DYNAMICS AND CONTROL THEORY OF QUANTUM WALKS ON GRAPHS

By

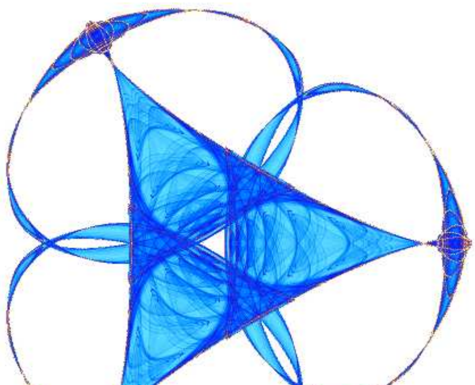
Francesca Albertini

and

Domenico D'Alessandro

IMA Preprint Series # 2324

(June 2010)



INSTITUTE FOR MATHEMATICS AND ITS APPLICATIONS

UNIVERSITY OF MINNESOTA

400 Lind Hall

207 Church Street S.E.

Minneapolis, Minnesota 55455–0436

Phone: 612-624-6066 Fax: 612-626-7370

URL: http://www.ima.umn.edu

Dynamics and Control Theory of Quantum Walks on Graphs

Francesca Albertini[1] Domenico D'Alessandro[2]

[1] *Dipartmento di Matematica Pura e Applicata, Universitá di Padova, Via Trieste 63, 35121 Paodva, Italy.*
e-mail:albertin@math.unipd.it
[2] *Department of Mathematics, Iowa State University*
440 Carver Hall,Ames IA 50011, U.S.A.
e-mail:dmdaless@gmail.com

Abstract. We present a study on the control theory and the dynamics of quantum walks on graphs. A controllability analysis is provided to characterize the set of possible states for such systems using algebraic and graph theoretic methods. Algorithms are described to drive the state of quantum walks in a desired manner. The results of the paper also give a method to obtain the dynamics of a continuous time quantum walk from an appropriate sequence of steps of the discrete time quantum walk and, more generally, to simulate given continuous Hamiltonian dynamics using the evolution of a discrete time quantum walk.

Keywords: Quantum Walks, Control Theory Methods in Quantum Information, Lie Algebras and Lie Groups, Graph Theory.

1 Summary of Results and Their Significance

In recent years, quantum walks have become objects of increasing interest as protocols for quantum algorithms [3], [9] and as models for natural phenomena [11]. A control theory for these models refers to the study of their dynamics and how it can be influenced using external variables. Central to this theory is the study of the *controllability* of these systems, that is, the description of the states the system can achieve. Also central is the *design of control algorithms*, that is, methods to steer the state between two values. In a quantum information context, a quantum algorithm is a way to perform an operation on the quantum state and therefore can be seen as a method of control.

We will consider general discrete time quantum walks on regular graphs, with the model explicitly including a coin degree of freedom giving the direction for a walker to move between the vertices of the graph. More specifically, the quantum system evolves on a Hilbert space $\mathcal{C} \otimes \mathcal{W}$ where the space $\mathcal{C}$, of dimension d, is the Hilbert space for a d-dimensional system called the *coin* and $\mathcal{W}$ of dimension N is the Hilbert space for a system called the *walker*. The associated graph has N vertices (each corresponding to a vector in a basis for $\mathcal{W}$) and has degree d, where elements in a basis of $\mathcal{C}$ indicate the direction for a walker from each vertex. The dynamics of the walk is given, at every step, by the sequence of two operations, C and S: an operation C on the coin space $\mathcal{C}$ referred to as *coin tossing* and an operation S on the walker space $\mathcal{W}$, which changes the state of the walker system according to the state of the coin system and is therefore referred to as a *conditional shift*. In our model, the coin tossing operation C is allowed to change at every step influencing the dynamics of the system and S is constant and is specified by d permutations, P_1,...,P_d, one for each coin result. There are various versions and extensions of this model. Most of the results presented in the paper will concern the case where C is allowed to change with the walker state but many methods and ideas are valid in general.

The first result discussed (**Theorem 1**) concerns the controllability of the model and, in particular, it describes the set of possible evolutions. It is shown that this set is a Lie group $\mathbf{G}$ whose Lie algebra $\mathcal{L}$ can be characterized exactly. In particular, a set of skew-Hermitian matrices is given which generates $\mathcal{L}$. Given an initial state $|\psi_0\rangle \in \mathcal{C} \otimes \mathcal{W}$, the set of states that can be reached from $|\psi_0\rangle$ is then $\{X|\psi_0\rangle \,|\, X \in \mathbf{G}\}$. The description of the reachable states is important for several reasons. Quantum algorithms correspond to transferring the state of a quantum system between two values. For example, in the application to *randomized* algorithms, we would like to drive the state of the walk to a value where the probability of finding the walker in a certain position is the desired one. In an application to *search* algorithms, the desired final state is such that there is certainty (or probability greater than a certain threshold) of finding the walker in the sought for position. The controllability analysis reveals whether or not these state transfers are possible. The knowledge of the Lie algebra $\mathcal{L}$ is also important because $\mathcal{L}$ contains all Hamiltonians on the full space $\mathcal{C} \otimes \mathcal{W}$ whose corresponding evolutions can be simulated with the discrete time quantum walk. The dynamics of the quantum walk consists of *local* (neighbor to neighbor) steps and the knowledge of $\mathcal{L}$ describes the *global* dynamics which can be obtained by combining these local steps.

Theorem 1, as described above, is a fundamental result but it presents some drawbacks. In particular, the calculation of the Lie algebra $\mathcal{L}$ from a generating set of matrices, although in principle always possible (see, e.g., [6]), it may be impractical as it may involve commutators with very large matrices. In fact, we are often interested in studying *classes* of quantum walks on graphs (e.g., on lattices) with the dimension as a parameter. To solve this problem **Theorem 3** gives a combinatorial test to describe the Lie algebra $\mathcal{L}$. The test is as follows: Consider an auxiliary graph with the same vertices as the graph of the walk. Consider the permutations associated with the conditional shift of the walk, $P_1,\ldots,P_d$, and, for every pair $l < m$, the permutations $P_l^k P_m^{-k}$ written in the cycle notation $P_l^k P_m^{-k} = (\cdots)(\cdots)\cdots(\cdots)$, which are in finite number since the permutations P_j have finite order. Connect, in the auxiliary graph, all the vertices that are next to each other in the same cycle in, at least, one instance. The resulting graph will have a certain number s of connected components of cardinality n_1, n_2, $\ldots$, n_s, with $n_1 + n_2 + \cdots + n_s = N$. The Lie algebra $\mathcal{L}$ is the direct sum of s Lie algebras, each isomorphic to $su(dn_j)$ where d is the dimension of the coin space $\mathcal{C}$ plus multiples of the $dN \times dN$ identity matrix. In the special case where the auxiliary graph is connected, i.e., $s = 1$, $\mathcal{L} = u(dN)$ and $\mathbf{G} = U(dN)$ which means that every unitary evolution on the full space $\mathcal{C}\otimes\mathcal{W}$ can be obtained by combining steps of the quantum walk. In this case, the system is called *completely controllable.* There are several important consequences of Theorem 3 and its proof. Among these is the fact that if the degree of the graph d is greater than $\frac{N}{2}$, then complete controllability is always verified. This is in particular always true for complete graphs (with $N > 2$).

In the next part of the paper we will discuss a graph theoretic and constructive approach to determine the controllability of a quantum walk. Considering the graph associated with the walk, we define $\mathcal{N}^k(j)$ as the set of vertices that can be reached from the vertex j in exactly k steps. A theorem (**Theorem 4**) will be stated giving one more characterization of complete controllability based on the sets $\mathcal{N}^k(j)$. In particular, Theorem 4 says that the quantum walk is completely controllable if and only if, given a vertex j, there is a k, with $\mathcal{N}^k(j)$ equal to the full set of vertices of the graph. It is easily seen that if this property holds for one j then it holds for every j. An immediate consequence of Theorem 4 is that complete controllability is a property of the graph only and it does not depend on the permutations $P_1,\ldots,P_d$ defining the walk. In this respect, it is interesting to notice that one could investigate graph theoretic properties using controllability tests and viceversa. In particular, given a graph, one might ask whether there exists a k such that $\mathcal{N}^k(j)$ contains all vertices for some (and therefore all) j. There are several graph theoretic properties that are equivalent to this one including the fact that the graph is not bipartite. An alternative approach to test these graph theoretic properties is to construct a (arbitrary) quantum walk on the graph, and apply the tests of Theorem 3 on the connectedness of an auxiliary graph. In synthesis, these results link the fact that a graph is not bipartite with the fact that an auxiliary graph is connected. Under the conditions of Theorem 4, we also give an explicit control algorithm to drive the state of the discrete time quantum walk between two arbitrary values in $\mathcal{C}\otimes\mathcal{W}$, that is, a sequence of coin tossing operations and conditional shifts accomplishing this task. As a byproduct, we obtain an upper bound on the number of steps needed for an arbitrary state transfer.

The last topic considered in the talk is the *simulation of Hamiltonian evolutions* on the full space $\mathcal{C}\otimes\mathcal{W}$ by a discrete time quantum walk. This means to find evolutions of the discrete-time quantum walk that coincide with a prescribed evolution e^{iHt} on the whole $\mathcal{C}\otimes\mathcal{W}$ Hilbert space. As mentioned above, the set of Hamiltonians for which this is possible is the Lie algebra $\mathcal{L}$ described in Theorem 1, and we shall give a general, constructive way to achieve this simulation. This constructive algorithm also offers an alternative method of control. The problem of simulation of Hamiltonian evolutions includes as a special case the problem of obtaining the dynamics of the continuous time quantum walk from that of a discrete time one on the same graph. A continuous time quantum walk on a graph G is a system which evolves on the walker space $\mathcal{W}$ according to an Hamiltonian $\tilde{H}$ which 'respects' the topology of the graph, i.e., the j,k-th entry of $\tilde{H}$ is different from zero if and only if there is an edge in the graph G between the vertices j and k. If, with a sequence of operations S and C, we are able to obtain an evolution on $\mathcal{C}\otimes\mathcal{W}$ of the form e^{iHt} with $H := \mathbf{1}\otimes\tilde{H}$, where $\mathbf{1}$ is the $d\times d$ identity, then we would have obtained the evolution in parallel of d continuous time quantum walks on the same graph. We note that this is always possible if the discrete time quantum walk is fully controllable in which case the set of admissible Hamiltonians iH is the full Lie algebra $u(dN)$ of $dN \times dN$ skew-Hermitian matrices. The problem of connecting the continuous and discrete time quantum walks has been open for some time and recent progress has been made in [4], [5], [15]. The results presented here provide a link between the two models in that a general method will be described in **Theorem 6** to obtain any evolution e^{iHt} on $\mathcal{C}\otimes\mathcal{W}$ with a sequence of steps of the discrete quantum walk. A count of the worst case number of steps of the discrete walk to obtain a general evolution will be given in that theorem. There is no claim of optimality in this count of steps and we will indicate ways to improve it in various situations. These include in particular specific types of Hamiltonians and specific quantum walks such as walks on lattices and other regular structures.

In summary, this paper will consist of five parts. In the first part, we describe the models to be studied, what a control theory for these models concerns and how this is relevant for quantum information. The remaining four parts of the talk are each centered about one theorem, Theorems 1,3,4 and 6. Theorems 1 and 3 describe the controllability of these systems, in Lie algebraic and combinatorial terms, respectively. Theorem 4 describes the controllability in terms of properties of the graphs underlying discrete time quantum walks and gives control algorithms to drive the state of these systems. Finally Theorem 6 gives a general method to simulate a continuous time evolution with a series of steps of the discrete time quantum walk and an estimate on the number of steps needed.

2 Theorems and Proofs

We provide here technical details for the results above described and include most of the proofs. Additional details and proofs can be found in the forthcoming paper [2]. We emphasize here the part which is not included in that paper, in particular a different treatment of Theorem 3 and the part concerning Theorem 6.

2.1 The Model

Let $G := \{V, E\}$ be a graph, where V denotes the set of vertices of cardinality N and E the set of edges. We assume that G *is a regular graph and we denote by* d *its degree* and assume G *connected and without self-loops.*

We consider two quantum systems: a *walker system* whose state varies in an N-dimensional space $\mathcal{W}$ (the *walker space*) and a *coin system* whose state varies in a d dimensional space $\mathcal{C}$ (the *coin space*). $\{|0\rangle, \ldots, |N-1\rangle\}$, denotes an orthonormal basis of the walker space $\mathcal{W}$ and by $\{|1\rangle, \ldots, |d\rangle\}$ an orthonormal basis of the coin space $\mathcal{C}$. The meaning of the state $|j\rangle$ in the walker space is that, if we measure the position of the walker, we find the position j with certainty. Analogously, the meaning of the state $|l\rangle$ for the coin is that the (d-dimensional) coin is giving the result l which indicates a direction of motion, between neighboring vertices on the graph. With this notation, we define a *coin tossing operation* on $\mathcal{C} \otimes \mathcal{W}$ as an operation of the type

$$C := \sum_{j=0}^{N-1} Q_j \otimes |j\rangle\langle j|, \tag{1}$$

where $Q_j \in U(d)$, that is, it is an element of the Lie group of $d \times d$ unitary matrices $U(d)$. The operation (1) applies to the coin state a unitary evolution Q_j which is allowed to depend on the current walker state j. This may be referred to as a 'decentralized' model as opposed to the 'centralized' case where the coin evolution Q_j does not depend on j, i.e., it is the same for every walker state. In that case

$$C = Q \otimes \mathbf{1}_N, \tag{2}$$

for some unitary operation Q and $\mathbf{1}_N$ is the identity on the walker space $\mathcal{W}$. In between the fully centralized and decentralized cases, one may consider intermediate cases where the coin transformation is allowed to change only for some states. We also define a *conditional shift* as an operator

$$S := \sum_{k=1}^{d} |k\rangle\langle k| \otimes P_k, \tag{3}$$

which applies to a state in $\mathcal{W}$ a permutation P_k depending on the current state of the coin system. In the basis $|k\rangle \otimes |j\rangle := e_{kj}$, $k = 1, \ldots, d$, $j = 0, \ldots, N-1$, of $\mathcal{C} \otimes \mathcal{W}$ S has the matrix representation

$$S = \begin{pmatrix} P_1 & 0 & \cdots & 0 \\ 0 & P_2 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & P_d \end{pmatrix}. \tag{4}$$

The conditional shift S has to be compatible with the graph underlying the walk. This means that for every permutation P_a, $a = 1, \ldots, d$, $P_a|j\rangle = |l\rangle$ implies that there exists an edge in the graph G connecting the vertices j and l. Moreover we will also have that for all $|j\rangle$, $a \neq k$ implies $P_a|j\rangle \neq P_k|j\rangle$, which means that different coin results have to induce different transitions on the graph. This requirement also implies that, if there is an edge in G connecting j and l there must be a permutation P_a such that $P_a|j\rangle = |l\rangle$ and that the sum of the matrix representations of the permutations P_a is the adjacency matrix of the graph. More general versions of the conditional shift S may be considered as, in principle, the only requirement is that for every $k = 1, \ldots, d$, P_k is unitary[1] and $P_k|j\rangle$ is in the subspace spanned by the states $\{|l\rangle \,|\, l \texttt{ is adjacent to } j \texttt{ in } G\}$. We shall continue to consider the case where S is made up of permutations but the issues and results described could be considered for the more general case as well.

Summarizing, the actions of the coin tossing operation and conditional shift on the vector space $\mathcal{C} \otimes \mathcal{W}$ are given, in the basis $e_{ij} = |i > \otimes |j > i = 1, \ldots, d$, and $j = 0, \ldots, N-1$, by

$$Ce_{ij} = (Q_j|i\rangle) \otimes |j\rangle,$$

$$Se_{ij} = |i\rangle \otimes (P_i|j\rangle).$$

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

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

The probability of finding the walker in position j, p_j, is found by tracing out the coin degrees of freedom, that is, $p_j = \sum_{k=1}^{d} |\alpha_{kj}|^2$.

The dynamics of the quantum walk is defined 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 (1). This leads to a point of view where the operations Q_j in (1) are seen as *control variables* in the evolution of the system.[2]

The study of **controllability** of a system and, in particular, a discrete time quantum walk (DTQW), refers to a description of the set of states a system can be in. The evolution of a closed quantum system is of the form $|\psi\rangle \rightarrow X|\psi\rangle$ with X unitary. The system is called *completely controllable* if every unitary evolution X is possible. The system is called *state controllable* if for every two states $|\psi_1\rangle$ and $|\psi_2\rangle$ there exists an admissible evolution X transferring $|\psi_1\rangle$ to $|\psi_2\rangle$, that is, $|\psi_2\rangle = X|\psi_1\rangle$. Complete controllability implies state controllability but the converse is in general not true [1].

[1] More general quantum operations could also be considered in the context of open systems. See e.g., [10] for a review of quantum walks in the context of open systems.

[2] The possibility of changing the coin operation at every step is motivated by current proposals for the implementation of quantum walks (cf. [7]). In principle, one may also consider a model where the conditional shift S is allowed to change at every time step.

2.2 Lie algebraic characterization of controllability: Theorem 1

The set of possible evolutions of the quantum walk on $\mathcal{C} \otimes \mathcal{W}$, which we denote by $\mathcal{E}$, is the set of all the unitary transformations that can be obtained as sequences of transformations of the form SC, where S is a conditional shift (3) and C a coin tossing operation (1).

Theorem 1 below gives a Lie algebraic characterization of the set $\mathcal{E}$. We consider for simplicity of exposition the fully decentralized model of (1) but only minor modifications are needed for the other cases.

Recall that S being a permutation matrix has a certain order r, such that S^r is the identity on $\mathcal{C} \otimes \mathcal{W}$. Define the set of matrices

$$\mathcal{F} := \{\mathcal{A}, S\mathcal{A}S^{r-1}, \ldots, S^{r-1}\mathcal{A}S\}, \tag{5}$$

where $\mathcal{A}$ is the set 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 $\mathcal{A}$ is a Lie algebra, which is, in fact, the direct sum of N $u(d)$'s.[3] 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. Denote by $\mathbf{G}$ the Lie group generated by $e^{\mathcal{L}}$ and $\{S\}$. We have the following result.

Theorem 1 *Let:*

1. $\mathbf{G}$ *be the Lie group generated by* $e^{\mathcal{L}}$ *and* $\{S\}$.
2. $\mathbf{K}$ *be the set defined as:*

$$\mathbf{K} := e^{\mathcal{L}} \cup e^{\mathcal{L}}S \cup e^{\mathcal{L}}S^2 \cup \cdots \cup e^{\mathcal{L}}S^{r-1} \tag{6}$$

where $e^{\mathcal{L}}S^j$ *is the set of all matrices* XS^j *with* $X \in e^{\mathcal{L}}$.[4]

3. *If* p *is the smallest integer* $1 \leq p \leq r$ *such that* $S^p \in e^{\mathcal{L}}$, *let* $\mathbf{C}$ *be the set defined as the disjoint union of* $e^{\mathcal{L}}$, $e^{\mathcal{L}}S$, ..., $e^{\mathcal{L}}S^{p-1}$.[5]

Then $\mathbf{G} = \mathbf{K} = \mathbf{C} = \mathcal{E}$.

Proof. We first prove $\mathbf{G} = \mathbf{K} = \mathbf{C}$. It follows from the definitions that $\mathbf{K} \subseteq \mathbf{G}$, $\mathbf{C} \subseteq \mathbf{G}$ and $\mathbf{C} \subseteq \mathbf{K}$. The claim follows if we show that $\mathbf{G} \subseteq \mathbf{K}$ and $\mathbf{K} \subseteq \mathbf{C}$. An element in $\mathbf{G}$ is a product $\prod_{k=0}^{m} Y_k$, with Y_0 equal to the identity, where $Y_k \in e^{\mathcal{L}}$ or $Y_k = S$, for $k \geq 1$. By induction on m, if $m = 0$, this product is the identity which is in $e^{\mathcal{L}}$ and therefore in $\mathbf{K}$. If $m > 0$, write $\prod_{k=0}^{m} Y_k$ as $Y \prod_{k=0}^{m-1} Y_k$, with $\prod_{k=0}^{m-1} Y_k \in \mathbf{K}$, i.e., $\prod_{k=0}^{m-1} Y_k = XS^j$ for some $0 \leq j \leq r-1$ and $X \in e^{\mathcal{L}}$. Now, if $Y \in e^{\mathcal{L}}$, then $YXS^j \in e^{\mathcal{L}}S^j \subseteq \mathbf{K}$. If $Y = S$ then $SXS^j = SXS^{r-1}S^1S^j$ and since $X \in e^{\mathcal{L}}$ implies $Z := SXS^{r-1} \in e^{\mathcal{L}}$, we have $YXS^j = ZS^{j+1} \in \mathbf{K}$. To see that $\mathbf{K} \subseteq \mathbf{C}$, we need to consider only XS^k with $k > p-1$. Choose n so that $0 \leq k - np \bmod r < p$. We have $XS^k = XS^{np}S^{k-np} := YS^j$ with $Y = XS^{np} \in e^{\mathcal{L}}$ and $j := k - np \bmod r$ and this is in $\mathbf{C}$.

We now prove that $\mathbf{G} = \mathcal{E}$. $\mathcal{E}$ is the set of products of transformations of the form SC with C a coin tossing operation and S a conditional shift. Since $C \in e^{\mathcal{L}} \subseteq \mathbf{G}$ and $S \in \mathbf{G}$ then $SC \in \mathbf{G}$ and therefore $\mathcal{E} \subseteq \mathbf{G}$. Viceversa, consider the characterization of $\mathbf{G}$ as $\mathbf{K}$ given above and consider an element $XS^j \in \mathbf{K}$, for some $0 \leq j \leq r-1$. Since $X \in e^{\mathcal{L}}$, it can be written as the product of matrices of the form $S^k e^A S^{r-k}$ with A a matrix of the form $A = \sum_{l=0}^{N-1} A_l \otimes |l\rangle\langle l|$ and $A_l \in u(d)$. e^A is a coin operation C, and therefore, we can write $S^k e^A S^{r-k}$ as $S^k C S^{r-k}$ and we can obtain it by performing $r-k$ steps with coin operation 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 $X \in e^{\mathcal{L}}$. 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 $\mathbf{G} \subseteq \mathcal{E}$ and concludes the proof of the theorem.

□

It follows from Theorem 1 that the Lie algebra $\mathcal{L}$ generated by the set $\mathcal{F}$ in (5) is the main object of interest when we want to describe the set of possible evolutions for a DTQW. Following common terminology in quantum control we shall refer to this Lie algebra as the *dynamical Lie algebra*. Calculation of $\mathcal{L}$ starting from the generating set $\mathcal{F}$ is always possible [6] but becomes cumbersome when dealing with high dimensional systems. This motivates the analysis in the following section.

2.3 Combinatorial characterization of controllability: Theorem 3

We study now more closely the matrices in $\mathcal{F}$ (5) (and $\mathcal{L}$) in the basis $e_{ij} := |i> \otimes |j>$, $i = 1, \ldots, d$, and $j = 0, \ldots, N-1$. With some abuse of notation, we shall indicate with the same symbol a matrix and the operator it represents in this basis. Given a matrix $S^k\tilde{C}S^{-k}$[6] in $\mathcal{F}$, for fixed k, we calculate

$$S^k\tilde{C}S^{-k} = \left(\sum_{l=1}^{d} |l\rangle\langle l| \otimes P_l^k\right) \times \tag{7}$$

[3] The direct sum of two or more Lie algebras is the sum in the sense of vector spaces with the additional requirement that every element in a Lie algebra commutes with any element in another Lie algebra. We refer to any introductory book on Lie algebras and Lie groups (see e.g., [8], [12], [14]) for basic notions of Lie theory. The book [6] presents introductory notions with a view to applications to quantum systems.

[4] Notice that this set is the same as the set of all matrices S^jY with $Y \in e^{\mathcal{L}}$. We can write XS^j as $S^jS^{r-j}XS^j$ and $S^{r-j}XS^j \in e^{\mathcal{L}}$ if $X \in e^{\mathcal{L}}$ and the claim follows by defining $Y := S^{r-j}XS^j$.

[5] To see that this is a disjoint union, notice that if there exists two different indices $0 \leq k < j \leq p-1$ and two elements in $e^{\mathcal{L}}$, X and Y such that $XS^j = YS^k$, we would have $S^{j-k} \in e^{\mathcal{L}}$ which contradicts the minimality of p.

[6] $\tilde{C}$ represents a matrix in the Lie algebra $\mathcal{A}$ defined in (5) and we use the notation $\tilde{C} := \sum_{j=0}^{N-1} \tilde{Q}_j \otimes |j\rangle\langle j|$, with $\tilde{Q}_j \in u(d)$, $j = 0, 1, \ldots, N-1$.

$$\left(\sum_{j=0}^{N-1}\tilde{Q}_j\otimes|j\rangle\langle j|\right)\left(\sum_{m=1}^{d}|m\rangle\langle m|\otimes P_m^{-k}\right)=$$
$$\sum_{\substack{l,m=1,\ldots,d\\ j=0,\ldots,N-1}}|l\rangle\langle l|\tilde{Q}_j|m\rangle\langle m|\otimes P_l^k|j\rangle\langle j|P_m^{-k}.$$

After defining

$$x_{jlm}:=\langle l|\tilde{Q}_j|m\rangle, \tag{8}$$

we can write

$$S^k\tilde{C}S^{-k}=\sum_{\substack{l,m=1,\ldots,d\\ j=0,\ldots,N-1}}x_{jlm}|l\rangle\langle m|\otimes P_l^k|j\rangle\langle j|P_m^{-k}. \tag{9}$$

This expression tells that, in the $N\times N$ block determined by l and m, ($l,m\in\{1,2,\ldots,d\}$), the only non zero entries are the ones corresponding to walker indices w and s such that there exists a $j=0,1,\ldots,N-1$ with $w=P_l^kj$ and $s=P_m^kj$. This means that the elements (w,s) which are possibly different from zero are such that $w=P_l^kP_m^{-k}s$, or, equivalently, they correspond to the entries which are different from zero in $P_l^kP_m^{-k}$. From (8) these entries can be chosen by changing the skew-Hermitian matrices $\tilde{Q}_j$ and one has the requirement that $S^k\tilde{C}S^{-k}$ is skew-Hermitian. That is, x_{jlm} is the (l,m)-th entry of the skew-Hermitian matrix $\tilde{Q}_j$ and one has $x^*_{jlm}=-x_{jml}$. Summarizing, the matrices $S^k\tilde{C}S^{r-k}$ in $\mathcal{F}$ are made up of $d\times d$ blocks each of dimension $N\times N$. The (l,m)-th block contains all zeros except for the entries corresponding to the nonzero entries of the permutation $P_l^kP_m^{-k}$. The (w,s) entry is equal to $x_{jlm}:=\langle l|\tilde{Q}_j|m\rangle$ where j is given by $j=P_l^{-k}w=P_m^{-k}s$. For fixed l,m x_{jlm} is allowed to depend on j according to the model we consider. They are all equal in the centralized case and they may be all different in the decentralized case and they are in general grouped in different sets where they are supposed to be same. In the following we will exclusively consider the fully decentralized case where the x_{jlm} are arbitrary except for the requirement that the whole matrix is skew-Hermitian. However extensions to other cases are possible.

Following Theorem 1, we now want to study the Lie algebra $\mathcal{L}$ generated by the elements in $\mathcal{F}$. If this Lie algebra is the full $u(dN)$ then every unitary evolution can be obtained from the evolution of the DTQW. In this case the system is *completely controllable*. To carry out this study, we first prove a general lemma below on the Lie algebra generated by a certain set. Our treatment here, leading to Theorem 3 below, differs from the one in [2] where Theorem 3 was obtained using a result in [16]. There are several advantages including a more self-contained treatment and a constructive method to obtain any unitary transformations on the full space $\mathcal{C}\otimes\mathcal{W}$ as we shall explore further in section 2.5. We first digress to study a general situation.

Consider an undirected graph $\tilde{G}$ with n vertices, $1,2,\ldots,n$, and an associated set of skew-Hermitian $n\times n$ matrices $\tilde{\mathcal{F}}$ which consists of arbitrary diagonal matrices and arbitrary skew-Hermitian matrices which have zeros everywhere except possibly in the (j,k)-th (and therefore $(k,j)-$th) entries corresponding to the edges in the graph $\tilde{G}$ connecting the vertices j and k. We have the following lemma.

Lemma 2 *The Lie algebra $\tilde{\mathcal{L}}$ generated by $\tilde{\mathcal{F}}$ is the direct sum*[7] *$su(n_1)\oplus su(n_2)\oplus\cdots\oplus su(n_g)\oplus$ **span**$\{i\mathbf{1}_n\}$, where g is the number of connected components of the graph $\tilde{G}$, and n_j is the number of vertices in the j-th component, and $n_1+n_2+\cdots+n_g=n$. In particular if $\tilde{G}$ is connected, then $\tilde{\mathcal{L}}=u(n)$.*

The proof uses recursively the **AIII** Cartan decomposition (cf., e.g., [8]) of $u(m)$ and the corresponding Lie group $U(m)$. Every $m\times m$ unitary matrix $X\in U(m)$ can be written as

$$X=KAK, \tag{10}$$

where K represents a general block diagonal matrix

$$K:=\begin{pmatrix}K_{1,1} & 0\\ 0 & K_{2,2},\end{pmatrix} \tag{11}$$

with $K_{1,1}$ and $K_{2,2}$ of dimensions $p\times p$ and $q\times q$, $p+q=m$ and (without loss of generality) $p\geq q$.[8] A is the exponential of a matrix $\tilde{A}$ having the form

$$\tilde{A}=\begin{pmatrix}\mathbf{0}_p & D\\ -D^T & \mathbf{0}_q,\end{pmatrix} \tag{12}$$

where D is $p\times q$ and it has the form

$$D:=\begin{pmatrix}0&\cdots&0&0&0\\ \cdots&\cdots&\cdots&\cdots&\cdots\\ 0&\cdots&0&0&0\\ 0&\cdots&0&0&a_q\\ 0&\cdots&0&a_{q-1}&0\\ \cdots&\cdots&\cdots&\cdots&\cdots\\ \cdots&\cdots&\cdots&\cdots&\cdots\\ \cdots&\cdots&\cdots&\cdots&\cdots\\ a_1&0&\cdots&0&0\end{pmatrix} \tag{13}$$

with the a_j's $j=1\ldots p$ real arbitrary.[9] Moreover, let us consider a matrix of the form $\tilde{A}$ in (12), with D in (13) with all the a_j's equal to 0 except a_k. Let us denote a general matrix of this form by $\tilde{A}_k$. One can obtain from $\tilde{A}_1$, performing a similarity transformation $\tilde{A}_1\rightarrow K\tilde{A}_1K^\dagger$, with K in (11) any other matrix of the form $\tilde{A}_k$. Combining this with the fact that all matrices of the form $\tilde{A}_k$ commute with each other, using (10), one obtains that every matrix $X\in U(m)$ can be written in the form

$$X=Ke^{\tilde{A}_1}Ke^{\tilde{A}_1}K\cdots Ke^{\tilde{A}_1}K, \tag{14}$$

[7] $su(n)$ is the Lie algebra of skew-Hermitian matrices with trace equal to zero. The corresponding Lie group $SU(n)$ is the *special unitary group* of unitary matrices with determinant equal to 1.

[8] This last requirement is just for notational convenience in what follows.

[9] Other forms can be considered for the matrices $\tilde{A}$ whose exponential will work in (10). The only needed feature is that $\tilde{A}$ is a general linear combination of q mutually commuting, linearly independent matrices with zero diagonal blocks.

where $e^{\tilde{A}_1}$ is the exponential of a matrix of the form $\tilde{A}_1$ and the exponentials appear q times. The proof of Lemma 2 uses this decomposition recursively for $m = 2$, $m = 3$, etc. always with $q = 1$. We have discussed the general case because it may be used in alternative and more efficient constructions (cf. Remark 1 below). We now give the proof of Lemma 2

Proof. (Proof of Lemma 2) Assume without loss of generality that the vertices of $\tilde{G}$ are ordered so that the first n_1 vertices belong to the first connected component of $\tilde{G}$, the next n_2 vertices to the second connected component of $\tilde{G}$, and so on. In the corresponding basis, the matrices in $\tilde{\mathcal{F}}$ have a block diagonal structure with g, $n_j \times n_j$ blocks on the main diagonal. This structure is preserved upon commutation and linear combination and therefore $\tilde{\mathcal{L}} \subseteq su(n_1) \oplus su(n_2) \oplus \cdots \oplus su(n_g) \oplus \texttt{span}\{i\mathbf{1}_n\}$. To prove that equality holds we prove equivalently that the Lie group corresponding to $su(n_1) \oplus su(n_2) \oplus \cdots \oplus su(n_g) \oplus \texttt{span}\{i\mathbf{1}_n\}$ is a subset of the Lie group corresponding to $\tilde{\mathcal{L}}$. In other terms, every element of the Lie group corresponding to $su(n_1) \oplus su(n_2) \oplus \cdots \oplus su(n_g) \oplus \texttt{span}\{i\mathbf{1}_n\}$ can be obtained, by combining in products, exponentials of matrices in $\tilde{\mathcal{F}}$. The Lie group of $su(n_1) \oplus su(n_2) \oplus \cdots \oplus su(n_g) \oplus \texttt{span}\{i\mathbf{1}_n\}$ consists, in the given basis, of block diagonal arbitrary unitary matrices with g blocks of dimensions $n_1 \times n_1$, $n_2 \times n_2$ etc. We can without loss of generality assume $g = 1$ for notational convenience. In the case $g > 1$, one just apply the procedure we are going to describe g times, once for each block.

Consider again the graph $\tilde{G}$ which is now assumed to be connected. Consider a path on $\tilde{G}$ which includes all the nodes and assume, without loss of generality, that the labels on the path are in the natural order. We use recursively the **AIII** Cartan decomposition above described to obtain a general matrix in $U(n)$. Consider the first two nodes in the path. Applying the decomposition (10) with $p = q = 1$ and $m = 2$ we obtain all $n \times n$ unitary matrices which are the identity everywhere except for the upper left corner which is an arbitrary 2×2, unitary matrix. Every matrix in the factorization (10) can be obtained as an exponential of elements in $\tilde{\mathcal{F}}$, the K matrices because they are diagonal in this case (and every diagonal skew-Hermitian matrix belongs to $\tilde{\mathcal{F}}$) and the matrix A, which is the exponential of a matrix having all zeros except in the position $(1, 2)$. This type of matrices also belong to $\tilde{\mathcal{F}}$ because 1 and 2 are connected in the graph $\tilde{G}$. Therefore every unitary matrix which is the identity everywhere except in the upper left 2×2 corner belongs to the Lie group corresponding to $\tilde{\mathcal{L}}$. In the next step of the procedure we apply Cartan **AIII** decomposition again with $p = 2$, $q = 1$, and $m = 3$, to obtain arbitrary 3×3 unitary matrices in the upper left corner. In this case, the matrices K in (10) can be obtained by multiplying a matrix obtained in the previous step with e matrix which is the exponential of a matrix equal to all zeros except in the $(3, 3)$ entry, which also belongs to $\tilde{\mathcal{F}}$. The matrix A is the exponential of a matrix which contains only zeros except in the position $(2, 3)$ and these matrices are in $\tilde{\mathcal{F}}$ because 2 and 3 are connected in the graph $\tilde{G}$. Applying this procedure $n - 1$ times we obtain that it is possible to have an arbitrary full $n \times n$ unitary matrix by taking products of matrices in $\tilde{\mathcal{F}}$. This concludes the proof of the Lemma.

□

Remark 1 *Assume for simplicity that $\tilde{G}$ is connected in the above lemma. The procedure described in the proof gives a method to construct an arbitrary unitary matrix using products of exponentials of the matrices in $\tilde{\mathcal{F}}$. A count of the worst case number of exponentials in the final product gives that it is $O(2^n)$. To see this, denote by d_j the number of exponentials needed at the $j-$th step. Consider the first step when $m = 2$. This needs three factors two diagonal ones (in the K matrices) and the one used in the A matrix. So we set $d_1 = 3$. At the j-th step we need 2 times d_{j-1} factors along with two diagonal matrices to construct the matrices K. However, by an inductive argument the K matrix obtained in the previous step has a diagonal as an 'external' factor so the diagonal factors can be included in the diagonal used in the previous steps. To this one has to add the factor giving the A matrix. Therefore the number of factors needed at the $j-$th step is $d_j = 2d_{j-1} + 1$ which gives that the number of factors is $O(2^n)$. An alternative, more efficient procedure, can be obtained by combining the steps achieving the various blocks. Assume that $n = 2^f$. At the first step one can obtain 2^{f-1} blocks of 2×2 arbitrary unitary matrix on the diagonal with 3 factors (like in (10)). Set $d_1 = 3$. In general at step j one obtains 2^{f-j}, $2^j \times 2^j$ blocks. The number of factors used, d_j, can be obtained inductively. From formula (14), there are 2^{j-1} factors $e^{\tilde{A}_1}$ and $2^{j-1} + 1$ factors K each requiring d_{j-1} elementary factors (i.e., exponentials of matrices in $\tilde{\mathcal{F}}$). Therefore*

$$d_j = (2^{j-1} + 1)d_{j-1} + 2^{j-1}. \tag{15}$$

Considering only the leading term we have that

$$d_f = O(2^{(f-1)+(f-2)+\cdots+1}) = O(2^{\frac{f(f-1)}{2}}), \tag{16}$$

which in terms of n becomes $O(\frac{n^{\log\sqrt{n}}}{\sqrt{n}})$. This growth is sub-exponential in n. In particular, it is easily seen that $\frac{n^{\log\sqrt{n}}}{\sqrt{n}}$ grows slower than 2^n.

We now combine the discussion on the form of the matrices $S^k \tilde{C} S^{-k}$ in $\mathcal{F}$ with the above general Lemma 2 to give the proof of the following Theorem 3.

Theorem 3 *Consider a DTQW with a decentralized model. Consider a graph G_a with N vertices, each corresponding to a vertex, of the graph G of the quantum walk. Write the permutations $P_l^k P_m^{-k}$, $l < m$, $l, m = 1, \ldots, d$, $k = 0, 1, 2, \ldots$ in cycle notation $P_l^k P_m^{-k} = (\cdots)(\cdots)\cdots(\cdots)$, which are in finite number since the permutations P_j have finite order. Connect two vertices in the graph G_a if the corresponding vertices are adjacent in one of the cycles corresponding to the above permutations. Let G_a have $\tilde{g}$ connected components each with a number N_j of vertices, with $N_1 + N_2 + \cdots + N_{\tilde{g}} = N$.*

Then the dynamical Lie algebra $\mathcal{L}$ is the direct sum $su(dN_1) \oplus su(dN_2) \oplus \cdots \oplus su(dN_{\tilde{g}}) \oplus \mathtt{span}\{i\mathbf{1}_{dN}\}$. In particular if the graph G_a is connected, i.e., $\tilde{g} = 1$ the quantum walk is completely controllable, i.e., $\mathcal{L} = u(dN)$ and every unitary evolution on the space $\mathcal{C} \otimes \mathcal{W}$ can be obtained as an evolution of the DTQW.

Proof. The dynamical Lie algebra $\mathcal{L}$ is generated by the set of $dN \times dN$ matrices $\mathcal{F}$. To apply Lemma 2 with $n = dN$ we denote the row and column indexes of these matrices by pairs (l, a) where $l = 1, 2, \ldots, d$ denotes the coin state and $a = 0, 1, \ldots, N-1$ denotes the walker state. In the associated graph, $\tilde{G}$ as in Lemma 2 (l, a) and (m, b) are connected if and only if there exists a k such that $a = P_l^k P_m^{-k} b$. In particular, (l, a) and (m, a) are always connected for every l and m and for every a (choose $k = 0$). Therefore the graph $\tilde{G}$ is made up of N connected sets of vertices of cardinality d, $\mathcal{S}_a := \{(l, a) \,|\, l = 1, 2, \ldots, d\}$ as a varies in $\{0, 1, \ldots, N-1\}$. Moreover, a set $\mathcal{S}_a$ is connected to a set $\mathcal{S}_b$ if and only if a and b are connected in the graph G_a. From this, applying Lemma 2, the theorem follows.

□

As an example of application of Theorem 3 consider a quantum walk on a cycle with vertices $0, 1, \ldots, N-1$ and two permutations: P_1 which moves the walk forward $\mathtt{mod}\, N$, i.e., in cycle notation, $P_1 = (012 \cdots N-1)$ and $P_2 = P_1^{-1}$, which moves the walk backwards. If N is odd we have $P_1 P_2^{-1} = P_1^2 = (0\,2\,4 \cdots N-1\,1\,3 \cdots N-2)$ and therefore all vertices in the auxiliary graph G_a are connected and the walk is completely controllable, i.e., $\mathcal{L} = u(2N)$. If N is even, for every k, $P_1^k P_2^{-k} = P_1^{2k}$ consists of two cycles, one containing only odd vertices and one containing only even vertices. Therefore $\mathcal{L} = su(2\frac{N}{2}) \otimes su(2\frac{N}{2}) \oplus \mathtt{span}\{i\mathbf{1}_N\}$.

Theorem 3 gives a test of controllability that can be easily applied and does not require the calculation of commutators of large matrices involved in the determination of a Lie algebra generated by a given set. Moreover, it can be used to study *classes* of quantum walks as discussed in the previous example. There are also some general interesting consequences of this theorem. For example, consider a DTQW with a graph G. *If the degree d of G is greater than $\frac{N}{2}$ then the corresponding quantum walk is always controllable.* To see this consider the permutations $P_1 P_2^{-1}$, $P_1 P_3^{-1}$,..., $P_1 P_d^{-1}$, applied to 1. If $l \neq m$ then $P_1 P_l^{-1} 1 \neq P_1 P_m^{-1} 1$ because this would imply that there exists a node w and two different permutations P_l and P_m such that $P_l w = P_m w$ which we have excluded in our model (different coin results induce different transitions). Therefore in the graph G_a considered in Theorem 3 1 is connected to $d-1$ different nodes. Repeating the same reasoning starting from the node 2 we find that 2 is connected to $d-1$ different vertices. The connected component containing 1 and 2 must have an element in common since $d > \frac{N}{2}$. Continuing this way one finds that all nodes must belong to the same connected component of the graph G_a and therefore we have controllability. This result in particular concerns complete graphs (with $N > 2$).

2.4 Graph theoretic and constructive characterization of controllability: Theorem 4

In the previous section, we partitioned V the set of vertices of the graph G into subsets and divided the dynamical Lie algebra $\mathcal{L}$ into a certain number of subalgebras each one corresponding to one of these subsets. In particular, if there is only one set, the Lie algebra is the full Lie algebra $u(dN)$ and the system is completely controllable. We now look more closely at the graph theoretic meaning of the partition of V and also give a constructive algorithm for control in Theorem 4 below.

We first notice that two vertices w and s are in the same subset (i.e., in the same connected component of the auxiliary graph G_a in Theorem 3) if and only if there exists a sequence of permutations of the form $P_l^k P_m^{-k}$, 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

$$w = \prod_j P_{l_j}^{k_j} P_{m_j}^{-k_j} s. \tag{17}$$

For any $y \in V$ and any P_m, y and $P_m^{-1} y$ are connected in the graph G. This means that there exists a P_l such that $P_m^{-1} y = P_l y$. Therefore we can replace every permutation with a negative power with a (possibly different) permutation with positive power in (17) and obtain our claim. Viceversa if

$$w = \prod_t P_{l_t} P_{m_t} s, \tag{18}$$

we can replace all the permutations P_{m_j} with negative powers of permutations and obtain an expression of the form (17). Notice that this also shows that we can restrict ourselves to considering $k_j = 1$ in using (17) and partitioning the set V. In view of these considerations controllability is verified if and only for any two nodes w and s there exists a sequence of permutations of even length mapping s in w. Equivalently, since to every permutation there corresponds an edge, and viceversa, controllability is verified if and only if for every pair w and s there exists a path of *even length* connecting w and s.[10] Now assume that this is the case and fix a $j \in V$. Then for any $w \in V$ there exists a sequence of even length mapping j to w. Let $2k_w$ be this length depending on w and let $2k_{max}$ 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 path with the given permutations for $2k_w$ steps and then 'oscillate' back and forth with any neighbor $k_{max} - k_w$ times. Therefore controllability implies that, given j, there exists a $k = k(j)$ (even) such that we can reach any vertex in V in exactly $k(j)$ steps on the graph (i.e., with a sequence of permutations of length $k(j)$). Viceversa assume that, given j, there

[10] The length of a path is the number of edges connecting the two vertices. Edges can be crossed in both directions and are counted as many time they are crossed.

exists a $k(j)$ such that for any w there exists a sequence of length k $P_{l_1} \cdots P_{l_k}$ mapping j to w. We have for w and s, from $w = P_{l_1} \cdots P_{l_k} j$, $s = P_{m_1} \cdots P_{m_k} j$

$$w = P_{l_1} \cdots P_{l_k} P_{m_k}^{-1} \cdots P_{m_1}^{-1} s. \tag{19}$$

Using the above argument to replace negative powers with positive ones, we can map any s to any w with a sequence of even length of permutations and the system is controllable.

To formulate this new condition of controllability we use the sets $\mathcal{N}^k(j)$ defined as follows. Fix a node $j \in \{0, \ldots, N-1\}$, let: $\mathcal{N}^0(j) := \{j\}$, $\mathcal{N}^{k+1}(j) := \{P_s(l) \,|\, l \in \mathcal{N}^k(j),\ 1 \leq s \leq d\}$, that is, $\mathcal{N}^k(j)$ is the set of nodes that can be reached from j in k steps.

Theorem 4 *Consider the fully decentralized model. Consider a node j of the graph G associated with the DTQW. The walk is controllable if and only if there exists a $k := k(j)$ such that $\mathcal{N}^k(j) = \{0, 1, \ldots, N-1\}$.*

Corollary 5 *Controllability of a DTQW does not depend on the choice of the permutations defining the walk but only on the underlying graph.*

Remark 2 *As discussed at the end of section 2.1 state controllability [1] [13] refers to the possibility of transferring between two arbitrary states while complete controllability refers to the situation where one can achieve any arbitrary unitary (or special unitary) evolution. The two notions are in general not equivalent. Complete controllability implies state controllability but the converse may not be true [1]. In our discussion above we have dealt with complete controllability. However, one consequence of Theorem 4 is that complete controllability is equivalent to state controllability for DTQW's. In fact assume that we have state controllability. Choose a node $j \in \{0, \ldots, N-1\}$ and consider a state $|\psi_0\rangle$ with probability* 1 *to find the walker in this position. Thus $|\psi_0\rangle$ is of the form $|\psi_0\rangle = |c\rangle \otimes |j\rangle$, for some state $|c\rangle \in \mathcal{C}$. From state controllability we have that there exists a sequence of coin tossing operations and conditional shifts of length k such that*

$$SC_k \cdots SC_1 |\psi_0\rangle = \sum_{s=0}^{N-1} \sum_{l=1}^{d} \alpha_{ls} |l\rangle \otimes |s\rangle.$$

for arbitrary α_{ls} and in particular for $\alpha_{ls} \neq 0$ for every s for at least some l. Since all s's in the above expression must be in $\mathcal{N}^k(j)$ we must have that $\mathcal{N}^k(j) = V := \{0, 1, \ldots, N-1\}$ and therefore we have complete controllability.

Remark 3 *The above analysis leading to Theorem 4 also gives more information on the structure of the dynamical Lie algebra $\mathcal{L}$. We have in Theorem 3 that the graph G_a has at most* 2 *connected components, that is $\tilde{g}$ is either 1 (controllable case) or* 2 *(not controllable case). 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 3 and 4 corresponds to a partition in equivalence classes with respect to this equivalence relation. 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 $V = V_o(j) \bigcup V_e(j)$. 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 of the graph G_a. The case where $V_o(j)$ and $V_e(j)$ are disjoint corresponds to the situation where the original graph G is* bipartite.[11] *In particular there is no edge in G connecting elements of $V_o(j)$ (or $V_e(j)$). If there was then one could go from j to an element of $V_o(j)$ ($V_e(j)$) in both an even and odd number of steps. Viceversa, if the graph G is bipartite and one fixes j, it is easily seen that the component of the graph containing j is $V_e(j)$ while the other component is $V_o(j)$ and they are disjoint. This discussion shows that the example of the cycle with an even or odd number of nodes discussed after Theorem 3 is somehow prototypical. It also shows that another equivalent condition of controllability is that the graph G is not a bipartite graph.*

The above theorem, corollary and remarks link the property of controllability to graph theoretic properties of the underlying graph G (bipartite-ness) and the latter to graph theoretic properties of the auxiliary graph G_a (connected-ness). In principle, one could study graph theoretic properties of G by constructing a quantum walk on it and checking connectedness of the auxiliary graph G_a. Given a regular graph G of degree d to construct a DTQW on G, one has to choose d permutations P_1,...,P_d which satisfy the constraints discussed in subsection 2.1.

In the rest of this subsection we assume controllability and discuss how to transfer between two arbitrary states, i.e., how to find a sequence of coin tossing transformations and conditional shifts to transfer between two arbitrary states. We give the general idea, discuss an example and refer to [2] for a formal treatment.

Assume controllability, then a node j exists and a k, $k = k(j)$, such that $\mathcal{N}^k(j) = V$. In fact this is true for every j. There are three steps in the procedure. First one shows how to go from a state $|c\rangle \otimes |j\rangle$ to a state of the form $\sum_{h=0}^{N-1} \alpha_h |c_h\rangle \otimes |h\rangle$ in k steps, for some appropriate states $|c_h\rangle$ in $\mathcal{C}$. Then one shows how, in at most r steps, one can transform a state $\sum_{h=0}^{N-1} \alpha_h |c_h\rangle \otimes |h\rangle$ into a general state $\sum_{h=0}^{N-1} \sum_{l=1}^{d} \alpha_{hl} |l\rangle \otimes |h\rangle$ and finally one shows how to go from this general state back to a state of the form $|c\rangle \otimes |j\rangle$ in $k(j)$ steps. Therefore the general procedure to transfer between two general states is to transfer first to a state $|c\rangle \otimes |j\rangle$ in $k(j)$ steps and then to the desired general state in $k(j)+r$ steps. This accounts for a number of steps $2k(j) + r$. As we can minimize over j, we obtain the bound $2\mathbf{k} + r$, where $\mathbf{k} := \min_j k(j)$. We include hereafter an example to illustrate the main ideas in the first step above. Ideas in the other steps are similar.

Example 1 *Consider the quantum walk whose graph is*

[11] The authors are grateful to Dr. Ryan Martin for helpful discussions on this point.

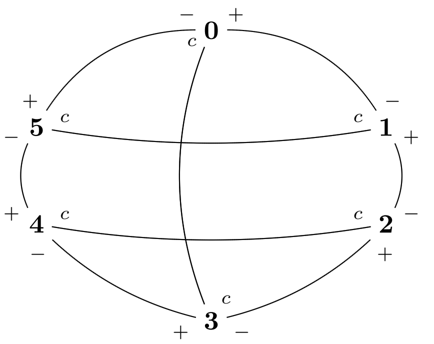


Figure 1: Graph with $N = 6$ and $d = 3$

given in Figure 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:

$$\begin{array}{rcl} \mathcal{N}^1(0) & = & \{1,\ 3,\ 5\}, \\ \mathcal{N}^2(0) & = & \{0,\ 1,\ 2,\ 4,\ 5\}, \\ \mathcal{N}^3(0) & = & \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}. \end{array}$$

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

$$|\psi_0\rangle = |+\rangle \otimes |0\rangle, \tag{20}$$

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*

$$|\psi_f\rangle = \frac{1}{\sqrt{6}} \sum_{j=0}^{5} |c_j\rangle \otimes |j\rangle \tag{21}$$

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* $P_+ = (012345)$ *and* $P_- = (054321)$ *while with the third coin value, which will be denoted by* $|c\rangle$*, we associate the permutation* $P_c = (03)(15)(24)$*. First consider* $\mathcal{N}^3(0)$.

$$\mathcal{N}^3(0) = \{0,\ 1,\ 4,\ 2,\ 3,\ 5\} =$$

$$= \{P_+(5), P_c(5), P_-(5), P_c(4), P_-(4), P_+(4)\}.$$

The expression suggests that if we were in a state

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}|c_4\rangle \otimes |4\rangle + \frac{1}{\sqrt{2}}|c_5\rangle \otimes |5\rangle, \tag{22}$$

and applied a coin operation

$$Q_5 \otimes |5\rangle\langle 5| + Q_4 \otimes |4\rangle\langle 4| + \mathbf{1}_3 \otimes (\mathbf{1}_6 - |5\rangle\langle 5| - |4\rangle\langle 4|), \tag{23}$$

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 (21). Therefore the problem is reduced to obtain a state of the form* $|\psi_2\rangle$ *in (22). To do that we examine* 4 *and* 5 *in* $\mathcal{N}^2(0)$ *and we have* $4 = P_-(5)$ *and* $5 = P_c(1)$*. This suggests that if we have a state*

$$|\psi_1\rangle := \frac{1}{\sqrt{2}}|d_5\rangle \otimes |5\rangle + \frac{1}{\sqrt{2}}|d_1\rangle \otimes |1\rangle, \tag{24}$$

we could transfer to a state of the form (22) by applying a coin transformation depending on the walker which maps $|d_5\rangle$ *to* $|+\rangle$ *and* $|d_1\rangle$ *to* $|c\rangle$ *followed by a conditional shift. Finally, examining* 5 *and* 1 *which are in* $\mathcal{N}^1(0)$*, we have that* $5 = P_-(0)$ *and* $1 = P_+(0)$*. Starting from a state* ψ_0 *in (20) and applying a coin transformation mapping* $|+\rangle$ *to* $\frac{1}{\sqrt{2}}|-\rangle + \frac{1}{\sqrt{2}}|+\rangle$ *followed by a conditional shift* S*, we obtain the state in (24). The procedure to go from* $|\psi_0\rangle$ *to* $|\psi_f\rangle$ *applies the above procedure in reverse.*

2.5 Simulation of continuous time dynamics by discrete time quantum walks

The last result of this paper, Theorem 6 below, and its improvements discussed thereafter, deal with simulating continuous time dynamics on $\mathcal{C} \otimes \mathcal{W}$ using the DTQW. Given a Hamiltonian H on $\mathcal{C} \otimes \mathcal{W}$ we want to find a sequence of steps of the DTQW $\{SC_k\}$ such that $\prod_k SC_k = e^{iHt}$, for some t. We consider the problem of *exact* simulation although one may consider the problem of approximate simulation as well, where the equality holds up to a certain tolerance. It is clear that this problem is strongly related to the controllability analysis above described in that one can find a sequence of steps $\{SC_k\}$ if and only if $iH \in \mathcal{L}$.[12] A special case of this problem is that of simulation of the dynamics of a continuous quantum walk on the same graph. Assume that $\tilde{H}$ is a Hamiltonian on $\mathcal{W}$ corresponding to a continuous time quantum walk, which means that $\tilde{H}_{jk} \neq 0$ if and only if there exists an edge connecting the vertices j and k in the graph. Then, if $i\mathbf{1}_d \otimes \tilde{H} \in \mathcal{L}$ we can obtain the dynamics $e^{i\mathbf{1}_d \otimes \tilde{H}t} = \mathbf{1}_d \otimes e^{i\tilde{H}t}$ on $\mathcal{C} \otimes \mathcal{W}$ from which we can obtain the dynamics $e^{i\tilde{H}t}$ on $\mathcal{W}$. For a general $iH \in \mathcal{L}$, the questions to be addressed are: how to do this constructively in practice and how many steps of the DTQW are needed to simulate a given Hamiltonian. Lemma 2 in the special case of quantum walks already gives a method to construct this simulating sequence and therefore to obtain an estimate on the number of steps needed in general. We always assume that we have a decentralized model so that we can change the coin operation not only with time but also depending on the walker position. Let us assume for simplicity that we are in the controllable case so that $\mathcal{L} = u(dN)$ and therefore every unitary evolution can be obtained as an evolution of the DTQW. An auxiliary graph $\tilde{G}$ can be associated with the system. The vertices in $\tilde{G}$ are given by pairs (l, j) with $l = 1, 2, \ldots, d$ denoting a coin result and $j = 0, 1, \ldots, N-1$ denoting a walker position. Because of the controllability assumption $\tilde{G}$ is connected. Following Lemma 2, we choose a path on $\tilde{G}$

[12]This assertion needs some some more technical explanations. In the general case, the Lie algebra $\mathcal{L}$ is always the direct sum of an Abelian subalgebra and a semisimple one in the Lie algebra $u(n)$. This implies that for the corresponding Lie group, the exponential map is always surjective. In other terms for every element X of the Lie group there exists an $iH \in \mathcal{L}$ such that $e^{iH} = X$.

which includes all the dN vertices. If (l,a) and (m,b) are connected, then there exists a matrix $F \in \mathcal{F}$ in (5) which is all zeros except in the $(l,a)-(m,b)$ position which can be arbitrarily chosen. It also exists an arbitrary diagonal matrix in $\mathcal{F}$.[13]. The number of steps needed to implement the exponential of every matrix in $\mathcal{F}$ can be easily shown to be bounded by r where r is the order of the matrix S as a permutation matrix. Following the procedure of Lemma 2 (cf. Remark 1) one obtains a first rough but general estimate on the number of steps needed to simulate an arbitrary Hamiltonian evolution on $\mathcal{C} \otimes \mathcal{W}$ and in particular an evolution corresponding to the continuous time quantum walk.

Theorem 6 *Assume a decentralized model and assume controllability. Any unitary evolution on* $\mathcal{C} \otimes \mathcal{W}$*,* e^{iHt}*, for a Hamiltonian* H *can be obtained with a number of steps* $O(2^{dN} r)$*, where* d *is the degree of the graph,* N *is the number of vertices and* r *is the degree of* S *as a permutation matrix.*

The procedure to obtain e^{iHt} can be described more in detail as follows (cf. Lemma 2). Given a path on the graph $\tilde{G}$, one first performs a permutation P on the rows and columns of e^{iHt} so as the first column and row correspond to the first vertex in the path in $\tilde{G}$, the second column and row correspond to the second vertex in the path in $\tilde{G}$ and so on. Then the next step is to decompose $X = Pe^{iHt}P^T$ recursively using the **AIII** Cartan decompositions as described before Lemma 2. Starting with X, the procedure to factorize it goes in reverse with respect to what is discussed in the lemma. One first applies the Cartan decomposition (10) with $q=1$ and $p = dN-1$. There are standard simple computational techniques to find the factors KAK in (10) starting from the matrix X (cf., e.g., [6] Section 5.2). Then one factorizes each of the left upper corner of the K factors by applying again the **AIII** Cartan decomposition (10), this time with $p = dN-2$ and $q=1$ and so on. At the end of the procedure one obtains a factorization of X in elements that are either diagonal or are exponentials of matrices of the form $\tilde{A}$ in (12) coupling nearby vertices in the chosen path. Both diagonal matrices and coupling matrices $\tilde{A}$ belong to $\mathcal{F}$ and therefore their exponentials can be obtained with at most r steps of the DTQW.

The above procedure and the estimate on the number of steps of the DTQW to simulate a continuous dynamics will be sharpened in future research. Different ways of recursively applying the **AIII** Cartan decomposition, such as the one described in Remark 1, reduce the number of steps to sub-exponential in dN. Moreover the procedure above described does not take into account the fact that, in the graph $\tilde{G}$, nodes of the form (l,a), for fixed $a \in \{0,1,\ldots,N-1\}$ and varying $l \in \{1,2,\ldots,d\}$, are always connected. More structure to be used in the problem might come from the particular quantum walk at hand or from the particular Hamiltonian to be simulated. This is the case for example, if the Hamiltonian is of the form $\mathbf{1}_d \otimes \tilde{H}$ corresponding to a continuous time quantum walk on the same graph. Several results can be obtained by applying the ideas described here on a case by case basis. Overall the methods described here provide tools to link, in a quantitative fashion, the dynamics of continuous and discrete time quantum walks.

[13] It is of the form $\sum_{j=0}^{N-1} Q_j \otimes |j\rangle\langle j|$, with the Q_j's $\in u(d)$.

ACKNOWLEDGEMENT: D. D'Alessandro research was supported by NSF under Grant No. ECCS0824085. D. D'Alessandro also acknowledges the kind hospitality by the Institute for Mathematics and its Applications (IMA) in Minneapolis where this work was performed.

References

[1] F. Albertini and D. D'Alessandro, Notions of controllability for bilinear multilevel quantum systems, *IEEE Transactions on Automatic Control*, 48, No. 8, 1399-1403 (2003).

[2] F. Albertini and D. D'Alessandro, Controllability of quantum walks on graph, xxx.arXiv/quant-ph/submit/0057501

[3] A. Ambainis, Quantum walks and their algorithmic applications, *International. Journal of Quantum Information*, **1**, 507?518, (2003).

[4] A. M. Childs, On the relationship between continuous and discrete-time quantum walk, *Communications in Mathematical Physics* 294, 581?603 (2010)

[5] D. D'Alessandro, Connection Between Continuous and Discrete Time Quantum Walks; From *d*-Dimensional Lattices to General Graphs, to appear in *Reports on Mathematical Physics.*

[6] D. D'Alessandro, *Introduction to Quantum Control and Dynamics*, CRC-Press, Boca Raton FL, 2007.

[7] W. Dür, R. Raussendorf, V. M. Kendon, and H.-J. Briegel, Quantum random walks in optical lattices, *Phys. Rev. A,* 66:052319, 2002.

[8] S. Helgason, *Differential geometry, Lie groups and symmetric spaces*, Academic Press, New York, 1978.

[9] J. Kempe, Quantum random walks - an introductory overview, *Contemporary Physics,* Vol. 44 (4), p. 307-327, 2003.

[10] V. Kendon, Decoherence in quantum walks - a review, *Math. Struct. in Comp. Sci* 17(6) pp 1169-1220 (2006).

[11] M. Mohseni, P. Rebentrost, S. Lloyd and A. Aspuru-Guzik, Environment-assisted quantum walks in photosynthetic energy transfer, *Journal of Chemical Physics* 129, 174106 (2008).

[12] A. A. Sagle and R. E. Walde, *Introduction to Lie Groups and Lie Algebras*, Academic Press, New York, 1973.

[13] S. G. Schirmer, J. V. Leahy and A. I. Solomon, Degrees of controllability for quantum systems and applications to atomic systems, *J. Phys. A*, 35, 4125-4141, (2002).

[14] M.R. Sepanski, Compact Lie Groups, Graduate Texts in Mathematics, Vol. 235, Springer 2007.

[15] F.W. Strauch, Connecting the discrete and the continuous-time quantum walks, Phys. Rev. A 74, 030301 (R) (2006).

[16] G. Turinici and H. Rabitz, Wavefunction controllability for finite-dimensional bilinear quantum systems, *J. Phys. A: Math. Gen.*, 36, 2565-2576, (2003).