum walk is as follows. At every step, $|\psi\rangle$ evolves as $|\psi\rangle \rightarrow SC|\psi\rangle$, i.e., a coin tossing operation $C$ is followed by a conditional shift $S$. The coin tossing operation may change at any time step preserving however the structure (3). This leads to a point of view where the operations $Q_j$ in (3) are seen as control variables in the evolution of the system. In this paper, we are interested in studying the set of states that can be obtained for the quantum walks just defined by varying in all possible ways the coin operations.

3 Controllability

The set of all possible evolutions is given by the set of all products of the form $\prod_{k=1}^{n} SC_k$ where $C_k$ are arbitrary coin tossing operations of the form (3). This set was already studied in [2,8] for the centralized case where the $Q_j$ in (3) are all equal. Improving the technique used in these references we obtain a complete characterization of this set for our case in Theorem 1. We first set up some definitions. Recall that $S$ being a permutation matrix has a certain order $r$, such that $Sr$ is the identity on $C \otimes W$. Define the set of matrices

$$F := \{A, S A S^{r-1}, \ldots, S^{r-1} A\},$$

where $A$ is the span of matrices of the form $\sum_{j=0}^{N-1} A_j \otimes |j\rangle \langle j|$ with $A_j \in u(d)$. Notice that $A$ is a Lie algebra (a Lie algebra has the structure of a vector space with the additional Lie bracket operation), since it is closed under the Lie bracket operation as it can be seen by taking

$$\left[\sum_{j=0}^{N-1} A_j \otimes |j\rangle \langle j|, \sum_{k=0}^{N-1} B_k \otimes |k\rangle \langle k| \right] = \sum_{j=0}^{N-1} [A_j, B_j] \otimes |j\rangle \langle j| \in A. \quad (9)$$

Here, we used the fact that the basis $\{|0\rangle, \ldots, |N - 1\rangle\}$ is orthonormal. In fact, $A$ is the direct sum (a direct sum of Lie subalgebras is a sum of subspaces which commute with each other) of $N$ subalgebras isomorphic to $u(d)$ as it can be easily seen with a change of coordinates which transforms $\sum_{j=0}^{N-1} A_j \otimes |j\rangle \langle j|$ into the block diagonal form $\sum_{j=0}^{N-1} |j\rangle \langle j| \otimes A_j$. Let $\mathcal{L}$ be the Lie algebra generated by $\mathcal{F}$, defined as the smallest Lie algebra containing $\mathcal{F}$, and let $e^\mathcal{L}$ be the connected Lie group associated with $\mathcal{L}$, that is, the connected component containing the identity.

**Proposition 3.1** Recall the definition of $S$ in (4). Let:

1. $K$ be the set defined as:

$$K := e^\mathcal{L} \cup e^\mathcal{L} S \cup e^\mathcal{L} S^2 \cup \ldots \cup e^\mathcal{L} S^{r-1} \quad (10)$$

where $e^\mathcal{L} S^j$ is the set of all matrices $X S^j$ with $X \in e^\mathcal{L}$.

2. $G$ be the group generated by $e^\mathcal{L}$ and $\{S\}$. 

\(\square\) Springer
3. If \( p \) is the smallest integer \( 1 \leq p \leq r \) such that \( S^p \in e^L \), let \( C \) be the set defined as the disjoint union of \( e^L, e^LS, \ldots, e^LS^{p-1} \).

Then \( K = C = G \) and they are Lie groups.

Before giving the proof, we notice that:

- The set defined in Eq. (10) is the same as the set of all matrices \( S^jY \) with \( Y \in e^L \). That is \( S^j e^L = e^L S^j \). To prove \( e^L S^j \subseteq S^j e^L \), write \( XS^j \) as \( S^j S^{-j} XS^j \). Since \( S^{-j} XS^j \in e^L \) if \( X \in e^L \) the claim follows. The converse inclusion is proved analogously.
- To see that the sets \( e^L, e^LS, \ldots, e^LS^{p-1} \) are disjoint, notice that if there exist two different indices \( 0 \leq k < j \leq p - 1 \) and two elements in \( e^L \), \( X \) and \( Y \) such that \( XS^j = YS^k \), we would have \( S^{j-k} = X^{-1}Y \in e^L \) which contradicts the minimality of \( p \).

**Proof** It follows from the definitions that \( K \subseteq G \), and \( C \subseteq K \). The equality \( K = C = G \) follows if we show that \( G \subseteq K \) and \( K \subseteq C \). An element in \( G \) is a product \( \prod_{k=0}^{m} Y_k \), with \( Y_0 \) equal to the identity, where \( Y_k \in e^L \) or \( Y_k = S^k \), for \( k \geq 1 \). By induction on \( m \), if \( m = 0 \), this product is the identity which is in \( e^L \) and therefore in \( K \). If \( m > 0 \), write \( \prod_{k=0}^{m} Y_k = Y \prod_{k=0}^{m-1} Y_k \), with \( \prod_{k=0}^{m-1} Y_k \in K \), i.e., \( \prod_{k=0}^{m-1} Y_k = XS^j \) for some \( 0 \leq j < r - 1 \) and \( X \in e^L \). Now, if \( Y \in e^L \), then \( YXS^j \in e^L S^j \subseteq K \). If \( Y = S^r \) then \( YXS^j = XS^rS^{-j}S^1 S^j \) and since \( X \in e^L \) implies \( Z := XS^rS^{-1} \in e^L \), we have \( YXS^j = ZS^{j+1} \in K \).

To see that \( K \subseteq C \), we need to consider only \( XS^k \) with \( kp - 1 \). Choose \( n \) so that \( 0 \leq k - np \mod r < p \) and define \( j := k - np \mod r \). We have \( XS^k = XS^{np}S^k - np := YS^j \). The matrix \( Y := XS^{np} \) is in \( e^L \), since \( X \) and \( S^{np} \) are both in \( e^L \). Moreover since \( j < p \), \( YS^j \) is in \( C \), that is, \( XS^k \in C \).

To see that \( C \) and therefore \( K \) and \( G \) are Lie groups, we notice that \( C \) naturally has the structure of a differentiable manifold inherited by \( e^L \). In fact, if \( \{ U_\alpha, \phi_\alpha \} \) is an atlas for \( e^L \), with \( \phi_\alpha : U_\alpha \to \mathbb{R}^n \), then \( \{ U_\alpha S^k, \phi_{\alpha,k} \} \) is an atlas for \( C \). Thus, if \( \Psi : e^L \to e^L C^\infty \), then, for all \( 1 \leq k, l \leq p - 1 \), the induced map \( \Psi_{k,l} : e^L S^k \to e^L S^l \), defined as \( \Psi_{k,l}(XS^k) := \Psi(X)S^l \), is also \( C^\infty \). (If \( \phi_{\alpha,k} \) and \( \phi_{\beta,l} \) are chart maps on \( e^L S^k \) and \( e^L S^l \), then \( \phi_{\beta,l} \circ \phi_{\alpha,k}^{-1} \) is by definition the same as \( \phi_{\beta} \circ \Phi \circ \phi_{\alpha}^{-1} \) which is a \( C^\infty \) map from \( \mathbb{R}^n \) to \( \mathbb{R}^n \) since \( \Psi \) is \( C^\infty \).) In particular, consider the inverse matrix map \( \Upsilon : (XS^k) \to (XS^k)^{-1} \). Write \( r - k \) as \((r - k - jp) + jp\) for some \( j \) where \( r - k - jp < p \). We have:

\[
\Upsilon(XS^k) := (XS^k)^{-1} = S^{-k}X^{-1} = S^{r-k-jp}S^{jp}X^{-1}S^{-r+k-jp}S^{r-k-jp}.
\]

This formula shows that, the inverse matrix map \( \Upsilon \) can be seen as the induced map \( \Psi_{k,r-k-jp} : e^L S^k \to e^L S^{r-k-jp} \), where the map \( \Psi : e^L \to e^L \) is defined as \( \Psi := \Psi_3 \circ \Psi_2 \circ \Psi_1 \) with \( \Psi_1 : X \to X^{-1} \), \( \Psi_2 : Y \to Y \) (recall that by definition of \( pS^{jp} \in e^L \)), and \( \Psi_3 : z \to S^{-r+k-jp}zS^{(r-k-jp)} \). Since the maps \( \Psi_1, \Psi_2 \) and \( \Psi_3 \) are \( C^\infty \) so is \( \Psi \) and therefore so is the inverse map. Analogously, one notices that a map \( \Phi : e^L \times e^L \to e^L \) which is \( C^\infty \) induces, for fixed \( k, l \) and \( m \), a map \( \Phi_{(k,l),m} : e^L S^k \times e^L S^l \to e^L S^m \) which is also \( C^\infty \) defined by \( \Phi_{(k,l),m}(XS^k,YS^l) := \Phi(XS^k,YS^l) \).
\[ \Phi(X, Y)S^m. \] Using this fact one shows that the product operation in \( C \) is also \( C^\infty \). Therefore, since both inverse and product operations on \( C(= K = G) \) are \( C^\infty \), this group is by definition a Lie group.

Notice that if \( S \in e^L \), \( G \) has only one connected component which is given by \( e^L \).

The following theorem characterizes the controllability of quantum walks.

**Theorem 1** Let \( \mathcal{E} \) be the set of possible evolutions of the quantum walk. Then

\[ \mathcal{E} = K \] (11)

**Proof** \( \mathcal{E} \) is the set of products of transformations of the form \( SC \) with \( C \) a coin tossing operation and \( S \) a conditional shift. Since \( C \in e^L \subseteq K \) and \( S \in K \) (because \( K = G \) in Proposition 3.1) then \( SC \in K \) and therefore \( \mathcal{E} \subseteq K \). Vice versa, consider an element \( XS^j \in K \), for some \( 0 \leq j \leq r - 1 \). Since \( X \in e^L \), it can be written as the product of matrices of the form \( S^k e^A S^{r-k} \) with the matrix \( A \in A \) of the form \( A = \sum_{l=0}^{N-1} A_l \otimes |l\rangle\langle l| \) and \( A_l \in u(d) \). (This is a consequence of the known fact that if a set \( \mathcal{F} \) generates a certain Lie algebra, then every element \( X \) in the corresponding Lie group can be written as the finite product of exponentials \( e^{Ft} \) with \( t \in R \) and \( F \in \mathcal{F} \).) The matrix \( C := e^A \) is a coin operation, and therefore, we can write \( S^k e^A S^{r-k} \) as \( S^k C S^{r-k} \). We can obtain \( S^k C S^{r-k} \) by performing \( r - k \) steps with coin operations equal to the identity, one step with coin operation equal to \( C \) and \( k - 1 \) steps with coin operation equal to the identity (in the case \( k = 0 \), we can use one step with coin operation equal to \( C \) followed by \( r - 1 \) operations with coin operation equal to the identity). Therefore every matrix of the form \( S^k e^A S^{r-k} \) can be obtained as an evolution of the quantum walk. So can every product of such matrices and therefore every \( X \in e^L \). To obtain \( XS^j \), just compose the sequence giving \( X \) with \( j \) steps of the walk with coin operation equal to the identity. This shows that \( K \subseteq \mathcal{E} \) and concludes the proof of the theorem.

**Remark 3.2** An analogous characterization of the set \( \mathcal{E} \) can be proved with just small notational modifications for the ‘centralized’ case where all the matrices \( Q_j \) in (3) are equal. In this case, the Lie algebra \( A \) in (8) has to be replaced by the Lie algebra of matrices \( A \otimes I \) with \( A \in u(d) \) and \( I_N \) the \( N \times N \) identity. This was the case treated in [2,8]. The above discussion goes however further with respect to the results in [2,8] where only the inclusion \( e^L \subseteq \mathcal{E} \) was proved.

From Theorem 1, it follows that the Lie algebra \( L \) plays a crucial role in the characterization of the set of available state transformations of the quantum walk. Following common terminology in quantum control, we shall call this Lie algebra the **dynamical Lie algebra** associated with the quantum walk. The following Theorem holds.

**Theorem 2** The quantum walk is completely controllable (every unitary operation is possible) if and only if \( L = u(dN) \).

**Proof** If \( L = u(dN) \) then \( e^L = U(dN) \). Since \( e^L \subseteq K \subseteq U(dN) \), we clearly have, from Theorem 1, \( \mathcal{E} = K = U(dN) \). Therefore the system is completely controllable. Conversely if a quantum walk is completely controllable, then \( U(dN) = \mathcal{E} = K \). Thus
\( K \) can only have one connected component since \( U(dN) \) is connected. The number of connected components is given by \( p \) in Proposition 3.1. Therefore \( p \) must be equal to 1, \( S \in eL \) and \( K = eL \). From the fact that \( eL = U(dN) \), using the correspondence between connected Lie groups and Lie algebras (see e.g., [15]), it follows that the Lie algebras of \( eL \) and \( U(dN) \) must coincide. Therefore \( L = u(dN) \). \( \square \)

**Remark 3.3** Another motivation to study the Lie algebra \( L \) is given by the work in [7] where a procedure was described to obtain continuous quantum walks as an appropriate limit of discrete quantum walks. This procedure generalized a method given in [18] for quantum walks on the line. In particular, the set \( iL \) represents the set of all Hamiltonians whose associated continuous dynamics over the full space \( C \otimes \mathcal{W} \) can be obtained with the procedure of [7].

In general, calculating a Lie algebra directly from a set of generators can be cumbersome since we have to compute commutators of possibly very large matrices. Therefore different criteria of controllability are desirable. In the following section, we shall characterize the dynamical Lie algebra \( L \) for every quantum walk in combinatorial terms, i.e., in terms of the permutations \( \pi_1, \ldots, \pi_d \) characterizing the walk.

### 4 Controllability and orbits of permutations

We take a closer look at the generating set \( F \) in (8) for the dynamical Lie algebra \( L \) and at how it relates to the orbits of the permutations \( \pi_1, \ldots, \pi_d \).

Given \( l \) and \( m \), with \( l, m \in \{1, 2, \ldots, d\} \), define the \((l, m)\)th joint orbit, \( O_{l,m} \), as the following subset of \( V \times V \),

\[
O_{l,m} := \bigcup_{k=0}^{r-1} \bigcup_{j=0}^{N-1} (\pi_l^k j, \pi_m^k j).
\] (12)

Notice that \((j, j)\) is in any joint orbit for every pair \((l, m)\). In the basis given by \( e_{ij} \) (see Eq. 5), we can enumerate the rows and columns of any matrix in \( F \) (and \( L \)) using an index \( i \) to identify a block row (or column) \((i = 1, 2, \ldots, d)\) and the index \( j \) \((j = 0, 1, \ldots, N - 1)\) to identify a position inside a block. We consider the matrices in \( F \) and \( L \) in this basis. The following theorem relates the structure of the matrices in \( F \) with the orbits defined in (12). In order to state this theorem we introduce \( \tilde{F} \), the vector space of all the skew-Hermitian matrices having the \((l, h) - (m, s)\)th position \( l, m = 1, 2, \ldots, d, h, s = 0, 1, \ldots, N - 1\) possibly different from zero and arbitrary if and only if \((h, s) \in O_{l,m} \). The vector space \( \tilde{F} \) is spanned by the set \( \tilde{B} \) defined as

\[
\tilde{B} := \left\{ \begin{array}{ll}
(\langle c_l | c_m | \otimes | h \rangle \langle s | - | c_m \rangle \langle c_l | \otimes | s \rangle \langle h |), & l, m = 1, \ldots, d, \\
i(\langle c_l | c_m | \otimes | h \rangle \langle s | + | c_m \rangle \langle c_l | \otimes | s \rangle \langle h |), & h, s = 0, 1, \ldots, N - 1,
\end{array} \right\}.
\] (13)

**Theorem 3** \( \text{span } F = \tilde{F} \).
Proof To show that $\tilde{\mathcal{F}} \subseteq \text{span } \mathcal{F}$ it is enough to show that for any $B \in \tilde{\mathcal{B}}, B \in \mathcal{F}$. Let $B := \langle c_l \rangle \langle c_m | \otimes | h \rangle \langle s | - \langle c_l \rangle \langle c_l | \otimes | s | \rangle \langle h |$, for fixed $l$ and $m$ in $\{1, \ldots, d\}$ and $h$ and $s$ in $\{0, 1, \ldots, N - 1\}$. Since $\langle h, s \rangle$ is required to be in $\mathcal{O}_{l,m}$, there exists a $j \in \{0, 1, \ldots, N - 1\}$ and a $k \geq 0$ such that $\pi^k_j j = h$ and $\pi^k_m j = s$. For the given $k$, consider now the matrix $S^k \mathcal{A} S^{-k} \in \mathcal{F}$ (cf. (8)), with $A$ given by $A := (\langle c_l \rangle \langle c_m | - \langle c_m | \langle c_l |) \otimes | j \rangle \langle j |$ and calculate (we will use the Kronecker delta notation $\delta_{ab} = 0$ if $a \neq b$, $\delta_{ab} = 1$ if $a = b$)

$$S^k \mathcal{A} S^{-k} = \left( \sum_{a=1}^d |c_a \rangle \langle c_a | \otimes P_a^k \right) \left( (\langle c_l \rangle \langle c_m | - \langle c_m | \langle c_l |) \otimes | j \rangle \langle j | \right)$$

$$\times \left( \sum_{b=1}^d |c_b \rangle \langle c_b | \otimes P_b^{-k} \right)$$

$$= \sum_{a=1}^d \sum_{b=1}^d \delta_{a,b} \delta_{b,m} |c_a \rangle \langle c_b | \otimes P_a^k | j \rangle \langle j | P_b^{-k}$$

$$- \delta_{a,m} \delta_{b,l} |c_a \rangle \langle c_b | \otimes P_a^k | j \rangle \langle j | P_b^{-k}$$

$$= |c_l \rangle \langle c_m | \otimes P_l^k | j \rangle \langle j | P_m^{-k} - |c_m \rangle \langle c_l | \otimes P_m^k | j \rangle \langle j | P_l^{-k}$$

$$= |c_l \rangle \langle c_l | \otimes | r \rangle \langle s | - | c_m \rangle \langle c_l | \otimes | s \rangle \langle h |,$$

(14)

since $P_l^k | j \rangle = | h \rangle$, $P_m^k | j \rangle = | s \rangle$. Thus $S^k \mathcal{A} S^{-k} = B \in \mathcal{F}$. A similar calculation choosing $A := i (\langle c_l \rangle \langle c_m | + | c_m \rangle \langle c_l |) \otimes | j \rangle \langle j |$ shows that $i (\langle c_l \rangle \langle c_m | \otimes | h \rangle \langle s | + | c_m \rangle \langle c_l | \otimes | s \rangle \langle h |)$ is in $\mathcal{F}$, so we conclude $\tilde{\mathcal{F}} \subseteq \text{span } \mathcal{F}$. To prove that $\text{span } \mathcal{F} \subseteq \tilde{\mathcal{F}}$, it is enough to show that every element in $\mathcal{F}$ of the form $S^k \mathcal{A} S^{-k}$, with $A = \sum_{j=0}^{N-1} A_j \otimes | j \rangle \langle j | \in \mathcal{A}$, for $j = 0, \ldots, N - 1$, where $A_j$ is a general matrix in $u(d)$, can be expressed as a linear combination of elements in $\tilde{\mathcal{B}}$ in (13). We write

$$S^k \mathcal{A} S^{-k} = \left( \sum_{l=1}^d |c_l \rangle \langle c_l | \otimes P_l^k \right) \left( \sum_{j=0}^{N-1} A_j \otimes | j \rangle \langle j | \right) \left( \sum_{m=1}^d |c_m \rangle \langle c_m | \otimes P_m \right)$$

$$= \sum_{l,m = 1, \ldots, d}^{l,m = 1, \ldots, d} |c_l \rangle \langle c_l | A_j | c_m \rangle \langle c_m | \otimes P_l^k | j \rangle \langle j | P_m^{-k}.$$  

After defining

$$x_{jml} := \langle c_l | A_j | c_m \rangle,$$

(15)

and noticing that, since $A^*_j = -A_j$, we have $x_{jml}^* = -x_{jml}$, we can write

$$S^k \mathcal{A} S^{-k} = \sum_{l,m = 1, \ldots, d}^{l,m = 1, \ldots, d} x_{jml} |c_l \rangle \langle c_m | \otimes P_l^k | j \rangle \langle j | P_m^{-k}$$

$$j = 0, \ldots, N - 1$$
\[
= \sum_{j=0,1,\ldots,N-1} \left( \sum_{l=1,2,\ldots,d} x_{jll} |c_l| \langle c_l | \otimes P^k_l |j | P^{-k}_l \right) \\
+ \left( \sum_{l,m=1,2,\ldots,d, l < m} x_{jlm} |c_m| \langle c_m | \otimes P^k_l |j | P^{-k}_m \right) \\
+ x_{jml} |c_m| \langle c_l | \otimes P^k_m |j | P^{-k}_l \right). \\
\tag{16}
\]

By defining \( R_{jlm} := \text{Re}(x_{jlm}) \) and \( I_{jlm} = \text{Im}(x_{jlm}) \) and since we have \( R_{jlm} = -R_{jml} \) and \( I_{jlm} = I_{jml} \), we have

\[
S^k AS^{-k} = \sum_{j=0,1,\ldots,N-1} \sum_{l=1,\ldots,d} i I_{jll} |c_l| \langle c_l | \otimes P^k_l |j | P^{-k}_l \\
+ \sum_{l<m} R_{jlm} \left( |c_l| \langle c_m | \otimes P^k_l |j | P^{-k}_m - |c_m| \langle c_l | \otimes P^k_m |j | P^{-k}_l \right) \\
+ \sum_{l<m} I_{jlm} \left( |c_l| \langle c_m | \otimes P^k_l |j | P^{-k}_m + |c_m| \langle c_l | \otimes P^k_m |j | P^{-k}_l \right).
\]

This is a linear combination (with real coefficient) of elements in \( \tilde{\mathcal{B}} \) since for every pair \((l, m)\) and every \(j, (\pi_l^k, j, \pi_m^k j) \in \mathcal{O}_{l,m}\). This shows that \( S^k AS^{-k} \in \mathcal{F} \) and concludes the proof of the theorem.

To study the nature of the Lie algebra \( \mathcal{L} \) generated by \( \mathcal{F} \), we shall apply some results proved in [20]. In order to do that, we associate with the quantum walk a connectivity graph, which will be denoted by \( G_{C} \), having \( dN \) vertices, each corresponding to a pair \((l, h)\), with \( l \in \{1, 2, \ldots, d\} \) and \( h \in \{0, 1, \ldots, N-1\} \). We connect two pairs \((l, h)\) and \((m, s)\) if and only if \((h, s) \in \mathcal{O}_{l,m}\). It follows from the proof of the above theorem that \((h, s) \in \mathcal{O}_{l,m}\) if and only if there exists a matrix in \( \mathcal{F} \) with the \([(l, h), (m, s)]\)th element different from zero. In the connectivity graph \( G_{C} \), we omit all self connections. These correspond to diagonal elements in the matrices in \( \mathcal{F} \), which can, in fact, be chosen arbitrarily (but must be purely imaginary). In [20] the authors studied the Lie algebra generated by two skew-Hermitian matrices, \( iH_0 \) and \( \Omega_0 \), with \( H_0 \) Hermitian and diagonal, and \( \Omega_0 \), purely real, i.e., skew-symmetric. A (connectivity) graph was associated with this pair of matrices with edges connecting vertices corresponding to the row (or column) indices \((a, b)\) if and only if the \((a, b)\)-th entry in \( \Omega_0 \) was different from zero. These edges were then labeled, with the label corresponding to \((a, b)\), equal to \(|\lambda_a - \lambda_b|\), where \(\lambda_a(\lambda_b)\) is the diagonal element (eigenvalue) of \(iH_0\) corresponding to \(a(b)\). The next theorem was proved in [20]; here it is stated in a form suitable for our purposes.

**Theorem 4** Assume that the labeled (connectivity) graph associated with the pair \((iH_0, \Omega_0)\) is connected and it remains connected after eliminating edges having equal labels. Consider the Lie algebra \( \mathcal{L} \) generated by \( iH_0 \) and \( \Omega_0 \). Then the corresponding...
Lie group $e^{\tilde{L}}$ is transitive on the complex sphere, i.e., for every pair of unit vectors $|\psi_0\rangle$ and $|\psi_1\rangle$ in $\mathbb{C}^n$, there exists an element $X \in e^{\tilde{L}}$ with $|\psi_1\rangle = X|\psi_0\rangle$. 

We shall use this theorem along with some results on the controllability of quantum systems proved in [1], to establish the following result.

**Theorem 5** The quantum walk is completely controllable, i.e., $\mathcal{L} = u(dN)$, if and only if the associated connectivity graph $G_C$ is connected.

**Proof** First assume that the connectivity graph $G_C$ is connected. Since $\mathcal{F}$ contains arbitrary skew-Hermitian diagonal matrices we can choose a matrix where all the differences between two diagonal elements are different from each other. Let $iH_0$ denote such a matrix in $\mathcal{F}$. Moreover we can choose a matrix $\Omega_0$ in span $\mathcal{F}$ with entries $(l, h) - (m, s)$ different from zero and real if and only if there exists an edge connecting the vertices $(l, h)$ and $(m, s)$ in $G_C$. Thus, the connectivity graph $G_C$ is the graph corresponding to the pair $iH_0$ and $\Omega_0$ considered in Theorem 4. Since this graph is connected and there are no edges to remove since all edges are labeled with a different label, we have that the Lie algebra $\tilde{\mathcal{L}}$ generated by $iH_0$ and $\Omega_0$, which is a subalgebra of $\mathcal{L}$, is such that the corresponding Lie group $e^{\tilde{L}}$ is transitive on the complex sphere. This is also the case for the Lie group $e^{\mathcal{L}}$ associated with $\mathcal{L}$ since $e^{\tilde{L}}$ is a subgroup of $e^{\mathcal{L}}$. This fact does not necessarily imply that the quantum walk is completely controllable, i.e., $\mathcal{L} = u(dN)$. However, according to general controllability results for quantum systems [1], the only other possibility is that $\mathcal{L}$ is conjugate to the symplectic Lie algebra $sp(dN/2)$ plus multiples of the identity matrix. (Notice that here $dN$ must be even since the hand-shaking lemma of graph theory [9] implies for regular graphs that $dN = 2|E|$, where $|E|$ is the number of edges.) This implies that there exists a matrix $\tilde{J}$ of the form $\tilde{J} = T^\dagger J T$ where

$$J = \begin{pmatrix} 0 & \mathbb{I}_{dN/2} \\ -\mathbb{I}_{dN/2} & 0 \end{pmatrix},$$

and $T$ is some unitary matrix, such that

$$A\tilde{J} + \tilde{J}A^T = 0,$$

for every $A \in \mathcal{L}$ with $Tr(A) = 0$. We now prove that (18) is not possible. To see this, partition $\tilde{J}$ into $d \times d$ blocks of dimension $N \times N$. Formula (18) has to hold, in particular, for every $A \in \mathcal{F}$, with $Tr(A) = 0$. Let $A$ be an arbitrary skew-Hermitian diagonal, zero trace matrix. This type of matrices are in $\mathcal{F}$. Denote $A$ by:

$$A = \begin{pmatrix} D_1 \\ D_2 \\ \vdots \\ D_d \end{pmatrix}$$

(19)
with \( D_l = \text{Diag}[i\lambda_1^l, \ldots, i\lambda_N^l] \), \( \lambda_j^l \in \mathbb{R} \) and \( \sum_{l=1}^d \sum_{j=1}^N \lambda_j^l = 0 \). Fix two block indices \( k, l \in \{1, \ldots, d\} \), then it holds that:

\[
(A\tilde{J} + \tilde{J}A^T)_{lk} = D_l\tilde{J}_{lk} + \tilde{J}_{lk}D_k.
\]

(20)

Thus, since from Eq. (18), the previous expression must be zero, we get:

\[
(D_l\tilde{J}_{lk} + \tilde{J}_{lk}D_k)_{sj} = i(\lambda_s^l + \lambda_j^k)(\tilde{J}_{lk})_{sj} = 0, \quad \forall s, j \in \{0, 1, \ldots, N - 1\}.
\]

Now, for fixed indices \( l, k \in \{1, \ldots, d\} \) and \( s, j \in \{0, 1, \ldots, N - 1\} \), we can choose \( A \), in Eq. (19), with \( \lambda_j^l + \lambda_j^k \neq 0 \); this is clearly possible since the coefficients \( \lambda_j^l \) can be chosen arbitrarily except for the trace condition. Choose for example \( \lambda_s^l = \lambda_j^k = 1, \lambda_j^l = -2 \) for one arbitrary \( s \in \{0, 1, \ldots, N - 1\} \) different from \( s \), and all other \( \lambda_i^m, m \in \{1, 2, \ldots, d\}, t \in \{0, 1, \ldots, N - 1\} \) equal to zero. So we get \( (\tilde{J}_{lk})_{sj} = 0 \). By varying the indexes \( l, k \) and \( s, j \) we conclude \( \tilde{J} = 0 \), which contradicts (17). This shows that \( \mathcal{L} = u(dN) \).

To see that the condition on the connectivity graph \( G_C \) being connected is also necessary, notice that if the graph is not connected then it can be divided in \( g \geq 2 \) connected components. Reordering the column and row indices of the matrices in \( \mathcal{F} \), according to the various connected components of the graph, we can write all the matrices in \( \mathcal{F} \) in block diagonal form. The Lie bracket operation preserves this block diagonal form. Therefore, not all the matrices in \( u(dN) \) can be generated from the elements of \( \mathcal{F} \) and \( \mathcal{L} \neq u(dN) \).

Elaborating further on the statement and the proof of Theorem 5, we obtain more information on the controllability of quantum walks on graphs. In particular, notice that for every \( j \in V \), \((j, j)\) is in the orbit \( \mathcal{O}_{l,m} \) for every \( l, m = 1, 2, \ldots, d \). This means that \((1, j), (2, j), \ldots, (d, j)\) are all connected in the connectivity graph \( G_C \). This observation suggests to use a \textit{reduced connectivity graph}, which will be denoted by \( G_R \). The graph \( G_R \) will have \( N \) vertices, each corresponding to a vertex position in \( V := \{0, 1, \ldots, N - 1\} \), and there is an edge connecting the two vertices \( h \) and \( s \) if and only if there exist two coin indices \( l \) and \( m \) so that \((l, h)\) and \((m, s)\) are connected in the connectivity graph \( G_C \). It follows from the fact that for every \( j \in \{0, 1, \ldots, N - 1\} \), \((1, j), (2, j), \ldots, (d, j)\) are all connected in \( G_C \), that \( G_R \) is connected if and only if \( G_C \) is connected. Moreover, from the definition of the orbits \( \mathcal{O}_{l,m} \), we get that two vertices \( h \) and \( s \) in \( G_R \) are connected by an edge if and only if there exists a \( j \in \{0, 1, \ldots, N - 1\} \) and two coin indices \( l \) and \( m \) and an integer \( k \) such that \( \pi_i^kj = h \) and \( \pi_m^kj = s \), i.e.,

\[
h = \pi_i^k \pi_m^{-k}s.
\]

(21)

This relation gives a method to construct \( G_R \). The algorithm is as follows: 

\( \mathbb{S} \) Springer
Algorithm 1

1. Given the permutations $\pi_1, \ldots, \pi_d$ characterizing the walk, consider for every pair $l < m$ the permutations $\pi^k_l \pi^{-k}_m$ written in the cycle notation, i.e., $\pi^k_l \pi^{-k}_m = (\cdots) \cdots (\cdots)$.

2. Connect in a graph all the vertices that pairwise belong to the same cycle at least in one instance. This is the reduced connectivity graph $G_R$ associated with the quantum walk.

The following theorem describes the structure of the dynamical Lie algebra $L$, in cases where controllability is not verified, i.e., $L \neq u(dN)$, in terms of the graphs $G_R$.

**Theorem 6** The dynamical Lie algebra $L$ is always the direct sum of $m > 0$ Lie algebras isomorphic to $su(d v_\ell)$ for some positive integers $v_\ell, \ell = 1, \ldots, m$ with $\sum_{\ell=1}^m v_\ell = N$ along with a one dimensional Lie algebra spanned by multiples of the identity matrix in $u(dN)$. Each subalgebra isomorphic to $su(d v_\ell)$ corresponds to a connected component of the reduced connectivity graph $G_R$ with $v_\ell$ vertices. Complete controllability is obtained in the case $m = 1$.

**Proof** Assume that $G_R$ has $m$ connected components, and that the $\ell$th component has $v_\ell$ elements (so $\sum_{\ell=1}^m v_\ell = N$). We can perform a change of coordinates (which corresponds to a relabeling of the vertices) to regroup together vertices corresponding to the same connected component. More precisely, this change of coordinates on $L$ has the form $X \rightarrow U X U^\dagger$, where $U = I \otimes P$, with $I$ the $d \times d$ identity and $P$ the permutation on $\{0, 1, \ldots, N-1\}$ which puts together all vertices in the same connected component of $G_R$. In these coordinates all matrices in $F$ and $L$ are block diagonal. Since the $\ell$th connected component has $v_\ell$ vertices the $\ell$th block has dimension $d v_\ell$. For each block, we can repeat the argument of Theorem 5 to conclude that we can get any matrix in $u(d v_\ell)$, and this shows the structure of the Lie algebra $L$. \( \square \)

In the rest of this section, we give two consequences of the results and methods summarized in Theorems 5 and 6 and Algorithm 1. Appendix A contains some further analysis which uses the results of the next section to show that the number $m$ in Theorem 6 can only be 1 (controllable case) or 2.

**Proposition 4.1** If $d > \frac{N}{2}$ the quantum walk is completely controllable.

**Proof** We will show that the reduced connectivity graph $G_R$ is connected. Fix two distinct vertices $i, j \in \{0, \ldots, N-1\}$. Consider the following two subset of vertices:

$$A_i = \{ \pi_l i \mid l \in \{1, \ldots, d\} \}, \quad A_j = \{ \pi_l j \mid l \in \{1, \ldots, d\} \}. \quad (22)$$

Since, by assumption on the model, all the vertices in $A_i$ and in $A_j$ are different, the number of different elements in $A_i$ and $A_j$ is $d$, i.e., $|A_i| = |A_j| = d$. Thus we have $|A_i| > \frac{N}{2}$ and the same inequality holds for $|A_j|$. These two inequalities imply that $A_i \cap A_j \neq \emptyset$. Thus there exist two coin indices $l_i$ and $l_j$ such that

$$\pi_{l_i} i = \pi_{l_j} j = k.$$
Since \( \pi_{l,j} = k \), in the graph \( G \) there is an edge connecting the two vertices \( j \) and \( k \). Therefore, there must exist a coin value \( c_{l,k} \) such that \( \pi_{l,k} = j \); analogously there exists a coin value \( c_{l,i} \) such that \( \pi_{l,i} = k \). This implies that

\[
i = \pi_{l,i}\pi_{l,k}^{-1}j,
\]

so the two indices \( i \) and \( j \) are connected in \( G_R \), since equation (21) holds. By the arbitrariness of \( i \) and \( j \), we get that \( G_R \) is connected, as desired. Another (graph theoretic) proof of this result can be obtained as a consequence of 4 in Theorem 8 below. \( \square \)

The bound in Proposition 4.1 is sharp in the sense that there are quantum walks that are not controllable with \( d = \frac{N}{2} \). In fact, we shall see in Sect. 7 that quantum walks on a cycle (therefore of degree 2) with 4 vertices are not controllable. Notice also that, as a special case of Proposition 4.1, quantum walks on complete graphs are always controllable (we always assume \( N \) as a special case of Proposition 4.1).

For the last result of this section, we need the concept of product of two quantum walks. Consider two quantum walks. The first one, \( W_1 \), is supported by a graph \( G_1 := \{V_1, E_1\} \) with a set of permutations \( \{\pi_1^1, \ldots, \pi_1^{d_1}\} \) and the second one, \( W_2 \), supported by a graph \( G_2 := \{V_2, E_2\} \) with a set of permutations \( \{\pi_2^1, \ldots, \pi_2^{d_2}\} \). The product walk \( W_1 \times W_2 \) is the walk whose graph is the Cartesian product of \( G_1 \) and \( G_2 \) and the associated permutations are \( \{\tilde{\pi}_1^1, \ldots, \tilde{\pi}_1^{d_1}, \tilde{\pi}_2^1, \ldots, \tilde{\pi}_2^{d_2}\} \) acting on the vertices \((j, k) \in V_1 \times V_2\) as \( \tilde{\pi}_1^1(j, k) := (\pi_1^1 j, k) \) and \( \tilde{\pi}_2^1(j, k) := (j, \pi_2^1 k) \). One example is a walk on a 2-dimensional lattice with \( N_1 \times N_2 \) vertices connected in a periodic fashion horizontally and vertically. Coin results can be labeled \( R, L, U, D \) (Right, Left, Up, Down (mod \( N_1 \)), respectively) and this is the product of two walks one evolving horizontally on a cycle with \( N_1 \) nodes and one evolving vertically on a cycle with \( N_2 \) nodes.

**Proposition 4.2** The product of two controllable walks is controllable.

**Proof** Let \( G^{1,2}_R \) denote the reduced connectivity graph of the product walk \( W_1 \times W_2 \). With the above notations, since the walk \( W_1 \) is controllable, for every \( j \in V_2 \) the vertices \((k, j), k = 1, \ldots, N_1\), are all connected in \( G^{1,2}_R \). Analogously, from the controllability of \( W_2 \), it follows that for every \( k \in V_1 \) the vertices \((k, j), j = 1, \ldots, N_2\), are all connected in \( G^{1,2}_R \). Therefore \( G^{1,2}_R \) is connected and the walk \( W_1 \times W_2 \) is controllable. \( \square \)

We remark that the above condition is not necessary and one can find two quantum walks with one or both of them uncontrollable whose product is controllable.

5 Constructive controllability algorithms

In this section, we discuss constructive controllability. We will focus on finding control algorithms to steer the state of the quantum walk between two values. Thus, for any given two state vectors \(|\psi_1\rangle, |\psi_2\rangle\) in \( \mathcal{C} \otimes \mathcal{W} \) we will find a sequence of coin tossing operations, \( C_1, \ldots, C_k \), such that

\[
|\psi_2\rangle = SC_k \cdots SC_1 |\psi_1\rangle.
\]
Moreover, we will give a \textit{bound} on the length \( k \) of the needed control sequence. Whether such a sequence exists or not can be checked with the methods of the previous two sections.

First, we define, for a given node \( j \), the set of all nodes that one can reach using the edges of the graph in a given number of steps. Fix a node \( j \in \{0, \ldots, N-1\} \), let:

\[
\begin{align*}
N^0(j) & := \{j\}, \\
N^{s+1}(j) & := \{\pi_s(l) \mid l \in N^s(j), \ 1 \leq s \leq d\}.
\end{align*}
\]

With these definitions, \( l \in N^k(j) \) means that there exists a sequence of permutations \( \tilde{\pi}_1, \ldots, \tilde{\pi}_k \) in the set \( \{\pi_1, \ldots, \pi_d\} \) such that \( l = \tilde{\pi}_k \tilde{\pi}_{k-1} \cdots \tilde{\pi}_1 j \). The connectedness assumption on the graph \( G \) implies that \( \forall \ i, \ j \in \{0, \ldots, N-1\} \) there exists a \( k \geq 0 \) such that \( i \in N^k(j) \). The set \( N^k(j) \) only depends on the graph. It is the set of vertices which are connected to \( j \) by a path of length \( k \).

From these observations, we can collect two properties of the sets \( N^k(j) \) in the next lemma.

\textbf{Lemma 5.1} \textit{Let} \( i, \ j, \ l \in \{0, \ldots, N-1\}, k, s \geq 0, \text{ we have:}

\begin{enumerate}
\item \( l \in N^k(j) \Leftrightarrow l \in N^k(l) \),
\item if \( l \in N^k(j) \) and \( i \in N^s(l) \) then \( i \in N^{k+s}(l) \).
\end{enumerate}

Choose a node \( j \in \{0, \ldots, N-1\} \) and consider a state \( |\psi_1\rangle \) with probability 1 to find the walker in position \( j \). Thus \( |\psi_1\rangle \) is of the form \( |\psi_1\rangle = |c_0\rangle \otimes |j\rangle \), for some state \( |c_0\rangle \in C \). If there exists a sequence of coin tossing operations of length \( k \) such that

\[
SC_0 \cdots SC_1 |\psi_1\rangle = \sum_s \sum_l \alpha_{ls} |c_{k_l}\rangle \otimes |j_{k_s}\rangle,
\]

then, \( j_{k_s} \in N^k(j) \) for all \( k_s \). This fact, in particular, implies that a necessary condition to have complete controllability is that \( \forall \ j \in \{0, \ldots, N-1\} \) there exists a \( k \geq 0 \) such that \( N^k(j) = \{0, \ldots, N-1\} \) since we have to be able to transfer to an arbitrary state in \( C \otimes \mathcal{W} \). By using property 2) of Lemma 5.1, we can substitute \( \forall \) with \( \exists \) in the previous sentence. In fact, if there exists a \( \tilde{j} \) such that with a path of length \( k \), we can reach any \( l \in \{0, 1, \ldots, N-1\} \), with a path of length \( 2k \) we can go from any \( j \in \{0, 1, \ldots, N-1\} \) to any \( l \in \{0, 1, \ldots, N-1\} \) (just go to \( \tilde{j} \) in \( k \) steps and then to \( l \) in \( k \) additional steps).

Thus, we get that:

\textit{Claim} \ C1: complete controllability \( \Rightarrow \exists \ j \in \{0, \ldots, N-1\} \) and \( k \geq 0 \) such that \( N^k(j) = \{0, \ldots, N-1\} \).

This necessary condition can be checked indirectly with the methods of the previous sections. The constructive algorithms we are going to describe will imply that this necessary condition is indeed sufficient to get controllability between two arbitrary states for our model. We shall refer to this type of controllability as \textit{state controllability}. Moreover our results will imply an upper bound on the number of steps needed for
arbitrary state transfer in terms of the maximal (over $j$) $k$ such $\mathcal{N}^k(j) = \{0, \ldots, N-1\}$ and of the order $r$ of the conditional shift matrix $S$.

The next proposition provides a first $k$-steps control algorithm to go from a state with probability 1 to find the walker in a fixed node $j$, i.e., a state of the type $|c_0\rangle \otimes |j\rangle$, to one where the probability is arbitrarily distributed on the nodes in $\mathcal{N}^k(j)$. Even if the proof of the next proposition, as well as the proof of Proposition 5.5, will be given by induction, they are constructive. We present an example where these constructive procedures are used in Sect. 7.2.

**Proposition 5.2** Let $j$ be any node and $A_k = \{v_1, \ldots, v_l\}$ be any subset of $\mathcal{N}^k(j)$. Fix a state of the type $|\psi_0\rangle = |c_0\rangle \otimes |j\rangle$ and complex coefficients $(\alpha_1, \ldots, \alpha_l)$ with $\sum_{a=1}^l |\alpha_a|^2 = 1$ on the nodes of $A_k$. Then it is always possible to construct a control sequence $C_1, \ldots, C_k$ of coin operations such that:

$$SC_k \cdots SC_1 |\psi_0\rangle = \sum_{h=1}^l \alpha_h |c_h\rangle \otimes |v_h\rangle,$$

for some values of the coin variables $c_h$ (not necessarily distinct).

**Proof** We will prove the statement by induction on $k$.

If $k = 0$, then the statement is obvious. Assume that the proposition holds for $k$.

Let $A_{k+1} = \{v_1, \ldots, v_l\} \subseteq \mathcal{N}^{k+1}(j)$. By definition of $\mathcal{N}^{k+1}(j)$ we have that $A_{k+1} = \{v_1, \ldots, v_l\} = \{\tilde{\pi}_1(w_1), \ldots, \tilde{\pi}_l(w_l)\}$, where for $i = 1, \ldots, l$ $w_i \in \mathcal{N}^k(j)$, and $\tilde{\pi}_1, \ldots, \tilde{\pi}_l$ are permutations in the set $\{\pi_1, \ldots, \pi_d\}$. The nodes $w_i$ need not to be different. Denote by $s$ the number of distinct elements in $\{w_1, \ldots, w_l\}$, and let $A_k = \{w_1, \ldots, w_l\} = \{z_1, \ldots, z_s\}$ where all elements are distinct in the second set notation. Without loss of generality, we assume that we have ordered the nodes $v_h \in A_{k+1}$ in such a way that the first $g_1$ of $w_i$ are equal to $z_1$, the second $g_2$ of $w_i$ are equal to $z_2$ and so on. We have:

$$z_1 = w_1 = \cdots = w_{g_1},$$

$$z_2 = w_{g_1+1} = \cdots = w_{g_1+g_2},$$

$$\vdots$$

$$z_s = w_{g_1+\cdots+g_{s-1}+1} = \cdots = w_{g_1+\cdots+g_s},$$

with $g_0 := 0$. Moreover denote by $c_h$ the coin value that corresponds to the transition from $w_h$ in $\mathcal{N}^k(j)$ to $v_h$ in $\mathcal{N}^{k+1}(j)$, i.e.,

$$\pi_{c_h} w_h = v_h.$$

Let $\alpha_1, \ldots, \alpha_l$ be the given coefficients (cf. (24)), satisfying $\sum_{h=1}^l |\alpha_h|^2 = 1$. We can assume these coefficients all different from zero, without loss of generality, as in the case where one of them is zero we can eliminate the corresponding $v_h$ from the sum (24).

© Springer
Define for $i = 1, \ldots, s$,
\[
\gamma_i := \sqrt{g_1 + \cdots + g_i} \sum_{h=g_1 + \cdots + g_{i-1}+1}^{\sum_{h=g_1 + \cdots + g_i+1}} |\alpha_h|^2.
\] (26)

By the inductive assumption, since $A_k$ is a subset of $N^k(j)$, it is possible to construct, from $|\psi_0\rangle = |c_0\rangle \otimes |j\rangle$, a sequence of $k$ coin operations that steers $|\psi_0\rangle$ to
\[
|\tilde{\psi}\rangle = \sum_{i=1}^{s} \gamma_i |\delta_i\rangle \otimes |z_i\rangle,
\]
for some states of the coin $|\delta_i\rangle$. Let $Q_{z_i}$ be any unitary matrix such that:
\[
Q_{z_i} |\delta_i\rangle := \frac{1}{\gamma_i} \sum_{h=g_1 + \cdots + g_{i-1}+1}^{g_1 + \cdots + g_i} \alpha_h |c_h\rangle,
\] (27)
where the $|c_h\rangle$ are the ones defined in (24) and the $\gamma_i$’s are all different from zero because so are the $\alpha_h$’s.

Define a coin tossing operation $C_{k+1}$ as the matrix where, for the nodes $z_i$ we use the previous matrix $Q_{z_i}$, and for the other ones we use an arbitrary $Q$ in $U(d)$, e.g., the identity. We have:
\[
SC_{k+1}(|\tilde{\psi}\rangle) = S \left( \sum_i \gamma_i (Q_{z_i} |\delta_i\rangle \otimes |z_i\rangle) \right)
= S \left( \sum_i \left( \sum_{h=g_1 + \cdots + g_{i-1}+1}^{g_1 + \cdots + g_i} \alpha_h |c_h\rangle \right) \otimes |z_i\rangle \right)
= S \left( \sum_{h=1}^{l} \alpha_h |c_h\rangle \otimes |w_h\rangle \right) = \sum_{h=1}^{l} \alpha_h |c_h\rangle \otimes |\pi_{ih}w_h\rangle = \sum_{h=1}^{l} \alpha_h |c_h\rangle \otimes |v_h\rangle,
\]
as desired. In the last equality, we used (25).

The next proposition shows how to reach a state of the form given by the right hand side of (24), where the $|c_h\rangle$’s are replaced by an arbitrary superposition of coin states.

**Proposition 5.3** Let $j$ be any node, assume that $N^k(j) = \{v_1, \ldots, v_l\}$, and fix any state of the type $|\psi_0\rangle := |c_0\rangle \otimes |j\rangle$, with $|c_0\rangle$ an arbitrary state in $C$. Then in at most $k + r$ steps (where $r$ is the order of the conditional shift matrix $S$), we can reach, from $|\psi_0\rangle$, any state of the type $|\psi_f\rangle := \sum_{h=1}^{l} \sum_{s=1}^{d} \alpha_{hs} |c_s\rangle \otimes |v_h\rangle$ for arbitrary coefficients $\alpha_{hs}$ such that $\sum_{h=1}^{l} \sum_{s=1}^{d} |\alpha_{hs}|^2 = 1$.

**Proof** Define $\beta_h = \sum_{s=1}^{d} |\alpha_{hs}|^2$. We can assume, without loss of generality, that $\beta_h \neq 0$. In fact, if $\beta_h = 0$, then necessarily $\alpha_{hs} = 0$ for all $s = 1, \ldots, d$, and so in...
this case we can just eliminate $|v_h\rangle$ from the sum that defines $|\psi_f\rangle$. From Proposition 5.2 we have a sequence of $k$ coin operations $C_1, \ldots, C_k$ such that

$$SC_k \cdots SC_1 |\psi_0\rangle = \sum_{h=1}^{l} \beta_h |c_h\rangle \otimes |v_h\rangle,$$

for some values of the coin variables $c_h$. Let $Q_{vh}$ be any unitary matrix such that

$$Q_{vh} |c_h\rangle := \frac{1}{\beta_h} \sum_{s=1}^{d} \alpha_{hs} |c_s\rangle.$$

Choose a coin tossing operation $C_{k+1}$ as the matrix where in the nodes $v_h$ we use the previous matrix $Q_{vh}$, and in the other nodes we use an arbitrary $Q$ in $U(d)$. Letting $C_{k+2} = \cdots = C_{k+r} = 1$, we have:

$$SC_{k+r} \cdots SC_1 |\psi_0\rangle = S^r C_{k+1} \left( \sum_{h=1}^{l} \beta_h |c_h\rangle \otimes |v_h\rangle \right)$$

$$= \sum_{h=1}^{l} \beta_h (Q_{vh} |c_{ih}\rangle) \otimes |v_h\rangle = \sum_{h=1}^{l} \sum_{s=1}^{d} \alpha_{hs} |c_s\rangle \otimes |v_h\rangle,$$

as desired. $\square$

**Remark 5.4** In some cases one can choose values $\tilde{C}_1$ and $\tilde{C}_2$ for the coin transformations so that

$$\tilde{C}_2 S \tilde{C}_1 = S^{-1}. \quad (28)$$

In these cases, we can replace $C_{k+1}$ above with $\tilde{C}_1 C_{k+1}$ and $C_{k+2} = 1$ with $\tilde{C}_2$ and omit all the following steps to have $SC_{k+2} \tilde{C}_1 = 1$ in the proof of the above theorem. In these cases, one can replace $r$ with 2 in the statement of the above proposition.

The previous propositions have shown how to go from a state with walker in a single node $j$ to a state where the walker is distributed according to an arbitrary superposition of states $v \in \mathcal{N}^k(j)$. The following proposition shows how to perform the converse type of state transfer.

**Proposition 5.5** Let $j$ be any node, let $\mathcal{N}^k(j) = \{v_1, \ldots, v_l\}$, and fix any state of the form

$$|\psi_0\rangle = \sum_{h=1}^{l} \sum_{s=1}^{d} \alpha_{hs} |c_s\rangle \otimes |v_h\rangle,$$

for arbitrary coefficients $\alpha_{hs}$ such that $\sum_{h=1}^{l} \sum_{s=1}^{d} |\alpha_{hs}|^2 = 1$. Then there exists a sequence of coin operations of length at most $k$ that steers the initial state $|\psi_0\rangle$ to a state of the type $|\psi_f\rangle = \sum_{s=1}^{d} \gamma_s |c_s\rangle \otimes |j\rangle$. 

\(\text{ Springer}\)
Proof As in Proposition 5.2, we will prove the statement by induction on $k$.

If $k = 0$, then the statement is obvious. Assume that the proposition holds for $k$.

Let $\mathcal{N}^{k+1}(j) = \{v_1, \ldots, v_l\} = \{\pi_1(w_1), \ldots, \pi_l(w_l)\}$, where $w_h \in \mathcal{N}^k(j)$. Notice that, for all $h = 1, \ldots, l$, since $\pi_h(w_h) = v_h$, there exists a coin value $c_{j(h)}$ such that $\pi_{j(h)}(v_h) = w_h$. Let

$$\gamma_h := \sqrt{\sum_{s=1}^d |\alpha_{hs}|^2},$$

where $\alpha_{hs}$ are the ones defined in (29). We can assume $\gamma_h \neq 0$, otherwise we can eliminate $|v_h\rangle$ from the sum in equation (29). Let $C_1$ be a coin tossing operation

$$C_1 := \sum_{h=1}^l Q_{v_h} \otimes |v_h\rangle\langle v_h| + Q \otimes \left(1 - \sum_{h=1}^l |v_h\rangle\langle v_h|\right), \quad (30)$$

where $Q$ is an arbitrary unitary on the coin space $C$ and

$$Q_{v_h} \left(\frac{1}{\gamma_h} \sum_{s=1}^d \alpha_{hs} |c_s\rangle\right) = |c_{j(h)}\rangle.$$  

Then we have:

$$SC_1 \left(\sum_{h=1}^l \sum_{s=1}^d \alpha_{hs} |c_s\rangle \otimes |v_h\rangle\right) = S \left(\sum_{h=1}^l \gamma_h |c_{j(h)}\rangle \otimes |v_h\rangle\right) = \sum_{h=1}^l \gamma_h |c_{j(h)}\rangle \otimes |w_h\rangle.$$  

This concludes the inductive step, since the nodes $w_1, \ldots, w_h$ are in $\mathcal{N}^k(j)$. $\square$

The following theorem combines the previous propositions to give an algorithm to transfer between arbitrary states. It also gives an upper bound on the number of steps required for an arbitrary state transfer.

**Theorem 7** If a quantum walk is completely controllable then there exists a node $j$ such that $\mathcal{N}^k(j) = \{0, 1, \ldots, N - 1\}$, for some finite $k$. Denote by $k_j$ the minimum $k$ such that this is possible. In that case the property is true for every $j$. Vice versa if such a $j$ exists, we can transfer between two arbitrary states (state controllability). Assume such a $j$ exists and let $k$ be defined as

$$k := \min_{j \in V} \{k_j | \mathcal{N}^k_j(j) = \{0, 1, \ldots, N - 1\}\}.$$  

Let $r$ be the order of the conditional shift matrix $S$. Then any state transfer can be performed in at most $2k + r$ steps.
Proof The fact that complete controllability implies that there exists a $j$ and a $k$ with $N^k(j) = \{0, 1, \ldots, N - 1\}$ was already proven in Claim C1. We now prove that the existence of such a $j$ implies state controllability. The previous results show how it is possible to go from a state of the form $|\psi_0\rangle := |c_0\rangle \otimes |j\rangle$ to any state of the form (29) where the $v_h$’s are in $N^k(j)$ (Proposition 5.3) and vice versa (Proposition 5.5). If there exists a $j$ such that $N^k(j) = \{0, 1, \ldots, N - 1\}$, then the state in (29) is just an arbitrary state and we can go from an arbitrary state to a state of the form $|\psi_0\rangle = |c_0\rangle \otimes |j\rangle$ in $k$ steps and from this state to an arbitrary state in $k + r$ steps. Therefore every state transfer is possible and it takes at most $2k + r$ steps. This shows state controllability with at most $2k + r$ number of steps. Now $k$ depends on $j$, and we can choose the minimum value $k = k_j$. By choosing $k$ as $k$ in (31), i.e., minimizing over $j \in V$, we have that an arbitrary state transfer can be obtained with at most $2k + r$ steps. ☐

6 Graph theoretic characterization of controllability

Theorem 7 deals with complete controllability and state controllability of a quantum walk. These two controllability notions, in general, are not equivalent [1] as complete controllability implies state controllability but not vice versa. The conditions proved in Theorems 5 and 6, (such as $G_R$ connected) which are equivalent to complete controllability, imply the existence of a $j$ with $N^k(j) = \{0, 1, \ldots, N - 1\}$. However, from Theorem 7 only follows (constructively) that the condition on $N^k(j)$ implies the weaker notion of state controllability. The next result fills this gap and gives a perfect if and only if condition. The theorem also summarizes the controllability criteria obtained so far and adds one more criterion of graph theoretic type (point 4 below).

**Theorem 8** For a quantum walk, with dynamics described by Eqs. (3)–(7), the following conditions are equivalent:
1. The quantum walk is completely controllable.
2. The reduced connectivity graph $G_R$ is connected.
3. The graph $G$ is such that for every couple of vertices $w$ and $s$ in $V$ there exists a path of even length connecting $w$ and $s$.
4. The connected graph $G$ is not a bipartite graph.
5. For every $j \in V$, there exists a $k_j$ such that $N^{k_j}(j) = \{0, 1, \ldots, N - 1\}$.
6. The quantum walk is state controllable.

Proof The equivalence between conditions 1 and 2 was proved in Theorem 6, while the equivalence between conditions 5 and 6 was proved in Theorem 7.

We next prove the equivalence of conditions 2 and 3. Two vertices $r$ and $s$ are connected by an edge in $G_R$ if and only if (21) is verified. Therefore two vertices $w$ and $s$ are in the same connected component of $G_R$ if and only if there exists a sequence of permutations of the form $\pi_l^k \pi_m^{-k}$, with $l, m \in \{1, 2, \ldots, d\}$ and some $k = 0, 1, 2, \ldots$ transferring $w$ to $s$. This is equivalent to the fact that there exists a sequence of permutations of even length transferring $s$ to $w$. To see this, first assume that

$$w = \prod_l \pi_{l_i}^{k_l} \pi_{m_l}^{-k_l} s,$$

(32)
for some $l_t, m_t \in \{1, 2, \ldots, d\}$ and positive integers $k_t$. For any $y \in V$, and any $\pi_m, m \in \{0, 1, \ldots, d\}$, $y$ and $\pi_m^{-1} y$ are connected in the graph $G$. This means that there exists a $\pi_l$ such that $\pi_m^{-1} y = \pi_l y$. Therefore we can replace every permutation with a negative power with a (possibly different) permutation with positive power in (32) and obtain our claim. Vice versa if

$$w = \prod_l \pi_l \pi_m s,$$

(33)

we can replace all the permutations $\pi_m$, with negative powers of permutations and obtain an expression of the form (32). Notice that this also shows that we can restrict ourselves to considering $k_t = 1$ in (32). Since to every permutation $\pi_l, l = \{1, 2, \ldots, d\}$, there corresponds an edge in $G$, this shows the equivalence between 2 and 3.

The equivalence between 3 and 4 is a standard fact in graph theory [9]. We give a proof for completeness. If the graph $G$ is bipartite, divide accordingly the set of vertices $V$ in two disjoint sets $V = V_1 \cup V_2$ such that only edges between elements in $V_1$ and elements in $V_2$ exist. Therefore if $w$ is in $V_1$ and $s$ is in $V_2$ the only paths connecting $w$ and $s$ have an odd number of edges and property 3 is not verified. This proves by contradiction 3 $\Rightarrow$ 4. To prove (again by contradiction) that 4 $\Rightarrow$ 3, assume that 3 is not verified. Introducing an equivalence relation saying that two vertices are equivalent if and only if there exists an even path between them, this partitions the set $V$ in two subsets $V_1$ and $V_2$ which are both non-empty if 3 is not verified. Every edge, being a path of odd length can only connect a vertex in $V_1$ and a vertex in $V_2$ and the graph is bipartite.

We conclude by proving the equivalence of 3 and 5. Assume 3 is verified and fix a $j \in V$. Then for any $w \in V$ there exists a path of even length from $j$ to $w$. Let $2k_w$ be the length of the path, depending on $w$, and let $2k_{\max}$ be the maximum length, maximized over the $w$’s. We can go from $j$ to any $w \in V$ in exactly $2k_{\max}$ steps. We just follow the previously mentioned path for $2k_w$ steps and then ‘oscillate’ back and forth with any neighbor $k_{\max} - k_w$ times. Therefore condition 3 implies that, given $j$, there exists a $k_j = 2k_{\max}$ (even) such that we can reach any vertex in $V$ in exactly $k_j$ steps on the graph. Vice versa, if, given $j$, there exists such a $k_j$ with $N^{k_j} = \{0, 1, \ldots, N - 1\}$, taken any pair $w$ and $s$ in $V$, they are both in $N^{k_j}$. Therefore, we can connect $w$ and $s$ with a path which connects first $w$ to $j$ in $k_j$ steps and then $j$ to $s$ in $k_j$ steps and obtain an even path from $w$ to $s$. This shows that 5 implies 3.

An important consequence of the controllability criterion given in Theorem 8 is that although the quantum walk and the concept of controllability were studied in connection with the defining permutations $\{\pi_1, \ldots, \pi_d\}$, the controllability of the model does not depend on the particular set of permutations $\pi_j$. In fact, we have the following:

**Theorem 9** Controllability of a quantum walk on a graph only depends on the topology of the graph and not on the particular permutations $\{\pi_1, \ldots, \pi_d\}$.

In view of this result, one may in principle use the criteria of Theorems 6 and 8 to investigate purely graph theoretic properties of a graph $G$ by constructing a quantum walk on it.
7 Examples

7.1 Graphs of degree 2

The simplest non-trivial example are quantum walks on cycles, i.e., graph of degree 2. For these examples, the controllability properties for the fully centralized case, i.e., with the coin operation identical for every vertex, were studied in [8] and generalized to lattices in [2]. Let us denote by $|+\rangle$ and $|−\rangle$ an orthonormal basis of the two-dimensional coin space $\mathbb{C}$. Thus the coin tossing operation will be of the form (3) with $Q_j \in U(2)$, and the conditional shift will be of the type:

$$S = \begin{pmatrix} P_+ & 0 \\ 0 & P_- \end{pmatrix}.$$  \hspace{1cm} (34)

Here $P_+$ and $P_-$ are two matrices representing the permutations associated with the two coin values $+$ and $-$, respectively. The possible quantum walks on the cycle are described in the following proposition.

**Proposition 7.1** If $d = 2$ then the matrices $P_+$ and $P_-$ of equations (34) are necessarily of the following form:

(a) $P_+$ is the matrix representing a complete cycle, $\pi_+$ i.e., (after possibly relabeling the vertices) $\pi_+ := (0 \ 1 \ 2 \ \cdots \ N - 1)$ and $P_- = P_+^{-1}$.

(b) $P_+$ and $P_-$ are the matrices representing permutations $\pi_+$ and $\pi_-$, respectively, that are sequences of exchanges of two adjacent symbols, i.e., (after possibly relabeling the vertices) $\pi_+ := (0 \ 1 \ 2 \ \cdots \ N - 2 \ N - 1)$, $\pi_- := (1 \ 2 \ 3 \ 4 \ \cdots \ (N - 3 \ N - 2)) \ (N - 10)$. This case is possible only when $N$ is even.

**Proof** Let $\pi_+$ be the permutation on the nodes given by the matrix $P_+$.

Write $\pi_+$ as a sequence of cycles, $(01 \cdots r_1)(r_1 + 1 \cdots r_1 + r_2) \cdots (r_1 + r_2 + \cdots r_k \cdots N - 1)$, for $k \geq 1$. Since from the assumption H2) (cf. Sect. 2) we do not have self-loops, all cycles must have length $\geq 2$. If all cycles are of length 2, then we have a sequence of $\frac{N}{2}$ exchanges, and we must necessarily have that $N$ is even. Assume now that there exists a cycle of order $p + 1 > 2$, therefore, modulo a possible relabeling of the vertices, we have $\pi_+ = (01 \cdots p)\pi'$.

We need to show that $p = N - 1$. Assume, by the way of contradiction, that $p < N - 1$. Since the permutation $\pi_+$ corresponds to the edges of the graph $G$, all the nodes $\{0, 1, \ldots, p\}$ must have two edges, one connecting $i$ to $i + 1$ and the other connecting $i$ to $i - 1$ (mod $N$). If $p < N - 1$, since $G$ is regular and of degree 2, there cannot be any edge connecting one of the first $p$ nodes with the remaining nodes. This fact contradicts the connectedness assumption on $G$, thus the only possibility is $p = N - 1$.

Now if we are in the case where $\pi_+ = (0 \ 1 \ \cdots \ N - 1)$, then, $\pi_+$ corresponds to motion along every edge in one direction. Necessarily $\pi_-$ will correspond to motion along the edges in the opposite direction, i.e., $\pi_- = \pi_+^{-1}$.
On the other hand, assume that $\pi_+$ is a sequence of exchanges, and let $\pi_-$ be the permutation corresponding to $P_-$. By repeating the same argument as before, we conclude that $\pi_-$ is either a sequence of exchanges or a complete cycle. However the last choice is not possible otherwise the permutation given by $\pi_+$ would have to be its inverse, which is again a complete cycle. By examining the graph, it also follows that if $\pi_+ := (01)(23) \cdots (N-2 N-1)$, then $\pi_- := (12)(34) \cdots (N-3 N-2)(N-1 0)$. 

$$\square$$

As we have seen in Theorem 9, the controllability of the quantum walk does not depend on the particular walk considered but only on the graph. According to the previous proposition, in the case $N$ odd we have only one possible type of quantum walk, while in the case $N$ even, for the same $N$ there may be two non-equivalent walks. However their controllability properties must coincide according to Theorem 9.

Let us treat the case $N$ odd first. Apply Algorithm 1, and compute $\pi_+ \pi_-^{-1}$. We obtain

$$\pi_+ \pi_-^{-1} = \pi_-^2 = (024 \cdot (N-1)13 \cdots N-2),$$

which is a full cycle. Therefore the reduced connectivity graph $G_R$, in this case, is connected and the system is controllable.

Alternatively, we can apply the test of Theorem 7, that is 5 of Theorem 8. In this case, we also get an upper bound on the number of steps needed for controllability. Consider the node 0 and the associated sets $\mathcal{N}^k(0)$. We have that $\mathcal{N}^{N-1}(0) = \{0,1,2,\ldots ,N-1\}$. In order to see this order the nodes of the cycle in clockwise order from 0 to $N-1$. To see that from 0 it is possible to reach in $N-1$ steps any node 0, 2, $\ldots$, $N-1$, notice that for $j = 0, \ldots, \frac{N-1}{2}$, we can reach the node $N-1-2j$ by moving $j$ times between 0 and 1 (so having $2j$ steps) plus performing $N-1-2j$ additional steps clockwise. Analogously, one can see that $\{1,3,\ldots, N-2\}$ are in $\mathcal{N}^{N-1}(0)$. To reach $1+2j$, for $j = 0, 1, \ldots, \frac{N-3}{2}$ in $N-1$ steps, one can move $j$ times between 0 and 1 (and this gives $2j$ steps) and then move counterclockwise with $N-1-2j$ additional steps. It is also easy to see that $N-1$ is the minimum $k$ so that $\mathcal{N}^k(0) = \{0,1,\ldots, N-1\}$ and this minimum value would be the same if we considered another node instead of 0. Therefore $k$ in (31) is $N-1$ and since $r = N$ in this case the upper bound on the number of steps given by Theorem 7 is $2(N-1)+N$. One can in fact get a better bound since in this case the conditions described in Remark 5.4 are verified with

$$\tilde{C}_1 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes 1 \quad \text{and} \quad \tilde{C}_2 = \tilde{C}_1^{-1} := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \otimes 1.$$  

(36)

Extensions of these controllability results can be obtained. For instance, applying Proposition 4.2 one has that $q$-dimensional lattices (with $q \geq 1$) with on odd number of vertices in every dimension necessarily give rise to controllable quantum walks.

For the case $N$ even, consider first the case where the two permutations $\pi_+$ and $\pi_-$ are full cycles. Applying the criterion of Algorithm 1 we study the permutations $\pi_+^k \pi_-^{-k} = \pi_+^{2k}$. We see that for every $k$, $\pi_+^{2k}$ is given by two cycles of length $\frac{N}{2}$ each containing only even or odd numbered vertices. Therefore the reduced connectivity
graph has two connected components each with \( \frac{N}{2} \) vertices and the system is not controllable. The dynamical Lie algebra is the direct sum of two \( su(N) \), plus multiples of the identity, according to Theorem 6. If we apply the criterion of Theorem 7 we find that \( \mathcal{N}^k(0) \) contains only even (odd) numbered nodes for \( k \) even (odd) and this implies that the system is not controllable. In the remaining case, an application of Algorithm 1 gives the same dynamical Lie algebra and using the criterion of Theorem 7 gives the same sets \( \mathcal{N}^k(0) \) (the criterion is independent of the defining permutations and the graph is the same) (Fig. 2).

7.2 Example of the controllability algorithm of Sect. 5

Consider the quantum walk whose graph is given in Fig. 1. The graph has 6 nodes and degree \( d = 3 \). Thus any associate quantum walk has state space of dimension \( 18 = 6 \cdot 3 \).

For this graph, it is easy to see that we have:

\[
\begin{align*}
\mathcal{N}^1(0) &= \{1, 3, 5\}, \\
\mathcal{N}^2(0) &= \{0, 1, 2, 4, 5\}, \\
\mathcal{N}^3(0) &= \{0, 1, 2, 3, 4, 5\}.
\end{align*}
\]

This fact implies that any quantum walk on this graph will be completely controllable. Let us consider the problem to steer the initial state

\[
|\psi_0\rangle = |+\rangle \otimes |0\rangle,
\]

i.e., a state where the probability is concentrated in the 0 node, to a final state \( |\psi_f\rangle \) with the probability uniformly distributed among all the nodes, i.e., \( |\psi_f\rangle \) of the form

\[
|\psi_f\rangle = \frac{1}{\sqrt{6}} \sum_{j=0}^5 |c_j\rangle \otimes |j\rangle
\]

where \( |c_j\rangle \) are general (not necessarily basis) states in \( \mathcal{C} \).
We assume, as described in the picture, that the two coin values \(|+\rangle\) and \(|-\rangle\) correspond to permutations \(\pi_+ = (0\ 1\ 2\ 3\ 4\ 5)\) and \(\pi_- = (0\ 5\ 4\ 3\ 2\ 1)\) while with the third coin value, which will be denoted by \(|c\rangle\), we associate the permutation \(\pi_c = (0\ 3)(1\ 5)(2\ 4)\). We proceed by using the procedure described in Proposition 5.2. First consider \(\mathcal{N}^3(0)\).

\[
\mathcal{N}^3(0) = \{0, 1, 4, 2, 3, 5\} = \{\pi_+(5), \pi_c(5), \pi_-(5), \pi_c(4), \pi_-(4), \pi_+(4)\}.
\]

(39)

Thus, using the notations of Proposition 5.2, here we have \(z_1 = 5\) and \(z_2 = 4\). Notice that this choice is not unique, in fact for example \(1 = \pi_c(5) = \pi_+(0)\). Any possible choice will lead to different sequence of coin tossing operations.

The expression (39) suggests that if we were in a state

\[
|\psi_2\rangle = \frac{1}{\sqrt{2}}|c_4\rangle \otimes |4\rangle + \frac{1}{\sqrt{2}}|c_5\rangle \otimes |5\rangle,
\]

(40)

and applied a coin operation (we denote by \(I_n\) the identity of dimension \(n\))

\[
Q_5 \otimes |5\rangle \langle 5| + Q_4 \otimes |4\rangle \langle 4| + I_3 \otimes (I_6 - |5\rangle \langle 5| - |4\rangle \langle 4|),
\]

(41)

with \(Q_5(Q_4)\) a unitary transformation mapping \(|c_5\rangle\) (\(|c_4\rangle\)) to \(\frac{1}{\sqrt{3}}(|+\rangle + |-\rangle + |c\rangle)\) we would obtain state of the form (38). Therefore the problem is reduced to obtaining a state of the form \(|\psi_2\rangle\) in (40). To do that we examine 4 and 5 in \(\mathcal{N}^2(0)\) and we have 4 = \(\pi_-(5)\) and 5 = \(\pi_c(1)\). This suggests that if we have a state

\[
|\psi_1\rangle := \frac{1}{\sqrt{2}}|d_5\rangle \otimes |5\rangle + \frac{1}{\sqrt{2}}|d_1\rangle \otimes |1\rangle,
\]

(42)

we could transfer to a state of the form (40) by applying a coin transformation depending on the walker which maps \(|d_5\rangle\) into \(|+\rangle\) and \(|d_1\rangle\) into \(|c\rangle\) followed by a conditional shift. Finally, examining 5 and 1 which are in \(\mathcal{N}^1(0)\), we have that 5 = \(\pi_-(0)\) and 1 = \(\pi_+(0)\). Starting from a state \(|\psi_0\rangle\) in (37) and applying a coin transformation mapping \(|+\rangle\) into \(\frac{1}{\sqrt{2}}|-\rangle + \frac{1}{\sqrt{2}}|+\rangle\) followed by a conditional shift \(S\), we obtain the state in (42). The procedure to go from \(|\psi_0\rangle\) to \(|\psi_f\rangle\) applies the above procedure in reverse.

7.3 Controllability for density matrices

If a quantum walk is controllable and in particular state controllable we can apply the algorithm described in Sect. 5 to transfer the state between two values \(|\psi_1\rangle\) and \(|\psi_2\rangle\) in \(\mathcal{C} \otimes \mathcal{W}\). In some applications, the state of the quantum walk is described by a density matrix \(\rho\). Density matrices are Hermitian, trace 1, positive semi-definite matrices of dimension equal to the dimension of the underlying Hilbert space (\(\mathcal{C} \otimes \mathcal{W}\) in this case). They represent the state of an ensemble of quantum systems (cf., e.g., [16]). In this...
case, the algorithm of Sect. 5 cannot be applied, unless \( \rho \) represents a pure state, i.e., \( \rho := |\psi\rangle \langle \psi| \) for some \( |\psi\rangle \in \mathbb{C} \otimes \mathcal{W} \). However since we have complete controllability, for every two density matrices \( \rho_1 \) and \( \rho_2 \) with the same spectrum, we know that it is possible to find a sequence of transformations \( X = \prod_j SC_j \) to transfer, according to \( \rho \to X\rho X^\dagger \), the density matrix \( \rho_1 \) to \( \rho_2 \), i.e., \( \rho_2 = X\rho_1 X^\dagger \). We did not give in this paper a general constructive algorithm for this. We remark however that the situation is a very familiar one in quantum control for which there exist many tools and techniques. The situation can be described as follows. We have a set of matrices \( \mathcal{F} \) in (8)) which generate all of \( \mathfrak{u}(dN) \) and we are able to perform the exponential of each one of these matrices (in this case via a sequence \( \prod_j SC_j \); cf. the proof of Theorem I and Proposition 3.1). Then, given \( X \) in the corresponding Lie group \( (U(dN) \) in this case), we want to find a way to express \( X \) as a product of these exponentials. In our case, this means that we obtain \( X \) by concatenating the various sequences giving the exponentials.

Let us illustrate this using a simple example on a cycle with 3 vertices which, as discussed in Sect. 7.1, is controllable. Assume we want to transfer the density matrix from a value \( \rho_1 = \text{diag}(\frac{1}{2}, 0, 0, \frac{1}{2}, 0, 0) \) to a value \( \rho_2 = \text{diag}(\frac{1}{2}, 0, 0, 0, 0, \frac{1}{2}) \). \( \rho_1 \) represents an ensemble where half of the systems are in \( |+\rangle \otimes |0\rangle \) and half are in \( |-\rangle \otimes |0\rangle \), while \( \rho_2 \) represents an ensemble where half of the systems are in \( |+\rangle \otimes |0\rangle \) and half are in \( |-\rangle \otimes |2\rangle \). A matrix \( X \in U(6) \) which performs such a transfer is a permutation matrix corresponding to the permutation \( \pi := (1)(2)(3 \ 6 \ 4)(5) \) of rows and columns. We need to express such a matrix \( X \) in \( U(6) \) as a sequence \( \prod_j SC_j \). In order to do that, we consider the matrices in \( \mathcal{F} \). A general matrix \( A_1 \) in \( \mathcal{A} \) and a general matrix \( SA_2S^{-1} \), with \( A_2 \in \mathcal{A} \) for this example have the form

\[
A_1 = \begin{pmatrix}
  ia_1 & 0 & 0 & \alpha_1 & 0 & 0 \\
 0 & ia_2 & 0 & 0 & \alpha_2 & 0 \\
 0 & 0 & ia_3 & 0 & 0 & \alpha_3 \\
 -\alpha_1^\dagger & 0 & 0 & ia_4 & 0 & 0 \\
 0 & -\alpha_2^\dagger & 0 & 0 & ia_5 & 0 \\
 0 & 0 & -\alpha_3^\dagger & 0 & 0 & ia_6
\end{pmatrix},
\]

\[
SA_2S^{-1} = \begin{pmatrix}
  ib_1 & 0 & 0 & 0 & \beta_1 & 0 \\
 0 & ib_2 & 0 & 0 & 0 & \beta_2 \\
 0 & 0 & ib_3 & \beta_3 & 0 & 0 \\
 0 & 0 & -\beta_3^\dagger & ib_4 & 0 & 0 \\
 -\beta_1^\dagger & 0 & 0 & 0 & ib_5 & 0 \\
 0 & -\beta_2^\dagger & 0 & 0 & 0 & ib_6
\end{pmatrix},
\]

for arbitrary real numbers \( a_1, \ldots, a_6, b_1, \ldots, b_6 \) and complex numbers \( \alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \). Choosing all elements equal to zero but \( \alpha_3 = \frac{\pi}{2} \) in \( A_1 \) we obtain that \( C_1 = e^{A_1} \) corresponds to a permutation \( \tilde{\pi}_1 := (1)(2)(4)(3 \ 6 \ 5) \). Choosing all entries equal to zero in \( SA_2S^{-1} \) except \( \beta_3 = \frac{\pi}{2} \) we obtain that \( e^{SA_2S^{-1}} = Se^{A_2S^{-1}} = SC_2S^{-1} \) corresponds to a permutation \( \tilde{\pi}_2 := (1)(2)(3 \ 4)(5 \ 6) \). Therefore \( C_1SC_2S^{-1} \) corresponds to the desired permutation \( \tilde{\pi}_1\tilde{\pi}_2 = (1)(2)(3 \ 6 \ 4)(5 \ 6) \). Notice now that
$C_1$ and $C_2$ are available coin tossing transformations. Using $\tilde{C}_1$ and $\tilde{C}_2$ as in Remark 5.4 (cf. (28)) and in (36), we obtain

$$C_1SC_2S^{-1} = S\tilde{C}_2S\tilde{C}_1C_1SC_2\tilde{C}_2S\tilde{C}_1,$$

which is an admissible sequence (of length 4) performing the desired transfer from the density matrix $\rho_1$ to the density matrix $\rho_2$.

The symplectic Lie group $Sp(3)$ would be sufficient to obtain arbitrary transfers between two pure states because of its transitivity on the complex sphere (see, e.g., [1]) but it would not be sufficient to perform the transfer between the two density matrices $\rho_1$ and $\rho_2$ in this example. In order to see this write $\rho_1$ and $\rho_2$ as block diagonal matrices

$$\rho_1 := \frac{1}{2} \begin{pmatrix} E_1 & 0 \\ 0 & E_1 \end{pmatrix}, \quad \rho_2 := \frac{1}{2} \begin{pmatrix} E_1 & 0 \\ 0 & E_3 \end{pmatrix},$$

with $E_j$ the $3 \times 3$ matrix which is all zeros except for the $(j, j)$–th position which is occupied by 1. Using the parametrization of a general element $X$ of the symplectic group as, $X := \begin{pmatrix} A & -\bar{B} \\ B & \bar{A} \end{pmatrix}$, with $A$ and $B$ $3 \times 3$ matrices, a straightforward computation shows that $X\rho_1X^\dagger$ has the form

$$X\rho_1X^\dagger := \begin{pmatrix} K_1 & K_2 \\ K_2^\dagger & \bar{K}_1 \end{pmatrix},$$

which is incompatible with the form of $\rho_2$.

**Acknowledgments**

D. D’Alessandro research was supported by NSF under Grant No. ECCS0824085 and by the ARO MURI grant W911NF-11-1-0268. D. D’Alessandro also acknowledges the kind hospitality by the Institute for Mathematics and its Applications (IMA) in Minneapolis where most of this work was performed. The authors also would like to thank the referees for a careful reading and pointing out a mistake in the previous version of the proof of Theorem 5.

**Appendix A: Further remarks on the structure of the dynamical Lie algebra $\mathcal{L}$**

In this short appendix, we remark that the the number $m$ of connected components of the reduced controllability graph in Theorem 6 can only be 1 or 2. In order to see this, define an equivalence relation $\sim$ on the set of vertices $V$ saying that $a \sim b$ if there exists a path of even length connecting $a$ and $b$. The partition of the set $V$ considered in Theorem 6 corresponds to partition in equivalence classes with respect to this equivalence relation according to the discussion in the proof of Theorem 8. Now, fix a $j \in V$ and consider a set $V_o(j)$ as the set of vertices that can be reached by $j$ in an odd number of steps and a set $V_e(j)$ of vertices that can be reached in an even number of steps. Clearly $V = V_o(j) \cup V_e(j)$. Moreover if $a$ and $b$ are in $V_o(j)$ (or $V_e(j)$), $a \sim b$. Therefore either $V = V_o(j) = V_e(j)$ or $V_o(j)$ and $V_e(j)$ are
disjoint and they give two connected components in the reduced connectivity graph. This discussion shows that the example of the cycle discussed in Sect. 7 is somehow prototypical. It also shows that another equivalent condition of controllability is that given a \( j \in V \) we are able to find a vertex which we can reach in both an odd and an even number of steps.

**References**

1. Albertini F, D’Alessandro D (2003) Notions of controllability for bilinear multilevel quantum systems. IEEE Trans Autom Control 48(8):1399–1403
2. Albertini F, D’Alessandro D (2009) Analysis of quantum walks with time-varying coin on \( d \)-dimensional lattices. J Math Phys 50:122106
3. Ambainis A (2003) Quantum walks and their algorithmic applications. Int J Quantum Inf 1:507–518
4. Ambainis A, Kempe J, Rivosh A (2005) Coins make quantum walks faster. In: Proceedings 16th ACM-SIAM SODA, pp 1099–1108
5. Childs AM (2010) On the relationship between continuous and discrete-time quantum walk. Commun Math Phys 294:581–603
6. D’Alessandro D (2007) Introduction to Quantum Control and Dynamics. CRC-Press, Boca Raton
7. D’Alessandro D (2010) Connection between continuous and discrete time quantum walks; From \( d \) dimensional lattices to general graphs, Reports on Mathematical Physics, vol 66
8. D’Alessandro D, Parlangeli G, Albertini F (2007) Nonstationary quantum walks on the cycle. J Phys A: Math Theor 40:14447–14455
9. Diestel R (2006) Graph Theory. Springer, Berlin
10. Helgason S (1978) Differential Geometry. Lie Groups and Symmetric Spaces. Academic Press, New York
11. Hillery M, Reitzner D, Bužek V (2010) Searching via walking: how to find a marked subgraph of a graph using quantum walks. Phys Rev A 81:062324
12. Kempe J (2003) Quantum random walks—an introductory overview. Contemp Phys 44(4):307–327
13. Kendon V (2006) Decoherence in quantum walks—a review. Math Struct Comput Sci 17(6):1169–1220
14. Mohseni M, Rebertrost P, Lloyd S, Aspuru-Guzik A (2008) Environment-assisted quantum walks in photosynthetic energy transfer. J Chem Phys 129:174106
15. Sagle AA, Walde RE (1973) Introduction to Lie Groups and Lie Algebras. Academic Press, New York
16. Sakurai JJ 1994 Modern Quantum Mechanics. Addison-Wesley Pub Co., Reading
17. Sepanski MR (2007) Compact Lie Groups. Graduate Texts in Mathematics, vol 235. Springer, Berlin
18. Strauch FW (2006) Connecting the discrete and the continuous-time quantum walks. Phys Rev A 74:030301 (R)
19. Tulsi A (2008) Faster quantum walk algorithm for two dimensional spatial search. Phys Rev A 78:012310
20. Turinici G, Rabitz H (2003) Wavefunction controllability for finite-dimensional bilinear quantum systems. J Phys A: Math Gen 36:2565–2576
21. Vlasov AY (2008) Programmable Quantum State Transfer. xxx.lanl.gov/quant-ph/0708.0145
22. Wiesner K (2008) Quantum Cellular Automata. In: Springer Encyclopedia of Complexity and Systems Science, September 18. Also xxx.lanl.gov/quant-ph/0808.0679v1