UNIVERSITY OF UDINE
hic sunt futura

Department of
Mathematics, Computer Science and Physics

ALPEN-ADRIA UNIVERSITÄT
KLAGENFURT | WIEN | GRAZ

Department of
Artificial Intelligence and Cybersecurity

MASTER THESIS IN
ARTIFICIAL INTELLIGENCE & CYBERSECURITY

Graph encoding in Quantum Computing

CANDIDATE
Alex Della Schiava

SUPERVISOR
Prof. Carla Piazza

CO-SUPERVISORS
Prof. Elisabeth Oswald
Dott. Riccardo Romanello

Academic Year 2021-2022

Institute Contacts
Dipartimento di Scienze Matematiche, Informatiche e Fisiche
Università degli Studi di Udine
Via delle Scienze, 206
33100 Udine — Italia
+39 0432 558400
https://www.dmif.uniud.it/

To Maurizio A. Catagni, M.D.,
a man that gave my life a chance when only few would.

Acknowledgements

In harshest times, my family organizes into two distinct categories of people: the ones who believe in me the most (my parents), the ones who do the least (me). I am glad I can count on them to put together the pieces, on the days in which I show up completely broken. Their unconditioned support is something I often take for granted. Sure enough, they will doubt my initiatives; arguments, even, may arise. However, a path is chosen, I may rest assured: they will be there backing me up.

These last two years have been an amazing journey. It would have not been the same without the companions who contributed in making it so pleasant. Among them are: Alan, Alex, Alice, Andrea, Dalila, Donald, Elide, Fabio, Loris, Massimiliano, Samuel. The list could well keep going.

I am grateful to each and every professor I have crossed paths with during my time at both the Università degli Studi di Udine and the Alpen-Adria-Universität Klagenfurt. The sense of joy that I get from studying Computer Science is something that was passed on to me by them.

In addition, some individual mentions are due. I thank Riccardo Romanello for the help and support he selflessly provided during my work on this thesis. I hope the interesting conversations we had during these months are only the first of a long series.

Then, I thank prof. Martin Gebser. I have had the luck to first approach research work under his supervision. I doubt I could have wished for a better experience. His contagious passion and enthusiasm made working with him extremely fun. At the end of our meetings, I would usually wish they could last five minutes more. I am thankful to him and the entire PROSYS research group for the warm hospitality they reserved me.

Last but not least, I thank prof. Carla Piazza. Apart from being my thesis supervisor, she has been a guiding figure throughout my studies. Prof. Piazza never hesitated to assist me even on matters concerning my academic future. My favourite subjects just so happen to be those she first introduced me to. I argue this is only partly a coincidence. Much of the merit lies on her engaging way of teaching, which fueled my own wish to become a professor. If I will ever become one that is only half as good as her, I may consider myself proud of my achievement.

Abstract

Quantum walks have become a fundamental tool in the field of Quantum Computing. Differently from classical random walks, the class of graphs over which quantum walks may be performed is severely restricted by the condition of *unitarity.*

After reviewing the general construction of quantum walks, this thesis investigates their limits, exploring the properties that characterize the directed graphs over which they may be performed. The analysis is also conducted with respect to *coined quantum walks,* a generalization of quantum walks. In this regard, the underlying graph of a coined quantum walk on a *regular graph* is known to be the *line graph* [16]. This thesis proposes a version of the result that is extended to the case of *regular multigraphs.* In turn, this allows to determine the underlying graph of coined quantum walks on *reversible graphs with self-loops* as constructed in [12].

In light of the rigid conditions that regulate quantum walks, the thesis proceeds to study techniques to circumvent them. These take shape into encoding procedures that edit general connected graphs into ones that are amenable to quantum walks. More specifically, the thesis is concerned with two *edge-addition* based procedures: encoding to *Eulerian graphs*, encoding to regular multigraphs.

Thus, the thesis extends the discussion to the notion of *encoding bias.* Through addition and duplication of edges, the aforementioned encoding procedures appear to affect the resulting quantum walks with local bias. Due to their nature, these local phenomena are here referred to as encoding bias. It is shown that there exists no *unitary remedy* to encoding bias, implying that any solution to the problem relies on the adopted encoding procedure. Finally, it is given proof that, for any *strongly connected,* irregular, Eulerian graph, the encoding procedure to regular multigraphs inevitably leads to encoding bias.

Contents

List of Figures

1

Introduction

In 1982, Richard Feynman was among the first to pose the question: *"Can classical computers efficiently simulate quantum phenomena?"* [8]. With the answer being *"generally not",* this would turn out to be only the first step towards a plethora of discoveries. In fact, Feynman himself would hint to a hypothetical computing device able to, ideally, meet the requirements of the question; one that would rely on the laws of Quantum Mechanics. David Deutsch would then proceed to refine the idea into what is known today as a *"quantum computer"* [6].

Through his contribution, however, David Deutsch did more than just formalize an esoteric model of computation. In arguing the existence of a *Universal Quantum Computer* he challenged the deeper meaning of computation itself. Prior to this proposal, the definition of computation would be tied to the classical *Church-Turing thesis:*

> *Any algorithmic process can be computed on a Turing machine.*

Because a Turing machine is an abstract device based on a set of logical operations, it follows that computation is a *logical process.* Via the same line of reasoning, claiming that any computable function may be performed by a device based on the laws of physics - as Deutsch's Universal Quantum Computer - would imply that computation is, instead, a *physical process.*

Perhaps on a less philosophical note, the study of quantum computers has abruptly entered the scene of various subfields in Computer Science. To some extent, this was justified by their inherent promise: providing a model of computation that would be more efficient than the classical one.

Early results would seemingly honour the promise, as for instance did Deutsch-Jozsa algorithm in showing that $QP \neq P$, that is, *there are problems that are efficiently solvable by quantum computers but not by classical ones* [7]. Other, equally remarkable results would, instead, have to wrestle with the notion of *efficiency* itself. One such example would be Shor's quantum algorithm for *integer factorization* [19]. Strikingly, Shor's work had provided a polynomial time solution with *bounded probability of error* to a problem which, classically, may only be solved in exponential time. However, the apparently proven *quantum speed-up* is, to this day, questioned by the unlikely yet possible existence of a polynomial time, classical algorithm. Nonetheless, Shor's algorithm remains noteworthy in that it efficiently solves a problem of major importance in the field of Cybersecurity. Integer factorization is, in fact, a crucial building block of several cryptosystems - such as *RSA* -, which rely on the absence of an efficient classical

- exact or probabilistic - algorithm to solve it.

These two examples perfectly summarize two of the main questions Quantum Computing has been dealing with during the last three decades.

Problem 1. *Are quantum computers* always *more efficient than classical ones?*

And, in the case where Problem 1 has negative answer,

Problem 2. *What are the problems that are characterized by* quantum advantage?

In hope to shed light on this matter, part of the efforts in Quantum Computing has been channelled into a *"hunt for the quantum algorithm":* a search for problems that would lend themselves to quantum speed-up. However, as the previous paragraph might have hinted already, the path towards a distinguished result is a strenuous one. To begin with, devising any correct quantum algorithm is no easy endeavour, as it requires aware manipulation of the principles of Quantum Mechanics, a subject known to challenge common intuition. Furthermore, for the algorithm to be relevant, it should provide a speed-up that is at least polynomial with respect to its best classical counterpart. Finally, the quantum algorithm developer should be mindful that, unless a lower bound prevents it, the classical solution to a problem may undergo improvements. Were these improvements to repeal the quantum speed-up, the relevance of her contribution would be deeply affected.

With that in mind, how does one design a quantum algorithm ticking all these boxes? As it is the case for classical algorithms, there exists no blueprint for efficiency. Typically, such pursuit involves ingenious manipulation of *quantum systems.* One that, upon *measurement* of the systems, leads *with high probability* to a solution of the problem at hand. In addition to that, several quantum algorithms employ subroutines characterized by quantum speed-up. Shor's algorithm is one such example, as it exploits the exponential advantage of quantum computers in performing the *Discrete Fourier Transform.*

Upon closer inspection, the given overview on quantum algorithms spontaneously links the subject to the branch of *randomized algorithms;* more specifically, due to the probabilistic nature of *quantum measurement.* In spite of this resemblance, it should be noted that probabilistic computers still suffer the comparison with their quantum counterparts, as witnesses the absence of any efficient probabilistic algorithm *with bounded error* to solve integer factorization. Nonetheless, elements from probabilistic computation have come in handy in Quantum Computing, the leading example arguably being *quantum walks.*

In devising randomized algorithms, an abstract tool that is often relied upon is that of *random walks.* A random walk is intended to be performed on a *graph* that somewhat encodes a considered problem. Each vertex of the graph should represent a state of the problem. Two states are connected by an edge if and only if, given a specified random action, there is a probability different from zero to transition from one state to the other. A random walk, then, simply consists of a finite sequence of steps over the states of the graph according to the given probabilities.

Quantum walks are the quantum mechanical counterpart of random walks. A *"quantum walker"* moves analogously to a classical one, albeit, with two key differences: (i) she may lie in a *superposition* of states; (ii) her steps are guided by *probability amplitudes.* Probability amplitudes differ from classical probabilities in that they are complex numbers. Although seemingly subtle, this peculiar property leads

to a behaviour that is strikingly different from that of random walks. Even more remarkably, this action significantly affects the time required by the walk to spread across the graph. Indeed, it has been shown that, for specific graphs, quantum walks spread faster than random walks [1, 2, 14]. The important consequence of these results is that, given any of these graphs, a quantum walk-based algorithm will outperform a random walk-based one. Hence, despite there not being any formula for efficient quantum algorithms, quantum walks seem to provide something curiously similar: a general method to prove quantum speed-up among walk-based algorithms. Interestingly, these observations lead to a weaker restatement of Problem 2.

Problem 3. *Over which graphs do quantum walks spread faster than random walks?*

The question owes its importance to the broad range of applications of quantum walks. Growing interest also concerns the employment of quantum walks in the area of Artificial Intelligence; for instance, in graph classification tasks [11]. With that being said, it should be clarified that quantum walks have been widely adopted well before their use in algorithmics. Quantum walks have been a fundamental tool in physics, where they have been employed to analyze the evolution of quantum systems. The quantum walker is meant to represent the quantum system under consideration and, as such, obeys the laws of Quantum Mechanics. Indeed, conditions (i) and (ii) given above are but a coarse summary of these laws. In reality, Quantum Mechanics are much stricter in that they assert that evolution of quantum systems be *unitary*. Quantum walks are impaired by unitarity in that it restricts the class of graphs over which they may be performed. This last observation leads to the central problem treated in this manuscript.

Problem 4. *Over which graphs can quantum walks be performed?*

Problem 4 asks for elucidations on the relationship between graphs and quantum computation. Graphs often emerge as the ideal data structure to encode relevant problems in Computer Science; partly for this reason, their theory is well-developed. Therefore, answers to Problem 4 could extend Graph Theory as a means to better understand Quantum Computing. Benefits would also flow in the opposite direction, as Graph Theory could be enriched with groundbreaking results (*e.g.* algorithms, graph representations, ...) relying on the quantum model of computation.

In this regard, the literature already provides partial answers to Problem 4. Childs exhaustively settled one way of the relationship, proving quantum walks to be a *universal model of computation* [4]. That is, *any quantum algorithm may be expressed as a quantum walk - i.e.,* a graph.

On the other hand, results concerning the opposite direction do not appear as satisfactory. Indeed, graphs have been shown to be amenable to quantum walks only under certain assumptions. Furthermore, the resulting quantum walk is often performed on a graph that only resembles the topology of the original. Investigations on this matter often involve thorough analyses of the *adjacency matrices* for such graphs. In particular, with focus on the relationships that these maintain with *unitary matrices*, that is, matrices that allow to encode discrete-time unitary evolution in matrix theoretical terms.

A recurrent notion throughout this manuscript is that of *"graph of a unitary matrix"*. These graphs are tightly related to unitary matrices, and constitute what could arguably be understood as the purest kind of quantum walk amenable graphs. In that respect, Severini has brought remarkable contributions.

In [18], he has shown that, given a *Eulerian* graph - or a disjoint union of Eulerian components -, its *line graph* is that of a unitary matrix. More specifically, the result is an immediate consequence of the fact that *specular, strongly quadrangular* graphs are graphs of unitary matrices.

Severini has also explored the opposite direction of the relationship, demonstrating that a graph of a unitary matrix is *bridgeless*, *inseparable* and contains no *directed bridges* [17].

Tackling Problem 4 from a different perspective, Montanaro has proved *reversibility* to be both a sufficient and necessary condition for *coined quantum walks* to be performed on a graph [12].[1] Coined quantum walks are a generalization of quantum walks, which implicitly encode graphs that normally would not allow quantum walks into ones that do. As for the case of regular graphs, Severini has made the image of such implicit encoding precise, showing that the line graph is the underlies the constructed coined quantum walk [16].

In light of these results, the class of graphs allowing quantum walks appears to be artificially extendable. In what appears a more liberal approach to Problem 4, one may creatively transform a graph so that a quantum walk may be performed on it. Obviously the editing procedure should not alter the topology of the graph too drastically, as the entire work would then lose its purpose. The observation leads to the final problem concerning this manuscript.

Problem 5. *How can one "non-invasively" encode graphs into ones that are amenable to quantum walks?*

In this regard, the literature does provide answers. In [5], Della Giustina et al. propose an encoding procedure based on the results from Severini. On the reasonable assumption that the graph be *connected*, they provide an optimal algorithmic solution that encodes the graph into a Eulerian one and, thus, proceeds in defining a suitable quantum walk on its line graph. Because the *"encoding to Eulerian"* does, in general, impact invasively the topology of the graph, measures are, *a posteriori,* put into place to keep the quantum walk faithful to the original graph.

Relying on his own result, Montanaro proposes an encoding from *irreversible* to reversible graphs [12]. The outcome is a collection of coined quantum walks, each defined on a given reversible component of the graph. Again, the encoding procedure equips the graph with adjacency relations that alter the structure of the graph. In a manner similar to [5], these are taken care of only in later stages of the encoding.

Despite paying the price in terms of computational cost, both solutions appear to allow quantum walks to be performed on general graphs. Albeit artificially, these effectively mitigate their own alterations on the adjacencies of the graph and may, thus, be deemed *"non-invasive"*. However, there are cases in which the two encoding procedures appear to alter the magnitude of already existing relations within the original graph. In turn, the resulting quantum walk appears to be affected by local bias, that is, there are edges that are prioritized over others. This phenomenon is here referred to as *"encoding bias"*.

This thesis aims at providing a structure to the aforementioned results, outlining how these are related to one another. Contributions are made extending part of these results. Furthermore, the thesis extends the discussion on quantum walks to the phenomenon of encoding bias. An analysis is provided

[1] It should be mentioned, however, that proof of sufficiency also relies on the assumption that all vertices of the graph be equipped with self-loops.

over the potential conditions that set the ground for encoding bias to occur; the existence of potential mitigating techniques is studied. The manuscript is structured as follows.

Chapter 2 provides the required prerequisites. These involve elements of Linear Algebra and Graph Theory. An introductory section to random walks is provided. For the purposes of this thesis, notions concerning time-analysis of random walks are not required and, thus, omitted. Finally, the theory of Quantum Mechanics is illustrated via exposition of the mathematical framework it provides.

Chapter 3 thoroughly introduces the notion of quantum walk. Via a constructive approach, the limits of quantum walks are exposed, and the more general notion of coined quantum walk is introduced. The journey run by the chapter chases an answer to the question: What does it mean for a graph to be amenable to quantum walks?

Chapter 4 explores the intricate relation between graphs and unitary matrices. To begin with, the graph property of quadrangularity is introduced in both its weaker and stronger form. As it turns out, quadrangularity is also involved in the study of bridgeless, inseparable graphs with no directed bridges. These properties are shown to support a direct link between graphs and unitary matrices. A more tortuous route is the one connecting unitary matrices with reversible graphs. The chapter introduces the property of reversibility and elaborates on its connection with coined quantum walks. Finally, the result from Severini, linking coined quantum walks on regular graphs and line graphs is extended to the case of regular multigraphs.

Chapter 5 runs through the encoding procedures introduced in [5, 12].

Chapter 6 deepens the problem of encoding bias in relation to the procedures illustrated in Chapter 5. The investigation conducted on the matter is twofold: on the one hand, conditions giving rise to encoding bias are analysed, on the other, potential techniques to mitigate the phenomenon are studied.

Conclusions and potential further developments are discussed in Chapter 7.

2

Background

The purpose of this chapter is that of providing all the required prerequisites for a thorough understanding of the contents presented later.

Acquaintance with elements in linear algebra is key in the understanding of Quantum Computing. To this end, the chapter starts off with a concise introduction of those elements that are most relevant. A gentle illustration of the rules of Quantum Mechanics follows. Although some results may appear overly trivial, they offer a chance to fix the adopted notation. For a more thorough review of these notions, the reader is referred to [15].

2.1 Complex numbers and linear algebra

A preliminary idea that Chapter 2.4 shall formalize is that a *quantum computation* sort of reduces to a sequence of manipulations over *vectors* in a *complex-valued vector space.* Let us first recall that a complex number $z \in \mathbb{C}$ is of the form:

$$z = a + ib, \tag{2.1}$$

where $a, b \in \mathbb{R}$ are, respectively, the *real* and *imaginary part* of z; $i \in \mathbb{C}$ is the *imaginary unit* where $i^2 = -1$. The complex number $z^* \in \mathbb{C}$ denotes the *complex conjugate* of z, that is, z with opposite imaginary part:

$$z^* = a - ib. \tag{2.2}$$

The *modulo* of z is denoted as:

$$|z| = \sqrt{a^2 + b^2}. \tag{2.3}$$

Apart from the one given in Equation (2.1), complex numbers may be given two alternative representations. The number $z \in \mathbb{C}$ described in *polar form* is:

$$z = r(\cos\theta + i\sin\theta), \tag{2.4}$$

where $r = |z| \in \mathbb{R}^+$, $a = r(\cos\theta)$ and $b = r(\sin\theta)$ for $\theta \in [0, 2\pi)$.

Recalling Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$, the *exponential form* of z is easily derived:

$$z = re^{i\theta}. \tag{2.5}$$

2.1.1 Hilbert space

A vector $\boldsymbol{v}$ - conventionally denoted in *bold notation* - in a complex-valued vector space $\mathbb{C}^n$ is of the form:

$$\boldsymbol{v} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}, \tag{2.6}$$

where $\alpha_i \in \mathbb{C}$ for $1 \leq i \leq n$. Unless otherwise specified, a vector should be understood to be in column form. The *adjoint* $\boldsymbol{v}^\dagger$ of $\boldsymbol{v}$ is the transposed $\boldsymbol{v}^T$ of $\boldsymbol{v}$, where the coordinates are replaced by their complex conjugates:

$$\boldsymbol{v}^\dagger = (\boldsymbol{v}^T)^* = \begin{pmatrix} \alpha_1^* & \alpha_2^* & \cdots & \alpha_n^* \end{pmatrix}. \tag{2.7}$$

The results presented in this thesis only concern *finite,* complex-valued vector spaces equipped with an *inner product* $(\cdot,\cdot)$.

Definition 2.1. Let V be a vector space over $\mathbb{C}$. An *inner product* over V is any function $(\cdot,\cdot) : V \times V \to \mathbb{C}$ such that, for any $\boldsymbol{x}, \boldsymbol{y} \in V$, the following properties are satisfied:

- *Commutativity.* $(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{y}, \boldsymbol{x})$;
- *First argument linearity.* $(\lambda\boldsymbol{x}, \boldsymbol{y}) = \lambda(\boldsymbol{x}, \boldsymbol{y})$;
- *Positive definiteness.* $(\boldsymbol{x}, \boldsymbol{x}) \geq 0$, with $(\boldsymbol{x}, \boldsymbol{x}) = 0$ if and only if $\boldsymbol{x} = \boldsymbol{0}$.

Because their definitions coincide in the finite case, a vector space satisfying these conditions shall be referred to as *Hilbert space.* Moreover, the equipped inner product is to be understood as the *dot product.* That is, given $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{C}^n$:

$$(\boldsymbol{x}, \boldsymbol{y}) = \boldsymbol{y}^\dagger \boldsymbol{x} = \sum_{i=1}^{n} y_i^* x_i. \tag{2.8}$$

The dot product, as well as any other inner product, induces a *norm.* Let $\mathbb{C}^n$ be a Hilbert space, then, the induced norm is the function $\|\cdot\| : \mathbb{C}^n \to \mathbb{C}$ such that, given $\boldsymbol{v} \in \mathbb{C}^n$:

$$\|\boldsymbol{v}\| = \sqrt{(\boldsymbol{v}, \boldsymbol{v})}. \tag{2.9}$$

The vector $\boldsymbol{v}$ is said to be a *unit vector* if $\|\boldsymbol{v}\| = 1$.

Dirac notation For the results yet to be introduced, bold notation shall be abandoned in favour of the more congenial *Dirac notation.* This way, a column vector $\boldsymbol{v} \in \mathbb{C}^n$ is equivalently described by a so-called *ket*: $|v\rangle$. On the other hand, a *bra* allows to describe the adjoint $\boldsymbol{v}^\dagger$ as $\langle v|$.

In turn, the inner product between two vectors $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{C}^n$ is written as:

$$(\boldsymbol{v}, \boldsymbol{w}) = \langle w|v\rangle. \tag{2.10}$$

Basis A vector space V is fully described by a *basis*. Consider a set $B = \{|v_i\rangle\}_{i=1}^{n}$ such that $|v_i\rangle \in V$ for $1 \leq i \leq n$. Then, B is said to be a basis of V if it is a minimal set such that vectors of the form:

$$|v\rangle = \sum_{i=1}^{n} \alpha_i |v_i\rangle , \tag{2.11}$$

are *all and only* the vectors laying in V, with $\alpha_i \in \mathbb{C}$ for $1 \leq i \leq n$. Moreover $\mathsf{dim}(V) = |B|$ is said to be the *dimensionality* of V.

A basis is said to be *orthogonal* if the inner product between any two distinct elements of the basis is zero.

A basis is said to be *orthonormal* if its elements are unit vectors that are orthogonal to each other. More formally, for an orthonormal basis $B = \{|v_i\rangle\}_{i=1}^{n}$ it holds that, for any $1 \leq i, j \leq n$:

$$\langle v_i | v_j \rangle = \delta_{i,j} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases} . \tag{2.12}$$

where $\delta_{i,j}$ is the *Kronecker delta*.

Given an n-dimensional vector space V, we denote the *canonical basis* as:

$$\{|0\rangle , |1\rangle , \ldots , |n-1\rangle\}, \tag{2.13}$$

where, for any $0 \leq i < n$, $|i\rangle$ has a single non-zero entry at the $(i+1)$-th coordinate equal to 1. When no ambiguity concerns the dimensionality of the vector space, the canonical basis shall be denoted simply as $\{|i\rangle\}$.

2.1.2 Linear operators

Let V, W be two vector spaces over $\mathbb{C}$. A *linear operator* is a map $A : V \to W$ which is linear with respect to vectors in V:

$$A\Big(\sum_i \alpha_i |v_i\rangle \Big) = \sum_i \alpha_i A |v_i\rangle . \tag{2.14}$$

where $A|v_i\rangle$ denotes the application of A onto vector $|v_i\rangle$.

Matrix representation Given $n = \mathsf{dim}(V)$ and $m = \mathsf{dim}(W)$, the linear operator A may be given a matrix representation $A \in \mathbb{C}^{m \times n}$:

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ A_{m1} & \cdots & \cdots & A_{mn} \end{pmatrix} , \tag{2.15}$$

where $A_{ij} \in \mathbb{C}$ for all $1 \leq i \leq m$, $1 \leq j \leq n$. The writings A_i and $A_{,j}$ denote, respectively, the i-th row and j-th column of matrix A. The matrix representation of A varies according to the input and output bases. To this end, it is assumed that, whenever $V = W$, input and output bases coincide. Analogously

to the case of vectors, one defines the adjoint $A^\dagger$ of A to be the $n \times m$ matrix

$$A^\dagger = \begin{pmatrix} A_{11}^* & A_{21}^* & \cdots & A_{m1}^* \\ A_{12}^* & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ A_{1n}^* & \cdots & \cdots & A_{mn}^* \end{pmatrix}. \tag{2.16}$$

Outer product representation Linear operators may also be given an *outer product* representation. This description especially shines when adopting Dirac notation. To see why this is the case, consider the linear operator $A : V \to W$:

$$A = \sum_i |w_i\rangle \langle v_i| , \tag{2.17}$$

where $w_i \in W$ and $v_i \in V$ for all i. Applying A to any $|v'\rangle \in V$ lays out the conveniently expressed the result:

$$|w'\rangle = \sum_i \langle v_i|v'\rangle |w_i\rangle . \tag{2.18}$$

Definition 2.2 (Identity operator)**.** Let V be a vector space. The action of the *identity operator* $\mathbb{I}_V : V \to V$ is defined as $\mathbb{I}_V |v\rangle \equiv |v\rangle$ for any $|v\rangle \in V$. Given an orthonormal basis $\{|i\rangle\}_i$ of V,

$$\mathbb{I}_V = \sum_i |i\rangle \langle i| . \tag{2.19}$$

$\mathbb{I}_V$ is denoted as $\mathbb{I}$ whenever no ambiguity concerns the considered vector space.

For the scope of this thesis, an important category of linear operators is that of *normal operators.*

Definition 2.3 (Normal operator)**.** A linear operator A is said to be *normal* if and only if $A^\dagger A = AA^\dagger$.

A relevant subclass of normal operators is that of *unitary operators.*

Definition 2.4. Unitary operators A linear operator U is said to be *unitary* if and only if $U^\dagger U = UU^\dagger = \mathbb{I}$.

A unitary operator $U : V \to V$ preserves:

1. **Angles.** $(U |v\rangle , U |w\rangle) = \langle w|U^\dagger U|v\rangle = \langle w|\mathbb{I}|v\rangle = \langle w|v\rangle$.
2. **Norm.** $\| U |v\rangle \| = \sqrt{\langle v|U^\dagger U|v\rangle} = \sqrt{\langle v|v\rangle} = \| |v\rangle \|$.

Unitary operators on $\mathbb{C}^n$ are all and only the operators represented by matrices where both columns and rows form an orthonormal basis in $\mathbb{C}^n$.

Hermitian operators define another category of normal operators that intersects that of unitary operators.

Definition 2.5 (Hermitian operators)**.** A linear operator H is said to be *Hermitian* if and only if $H = H^\dagger$.

Intuitively, *hermiticity* may be understood as the complex-valued analogue of *symmetry.*

Definition 2.6 (Projectors)**.** Let V be a vector space and W a subspace of V, where $n = \mathsf{dim}(V), m = \mathsf{dim}(W)$. A projector is a linear operator $P : V \to W$. More specifically, let $\{|1\rangle, \ldots, |m\rangle, \ldots, |n\rangle\}$ and $\{|1\rangle, \ldots, |m\rangle\}$ be, respectively, the orthonormal bases of V and W. Then,

$$P = \sum_{i=1}^{m} |i\rangle \langle i| . \tag{2.20}$$

The outer product representation of P immediately demonstrates hermiticity of projectors.

Spectral decomposition Let us first recall that, given a linear operator A, an *eigenvector* of A is a vector $|v\rangle$ such that $A|v\rangle = \lambda|v\rangle$, where $\lambda \in \mathbb{C}$ denotes the respective *eigenvalue* of $|v\rangle$. With that being said, a notable advantage of working with normal operators stems from their related *spectral theorem.*

Theorem 1 (Spectral theorem)**.** *A linear operator A is normal if and only if it has spectral decomposition - or, equivalently, diagonal representation:*

$$A = \sum_{i} \lambda_i |\lambda_i\rangle \langle\lambda_i| , \tag{2.21}$$

where λ_i denote the eigenvalues of A and $|\lambda_i\rangle$ the respective eigenvectors.

We emphasize that the representation given in Equation (2.21) is equivalent to the more common expression $A = PDP^\dagger$, where D is the diagonal matrix with eigenvalues of A as entries and P is structured with the eigenvectors being its columns.

The spectral decomposition is extremely useful in that it allows to easily compute functions over operators. Let $f : \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n}$ be a function over linear operators. Then, given $A \in \mathbb{C}^{n\times n}$,

$$f(A) = \sum_{i} f(\lambda_i) |\lambda_i\rangle \langle\lambda_i| . \tag{2.22}$$

Definition 2.7 (Direct sum of matrices)**.** Let $M \in \mathbb{C}^{n\times m}$ and $M' \in \mathbb{C}^{n'\times m'}$ be two matrices. The *direct sum* of M and M' is the $(n + n') \times (m + m')$ matrix

$$M \oplus M' = \begin{pmatrix} M & \mathbf{0} \\ \mathbf{0} & M' \end{pmatrix},$$

where $\mathbf{0}$ denotes two matrices with only zero entries.

2.1.3 Tensor product

Let V and W be two Hilbert spaces, respectively, of dimension n and m. The tensor product of V and W is the nm-dimensional vector space $V \otimes W$.

Suppose $\{|v_i\rangle\}_{i=1}^n$ and $\{|w_j\rangle\}_{j=1}^m$ to be, respectively, orthonormal bases for V and W, then the set:

$$\{|v_i\rangle \otimes |w_j\rangle : 1 \leq i \leq n, 1 \leq j \leq m\}, \tag{2.23}$$

is an orthonormal basis for $V \otimes W$. The *Kronecker product* comes in handy to clarify the effects of the

tensor product. Given $|v\rangle \in V, |w\rangle \in W$,

$$|v\rangle \otimes |w\rangle = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \otimes \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{pmatrix} = \begin{pmatrix} v_1 |w\rangle \\ v_2 |w\rangle \\ \vdots \\ v_n |w\rangle \end{pmatrix}. \tag{2.24}$$

Often, we shall abbreviate $|v\rangle \otimes |w\rangle$ as simply $|v\rangle |w\rangle$ or even $|vw\rangle$.

Analogously, given linear operators A, B, respectively, in V and W, the operator $A \otimes B$ is a linear operator in $V \otimes W$.

2.2 Graph Theory

Graphs are fundamental data structures that encode local, binary relations between entities in a given set.

More formally, a directed graph is a pair $G = (V(G), E(G))$ where $V(G)$ is the set of vertices and $E(G) \subseteq V(G) \times V(G)$ is the set of directed edges. When no confusion arises, $V(G), E(G)$ are simply referred to as V, E. Given two vertices $u, v \in V$, there exists a directed edge from u to v if and only if $(u, v) \in E$. Given the directed edge (u, v), u and v denote, respectively, the *source* and *target* of (u, v). Two directed edges $(u, v), (w, z)$ are said to be *consecutive* if and only if $v = w$. G is said to be *undirected* when $(u, v) \in E$ if and only if $(v, u) \in E$. Because this manuscript mostly deals with *directed* graphs, these shall be referred to simply as graphs. The same holds for *"directed edges"* and *"edges"*.

Given a vertex $v \in V$, the *out-neighborhood* of v, $\delta^+(v)$ is defined as the set of all vertices connected via a directed edge *from* v. Analogously, the *in-neighborhood* $\delta^-(v)$ is the set of all vertices connected via a directed edge *to* v. More formally,

$$\delta^+(v) = \{v' : v' \in V, (v, v') \in E\}; \qquad \delta^-(v) = \{v' : v' \in V, (v', v) \in E\}. \tag{2.25}$$

In turn, the *out-degree* and the *in-degree* of v are defined, respectively, as $d^+(v) = |\delta^+(v)|$ and $d^-(v) = |\delta^-(v)|$.

A graph $G = (V, E)$ with $n = |V|$ can be exhaustively described by its *adjacency matrix* $M(G) \in \{0, 1\}^{n \times n}$, where

$$M(G)_{u,v} = \begin{cases} 1 & \text{if } (u, v) \in E; \\ 0 & \text{otherwise.} \end{cases} \tag{2.26}$$

When no ambiguity concerns the graph under consideration, we refer to $M(G)$ simply as M. From the given definitions it follows that G is undirected if and only if $M(G)$ is symmetric. Unless otherwise specified for a given graph $G = (V, E)$ it is assumed that vertices be labeled $V = \{v_1, v_2, \ldots, v_n\}$ and, in turn, that the order of rows and columns of $M(G)$ be following the order given by the subscript.

Part of the following discussion shall require a more general data structure: the *multigraph*. A multigraph is a graph where a source-target pair (u, v) may be connected by more than one edge. Formally, a multigraph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is a graph where $\mathcal{E}$ is a multiset. Let $\{(u, v)_1, (u, v)_2, \ldots, (u, v)_k\} \subseteq \mathcal{E}$

be k edges sharing source-target pair (u, v). Then, $\mathsf{m}((u, v)) = k$ is said to be the *multiplicity* of edge (u, v). For $(u, v)_x \in \mathcal{E}$, the subscript x allows to unambiguously refer to a specific edge. The entries of the adjacency matrix of a multigraph $M(\mathcal{G})$ are, for any $(u, v) \in \mathcal{E}$, $M(\mathcal{G})_{u,v} = \mathsf{m}((u, v))$. Finally, let $\mathcal{E}, \mathcal{E}'$ be two multisets where m, m' denote, respectively, the multiplicities in $\mathcal{E}$ and $\mathcal{E}'$. Then the *multiset sum* between $\mathcal{E}, \mathcal{E}'$ is the multiset $\mathcal{E} \uplus \mathcal{E}'$ with multiplicity m^+, such that, for any $(u, v) \in \mathcal{E} \cup \mathcal{E}'$, $\mathsf{m}^+((u, v)) = \mathsf{m}((u, v)) + \mathsf{m}'((u, v))$.

Be G a graph or a multigraph, there need to be as many incoming edges as there are outgoing edges.

Theorem 2. *Let $G = (V, E)$ be a (multi)graph. Then,*

$$\sum_{v \in V} d^+(v) - d^-(v) = 0. \tag{2.27}$$

We introduce two specific classes of graphs. Later chapters are not concerned with these graphs directly, however, they often emerge as *subgraphs*. Given a graph $G = (V, E)$, a subgraph $G' = (V', E')$ of G is such that $V' \subseteq V$, $E' \subseteq E$ and, for any $(u, v) \in E'$, $u, v \in V'$. Finally, a *directed n-path* is a graph $P_n = (V, E)$ where $V = \{v_1, v_2, \ldots, v_n\}$ and $E = \{(v_i, v_{i+1}) : v_i, v_{i+1} \in V\}$. In such case, we say P_n is a directed path from v_0 to v_n. A *directed n-cycle* is a directed n-path where $(v_n, v_1) \in E$.

As anticipated by the introductory chapter, specific graph properties determine whether a graph is amenable to quantum walks or not. We hereby review the most generally known, leaving the more peculiar ones to when context requires.

Definition 2.8. A graph $G = (V, E)$ is said to be *connected* if and only if, for any $(u, v) \in E$, there exists a directed path either from u to v or vice-versa.

G is said to be *strongly connected* if and only if, for any $(u, v) \in E$ there exists a directed path from u to v.

Definition 2.9. Let $G = (V, E)$ be a graph. A subgraph $H = (V', E')$ of G is said to be a (strongly) connected component of G if H is (strongly) connected.

Definition 2.10. Given a graph $G = (V, E)$, the subgraph $G' = (V', E')$ is said to be a *spanning subgraph* of G if and only if $V' = V$.

Definition 2.11. A graph $G = (V, E)$ is said to be *Hamiltonian* if and only if there exists a spanning graph G' that is a directed cycle.

Definition 2.12. Given $G = (V, E)$, a *tour* is a sequence of consecutive edges $(v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n)$, where each edge occurs exactly once. Then, a graph is said to be *Eulerian* if and only if it contains a tour that traverses all edges in G such that $v_0 = v_n$.

Theorem 3. *A graph $G = (V, E)$ is Eulerian if and only if, for any $v \in V$, $d^+(v) - d^-(v) = 0$.*

Definition 2.13. Given $k \in \mathbb{N}$, a *k-regular directed graph* $G = (V, E)$ is such that, for any $v \in V$,

$$d^+(v) = d^-(v) = k. \tag{2.28}$$

Definition 2.14. Given $n \in \mathbb{N}_{>0}$, the *n-complete graph* is the graph $K_n = (V, E)$, where $|V| = n$ and $E = \{(u, v) : u, v \in V, u \neq v\}$.

The *n-complete graph with self-loops* is the graph $K_n^+ = (V, E)$ where $|V| = n$ and $E = V \times V$.

Part of the results in this manuscript shall also require the fundamental notion of *isomorphism.*

Definition 2.15. Let $G = (V, E)$ and $G' = (V', E')$ be two graphs. Then G and G' are said to be *isomorphic* if and only if there exists a bijective mapping $\phi : V \to V'$ such that, for any $u, v \in V$,

$$(u, v) \in E \iff (\phi(u), \phi(v)) \in E'.$$

When G, G' are isomorphic we write $G \cong G'$.

Tools are set to introduce the first - and, arguably, simplest - form of graph encoding: the *line graph.*

Definition 2.16. Given a graph $G = (V, E)$, the respective line graph is $\overrightarrow{G} = (\overrightarrow{V}, \overrightarrow{E})$ where:

- $\overrightarrow{V} = E$. The vertices in $\overrightarrow{G}$ represent the edges from G.
- $\overrightarrow{E} = \{\big((u, v), (v, w)\big) : (u, v), (v, w) \in E\}$. Two vertices are adjacent in $\overrightarrow{G}$ if and only if they represent consecutive edges in G.

The following definition formalizes a property that is tightly related to line graphs.

Definition 2.17. A graph $G = (V, E)$ is said to be *specular* if and only if, for any pair of vertices $u, v \in V$, the following two conditions are satisfied:

$$\delta^+(u) \cap \delta^+(v) = \emptyset \text{ or } \delta^+(u) = \delta^+(v); \qquad \text{and} \qquad \delta^-(u) \cap \delta^-(v) = \emptyset \text{ or } \delta^-(u) = \delta^-(v). \tag{2.29}$$

In other words, if two vertices share an *out-neighbour* (*in-neighbour*), then they must share the entire out-neighborhood (in-neighborhood).

The following Lemma represents a key result for the purposes of this thesis.

Lemma 2.1. *Let $G = (V, E)$ be a graph, then its line graph $\overrightarrow{G}$ is specular.*

Proof. Assume, by contradiction, $\overrightarrow{G}$ not to be specular. Then, there exist $e_i = (u, v), e_j = (u', v') \in \overrightarrow{V}$ such that $\delta^+(e_i) \cap \delta^+(e_j) \neq \emptyset$ but $\delta^+(e_i) \neq \delta^+(e_j)$ (reasoning with respect to the in-neighborhood is analogous).

This implies the existence of two edges $e = (w, z)$, $e' = (w', z')$ such that $e \in \delta^+(e_i) \backslash \delta^+(e_j)$ and $e' \in \delta^+(e_i) \cap \delta^+(e_j)$ (the case $e \in \delta^+(e_j) \backslash \delta^+(e_i)$ is symmetric). Thus, e' is consecutive to both e_i and e_j, implying

$$v = w = v'. \tag{2.30}$$

Via the same line of reasoning, because $e \in \delta^+(e_i)$, $w = v$. This implies that $w = v'$, hence, that e is consecutive to e_j. A contradiction has arisen since $e \notin \delta^+(e_j)$. □

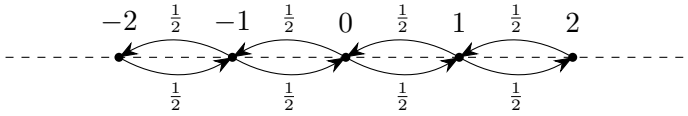


Figure 2.1: Random walk on the infinite line.

2.3 Random walks on graphs

Random walks are a fundamental tool in the study of randomized processes. In line with our purposes, this section shall review random walks with emphasis on their algorithmic applications.

Given a graph $G = (V, E)$ and a vertex $v \in V$, a random walk on G consists in the following trivial process: starting from v, walk to a vertex v' chosen from the out-neighborhood of v uniformly at random. Repeat the process starting from v' for a discrete number of steps. A more formal representation of the process is given by Algorithm 1.

Algorithm 1 The random walk algorithm.

Require: $G = (V, E),\ v \in V,\ T \in \mathbb{N}$.
1: **for** $i := 1$ to T **do**
2: Choose $v' \in \delta^+(v)$ uniformly at random;
3: $v \leftarrow v'$;

Before proceeding any further, let us observe an example that shall be useful also for future parts.

Example 2.1 (Random walk on the infinite line)**.** Consider the graph $G = (\mathbb{Z}, E)$ visualized in Figure 2.1, where $E = \{\{i, j\} : i, j \in \mathbb{Z}, i = j + 1\}$. Assuming the walk to start from vertex 0, the first step may reach either vertex 1 or -1, both with probability $1/2$ - a *fair coin toss*.

Once the first step is performed, say towards vertex 1, the second step involves the exact same procedure with respect to vertices 0 and 2.

Discrete-time Markov chains Discrete-time Markov chains (DTMC) are abstractions apt to describe a particular class of *discrete-time* stochastic processes; these include random walks on graphs. More formally, a DTMC is a triple $\mathcal{M} = (S, \mathbf{P}, \boldsymbol{u})$, where

- S is the set of states of the Markov chain with $n = |S|$. Without loss of generality it is assumed that $S = \{1, 2, \ldots, n\}$;
- $\mathbf{P} \in (0, 1)^{n \times n}$ is the *transition probability matrix*. Given $1 \leq i, j \leq n$, the entry $\mathbf{P}_{ij}$ describes the probability of reaching state j provided i is the current state. It follows that $\sum_{j=1}^{n} P_{ij} = 1$;
- $\boldsymbol{u} \in (0, 1)^n$ is the *initial state*. The initial state need not be deterministic, as such it is given in the form of a probability distribution over all states in S.

A DTMC evolves through *discrete* time-steps. Because the evolution is a stochastic process, a random variable describes its state at any given instant. We let X_t with $t \geq 0$ be the random variable that describes the state of a Markov chain at time t.

DTMC are selective about stochastic processes in that they may only describe those that satisfy the *memorylessness property.*

Definition 2.18 (Memorylessness property)**.** The state of a DTMC at time $t+1$ solely depends on the state at time t. Formally,

$$\mathbb{P}[X_{t+1} = j \mid X_0 = i_0, X_1 = i_1, \ldots, X_t = i] = \mathbb{P}[X_{t+1} = j \mid X_t = i] = \mathbf{P}_{ij}. \tag{2.31}$$

Given a time-instant $t \geq 0$, the *probability state vector* $\boldsymbol{q}^{(t)} \in (0,1)^n$ represents the probability distribution of random variable X_t. For $1 \leq i \leq n$, the i-th entry of $\boldsymbol{q}^{(t)}$ is the probability for the DTMC to be at state i after t steps. Clearly, $\boldsymbol{q}^{(0)} = \boldsymbol{u}$.

Defining $\boldsymbol{q}^{(t)}$ to be a row vector, allows to conveniently express a step of the DTMC through the following vector-matrix multiplication

$$\boldsymbol{q}^{(t+1)} = \boldsymbol{q}^{(t)}\mathbf{P}. \tag{2.32}$$

It immediately follows that $\boldsymbol{q}^{(t)} = \boldsymbol{u}\mathbf{P}^t$.

Random walks on directed graphs Let $G = (V, E)$ be a directed graph with $n = |V|$. A random walk over G can be understood in terms of a DTMC $\mathcal{M} = (S, \mathbf{P}, \boldsymbol{u})$ where $S = V$ and for $u, v \in V$,

$$\mathbf{P}_{uv} = \begin{cases} \frac{1}{d^+(u)} & \text{if } v \in \delta^+(u), \\ 0 & \text{otherwise.} \end{cases} \tag{2.33}$$

Finally, $\boldsymbol{u}$ may be an arbitrary probability distribution over the vertices of G.

Typically, a thorough introduction on random walks and DTMCs would involve a great deal of definitions and results aimed to their asymptotic time-analysis. However, this thesis is concerned with the conditions upon which random walks may be extended to quantum walks, rather than the behaviour of the walks themselves. That being the case, these notions are hereby omitted, and the reader referred to [13] for a more rigorous review.

2.4 Quantum Mechanics

In the context of Quantum Computing, a *computation* is to be understood as a physical process obeying the laws of *Quantum Mechanics*. As such, a quantum computation consists in a careful manipulation of *quantum systems* aimed at carrying out a specific task. This chapter elaborates on the rules and the limits such manipulation must adhere to.

The discussion proposed by this thesis only concerns Quantum Computing on an abstract, theoretical level. With that being the case, it shall suffice to understand Quantum Mechanics as the mathematical framework established by four of its postulates.

Quantum mechanics speak of quantum systems. Let us start by formalizing this notion.

Postulate 1. *A quantum system is fully described by a unit state vector lying in a Hilbert space. Such Hilbert space is called the state space of the system.*

To understand the meaning of Postulate 1, let us consider what is arguably the simplest quantum system there is: the *qubit*. A qubit is the quantum mechanical counterpart of a *bit*, that is, the elementary unit of information in Quantum Computing. Notoriously, a bit may take either state 0 or 1. A qubit,

however, is represented by a *state vector* in $\mathbb{C}^2$. Assuming states $0, 1$ to be represented by computational basis $|0\rangle, |1\rangle$, it makes sense for the qubit to possibly lie in a *linear combination* of the two!

More formally, let the qubit be described by $|\psi\rangle \in \mathbb{C}^2$ (in the following, a quantum system is often identified directly as its quantum state $|\psi\rangle$, *i.e.,* omitting "described by"),

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle , \tag{2.34}$$

where $\alpha, \beta \in \mathbb{C}$. Postulate 1 additionally requires $|\psi\rangle$ to be a unit vector, thus

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.35}$$

In Quantum Mechanics, coefficients α and β are known as the *probability amplitudes* of, respectively, states $|0\rangle$ and $|1\rangle$. Whenever $\alpha, \beta \neq 0$ we say that the qubit described by $|\psi\rangle$ lies in a *superposition* of states $|0\rangle, |1\rangle$.

Interestingly, Equation (2.35) gives the squared moduli - $|\alpha|^2, |\beta|^2$ - the shape of a *probability distribution.* Indeed, these two quantities represent the probabilities for the qubit to be either in state $|0\rangle$ or $|1\rangle$ upon measurement. Concerns on the meaning of *"upon measurement"* are to be addressed later in this section.

Having clarified the notion of quantum system - or, at least, how a quantum system may be addressed - we turn now the attention to how a quantum system may *evolve* through time.

Postulate 2. *The evolution of a closed quantum system through time is described by a unitary transformation.*

Before beginning to inspect the meaning of Postulate 2, let us clarify what one means by *closed* quantum system. A quantum system is a rather sophisticated entity, in that the environment - *i.e.,* other quantum systems - may interact with it and, hence, interfere with its state. Of course, if one is to construct a computational device relying on quantum systems, she requires any unwanted interference be prevented. Turns out this is no easy task, and is a primary concern in various active areas of research. With that being said, we shall avoid such trouble assuming any quantum system considered in this thesis to be closed.

More formally, Postulate 2 states that, given a quantum state $|\psi\rangle \in \mathbb{C}^n$ and a unitary transformation U operating on $\mathbb{C}^n$, the state $|\psi'\rangle$ resulting from the application of U onto $|\psi\rangle$ is

$$|\psi'\rangle = U |\psi\rangle . \tag{2.36}$$

At a first glance, Postulate 2 appears to set a fairly strong constraint on the evolution of quantum systems. Indeed, quantum systems may only undergo transformations which are *reversible.* In fact, because U is unitary, there exists $U^\dagger$ such that

$$U^\dagger |\psi'\rangle = U^\dagger U |\psi\rangle = |\psi\rangle . \tag{2.37}$$

It should be made clear that the one here provided is the *discrete-time* version of Postulate 2. *Continuous-time* evolution of quantum systems may, in fact, be described via *Schrödinger's equation.*

$$i\hbar\frac{d\left|\psi\right\rangle}{dt} = H\left|\psi\right\rangle, \tag{2.38}$$

where $\hbar$ is *Planck's constant* and H is a Hermitian operator known as the *Hamiltonian* of the system. As for our purposes, the continuous-time dynamics of quantum systems shall not be expanded any further, the focus being on discrete-time evolution.

As implicitly noted above, Postulate 2 is silent about the evolution of *non-closed* quantum systems. That is, our current construction for a mathematical framework of quantum mechanics lacks a means to describe interference from the environment. Being quantum systems extremely vulnerable to such alterations, there is arguably no chance - nor interest - to formalize all of them. There is, however, one interfering operation that one needs in order to extract *classical information* from a quantum system: *measurement.* Intuitively, a measuring device should be understood as an additional physical system that, measuring - *i.e.,* interacting with - the system, ends up disturbing its quantum state.

With that being said, our focus will be restricted on a particular subclass of quantum measurements: *projective measurements.*[1]

Postulate 3. *A projective measurement is described by a Hermitian operator M with spectral decomposition:*

$$M = \sum_i \lambda_i P_{\lambda_i}, \tag{2.39}$$

where the eigenvalues λ_i denote the possible outcomes of the operation and $P_{\lambda_i} = \left|\lambda_i\right\rangle\left\langle\lambda_i\right|$ are the projectors on the respective eigenspaces of λ_i. Given a quantum system in state $\left|\psi\right\rangle$, the probability of obtaining outcome λ_i upon measuring $\left|\psi\right\rangle$ is defined by the Born rule:

$$p(\lambda_i) = \left\langle\psi\right| P_{\lambda_i}\left|\psi\right\rangle = \left|\left\langle\lambda_i|\psi\right\rangle\right|^2. \tag{2.40}$$

Provided outcome λ_i was measured, the post-measurement state of the system is given by

$$\left|\psi'\right\rangle = \frac{P_{\lambda_i}\left|\psi\right\rangle}{\sqrt{p(\lambda_i)}}. \tag{2.41}$$

Differently from linear operators as illustrated thus far, the purpose Postulate 3 gives to M is *not* that of being applied to $\left|\psi\right\rangle$. Instead, M provides us with an orthonormal basis - its *eigenbasis* - onto which *project* the state vector $\left|\psi\right\rangle$. Via its eigenvalues, M also describes potential *classical information* that resulting from measurement.

With that being said, Postulate 3 declares measurement a *probabilistic operation.* Consider $\left|\psi\right\rangle$ as expressed in the orthonormal eigenbasis $\{\left|\lambda_i\right\rangle\}_i$:

$$\left|\psi\right\rangle = \sum_i \alpha_i\left|\lambda_i\right\rangle. \tag{2.42}$$

Because $\left|\psi\right\rangle$ is a unit vector, the $p(\lambda_i) = \left|\alpha_i\right|^2$ values, indeed, respect the structure of a probability distribution.

[1] This restriction causes no loss in generality as there are ways for general measurement operators to be expressed in the form of projective ones.

Once outcome λ_i is known to occur, $|\psi\rangle$ is projected onto its $|\lambda_i\rangle$ coordinate and normalized. Given $|\psi'\rangle$, the original linear combination from Equation (2.42) cannot be retrieved. The evolution defined in Equation (2.41) is, thus, *irreversible.*

Example 2.2. Consider a qubit described by state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Suppose to measure the qubit according to the measurement described by the operator Z, where

$$Z = 1|0\rangle\langle 0| - 1|1\rangle\langle 1|. \tag{2.43}$$

Then $p(1) = \langle\psi|0\rangle\langle 0|\psi\rangle = |\alpha|^2$ and $p(-1) = \langle\psi|1\rangle\langle 1|\psi\rangle = |\beta|^2$. Depending on the outcome, the resulting state is, respectively,

$$|\psi'_{-1}\rangle = \frac{\alpha}{|\alpha|}|0\rangle = |0\rangle; \qquad |\psi'_1\rangle = \frac{\beta}{|\beta|}|1\rangle = |1\rangle, \tag{2.44}$$

where, for both results, the last equality holds *up to a global phase:* Having modulo 1, the phase factors $\alpha/|\alpha|, \beta/|\beta|$ are irrelevant to any future dynamics concerning the quantum system.

Observe how, as the system *collapses* to either state $|0\rangle$ or $|1\rangle$, information over the former superposition state $|\psi\rangle$ is irreparably lost.

Postulates 2 and 3 exhaustively describe the behaviour of a single quantum system. However, despite being formulated in a general manner, these tools alone are insufficient to generalize the discussion over *multiple* quantum systems.

Postulate 4. *A composite quantum system is described by the tensor product of the state vectors of its component quantum systems. As such, the state space of the composite system is the tensor product of the state spaces of the components.*

According to Postulate 4, speaking of different quantum systems altogether means speaking of a single, broader quantum system. Let us formalize these statements with respect to qubits. Let $|\psi\rangle, |\varphi\rangle \in \mathbb{C}^2$ be the state vectors describing two distinct qubits:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle; \qquad |\varphi\rangle = \gamma|0\rangle + \delta|1\rangle, \tag{2.45}$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{C}$. Considering $|A\rangle$ to describe the composite system of the two qubits,

$$|A\rangle = |\psi\rangle \otimes |\varphi\rangle \tag{2.46}$$

$$= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle, \tag{2.47}$$

where $|A\rangle$ can easily be shown to be a unit vector.

Observe that $|A\rangle$ lies in the 4-dimensional Hilbert space:

$$\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4, \tag{2.48}$$

where $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ is the respective computational basis.

The tensor product intuitively outlines the purpose of a composite quantum system: Describing all possible combinations among the states of the components.

Generalizing to the case of N qubits, the associated state space is:

$$\bigotimes_{i=1}^{N} \mathbb{C}^2 = \mathbb{C}^{2^N}, \tag{2.49}$$

where the states of the computational basis $\{|00\ldots00\rangle, |00\ldots01\rangle, \ldots, |11\ldots11\rangle\}$ describe all the 2^N *classical states* the qubits might lie in. Again, apart from those states, the N qubits may lie in a superposition of them, that is, a superposition of bit sequences.

In order to solidify the understanding on multiple quantum systems as well as verify how measurement extends to them, we propose an example before concluding this section.

Example 2.3. Consider state $|A\rangle = |\psi\rangle \otimes |\varphi\rangle$ as given in Equation (2.47), which may equivalently be rewritten as

$$\Big(\alpha\,|0\rangle + \beta\,|1\rangle\Big) \otimes \Big(\gamma\,|0\rangle + \delta\,|1\rangle\Big). \tag{2.50}$$

Now suppose to measure the first qubit according, again, to the projective measurement operator Z (see Equation (2.43)). Intuitively, one would want to restrict all work on $|\psi\rangle$, leaving $|\varphi\rangle$ unaltered. To this end, we extend the projection operation on the first Hilbert space with the identity operator on the second:

$$p(\lambda_i) = \langle\psi|\,\langle\varphi|\,(P_{\lambda_i} \otimes \mathbb{I})\,|\psi\rangle\,|\varphi\rangle \tag{2.51}$$

$$= \langle\psi|P_{\lambda_i}|\psi\rangle\ \ \langle\varphi|\mathbb{I}|\varphi\rangle\,. \tag{2.52}$$

Because $\langle\varphi|\varphi\rangle = 1$, calculations are analogous to those of Example 2.2. As for the post-measurement state, depending on whether -1 or 1 was measured, we obtain

$$|A'_{-1}\rangle = \gamma\,|00\rangle + \delta\,|01\rangle\,; \qquad\qquad |A'_{+1}\rangle = \gamma\,|10\rangle + \delta\,|11\rangle\,. \tag{2.53}$$

As initially desired, information over qubit $|\varphi\rangle$ is left unaltered. What we are left with is, again, a superposition of bit sequences. Albeit this time, the superposition only includes those where the first qubit is fixed.

3

Quantum walks

Quantum walks present themselves as the extension of random walks to the principles of Quantum Mechanics. To set off the transition to the quantum realm, the particle roaming over the graph is to be understood as a quantum system. This statement alone lets the entire theory of quantum walks fall into place: one merely requires to spell out the four postulates introduced in Section 2.4 with respect to the particle. However, the construction of quantum walks is filled with subtleties which shall be taken care of throughout this section.

Before diving into the topic, it should be noted that quantum walks as hereby defined are restricted to *discrete-time* evolution. Henceforth, when writing "quantum walk", it is assumed to speak of a discrete quantum walk.

3.1 Unitary Markov chains

A straightforward way to introduce *discrete-time* quantum walks is through the notion of *unitary Markov chains* (or *quantum Markov chains*). A unitary Markov chain is a triple $\mathcal{Q} = (\mathbb{C}^n, W, |u\rangle)$ where $\mathbb{C}^n$ is a Hilbert space with orthonormal basis $\{|i\rangle\}$, W is a unitary operator on $\mathbb{C}^n$ and $|u\rangle \in \mathbb{C}^n$ is the *initial state vector.*

Compared to their classical counterpart shown in Section 2.3, unitary Markov chains do not appear too different. Albeit in a new form, the memorylessness property still stands: the *probability amplitude* for $\mathcal{Q}$ to lie in state $|j\rangle$ at time t solely depends on the state at time $t-1$. Replacing state space S with Hilbert space $\mathbb{C}^n$ endows $\mathcal{Q}$ with the ability to lie in a superposition of basis states: $\sum_i c_i |i\rangle$. Thus, denoting as $|\psi(t)\rangle$ the state of $\mathcal{Q}$ at time t, the state at time $t+1$ is

$$|\psi(t+1)\rangle = W |\psi(t)\rangle . \tag{3.1}$$

One should here carefully take into account the change in notation with respect to Equation (2.32). Indeed, state vector $|\psi(t)\rangle$ is to be understood as a column vector. As a consequence, the probability amplitude for $\mathcal{Q}$ to transition from state $|i\rangle$ to $|j\rangle$ is now given by W_{ji}.

In turn, we may now say that a directed graph $G = (V, E)$ with $n = |V|$ induces a unitary Markov

chain $\mathcal{Q} = (\mathbb{C}^n, W, |u\rangle)$ if it holds that

$$W_{ji} \neq 0 \iff (i,j) \in E. \tag{3.2}$$

Differently from Equation (2.33), amplitudes need not be equally distributed: for any $(i,j) \in E$, it is merely required there be a chance to transition from state $|i\rangle$ to $|j\rangle$. On an added note, since state space $\mathbb{C}^n$ may be derived from W and the initial state $|u\rangle$ is only relevant to the time-analysis of $\mathcal{Q}$, we shall identify a unitary Markov chain $\mathcal{Q} = (\mathbb{C}^n, W, |u\rangle)$ simply as W.

Unitary Markov chains are all good and well, however, they might leave the reader feeling distant from the actual significance carried by quantum walks. These concerns are soon to be addressed, for the time being, the major take-away is that unitary Markov chains act as a certificate for quantum walks: a graph is amenable to quantum walks if it induces a unitary Markov chain. Why is the condition only sufficient? As it turns out, the restriction enforced by Equation (3.2) on unitary W is harder than the one Equation (2.33) sets on *stochastic* $\mathbf{P}$. In order not to over restrict the playground of quantum walks, coarser necessary conditions are due.

3.2 A naïve construction

Let us attempt a construction of a quantum walk starting from the random walk on the infinite line seen in Example 2.1.

To begin with, Postulate 1 demands the particle to be described by some unit state vector. The state should represent the pertinent feature - in this case, the position of the particle on graph $G = (\mathbb{Z}, E)$. To this end, consider the canonical basis $\{|i\rangle : i \in \mathbb{Z}\}$, where $|i\rangle$ is the state for the particle lying on vertex i. The span of the basis is, then, the Hilbert space associated to the particle: $\mathbb{C}^\infty$. An immediate observation is that now the particle may lie in a superposition of different vertices.

Concerning the action of movement, it should be recalled that Postulate 2 enforces unitarity upon steps of the particle. Let us ingenuously test the limits implied by this condition. Assume the particle to lie on vertex 0, *i.e.,* to be described by state $|0\rangle$. To emulate the actions of the classical random walk from Example 2.1, one would ideally consider a unitary operator W such that, for any $i \in \mathbb{Z}$ and $\theta_1, \theta_2 \in \mathbb{R}$,

$$W|i\rangle = \frac{e^{i\theta_1}|i-1\rangle + e^{i\theta_2}|i+1\rangle}{\sqrt{2}}. \tag{3.3}$$

That is, an operator that produces any superposition inducing equal probabilities for the particle to collapse at either the previous or successive position.

Let us temporarily take for granted that such operator W indeed exists. Then, denoting as $|\psi(t)\rangle$ the state of the particle after t steps, we obtain

$$|\psi(1)\rangle = \frac{e^{i\theta_1}|-1\rangle + e^{i\theta_2}|1\rangle}{\sqrt{2}}. \tag{3.4}$$

So far, all seems up to code: $|\psi(1)\rangle$ is a unit vector and there is equal chance to find the particle at

either vertex -1 or 1. Let us perform a second step:

$$|\psi(2)\rangle = \frac{1}{2}\Big(e^{2i\theta_1}\,|-2\rangle + 2e^{i(\theta_1+\theta_2)}\,|0\rangle + e^{2i\theta_2}\,|2\rangle\Big) \tag{3.5}$$

$$= \frac{1}{2}\Big(e^{2i\theta_1}\,|-2\rangle + e^{2i\theta_2}\,|2\rangle\Big) + e^{i(\theta_1+\theta_2)}\,|0\rangle\,. \tag{3.6}$$

Clearly, $|\psi(2)\rangle$ is no unit state vector and, thus, contradicts Postulate 1. In turn, this allows for the conclusion that W cannot be unitary.

To which considerations does this simple example lead? Could one say that the infinite line is *not* amenable to *unbiased* quantum walks? The answer appears to be *yes*. However, we briefly postpone this discussion to appreciate how the example outlines two conditions that one would reasonably wish a quantum walk to satisfy:

- *Translation invariance.* A step of the quantum walk always exhibits the same behaviour, independently of the vertex from which it is performed;

- *One-dimensionality.* Not to be mistaken with the geometrical dimensionality of the line. With one-dimensional quantum walk one means that the state describing the particle only enjoys one *degree of freedom* - in this case, the position on the graph.

Obviously, unitarity is also part of these conditions.

What the example perhaps fails to highlight is the clash these conditions hold against each other. This peculiar behaviour was rigorously formalized by Meyer in [10] in the form of the No-go Lemma.

Lemma 3.1 (No-go Lemma)**.** *In one-dimension, if a unitary quantum walk operator W satisfies the condition of translation invariance, then W always moves towards the same direction.*

The No-go Lemma is a general result that applies to any undirected n-path with $n \geq 2$. With that being said, little modifications to the previous example demonstrate the result for the specific case of the infinite line. Let us give a more general definition to W. That is, for any $i \in \mathbb{Z}$,

$$W\,|i\rangle = \alpha\,|i-1\rangle + \beta\,|i+1\rangle\,. \tag{3.7}$$

The first two steps of the walk lead to state

$$|\psi(2)\rangle = \alpha^2\,|-2\rangle + 2\alpha\beta\,|0\rangle + \beta^2\,|2\rangle\,. \tag{3.8}$$

We then verify unitarity of $|\psi(2)\rangle$ considering its squared norm,

$$\|\,|\psi(2)\rangle\,\|^2 = |\alpha|^4 + 4|\alpha|^2|\beta|^2 + |\beta|^4 \geq (|\alpha|^2 + |\beta|^2)^2, \tag{3.9}$$

where the right-hand inequality of Equation (3.9) turns to equality if and only if one between $|\alpha|$ and $|\beta|$ equals 0. However, because $|\alpha|^2 + |\beta|^2 = 1$, if $|\alpha|, |\beta| \neq 1$ it follows that

$$\|\,|\psi(2)\rangle\,\|^2 > (|\alpha|^2 + |\beta|^2)^2 = 1. \tag{3.10}$$

In other words, if both $|\alpha|, |\beta| \neq 1$, then $|\psi(2)\rangle$ cannot be a unit state vector. Thus, given the definition from Equation (3.7), W either moves always to the left ($|\alpha| = 1$) or to the right ($|\beta| = 1$).

3.3 Coined quantum walks

The No-go Lemma clearly represents an obstacle in the construction of quantum walks on graphs. However, it also provides with hints on how to circumvent it, in the sense that it clearly asserts what a quantum walk *is not*. Having laid down a set of conditions that may not be satisfied all together, a legitimate attempt would be that of abandoning one of them. Let us overview our options.

Giving up on unitarity does not appear as a reasonable suggestion: to allow systems non-unitary evolution is to cease talking about Quantum Computing. On the other hand, translation invariance may be deemed a non-fundamental characteristic of quantum walks. Meyer himself relaxed this condition in developing Quantum Cellular Automata [10]. However, relaxing translation invariance may, in turn, alter the topology of the given graph. Because this thesis makes graph encoding its fundamental cause, it is of uttermost importance to maintain quantum walks as possibly faithful to the underlying graph. Translation invariance shall, thus, be preserved. Finally, one option is left: rejecting one-dimensionality. Enhancing the particle of a quantum walk with a second degree of freedom elegantly eludes the No-go Lemma. It is arguably the most popular solution in the literature; adopting it produces what is best known as a *coined quantum walk* (CQW) [1, 2, 14].

As previously stated, in its most basic form the particle of a quantum walk is characterized by a single degree of freedom: the position. A coined quantum walk equips the particle with a second: the *coin.* Here the nomenclature is rather unfortunate as a coin should be thought of as having an arbitrary number of faces. Intuitively, the coin should indicate the direction from where the particle came from. Let us formalize the last few statements with respect to regular directed graphs. Regular graphs are ideal to introduce CQWs as their structure is weaker than that of the infinite line, albeit strong enough to keep the explanation intuitive.

Consider the directed k-regular graph $G = (V, E)$, with $n = |V|$. Once more, to the position of the particle is associated the Hilbert space induced by the vertices of the graph, that is, $\mathbb{C}^n$ with orthonormal basis $\{|v\rangle\}_{v \in V}$. In addition, we consider the coin as a second quantum system. To the coin, Hilbert space $\mathbb{C}^k$ is associated, with orthonormal basis $\{|e\rangle\}_{e=1}^{k}$. Clearly, the idea is to have the particle described by both systems. To this end, Postulate 4 comes in handy, allowing to define the particle in the form of a composite quantum system. Thus, the particle shall be described by state vectors in Hilbert space $\mathbb{C}^k \otimes \mathbb{C}^n$, with orthonormal basis

$$\{|e\rangle\,|v\rangle : 1 \leq e \leq k, v \in V\}. \tag{3.11}$$

Before proceeding any further, let us intuitively justify the convenience behind working with quantum states of this form. Because G is k-regular, for any vertex u it is possible to number its outgoing edges from 1 to k. A slightly braver statement is that there exists a numbering such that, for any v, all its *incoming* edges are uniquely numbered (follows from Lemma 4.7). With that in mind, a particle in state $|e\rangle\,|v\rangle$ may be understood as a particle lying on vertex v after having traversed its e-th incoming edge.

Having reshaped the structure of our particle, its evolving behaviour also needs be rethought. As is the case for classical random walks, a step may be structured into two stages: (i) The flip of the

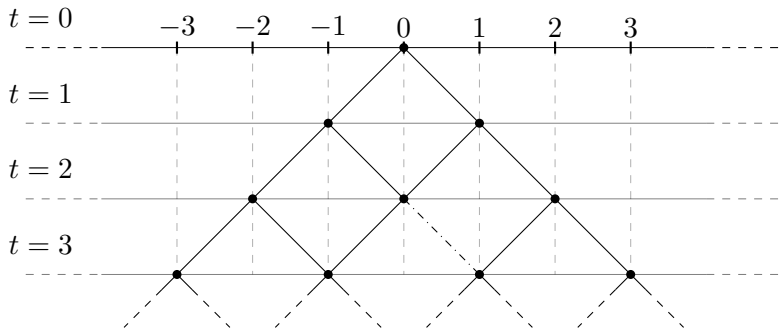


Figure 3.1: Coined quantum walk on the infinite line.

coin; (ii) The actual step. These two phases are outlined, respectively, by Lines 2 and 3 of Algorithm 1. Analogously, let us begin our *"quantum step"* evolving the coin quantum system. As now should be well understood, this needs to be done according to some unitary operator, say C, operating on $\mathbb{C}^k$. In a way similar to that of Example 2.3, we consider the extension $C \otimes \mathbb{I}_{\mathbb{C}^n}$, in order for C to operate on the whole composite system, albeit leaving the position unaltered.

Provided C has decreed the edge - or a superposition edges - to be traversed, all the particle must do is to reach its target. To this end, we rely on a *shift operator* T operating on $\mathbb{C}^k \otimes \mathbb{C}^n$. Given state $|e\rangle\,|u\rangle$,

$$T(|e\rangle\,|u\rangle) = |e\rangle\,|v\rangle\,, \tag{3.12}$$

where $(u, v) \in E$ is the e-th outgoing edge from u. Observe that T is a block-diagonal matrix, with each block being a permutation of vertices in V. Ideally, edge e determines the block to be applied. Moreover, because permutations are unitary matrices, T is unitary.

Finally, the CQW may be defined as the unitary operator $W = T(C \otimes \mathbb{I}_{\mathbb{C}_n})$. Since this entire construction might, at a first glance, appear obscure, let us verify whether a coin can help fixing our quantum walk on the infinite line.

Example 3.1 (Coined quantum walk on the infinite line)**.** To begin with, let us observe that the infinite line $G = (\mathbb{Z}, E)$ is a 2-regular graph. Accordingly, to the coin is associated to Hilbert space $\mathbb{C}^2$ with orthonormal basis $\{|0\rangle\,, |1\rangle\}$. As a more convenient nomenclature, let us relabel the basis as $\{|\mathtt{L}\rangle\,, |\mathtt{R}\rangle\}$, where the basis states represent, respectively, the edges going left and right.

The quantum walk is unbiased as long as its coin is. To this end, we define it to evolve according to *Hadamard operator* H:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \text{where} \quad \begin{matrix} H\,|\mathtt{L}\rangle = \frac{|\mathtt{L}\rangle + |\mathtt{R}\rangle}{\sqrt{2}}; \\ H\,|\mathtt{R}\rangle = \frac{|\mathtt{L}\rangle - |\mathtt{R}\rangle}{\sqrt{2}}. \end{matrix} \tag{3.13}$$

Defining the shift operator T is now intuitive:

$$T(|\mathtt{L}\rangle\,|i\rangle) = |\mathtt{L}\rangle\,|i-1\rangle\,; \qquad T(|\mathtt{R}\rangle\,|i\rangle) = |\mathtt{R}\rangle\,|i+1\rangle\,; \tag{3.14}$$

All appears to be set to verify where the first two steps of $W = T(H \otimes \mathbb{I}_{\mathbb{C}^\infty})$ will lead to. Figure 3.1 provides a visualization to follow along. Each horizontal line describes the walk at a given time-step. Black dots denote possible positions of the particle at a given step.

Let us assume to start from state $|\mathtt{L}\rangle|0\rangle$. Tossing the quantum coin gives

$$H \otimes \mathbb{I}_{\mathbb{C}^\infty} |\mathtt{L}\rangle|0\rangle = \frac{|\mathtt{L}\rangle|0\rangle + |\mathtt{R}\rangle|0\rangle}{\sqrt{2}}. \tag{3.15}$$

Then, finishing the first step we obtain

$$|\psi(1)\rangle = \frac{|\mathtt{L}\rangle|-1\rangle + |\mathtt{R}\rangle|1\rangle}{\sqrt{2}}. \tag{3.16}$$

Analogously, performing the second steps leads us to

$$|\psi(2)\rangle = \frac{|\mathtt{L}\rangle|-2\rangle + |\mathtt{R}\rangle|0\rangle + |\mathtt{L}\rangle|0\rangle - |\mathtt{R}\rangle|2\rangle}{2}. \tag{3.17}$$

Differently from Equation (3.8), $|\psi(2)\rangle$ is now a unit state vector. Due to the additional degree of freedom, particle states $|\mathtt{L}\rangle|0\rangle$ and $|\mathtt{R}\rangle|0\rangle$ are distinct: their amplitudes may not be summed.

Although seemingly tedious, it is worth observing the effects of a third step of the CQW. To avoid too cumbersome equations, let us solely focus on the evolution of states $|\mathtt{R}\rangle|0\rangle, |\mathtt{L}\rangle|0\rangle$,

$$W|\mathtt{R}\rangle|0\rangle = \frac{|\mathtt{L}\rangle|-1\rangle - |\mathtt{R}\rangle|1\rangle}{\sqrt{2}}; \qquad W|\mathtt{L}\rangle|0\rangle = \frac{|\mathtt{L}\rangle|-1\rangle + |\mathtt{R}\rangle|1\rangle}{\sqrt{2}}. \tag{3.18}$$

State $|\psi(3)\rangle$ will have these two results summed together, leading to

$$|\psi(3)\rangle = \frac{1}{2\sqrt{2}}\Big[\cdots + \Big(|\mathtt{L}\rangle|-1\rangle + |\mathtt{L}\rangle|-1\rangle\Big) + \Big(|\mathtt{R}\rangle|1\rangle - |\mathtt{R}\rangle|1\rangle\Big) + \cdots\Big]. \tag{3.19}$$

This could be understood as the quantum walk equivalent of the notorious *double-slit experiment:* whereas two paths converging to state $|\mathtt{L}\rangle|-1\rangle$ double the respective probability amplitude, the two paths heading towards state $|\mathtt{R}\rangle|1\rangle$ end up canceling each other out. These two phenomena are known, respectively, as *constructive* and *destructive interference* and characterize the peculiar behaviour of quantum walks: *more paths leading to the same position do not necessarily imply a higher probability of reaching it.*

3.4 Measurement

Thus far, each postulate of quantum mechanics has been employed in the definition of quantum walks except for the third; where does measurement fit into the formalism? Because measurement acts as the single tool to extract classical information from quantum systems, it should eventually be used to obtain insights about the position of the particle.

To this end, one may define a projective measurement M_V on the vertices of the graph:

$$M_V = v|v\rangle\langle v|. \tag{3.20}$$

According to Postulate 3, such operation causes the particle to collapse on the measured vertex. With that in mind, it is possible to show that intertwining steps of a quantum walk with measurements leads to a behaviour equivalent to that of classical random walks.

Typically, measurement is linked to quantum walks with respect to their time-analysis [1, 14]. Because this connection does not quite meet the purposes of this thesis it shall not be expanded any further. On this matter, the curious reader is also referred to [2], where measurement operators have been alternatively used to define quantum walks with absorbing boundaries.

3.5 Quantum walk amenable graphs

In light of the definitions and reflections provided by this chapter, it is only fair to outline how these relate to the central question of this manuscript: What does it mean for a graph to be amenable to quantum walks?

Throughout this chapter, the question was tackled through two distinct notions. Beginning with unitary Markov chains, this approach soon revealed itself to be over-restrictive, requiring us to turn to coined quantum walks. Do these tools together finally provide both necessary and sufficient conditions for a graph to be quantum walkable? That is, can we state that a quantum walk may be performed on a graph if and only if it induces a unitary Markov chain *or* a coined quantum walk?

A purist answer could argue that no, a coined quantum walk cannot witness a graph as quantum walkable; deeming matrix $W = T(C \otimes \mathbb{I})$ as too far related from the given adjacency matrix. In contrast, one should admit that coined quantum walks do formalize the step-action in a meaningful and natural way. At the end of the day, any potential answer appears to boil down to the adopted definitions: Where does one draw the line over which the link between graph and quantum walk becomes too thin?

Our approach on this matter is liberal. The goal being that of *encoding* the graph so that a (coined) quantum walk may be performed. An obvious constraint requires the topology of the graph to be, to a certain extent, unaffected by the alterations of the encoding. A coined quantum walk may, itself, be thought of as a sort of encoding. As shown in Section 4.4, matrix $W = T(C \otimes \mathbb{I})$ indeed refers to a graph that is, only in appearance, unrelated to the original.

4

Directed graphs and unitary matrices

In defining unitary Markov chains, a bond between graphs allowing quantum walks and unitary matrices has been stated. This chapter clarifies the terms and conditions the bond agrees upon.

To begin with, let us define how the relationship between a graph and a matrix is established. To this end, the notion of *support* of a matrix comes in handy.

Definition 4.1. Given a matrix $M \in \mathbb{C}^{n\times n}$, the *support* of M is the matrix $M^S \in \{0,1\}^{n\times n}$ where, for any $1 \leq i,j \leq n$,

$$M^S_{ij} = \begin{cases} 1 & \text{if } M_{ij} \neq 0, \\ 0 & \text{otherwise.} \end{cases} \tag{4.1}$$

The relationship can, thus, be stated in matrix theoretical terms, considering the adjacency matrix of the graph.

Definition 4.2. A directed graph $G = (V, E)$ is said to be *the graph of a matrix* M if and only if M is supported by the adjacency matrix M_G.

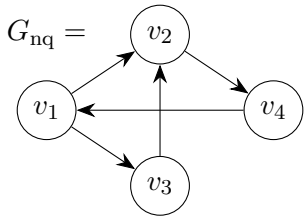
These definitions allow the following rephrasing: a directed graph $G = (V, E)$ induces a unitary Markov chain W if and only if G is the graph of $W^\dagger$. The use $W^\dagger$ is an unfortunate consequence of the divergence between definitions in Equations (2.32) and (3.1). In sections where, given G, the existence of unitary W supported by $M(G)$ is investigated, this notational trouble is irrelevant and thus ignored.

In turn, we let $\mathcal{U}$ be the *set including all graphs of unitary matrices.* Before investigating which graphs belong to $\mathcal{U}$, let us briefly outline the ones that certainly *do not.* A unitary matrix does not admit zero-rows or columns. The adjacency matrix of some $G \in \mathcal{U}$ should, then, satisfy the same condition. That is, all vertices in G should own at least one in- and out-neighbour.

4.1 Specular, strongly quadrangular directed graphs

Specular, strongly quadrangular graphs are graphs of unitary matrices. The result was first shown by Severini in [18]. It constitutes an early milestone in the study on graphs of unitary matrices.

Having already reviewed the notion of specularity (see Definition 2.17), let us introduce the property of quadrangularity; first, in its weaker form.



$$M(G_{\text{nq}}) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Figure 4.1: Non-quadrangular graph.

Definition 4.3. A graph $G = (V, E)$ is said to be *quadrangular* if and only if, for any pair of vertices $u, v \in V$, where $u \neq v$, it is always the case that

$$|\delta^+(u) \cap \delta^+(v)| \neq 1 \quad \text{and} \quad |\delta^-(u) \cap \delta^-(v)| \neq 1. \tag{4.2}$$

In other words, when a graph is quadrangular, two distinct vertices never share *exactly one* in- or out-neighbour. Graph G_{nq}, displayed in Figure 4.1, violates quadrangularity twice. One violation involves vertices v_1, v_3: v_2 being their only shared out-neighbour.

With Lemma 4.1, we give proof as to why quadrangularity is a necessary condition for graphs of unitary matrices. Because the same result is shown below for strong quadrangularity, Lemma 4.1 trivially follows. However, being quadrangularity a seemingly abstract property, it is useful to gradually observe its effects on adjacency matrices. This also sets us off on our study on the relationship between graphs of unitary matrices and quadrangularity.

Lemma 4.1. *Any directed graph of a unitary matrix is quadrangular.*

Proof. Let $G = (V, E)$ be the graph of unitary matrix U and assume, by contradiction, G *not* to be quadrangular. Then there exist $v_i, v_j \in V$ such that $\delta^+(v_i) \cap \delta^+(v_j) = \{u_k\}$ (the case for the in-neighborhoods is analogous). Because U is supported by $M(G)$, rows U_i, U_j share a single non-zero entry at column k. As a consequence, their inner product is determined by $U_{ik} \cdot U_{jk} \neq 0$. Since U is shown to own two distinct non-orthogonal rows, its unitarity is contradicted. □

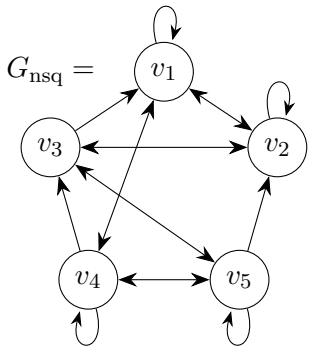
Referring to the example in Figure 4.1, observe the first and third row of $M(G_{\text{nq}})$. Any matrix U supported by $M(G)$ shall follow the same pattern of zero-entries. The inner product between rows U_1, U_3 is, then, determined by $U_{1,2} \cdot U_{3,2}$. Being the two entries necessarily non-zero, their product is non-zero.

Let us proceed one step further with the introduction of strong quadrangularity.

Definition 4.4. Given a graph $G = (V, E)$, consider sets of the two following forms:

- $S_{\text{out}} \subseteq V$, where, for any $u \in S_{\text{out}}$ there exists $v \in S_{\text{out}}$ such that $\delta^+(u) \cap \delta^+(v) \neq \emptyset$.
- $S_{\text{in}} \subseteq V$, where, for any $u \in S_{\text{in}}$ there exists $v \in S_{\text{in}}$ such that $\delta^-(u) \cap \delta^-(v) \neq \emptyset$.

Then, G is said to be *strongly quadrangular* if and only if for any set of the form S_{out} or S_{in} it holds



$$M(G_{\text{nsq}}) = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Figure 4.2: Quadrangular graph that is not strongly quadrangular.

that

$$\left| \bigcup_{u,v \in S_{\text{out}}} \delta^+(u) \cap \delta^+(v) \right| \geq |S_{\text{out}}|; \tag{1}$$

$$\left| \bigcup_{u,v \in S_{\text{in}}} \delta^-(u) \cap \delta^-(v) \right| \geq |S_{\text{in}}|. \tag{2}$$

Let us first verify that this version of quadrangularity, indeed, is stronger. G non-quadrangular implies the existence of a subset $S_{\text{out}} = \{u, v\}$ (or S_{in}) where $|\delta^+(u) \cap \delta^+(v)| = 1$. Thus, because $1 < |S_{\text{out}}|$, G is not strongly quadrangular either.

This fact is also supported by the existence of graph G_{nsq} displayed in Figure 4.2. G_{nsq} is quadrangular though not strongly quadrangular. To verify quadrangularity, observe that, in $M(G_{\text{nsq}})$, there exists no pair of rows (or columns) sharing exactly one non-zero entry. On the other hand, detecting non-strong-quadrangularity of G_{nsq} is more involved. Consider the set $S_{\text{out}} = \{v_1, v_2, v_3\}$, and observe that their common out-neighbours are $\{v_1, v_2\}$. Orange and green colors have been used in $M(G_{\text{nsq}})$ to highlight this fact. Because $|\{v_1, v_2\}| < |S_{\text{out}}|$, Rule *1* of strong quadrangularity is violated.

Lemma 4.2. *[18] Any graph of a unitary matrix is strongly quadrangular.*

Proof. Let $G = (V, E)$ (with $n = |V|$) be the graph of a unitary matrix U and assume, by contradiction, G *not* to be strongly quadrangular. Then there exists $S_{\text{out}} \subseteq V$ with $k = |S_{\text{out}}|$ violating Rule *1*. That is, for any $u \in S_{\text{out}}$, there exists $v \in S_{\text{out}}$ such that $\delta^+(u) \cap \delta^+(v)$ but,

$$s = \left| \bigcup_{u,v \in S_{\text{out}}} \delta^+(u) \cap \delta^+(v) \right| < k \tag{4.3}$$

The first condition implies $M(G)$ has a set of k rows $\{r_1, r_2, \ldots, r_k\}$, where each row shares at least one non-zero entry with another row of the set. The second condition implies that only s non-zero entries are shared among the k rows.

Let R be the submatrix of $M(G)$ restricted to rows $\{r_1, r_2, \ldots, r_k\}$. For a clearer representation and

without loss of generality, the s shared non-zero entries may be assumed to all lie in the first s columns.

$$R = \left(\begin{array}{ccc|ccc} \alpha_{1,1} & \cdots & \alpha_{1,s} & \alpha_{1,s+1} & \cdots & \alpha_{1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{k,1} & \cdots & \alpha_{k,s} & \alpha_{k,s+1} & \cdots & \alpha_{k,n} \end{array}\right). \tag{4.4}$$

(Color-coding matches that of the example in Figure 4.2).

Because U is supported by $M(G)$, its submatrix U_R restricted to the same set of rows describes the same pattern of non-zero entries as R. Let us consider the inner products of these rows to check their orthonormality. Recall that rows of R *do not* share non-zero entries in the green side. It follows that their inner products are fully determined by orange entries, *i.e.,* subvectors of length s. If all rows are to be orthonormal, it is required that inner products of all distinct k subvectors be zero. However, because $s < k$, there cannot exist k linearly independent vectors of length s. This implies that rows $\{r_1, r_2, \ldots, r_k\}$ are *not* orthonormal, contradicting unitarity of U.

The case where G violates Rule *2* is analogous with respect to the columns of U. □

The proof for Lemma 4.1 describes a specific case of the one in Lemma 4.2. While the former relies on the non-existence of two orthonormal, one-dimensional vectors, the latter generalizes: for any $s < k$, there exist no k orthonormal s-dimensional vectors.

Having gained acquaintance with strong quadrangularity, it is yet to be shown how, together with specularity, these make sufficient conditions for a graph G to be that of a unitary matrix. A pair of preliminary notions are still due.

Claim 4.1. *For $n > 0$, the n-complete graph with self loops K_n^+ is the graph of a unitary matrix.*

Proof. For any n, the adjacency matrix $M(K_n^+)$ has no zero-entries. For any n, the *Discrete Time Fourier* (DFT) orthonormal basis induces a unitary matrix $\mathrm{DFT}(n)$ without zero entries, where, for any $0 \leq i, j \leq n-1$

$$\mathrm{DFT}(n)_{ij} = \frac{1}{\sqrt{n}} e^{2ijk/n}. \tag{4.5}$$

□

Definition 4.5. Let M be a $n \times m$ matrix. M' is an *independent full submatrix* of M if and only if, for any $1 \leq i, k \leq n$ and $1 \leq j, l \leq m$, if an entry M_{ij} is also an entry of M', then, any M_{il}, M_{kj} is either another entry of M' or a zero entry.

To better understand the notion of independent full submatrix, consider the matrix

$$M = \begin{pmatrix} 0 & 0 & 0 & \alpha_{1,1} & \alpha_{1,2} & 0 & 0 \\ \beta_{1,1} & \beta_{1,2} & 0 & 0 & 0 & \beta_{1,3} & 0 \\ 0 & 0 & 0 & \alpha_{2,1} & \alpha_{2,2} & 0 & 0 \\ 0 & 0 & 0 & \alpha_{3,1} & \alpha_{3,2} & 0 & 0 \\ \beta_{2,1} & \beta_{2,2} & 0 & 0 & 0 & \beta_{2,3} & 0 \\ 0 & 0 & \gamma_{1,1} & 0 & 0 & 0 & \gamma_{1,2} \end{pmatrix}, \tag{4.6}$$

where A, B, C are independent full submatrices of M:

$$A = \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} \\ \alpha_{2,1} & \alpha_{2,2} \\ \alpha_{3,1} & \alpha_{3,2} \end{pmatrix}; \quad B = \begin{pmatrix} \beta_{1,1} & \beta_{1,2} & \beta_{1,3} \\ \beta_{2,1} & \beta_{2,2} & \beta_{2,3} \end{pmatrix}; \quad C = \begin{pmatrix} \gamma_{1,1} & \gamma_{1,2} \end{pmatrix}. \tag{4.7}$$

All is set for the main result of this section. Lemma 4.3 makes the first and hardest step through the endeavour.

Lemma 4.3. *[18] A specular, strongly quadrangular graph is the graph of a matrix composed of square independent full submatrices.*

Proof. Let $G = (V, E)$ be a specular, strongly quadrangular graph. Because G is specular, V may be partitioned into vertices sharing the entire out-neighborhood (reasoning for in-neighborhoods is analogous). Let P_{out} be one such partition. Thus, for any $u, v \in P_{\text{out}}$, $\delta^+(u) \cap \delta^+(v) \neq \emptyset$, satisfying the premise of Rule *1* of strong quadrangularity. Because G is specular and strongly quadrangular, for any $u' \in P_{\text{out}}$,

$$\left| \bigcup_{u,v \in P_{\text{out}}} \delta^+(u) \cap \delta^+(v) \right| = |\delta^+(u')| \geq |P_{\text{out}}|. \tag{4.8}$$

Consider the rows in $M(G)$ describing the adjacencies of vertices in P_{out}. For specularity, these all have same zero and non-zero entries, inducing a $|P_{\text{out}}| \times |\delta^+(u)|$ independent full submatrix. Thus, to show the submatrix to be square, it must be proved that $|\delta^+(u)| = |P_{\text{out}}|$.

To this end, let $w \in \delta^+(u)$ for some $u \in P_{\text{out}}$. Then, $\delta^-(w) = P_{\text{out}}$. Moreover, for any $w, z \in \delta^+(u)$, it holds that $\delta^-(w) = \delta^-(z) = P_{\text{out}}$, satisfying the premise of Rule *2* of strong quadrangularity. Since G is strongly quadrangular, for $u \in P_{\text{out}}$,

$$\left| \bigcup_{w,z \in \delta^+(u)} \delta^-(w) \cap \delta^-(z) \right| = |\delta^-(w)| = |P_{\text{out}}| \geq |\delta^+(u)|. \tag{4.9}$$

Putting together Equations (4.8), (4.9) gives, for any $u \in P_{\text{out}}$, $|\delta^+(u)| = |P_{\text{out}}|$. It follows that G is the graph of a matrix composed of square independent full submatrices. □

Lemma 4.4. *The graph of a matrix composed of square independent full submatrices is the graph of a unitary matrix.*

Proof. The result follows from Claim 4.1. The independent full $k \times k$ submatrices of the adjacency matrix each support a $k \times k$ unitary matrix with no zero entries. □

At last, Theorem 4 follows from Lemmata 4.3 and 4.4.

Theorem 4. *[18] A specular, strongly quadrangular graph is the graph of a unitary matrix.*

4.1.1 Strongly quadrangular line graphs

Theorem 4 decreed specularity and strong quadrangularity as sufficient conditions for a graph to be that of a unitary matrix. On the other hand, Lemma 2.1 states that all line graphs are specular. Corollary 4.1 trivially follows.

Corollary 4.1. *A strongly quadrangular line graph is the graph of a unitary matrix.*

That being the case, a spontaneous way to characterize part of set $\mathcal{U}$ answers the question: Which graphs give rise to strongly quadrangular line graphs? The following result has been shown by Severini in [18] and exhaustively solves the problem.

Theorem 5. *[18] Let G be a graph. Then, $\overrightarrow{G} \in \mathcal{U}$ if and only if G is Eulerian or the disjoint union of Eulerian components.*

Proof. From left to right, let $\overrightarrow{G} = (\overrightarrow{V}, \overrightarrow{E}) \in \mathcal{U}$. By Lemma 4.2, $\overrightarrow{G}$ is strongly quadrangular. By Lemma 4.3, the adjacency matrix $M(\overrightarrow{G})$ is composed of square independent full submatrices. Any such $k \times k$ submatrix R describes a set of k vertices $I = \{i_1, i_2, \ldots, i_k\} \subseteq \overrightarrow{V}$ sharing the same out-neighborhood $O = \{o_1, o_2, \ldots, o_k\} \subseteq \overrightarrow{V}$. Let $i_j \in I$ represent edge $(u, v) \in E$. Then, since any $i_x \in I$ has the same out-neighborhood as i_j it must be the case that all edges represented by i_x have $v \in V$ as their target, implying $d^-(v) = k$. On the other hand, $(i_j, o_y) \in \overrightarrow{E}$ implies that i_j, o_y are consecutive edges: any $o_y \in O$ is of the form (v, w). It follows that $d^+(v) = k$ and, more broadly, that v is balanced. By Theorem 3, G is Eulerian.

From right to left is now simple, let $G = (V, E)$ be an Eulerian graph. Because any $v \in V$ is balanced, $\delta^+(v) = \delta^-(v)$. Let $k = d^-(v)$ and $S_v \subseteq \overrightarrow{V}$ be the set of edges targeting v. Then, for $i' \in S$,

$$\left| \bigcup_{i,j \in S} (\delta^+(i) \cap \delta^+(j)) \right| = d^+(i'). \tag{4.10}$$

Since $d^+(i') = k$ and $|S| = k$, Rule *1* of strong quadrangularity is respected by S_v for any $v \in V$. □

4.2 Bridgeless, inseparable directed graphs

Severini has also explored the relationship between graphs and unitary matrices in the opposite direction [17]. Let us consider G, graph of a unitary matrix. It is possible to define appropriate metrics to assess the *connectivity* of G. As it turns out, having $G \in \mathcal{U}$ requires its connectivity be *not too fragile.*

The following preliminary definitions will help formalize the opening statement. Let $G = (V, E)$ be a graph.

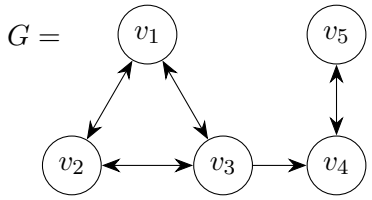
Definition 4.6. A set $E' \subset E$ is said to be a *disconnecting set of directed edges* if and only if the graph $G' = (V, E \backslash E')$ has more connected components than G.

An analogous definition may be given with respect to vertices.

Definition 4.7. A set $V' \subset V$ is said to be a *disconnecting set of vertices* (or a *cut*) if and only if the graph $G' = (V \backslash V', E_{V'})$ has more connected components than G, where $E_{V'}$ is the subset of edges restricted to vertices in V'.

Finally, we can define the primitives that will characterize the results of this section.

Definition 4.8. A *bridge* is a disconnecting set of edges $E' = \{(u, v), (v, u)\}$. In other words, a *bridge* is a disconnecting undirected edge.



$$M(G) = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Figure 4.3: Graph including a bridge, a directed bridge and two cut-vertices.

Definition 4.9. A *directed bridge* is a disconnecting set of edges $E' = \{(u, v)\}$.

Definition 4.10. A *cut-vertex* is a disconnecting set of vertices $V' = \{v\}$.

Definition 4.11. Let E' be a set of edges such that, were edges E' to be deleted, the given graph would be split in two connected components C_1, C_2. Then, E' is said to be a disconnecting set of directed bridges if and only if, for all $(u, v) \in E'$, $u \in C_1$ and $v \in C_2$.

Figure 4.3 provides an example covering all three definitions. The undirected edge $\{v_4, v_5\}$ is a bridge. Edge (v_3, v_4) is a directed bridge. Vertex v_3 is one of the two cut-vertices in the graph.

Finally, G is said to be *bridgeless* if it contains no bridges; analogously, *inseparable* if it contains no cut-vertices. In connection with the opening statement of this section, one could - rather informally - deem a graph violating any of these three properties to be - *"not so connected."*

At last, let us introduce the central result of this section.

Theorem 6. *[17] Let G be the graph of a unitary matrix U. Then, the following conditions are satisfied:*

1. *G has no directed bridges.*

2. *Either G is bridgeless, or all bridges belong to connected components that are K_2 or K_2^+.*

3. *Either G is inseparable, or all cut-vertices are isolated vertices with self-loops.*

Let us provide proofs for all three conditions of Theorem 6. Let $G = (V, E) \in \mathcal{U}$, with $n = |V|$.

Proof 1. Assume, by contradiction, there exists a directed bridge $(v_i, v_j) \in E$. Removing (v_i, v_j) would split G into two separate connected components $G_1 = (V_1, E_1), G_2 = (V_2, E_2)$. The directed bridge (v_i, v_j) shall not be removed, however, it is useful to reason in terms of the two potential partitions. Let $k = |V_1|$. V may be relabeled so that the directed bridge becomes $(v_k, v_{k+1}) = (v_i, v_j)$ and

$$V_1 = \{v_1, v_2, \ldots, v_k\}; \qquad V_2 = \{v_{k+1}, v_{k+2}, \ldots, v_n\}. \tag{4.11}$$

The situation up to this point is visualized in Figure 4.4. Then, let A, B be submatrices of $M(G)$. Let A be restricted to rows $\{r_1, r_2, \ldots, r_{k-1}\}$ and columns $\{c_1, c_2, \ldots, c_k\}$; let B be restricted to rows

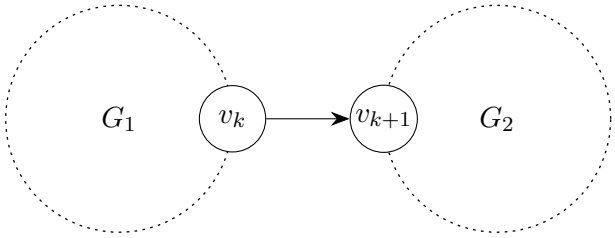


Figure 4.4: General graph with directed bridge (v_k, v_{k+1}).

$\{r_{k+1}, r_{k+2}, \ldots, r_n\}$ and columns $\{c_{k+2}, c_{k+3}, \ldots, c_n\}$. $M(G)$ may, thus, be written as

$$M(G) = \left(\begin{array}{ccc|c|ccc} & & & 0 & & & \\ & A & & 0 & & \mathbf{0} & \\ & & & \vdots & & & \\ & & & 0 & & & \\ \hline M_{k,1} & M_{k,2} & \cdots\ M_{k,k} & 1 & 0 & 0 & \cdots\ 0 \\ \hline & & & M_{k+1,k+1} & & & \\ & \mathbf{0} & & M_{k+2,k+1} & & B & \\ & & & \vdots & & & \\ & & & M_{n,k+1} & & & \end{array}\right), \tag{4.12}$$

where $\mathbf{0}$ is denotes a zero matrix of appropriate size. Zero matrices adjacencies between vertices of G_1 and G_2. Observe that, were there to be a 1 in the top-right or bottom-left corners, (v_k, v_{k+1}) would cease to be a directed bridge.

Let us proceed recalling that, by Lemma 4.1, G is quadrangular. It follows that

$$M_{k,p} = 0, \text{ for } p \leq k; \qquad\qquad M_{q,k+1} = 0, \text{ for } q \geq k+1. \tag{4.13}$$

To justify this claim assume, by contradiction, there was $M_{k,p} = 1$, with $p \leq k$, implying $(v_k, v_p) \in E$. Because $v_p \in V_1$ and $v_{k+1} \in V_2$, they can have no common in-neighbour other than v_k, contradicting quadrangularity of G. The argument in support of $M_{q,k+1} = 0$, for $q \geq k+1$, is analogous.

As a consequence, it is possible to conclude that A and B are two independent full submatrices, respectively, of dimension $(k-1) \times (k)$ and $(n-k) \times (n-k-1)$. Being non-square, they cannot support unitary matrices; it follows that $G \notin \mathcal{U}$. □

Remark 4.1. The last step of the proof might mislead to a stronger version of Lemma 4.4; one where $M(G)$ being structured in square independent full submatrices also constitutes a necessary condition for $G \in \mathcal{U}$. However, *there are unitary submatrices that are not full independent.* For instance,

$$U = \begin{pmatrix} 1/\sqrt{2} & 1/2 & 1/2 \\ 0 & 1/\sqrt{2} & -1/\sqrt{2} \\ -1/\sqrt{2} & 1/2 & 1/2 \end{pmatrix}. \tag{4.14}$$

Proof 2. Let $(v_i, v_j), (v_j, v_i) \in E$ be a bridge. Repeating the relabeling from the previous proof gives G

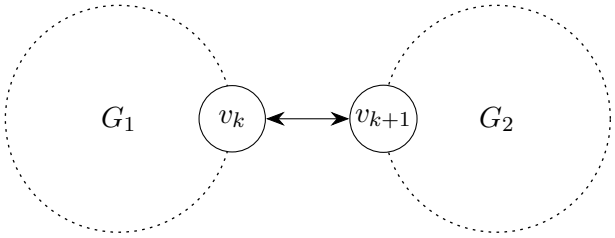


Figure 4.5: General graph with bridge $\{(v_k, v_{k+1}), (v_{k+1}, v_k)\}$.

the representation visualized in Figure 4.5.

In order not to contradict the definition of bridge, there can be no $v_p \in V_1$ such that (v_p, v_{k+1}) or $(v_{k+1}, v_p) \in E$. Vice-versa, there exists no $v_q \in V_2$ such that (v_q, v_k) or $(v_k, v_q) \in E$. Through the same argument of the previous proof, quadrangularity also implies that (v_p, v_k) and $(v_k, v_p) \notin E$ and $(v_q, v_{k+1}), (v_{k+1}, v_q) \notin E$ for any $v_p \in V_1, v_q \in V_2$.

Moreover, quadrangularity also implies that either both vertices v_k, v_{k+1} are equipped with self-loops, or none of the two. Indeed, assuming by contradiction $(v_k, v_k) \in E$ and $(v_{k+1}, v_{k+1}) \notin E$, vertices v_k, v_{k+1} would share v_k as their unique in-neighbour, thus violating quadrangularity and implying $G \notin \mathcal{U}$.

These conditions reflect on the adjacency matrix of G, allowing $M(G)$ to take one of the two following forms depending on the presence of self-loops.

$$M(G) = \left(\begin{array}{c|cc|c} A & \mathbf{0} & & \mathbf{0} \\ \hline & 0 & 1 & \\ \mathbf{0} & & & \mathbf{0} \\ & 1 & 0 & \\ \hline \mathbf{0} & \mathbf{0} & & B \end{array}\right); \quad \text{or} \quad M(G) = \left(\begin{array}{c|cc|c} A & \mathbf{0} & & \mathbf{0} \\ \hline & 1 & 1 & \\ \mathbf{0} & & & \mathbf{0} \\ & 1 & 1 & \\ \hline \mathbf{0} & \mathbf{0} & & B \end{array}\right). \tag{4.15}$$

On this occasion, matrices A, B do not cause trouble, as they represent square submatrices. Attention should, instead, fall on the central rows and columns, concerning the adjacencies of vertices v_k, v_{k+1}. These characterize vertices v_k, v_{k+1} as part of their own connected component, be it either K_2 or K_2^+. □

Proof 3. Let v_i be a cut-vertex of G. Once again, G is relabeled in order to distinct the potential connected components G_1, G_2. Thus, obtaining $v_k = v_i$ and

$$V_1 = \{v_1, \dots, v_{k-1}\}; \qquad V_2 = \{v_{k+1}, \dots, v_n\}. \tag{4.16}$$

Figure 4.6 visualizes G after relabeling. The adjacency matrix presents itself as follows:

$$M(G) = \begin{pmatrix} M(G_1) & & M_{1,k} & & \mathbf{0} \\ & & \vdots & & \\ M_{k,1} & \cdots & M_{k,k} & \cdots & M_{k,n} \\ & & \vdots & & \\ \mathbf{0} & & M_{n,k} & & M(G_2) \end{pmatrix}. \tag{4.17}$$

To begin our study on $M(G)$, we observe that, among the i-th column and row, there must be at least one non-zero entry, as otherwise v_k would be an isolated node implying $G \notin \mathcal{U}$. The case where

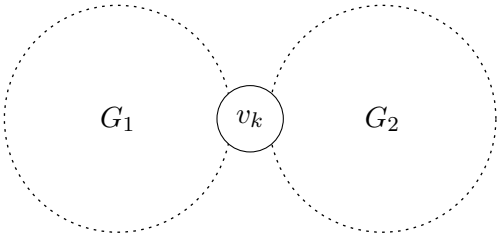


Figure 4.6: General graph with cut-vertex v_k.

$M_{k,k}$ is the only non-zero entry is trivial: $M(G_1), M(G_2)$ are square independent full submatrices, and so is the 1×1 matrix $M_{k,k}$. It follows that v_k is an isolated vertex.

A more interesting case concerns the existence of $v_q \in V_2$ such that $(v_k, v_q) \in E$ (the cases where $(v_q, v_k) \in E$ and, with $v_p \in V_1$, (v_k, v_p) or $(v_p, v_k) \in E$ are analogous). Before proceeding any further, for simplicity let us relabel $v_{k+1} = v_q$.

Similarly to previous demonstrations, quadrangularity implies $M_{k,p} = 0$ for any $p < k$. In turn, it also follows that $M_{p,k} = 0$ for any $p < k$. Were this not the case, $M(G)$ would present a $(k-1) \times k$ independent full submatrix in the top-left corner, implying $G \notin \mathcal{U}$.

Let us plot these deductions on the adjacency matrix.

$$M(G) = \left(\begin{array}{c|ccc} M(G_1) & \multicolumn{3}{c}{\mathbf{0}} \\ \hline & M_{k,k} & \cdots & M_{k,n} \\ \mathbf{0} & \vdots & & \\ & M_{n,k} & & M(G_2) \end{array}\right). \tag{4.18}$$

The result obtained may be informally restated as: *if $G \in \mathcal{U}$, then no cut-vertex can lie between two distinct connected components.* Indeed, suppose G_2 could be divided into two connected components G_2', G_2'', such that v_k is a cut-vertex between them, the reasoning illustrated above would simply reapply.

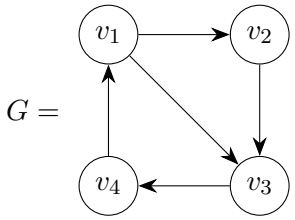
If no contradiction arises before, constantly reapplying the reasoning leads to v_k being part of a connected component alone with some other vertex v_{k+1}. It follows that both $(v_k, v_{k+1}), (v_{k+1}, v_k) \in E$, as otherwise a single edge would constitute in a directed bridge, implying $G \notin \mathcal{U}$. However, existence of both edges leads to contradiction, as v_k would not be a cut-vertex.

This proves the result: either G has cut-vertex $v_k \in V$ as an isolated vertex with self-loop, or G is inseparable. □

4.3 Reversible directed graphs

In [12], Montanaro tackled both directions of the relation between graphs and unitary matrices. On the one hand, he has shown that any coined quantum walk is performed over a *reversible* graph. On the other, he has given constructive proof that, provided all vertices be equipped with self-loops, a coined quantum walk may be defined over any reversible graph. Before diving into the study of this result, let us carefully assess what it says and what it does not.

The statement declares reversibility to be both a sufficient and necessary condition for a coined



$$M(G) = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Figure 4.7: Reversible graph that is not the graph of a unitary matrix.

quantum walk to be defined on a graph (with self-loops). By sufficiency, all reversible graphs with self-loops allow coined quantum walks. However, not all graphs allowing coined quantum walks are graphs of unitary matrices (see the infinite line from Example 3.1). Proof of sufficiency thus does *not* speak about graphs of unitary matrices. Instead, it speaks about how reversible graphs with self-loops may be mapped onto graphs of unitary matrices. That being the case, it is postponed to Chapter 5.

As for this section, the proof of necessity is reviewed, providing a comparison with previously illustrated conditions. Let us introduce the main character of this section.

Definition 4.12. Let $G = (V, E)$ be a graph. An edge $(u, v) \in E$ is said to be reversible if and only if there exists a path from v to u.

Initially, one could be misled to think that reversible edges are all and only those edges that *are not* directed bridges. However, whereas *any directed bridge is an irreversible edge*, the opposite is not true.

Remark 4.2. An edge is reversible if and only it does not belong to any disconnecting set of directed bridges.

Defining reversible graphs is now straightforward.

Definition 4.13. A graph $G = (V, E)$ is said to be *reversible* if and only if all its edges are reversible.

From Definition 4.13, it immediately follows that a connected component is *strongly* connected if and only if it is reversible.

In light of the observations made above, the condition of reversibility does not appear too distant from that asked by point (1) from Theorem 6. This similarity is briefly elaborated at the end of this chapter. In contrast, the comparison between reversibility and conditions (2),(3) immediately to state the following remark.

Remark 4.3. There are reversible graphs that are not those of unitary matrices. Figure 4.2 provides an example. Because G is not quadrangular it cannot be the graph of a unitary matrix.

At last begins the path towards the main result of this section, which may be formally stated as follows.

Theorem 7. *[12] Any coined quantum walk is performed on a reversible graph.*

Let us start off on our path from a notorious result from Quantum Mechanics.

Theorem 8 (Quantum Recurrence Theorem [3])**.** *Let W be any unitary operator over $\mathbb{C}^n$, then for any $\epsilon > 0$ and any $|\psi\rangle \in \mathbb{C}^n$, there exists $k \geq 1$ such that $\langle\psi| W^k |\psi\rangle > 1 - \epsilon$.*

In other words, given an initial state $|\psi\rangle$, merely reapplying unitary operator W must, sooner or later, lead back to a state arbitrarily close to $|\psi\rangle$.

Lemma 4.5. *Let $|\psi\rangle, |\varphi\rangle \in \mathbb{C}^n$ be two states such that $\langle\varphi| W |\psi\rangle \neq 0$, for some unitary W. Then, there exists $m \geq 0$ such that $\langle\psi| W^m |\varphi\rangle \neq 0$.*

Proof. To begin with, observe that from $\langle\varphi| W |\psi\rangle$ follows $\langle\psi| W^{-1} |\varphi\rangle$. Then, by Theorem 8, for any $\epsilon > 0$ there exists $k > 0$ such that $\langle\varphi| W^k |\varphi\rangle > 1 - \epsilon$. Let $|\varphi'\rangle = W^k |\varphi\rangle$, then $\langle\psi| W^{-1} |\varphi'\rangle \neq 0$. Moreover, it follows that

$$\langle\psi| W^{-1} W^k |\varphi\rangle = \langle\psi| W^m |\varphi\rangle , \tag{4.19}$$

for $m = k - 1 \geq 0$. □

Lemma 4.5 appears to characterize unitary operators through a sort of quantum analog of graph reversibility as given in Definition 4.12, hinting a connection to the notion of reversibility given in discussing of Postulate 2. Such fortunate use of terminology is briefly elaborated in Section 5.3.

Let us proceed on our path. The next step applies knowledge of the newly proven findings over coined quantum walk operators.

Lemma 4.6. *Let $G = (V, E)$ be a graph with $V = \{v_1, v_2, \ldots, v_n\}$ and let W be a quantum walk on G with a coin C operating on $\mathbb{C}^k$ with $k \geq 1$. For any $|c_p\rangle |v_i\rangle, |c_q\rangle |v_j\rangle$, if there exists $m \geq 0$ such that $\langle c_q| \langle v_j| W^m |c_p\rangle |v_i\rangle \neq 0$, then there exists a path from v_i to v_j in G.*

Proof. From v_i, consider the m-steps walk $|w\rangle = W^m |c_p\rangle |v_i\rangle$, for any face $|c_p\rangle$ of the coin. From $\langle c_q| \langle v_j| W^m |c_p\rangle |v_i\rangle \neq 0$, it follows $|w\rangle$ contains a non-zero amplitude for the particle to reach v_j traversing edge c_q. The non-zero amplitude witnesses a path from v_i to v_j. □

By Lemma 4.6, states encountered by a coined quantum walk describe paths on the underlying graph. The proof carefully considers m-step walks regardless of the coin. This allow to bypass any effects of destructive interference that could, potentially, cancel out amplitudes for a given path.

Finally, Theorem 7 immediately follows from Lemmata 4.5 and 4.6. Furthermore, because all graphs of unitary matrices allow for coined quantum walks, the following corollary is implied.

Corollary 4.2. *All graphs of unitary matrices are reversible.*

4.4 A coined quantum walk is performed on the line graph

Section 3.3 has shown how a mere increase in dimensionality provides a brilliant expedient to perform quantum walks on graphs that would not otherwise allow them. These quantum walks have been referred to as coined quantum walks. While the walk may intuitively be understood to happen over the original graph, the shape of the unitary matrix $W = T(C \otimes \mathbb{I})$ clearly begs to bring a different graph into the discussion. In [16], Severini made the shape of this graph precise, showing that a CQW on a regular graph G is performed on its line graph $\overrightarrow{G}$. Hereby, the same result is proposed in a form that covers the case of regular multigraphs. In light of the findings later to be discussed in Section 5.2, this allows us to provide a crispier image of CQWs on reversible graphs with self-loops.

This section pullulates with technicalities and abstract definitions. We establish here a checkpoint for the reader to come back to whenever the final objective feels obscure: *Given a k-regular multigraph $\mathcal{G}$ the goal is to show that its line graph $\overrightarrow{\mathcal{G}}$ is the graph of unitary matrix $W = T(C \otimes \mathbb{I})$, with W defined according to the procedure from Section 5.2.*

Let us begin by introducing the characteristic that makes regular (multi)graphs so special.

Definition 4.14 (1-Factor)**.** Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a multigraph, and H be a subgraph of $\mathcal{G}$. H is said to be a 1-*factor* of $\mathcal{G}$ if and only if it is a 1-regular spanning subgraph of $\mathcal{G}$.

In other words, a 1-factor is a directed cycle - *or* a set of vertex-disjoint cycles - that spans all vertices of $\mathcal{G}$. That being the case, a 1-factor may well be understood as a permutation matrix.

Definition 4.15 (1-Factorization)**.** Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a multigraph. A *1-factorization* of $\mathcal{G}$ is a multiset $\mathcal{F} = \{P_1, P_2, \ldots, P_k\}$, where, for any $1 \leq i, j \leq k$, P_i is a 1-factor of $\mathcal{G}$, and, if $i \neq j$, P_i, P_j are edge disjoint. In a 1-factorization, each $(u, v)_x \in \mathcal{E}$ occurs exactly once.

Lemma 4.7. *Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ (with $n = |\mathcal{V}|$) be a multigraph. Then $\mathcal{G}$ is k-regular if and only if it has 1-factorization of cardinality k.*

Proof. The proof from right to left is straightforward. Let $\mathcal{F} = \{P_1, P_2, \ldots, P_k\}$ be a 1-factorization of $\mathcal{G}$. Summing up the k permutation matrices representing the k 1-factors gives the adjacency matrix of $\mathcal{G}$. Because the sum of k permutation matrices is a matrix with all rows and columns summing up to k, $M(\mathcal{G})$ is the adjacency matrix of a k-regular multigraph.

From left to right, consider $M \in \mathbb{N}^{n \times n}$, the adjacency matrix of $\mathcal{G}$. For any $1 \leq i \leq n$,

$$\sum_{j=1}^{n} M_{i,j} = k; \qquad \sum_{j=1}^{n} M_{j,i} = k.$$

Dividing all entries of $M(\mathcal{G})$ by k gives a matrix M' where all rows and columns sum up to 1, *i.e.,* a *doubly stochastic matrix*. By Birkhoff's theorem [9], all doubly stochastic matrices may be re-expressed as a linear combination of permutation matrices. Multiplying all coefficients of the linear combination by k gives again $M(\mathcal{G})$ as

$$M(\mathcal{G}) = \sum_{i=1}^{l} c_i P_i = \sum_{i=1}^{k} P_i,$$

where the $l \leq k$ coefficients $c_i \in \mathbb{N}$ have been removed, re-expressing the linear combination as a sum of k permutation matrices, where, potentially, $P_i = P_j$ for $i \neq j$. It remains to show all permutations to be pair-wise disjoint. In dealing with multigraphs, the statement is generalized as: for any $(v_i, v_j) \in \mathcal{E}$, there exist exactly m permutations sharing the non-zero entry (i, j), where $m \leq k$ is the multiplicity of (v_i, v_j) in $\mathcal{G}$. Since all non-zero entries of any permutation is 1, the result follows. □

The following definition constitutes a key apparatus in the connection between the 1-factors of $\mathcal{G}$ and $\overrightarrow{\mathcal{G}}$.

Definition 4.16. Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a multigraph and $\mathcal{H} = (\mathcal{V}, \mathcal{E}_{\mathcal{H}})$ be a spanning sub-multigraph of $\mathcal{G}$. For $v \in \mathcal{V}$, let $d^+_{\mathcal{G}}(v)$ be the out-degree of v in $\mathcal{G}$. The *growth* of $\mathcal{H}$ is the multigraph $\Upsilon_{\mathcal{G}}(\mathcal{H}) = (\mathcal{V}', \mathcal{E}')$,

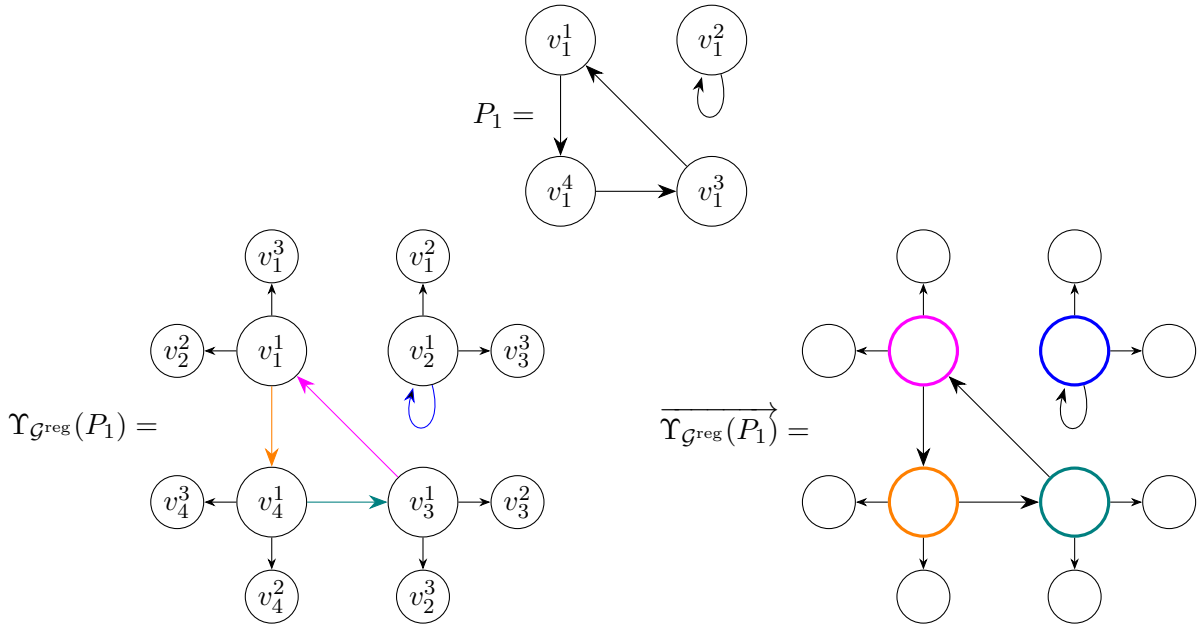


Figure 4.8: The 1-factor P_1 of multigraph $\mathcal{G}^{\text{reg}}$, its growth and line graph of the growth.

where, for each $v \in \mathcal{V}$, vertices $\{v_1, v_2, \ldots, v_l\}$ are added, with $l = d^+_{\mathcal{G}}(v) - d^+_{\mathcal{H}}(v)$. The added vertices are all connected to v via edges $\{(v, v_1), (v, v_2), \ldots, (v, v_l)\}$.

With the purpose of making the definition of growth - as well as the following steps - clearer, we provide visual examples to follow along. Figure 4.8 considers permutation P_1 of the 3-regular multigraph $\mathcal{G}^{\text{reg}}$ shown in Figure 5.2, displaying the growth of P_1 with respect to $\mathcal{G}^{\text{reg}}$. Each vertex has been equipped with edges to $3 - 1$ newly added out-neighbours.

Lemma 4.8. *Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ be a k-regular multigraph with 1-factorization $\{P_1, P_2, \ldots, P_k\}$. Then, for any $1 \leq s \leq k$, $\Upsilon_{\mathcal{G}}(P_s) \cong \overrightarrow{\Upsilon_{\mathcal{G}}(P_s)}$.*

Proof. For any $1 \leq i \leq k$, consider the 1-factor P_s. Let us relabel $\mathcal{V} = \{v_1^s, v_2^s, \ldots, v_n^s\}$. Then, the growth $\Upsilon_{\mathcal{G}}(P_s)$ adds $k-1$ adjacent vertices to each $v_i^s \in V(P_s)$. For purposes clarified in Corollary 4.3, newly added vertices need be carefully labeled. Any new vertex adjacent to v_i^s is labeled v_j^p if, for some x, $(v_i, v_j)_x \in E(P_p)$. Because v_i appears in all other $(k-1)$ 1-factors of $\mathcal{G}$, the labeling is well-defined.[1]

Let us then construct the respective line graph, $\overrightarrow{\Upsilon_{\mathcal{G}}(P_s)}$. By definition, its vertex set is $E(\Upsilon_{\mathcal{G}}(P_s))$ which, thanks to the given labeling may be expressed as

$$V(\overrightarrow{\Upsilon_{\mathcal{G}}(P_s)}) = \{(v_i^s, v_j^p) : v_i \in V(P_s), (v_i, v_j)_x \in \mathcal{E}\}. \tag{4.20}$$

On the other hand, the edge set is defined as

$$E(\overrightarrow{\Upsilon_{\mathcal{G}}(P_s)}) = \left\{\Big((u, v)_x, (v, w)_y\Big) : (u, v)_x \in E(P_s), (v, w)_y \in \mathcal{E}\right\}. \tag{4.21}$$

At a first glance, these two expressions might appear obscure. To get a better grasp, the color coding from Figure 4.8 comes in handy: the sources of edges in $\overrightarrow{\Upsilon_{\mathcal{G}}(P_s)}$ *always* represent edges in P_s.

[1] If no superscript is used, vertex v_i is referred to with respect to the original labeling of $\mathcal{V}$.

Finally it is possible to define the following isomorphism $\phi : V(\Upsilon_{\mathcal{G}}(P_s)) \to V(\overrightarrow{\Upsilon_{\mathcal{G}}(P_s)})$ such that, $\phi(v) = (u, v)$. Because, for any $u \in V(\Upsilon_{\mathcal{G}}(P_s))$, $d^-(u) = 1$, ϕ is a bijection. It remains to show that

$$(u, v) \in E(\Upsilon_{\mathcal{G}}(P_s)) \iff (\phi(u), \phi(v)) = \Big((w, u), (z, v)\Big) \in E(\overrightarrow{\Upsilon_{\mathcal{G}}(P_s)}). \tag{4.22}$$

From left to right, if $(u, v) \in E(\Upsilon_{\mathcal{G}}(P_s))$, then, because $d^-(v) = 1$, $z = u$. Vice-versa, if $\Big((w, u), (z, v)\Big) \in E(\overrightarrow{\Upsilon_{\mathcal{G}}(P_s)})$, it must be the case that $u = z$, and thus $(u, v) \in E$. Thus, $\Upsilon_{\mathcal{G}}(P_s) \cong \overrightarrow{\Upsilon_{\mathcal{G}}(P_s)}$. □

Corollary 4.3. *Let $\mathcal{G}$ be a k-regular multigraph with 1-factorization $\{P_1, P_2, \ldots, P_k\}$. Then, for $1 \leq s \leq k$,*

$$M(\Upsilon_{\mathcal{G}}(P_s)) = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ M(P_1) & M(P_2) & \cdots & M(P_k) \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \end{pmatrix} \tag{4.23}$$

Proof. Strikingly, this result comes as a natural consequence of the labeling adopted for $\Upsilon_{\mathcal{G}}(P_s)$ during proof of Lemma 4.8. Indeed, the growth of P_s somewhat encodes all adjacencies of $\mathcal{G}$.

Formally, consider order $(v_1^1, v_2^1, \ldots, v_n^1, v_1^2, v_2^2, \ldots v_n^k)$. $M(\Upsilon_{\mathcal{G}}(P_s))$ is, thus, organized into k blocks, the p-th being $M(P_p)$. Indeed, entry (i, j) of the block is 1 if and only if $(v_i^s, v_j^p) \in \Upsilon_{\mathcal{G}}(P_s)$, which, by definition of the labeling, is true if and only if - according to the original labeling - $(v_i, v_j)_x \in E(P_p)$. □

We come to the harshest step of this section. It is possible to show that any k-regular multigraph $\mathcal{G}$ gives rise to a k-regular line graph $\overrightarrow{\mathcal{G}}$. By Lemma 4.7, $\overrightarrow{\mathcal{G}}$ admits 1-factorization. Here we aim higher, as we wish to relate such 1-factorization to the one admitted by $\mathcal{G}$. The following result is an extension of Lemma 2.2 from [20] to the case of multigraphs.

Lemma 4.9. *Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a k-regular multigraph. Then, $\overrightarrow{\mathcal{G}} = (\overrightarrow{V}, \overrightarrow{E})$ has 1-factorization*

$$\{\Upsilon_{\mathcal{G}}(P_1), \Upsilon_{\mathcal{G}}(P_2), \ldots, \Upsilon_{\mathcal{G}}(P_k)\}.$$

Proof. For any $(u, v)_x \in \overrightarrow{V}$ let $\overrightarrow{E}_{(u,v)_x}$ be the set of all outgoing edges from vertex $(u, v)_x$, that is,

$$\overrightarrow{E}_{(u,v)_x} = \Big\{\big((u, v)_x, (v, w)_y\big) : (v, w)_y \in E\Big\}.$$

The whole set of adjacencies can thus be given the following representation:

$$\overrightarrow{E} = \bigcup_{e \in E} \overrightarrow{E}_e.$$

Let $\{P_1, P_2, \ldots P_k\}$ be the 1-factorization of $\mathcal{G}$. Recall that for any $i \neq j$, $E(P_i) \cap E(P_j) = \emptyset$. As a consequence, $\overrightarrow{E}$ may be partitioned as

$$\left\{ \bigcup_{e \in E(P_1)} \overrightarrow{E}_e, \bigcup_{e \in E(P_2)} \overrightarrow{E}_e, \ldots, \bigcup_{e \in E(P_k)} \overrightarrow{E}_e \right\}, \tag{4.24}$$

where $\left(\bigcup_{e_i \in E(P_i)} \overrightarrow{E}_{e_i}\right) \cap \left(\bigcup_{e_j \in E(P_j)} \overrightarrow{E}_{e_j}\right) = \emptyset$, since it always holds that $e_i \neq e_j$.

For $1 \leq i \leq k$, consider the component of the partition:

$$\bigcup_{(u,v)_x \in E(P_s)} \overrightarrow{E}_{(u,v)_x} = \bigcup_{(u,v)_x \in E(P_s)} \left\{ \left((u,v)_x, (v,w)_y \right) : (v,w)_y \in \overrightarrow{V} \right\} \tag{4.25}$$

$$= \left\{ \left((u,v)_x, (v,w)_y \right) : (u,v)_x \in E(P_s), (v,w)_y \in \mathcal{E} \right\}. \tag{4.26}$$

The edge set given by Equation (4.26) is exactly the same as $E(\overrightarrow{\Upsilon_{\mathcal{G}}(P_s)})$ defined in Equation (4.21)! Then, because all components of the partition from Equation 4.24 are disjoint, so are all graphs $\overrightarrow{\Upsilon_{\mathcal{G}}(P_s)}$. And because all $\overrightarrow{\Upsilon_{\mathcal{G}}(P_s)}$ span $\overrightarrow{\mathcal{G}}(P_s)$, $\overrightarrow{G}$ has 1-factorization

$$\{\overrightarrow{\Upsilon_{\mathcal{G}}(P_s)}, \overrightarrow{\Upsilon_{\mathcal{G}}(P_s)}, \ldots, \overrightarrow{\Upsilon_{\mathcal{G}}(P_k)}\}. \tag{4.27}$$

Finally, by Lemma 4.8, $\overrightarrow{\Upsilon_{\mathcal{G}}(P_s)} \cong \Upsilon_{\mathcal{G}}(P_s)$, for any $1 \leq s \leq k$. Then $\mathcal{G}$ also has 1-factorization

$$\{\Upsilon_{\mathcal{G}}(P_1), \Upsilon_{\mathcal{G}}(P_2), \ldots, \Upsilon_{\mathcal{G}}(P_k)\}.$$

□

Corollary 4.4. *Let $\mathcal{G}$ be a k-regular multigraph with 1-factorization $\{P_1, P_2, \ldots, P_k\}$. Then,*

$$M(\overrightarrow{\mathcal{G}}) = \begin{pmatrix} M(P_1) & M(P_2) & \cdots & M(P_k) \\ M(P_1) & M(P_2) & \cdots & M(P_k) \\ \vdots & \vdots & \ddots & \vdots \\ M(P_1) & M(P_2) & \ldots & M(P_k) \end{pmatrix}. \tag{4.28}$$

Proof. By Lemma 4.9, $\overrightarrow{\mathcal{G}}$ has 1-factorization $\{\Upsilon_{\mathcal{G}}(P_1), \Upsilon_{\mathcal{G}}(P_2), \ldots, \Upsilon_{\mathcal{G}}(P_k)\}$. Then, $M(\overrightarrow{\mathcal{G}}) = \sum_{i=1}^{k} M(\Upsilon_{\mathcal{G}}(P_i))$. By Corollary 4.3, the result immediately follows. □

Up to this point, all efforts have been put to give $M(\overrightarrow{\mathcal{G}})$ the form in Equation (4.28). All is left to do is to justify this elaborate endeavour.

Theorem 9. *Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ (with $n = |\mathcal{V}|$) be a k-regular multigraph. Then $\overrightarrow{\mathcal{G}}$ is the graph of a unitary matrix W, where W is a coined quantum walk.*

Proof. By Corollary 4.4, $M(\overrightarrow{\mathcal{G}})$ takes the form given in Equation (4.28), which may be rewritten as:

$$M(\overrightarrow{\mathcal{G}}) = \begin{pmatrix} \mathbb{I}_{\mathbb{C}^n} & \cdots & \mathbb{I}_{\mathbb{C}^n} \\ \vdots & \ddots & \vdots \\ \mathbb{I}_{\mathbb{C}^n} & \cdots & \mathbb{I}_{\mathbb{C}^n} \end{pmatrix} \begin{pmatrix} M(P_1) & & & \\ & M(P_2) & & \\ & & \ddots & \\ & & & M(P_k) \end{pmatrix} \tag{4.29}$$

$$= (\mathbf{1}_{\mathbb{C}^k} \otimes \mathbb{I}_{\mathbb{C}^n}) \cdot T, \tag{4.30}$$

where $\mathbf{1}_{\mathbb{C}^k}$ is the matrix with all entries 1 operating on $\mathbb{C}^k$, and $T = \bigoplus_{i=1}^{k} M(P_i)$, with $M \oplus M'$ denoting the direct sum of matrices M, M'. T is clearly a permutation and, thus, unitary.

Then, consider C to be a coin with no zero entries operating on $\mathbb{C}^k$ (by Claim 4.1, such C exists). It follows that $M(\overrightarrow{\mathcal{G}})$ supports the matrix $W^\dagger = (C \otimes \mathbb{I}_{\mathbb{C}^n})T$. Recalling that CQWs are defined via matrix-vector multiplication (see discussion at the beginning of the chapter), $W = T(C \otimes \mathbb{I}_{\mathbb{C}^n})$ is a CQW on graph $\mathcal{G}$. □

4.5 Can this intricate relationship be simplified?

The contents of this chapter have gradually unraveled the intertwined connection that lies between graphs and unitary matrices. The reader is referred to Section 5.4, for a conceptual summary of the results illustrated above. On this matter, a few additional observations are due.

In introducing reversible graphs, Section 4.3 hinted to a potential equivalence to graphs with no disconnecting sets of directed bridges. Because all graphs of unitary matrices are reversible (Corollary 4.2), proving the equivalence would provide a generalization of Theorem 6 point (1). In turn, this would allow to condense part of the contents from Sections 4.2 and 4.3.

On a related matter, all points (1),(2) and (3) of Theorem 6 appear to lend themselves to generalizations. The attentive reader might have noticed the three proofs to merely rely on quadrangularity of graphs of unitary matrices. Further investigations should be conducted on how strong quadrangularity affects the presence of disconnecting sets of directed bridges, disconnecting sets of edges and cuts.

Finally, potentially adding up to the stack of graph properties, Severini has conjectured Hamiltonicity to be a necessary condition for a graph to be that of a unitary matrix [17]. To the best knowledge of the author, the conjecture still remains to be proven.

5

Encoding graphs into unitary matrices

The previous chapter established the conditions needed for a graph to induce - either directly or indirectly - a unitary Markov chain. As informally shown by the example on the infinite line (see Section 3.2), these conditions severely restrict the class of graphs of unitary matrices. While further studies may be conducted to extend the class, this chapter shall walk another path, providing an overview of the methods that *"non-invasively"* edit a graph $G \notin \mathcal{U}$ to a graph $G' \in \mathcal{U}$.

5.1 General graphs to Eulerian

Let us begin from the contents presented in [5], where Della Giustina et al. proposed an optimal algorithmic solution aimed at encoding multigraphs into unitary matrices. The encoding procedure is fully based on the contents hereby illustrated in Section 4.1 and operates according to the sole assumption that the given multigraph be connected. Let us briefly review its most salient points.

Multigraph conversion to Eulerian Function EULERIFY - given here as Algorithm 2 - marks the first and only editing operation throughout the course of actions. Exploiting Theorem 3, the function provides a *"Eulerian version"* of the given multigraph balancing all of its vertices. Let us formalize.

Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be a multigraph, the call EULERIFY$(\mathcal{G}, b)$ involves the integer, $|\mathcal{V}|$-dimensional array b. Array b stores balance of each vertex and witnesses Eulericity: $\mathcal{G}$ is Eulerian if and only if $b = \mathbf{0}$. Let B^-, B^+ be, respectively, the sets of vertices with negative and positive balance. Then, for all $u \in B^-$, the function adds outgoing edges from u to vertices in B^+, nearing the balance of all involved vertices to zero. By Theorem 2, given vertex $u \in B^-$, there must be $v \in B^+$. The same result also ensures EULERIFY to converge. To see why this is the case, consider X to be the quantity of overall unbalance,

$$X = \sum_{u \in B^-} |b_u| + \sum_{v \in B^+} b_v = 2\left(\sum_{u \in B^-} |b_u| \right). \tag{5.1}$$

Then, $b = \mathbf{0}$ if and only if $X = 0$. Each iteration of the inner while loop at Line 6 decreases X by two. Moreover, considering the outer while loop - Line 4 -, it can be stated that the inner loop iterates $\sum_{u \in B^-} |b_u|$ times. It immediately follows that, after this number of iterations, $b = \mathbf{0}$. Finally, $|\mathcal{E}_\perp| = \sum_{u \in B^-} |b_u| \leq |\mathcal{E}|$ implies the overall time complexity for EULERIFY be $\Theta(|\mathcal{V}|+|\mathcal{E}_\perp|) \subseteq \mathcal{O}(|\mathcal{V}|+|\mathcal{E}|)$.

Algorithm 2 A procedure to edit a multigraph into a Eulerian one.

Require: $\mathcal{G} = (\mathcal{V}, \mathcal{E})$.
Require: $b \in \mathbb{Z}^{|\mathcal{V}|}$, where $b_v = d^+(v) - d^-(v)$, for $v \in \mathcal{V}$.
1: **function** EULERIFY($\mathcal{G}, b$)
2: $\quad\mathcal{E}_\perp := \emptyset$;
3: $\quad B^+ = \{v \in \mathcal{V} : b(v) > 0\}$; $B^- = \{v \in \mathcal{V} : b(v) < 0\}$;
4: $\quad$**while** $B^- \neq \emptyset$ **do**
5: $\quad\quad u \leftarrow$ POP(B^-);
6: $\quad\quad$**while** $b_u \neq 0$ **do**
7: $\quad\quad\quad v \leftarrow$ CHOOSE(B^+); ▷ Choose without extraction.
8: $\quad\quad\quad \mathcal{E}_\perp = \mathcal{E}_\perp \uplus \{(u, v)\}$;
9: $\quad\quad\quad b_u \leftarrow b_u + 1$; $b_v \leftarrow b_v - 1$;
10: $\quad\quad\quad$**if** $b_v = 0$ **then**
11: $\quad\quad\quad\quad B^+ \leftarrow B^+ \backslash \{v\}$;
12: $\quad$**return** $\mathcal{E}_\perp$;

EULERIFY($\mathcal{G}, b$) collects all added edges inside multiset $\mathcal{E}_\perp$. Once the procedure has finished, *"Eulerified"* $\mathcal{G}$ takes shape into the multigraph $\mathcal{G}' = (\mathcal{V}, \mathcal{E}')$, where $\mathcal{E}' = \mathcal{E} \uplus \mathcal{E}_\perp$.[1] On an added note, function EULERIFY($\mathcal{G}, b$) appears to impact the topology of $\mathcal{G}$. While this is indeed the case, this matter is addressed in later stages of the encoding.

Line graph construction The second step in the pipeline consists in the computation of line graph $\overrightarrow{\mathcal{G}'}$. Being the procedure rather trivial, it shall suffice a brief analysis of its time-complexity. Iterating over edges $(u, v)_x \in \mathcal{E}'$, one requires to find all consecutive edges $(v, w)_y \in \mathcal{E}'$, so to compute all adjacencies of $\overrightarrow{\mathcal{G}'}$. The process clearly requires $\Theta(|\mathcal{E}'|^2)$ time.

Assembly of the supported unitary matrix Theorem 5 guarantees that, by this stage, graph $\overrightarrow{\mathcal{G}'}$ is the graph of a unitary matrix. All it remains to be done is to construct one that respects non-zero entries in $M(\overrightarrow{\mathcal{G}'})$. To this end, Lemma 4.3 provides a detailed blueprint: $M(\overrightarrow{\mathcal{G}'})$ is structured into square independent full submatrices. These all support unitary matrices without zero entries. Thus, given a set of such matrices, one merely requires to arrange their entries in the submatrices that support them. The process is taken care of by function UNITARIZE, here given in Algorithm 3. Whereas in [5] UNITARIZE is defined to operate on strongly quadrangular line graphs, Algorithm 3 defines it to operate on any specular, strongly quadrangular graph $G = (V, E)$.

UNITARIZE assumes the required unitary matrices to be given in the form of parameter $\mathcal{U}_G$. $\mathcal{U}_G$ is a set of unitary matrices with no zero entries such that, for any $v \in V$, there exists a $d^-(v) \times d^-(v)$ matrix $\mathcal{U}_G(d^-(v)) \in \mathcal{U}_G(d^-(v))$ (the statement is equivalent with respect to $d^+(v)$). By Lemma 4.3, each independent full submatrix of $M(G)$ supports some $U \in \mathcal{U}_G$.

UNITARIZE($G, \mathcal{U}_G$) performs its task in a *"submatrix-by-submatrix"* modality. Let $W = M(G)$ be the - soon to become - unitary matrix. Set Q should be understood as the set of rows yet to be edited. The loop at Line 4 picks some $v_i \in V$. Because G is specular, strongly quadrangular, the in-neighborhood $\delta^-(v_i)$ consists of $d^-(v_i)$ vertices which share the exact same $d^-(v_i)$ out-neighbours. Thus, v_i fully induces a $d^-(v_i) \times d^-(v_i)$ independent full submatrix W^{v_i}. To make it unitary, a $d^-(v_i) \times d^-(v_i)$ matrix

[1] Hereby, '$\uplus$' denotes the operation of multiset sum.

Algorithm 3 Function constructing a unitary matrix for a specular, strongly quadrangular graph.

Require: $G = (V, E)$ specular, strongly quadrangular graph with $V = \{v_1, v_2, \ldots, v_n\}$.
Require: $\mathcal{U}_G$ set of unitary matrices such that, for any $v \in V$, $\mathcal{U}_G(d^-(v)) \in \mathcal{U}_G$ is a $d^-(v) \times d^-(v)$ unitary matrix with no zero entries.

```
1:  function UNITARIZE(G,U_G)
2:      W := M(G);
3:      Q := V;
4:      while v_i ∈ V do
5:          U ← U_G(d⁻(v_i));
6:          c ← 1;
7:          for all v_j ∈ (δ⁻(v_i) ∩ Q) do
8:              SPARSESUB(W_j, U_c);          ▷ Unitarize row W_j resembling row U_c.
9:              Q ← Q\{v_j};
10:             c ← c + 1;
11:     return W;
```

Algorithm 4 Procedure to turn a 0-1 row into a unitary row.

Require: $r \in \{0, 1\}^n$;
Require: $u \in \mathbb{C}^d$ unitary vector such that $d \leq n$.

```
1: procedure SPARSESUB(r, u)
2:     h ← 1;
3:     for k := 1 to n do
4:         if r_k = 1 then
5:             r_k ← u_h;
6:             h ← h + 1;
```

$U \in \mathcal{U}_G$ is chosen.

Independent full submatrix W^{v_i} is unitarized row-by-row. The task is performed by the loop at Line 6, which iterates over the in-neighbours $v_j \in \delta^-(v_i)$ that still belong Q. In other words, it iterates over rows j, such that $W_{j,i} \neq 0$ which are yet to be edited. By definition of independent full submatrix (see Definition 4.5), these are all and only the rows containing entries of submatrix W^{v_i}.

The c-th iteration of the loop overwrites the $d^-(v_i)$ non-zero entries of row W_j with the $d^-(v_i)$ entries of row U_c. In reality, the quest is delegated to procedure SPARSESUB. Call SPARSESUB(W_j, U_c) carefully edits the h-th non-zero entry of W_j to the h-th entry of U_c.

Once SPARSESUB(W_j, U_c) has finished, vertex v_j is removed from Q. The effects of the removal are later to be elaborated. For the time being, the two following claims certify for the correct behaviour of SPARSESUB.

Claim 5.1. SPARSESUB(W_j, U_c) *turns* W_j *into a unit vector.*

Proof. Upon termination of the procedure, W_j has its non-zero entries replaced by the entries from U_c. Because U_c is the row of unitary matrix U,

$$\langle W_j | W_j \rangle = \langle U_c | U_c \rangle = 1.$$

Thus justifying the claim. □

Now, let $W_{j',i} = 0$ where $j' \neq j$. That is, j' is another row containing entries of submatrix W^{v_i},

found at iteration $c' \neq c$. Another Claim follows.

Claim 5.2. *Let $j' \neq j$, then, after calls* SparseSub(W_j, U_c) *and* SparseSub$(W_{j'}, U_{c'})$, *rows $W_j, W_{j'}$ are orthonormal.*

Proof. Once edited, $W_j, W_{j'}$ take as non-zero entries the entries from, respectively, $U_c, U_{c'}$. Moreover, because they contribute to the same independent full submatrix, the positions of the non-zero entries of $W_j, W_{j'}$ coincide. Then,

$$\langle W_{j'} | W_j \rangle = \langle U_{c'} | U_c \rangle = 0.$$

□

In turn, once Line 6 of Unitarize has iterated through $\delta^-(v_i)$, the two claims ensure independent full submatrix W^{v_i} to be unitary. The loop at Line 4 allows to repeat the procedure for all remaining vertices/columns. By definition of independent full submatrix, rows/columns of submatrices $W^{v_i} \neq W^{v_j}$ share no non-zero entries. This implies unitarity of W after exiting loop at Line 4.

Finally, let us investigate the effects of Line 9 of Unitarize. Operating on submatrix W^{v_i}, in-neighborhood $\delta^-(v_i)$ is removed from Q, as all rows of these vertices have been unitarized. Let $v_k \in V$ with $\delta^-(v_k) = \delta^-(v_i)$ be a vertex chosen later on by loop at Line 4. This, in turn, implies $W^{v_i} = W^{v_k}$. Removing $\delta^-(v_i)$ from Q prevents the same submatrix to be re-constructed all over, and guarantees each row W_j, with $v_j \in \delta^-(v_i)$, is operated upon one single time. It immediately follows that Unitarize performs in $\mathcal{O}(|V|^2)$ time. Translated in terms of the Eulerian multigraph $\mathcal{G}'$ from the encoding : $\mathcal{O}(|\mathcal{E}'|^2)$.

Lastly, preconditions for function Unitarize subtly differ depending on whether G is a general specular, strongly quadrangular graph or a strongly quadrangular line graph. More specifically, the latter case allows matrices in $\mathcal{U}_G$ to present zero entries. This stems from the different interpretation the two cases give to "lie on a vertex v". Whereas for a general graph the meaning is literal, in the case of a line graph to "lie on vertex v" means "having just traversed edge v" (vertices in the line graph are edges from the original graph). Thus, a zero entry in the first case would fail to encode some edge $(u, v) \in E$. In the second case, however, $W_{u,v} = 0$ would simply prevent v to be traversed right after edge u. Nonetheless, because W is unitary, there must be some non-zero entry at column $W_{,v}$ ensuring that v may be traversed.

Let us provide an example to elucidate this last remark as well as the entire workings of Unitarize.

Example 5.1. Let $G = (V, E)$ be a specular, strongly quadrangular graph. In preparation for the playground of function Unitarize, let us define matrix $W = M(G)$ and the set $\mathcal{U}_G = \{U, U'\}$, where

$$W = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}; \quad U = \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} \\ \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} \\ \alpha_{3,1} & \alpha_{3,2} & \alpha_{3,3} \end{pmatrix}; \quad U' = \begin{pmatrix} \beta_{1,1} & \beta_{1,2} \\ \beta_{2,1} & \beta_{2,2} \end{pmatrix}.$$

To begin with, set $Q = \{v_1, v_2, v_3, v_4, v_5\}$ is prepared. Let v_1 be the first chosen vertex at the while loop from Line 4. Let us follow the evolution of both set Q and matrix W.

$$Q = \{v_1, v_2, v_3, v_4, v_5\} \qquad Q = \{v_1, v_3, v_4, v_5\} \qquad Q = \{v_1, v_3, v_5\}$$

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ \mathbf{1} & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ \mathbf{1} & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \xrightarrow{\textsc{SparseSub}(W_2, U_1')} \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ \beta_{1,1} & 0 & \beta_{1,2} & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ \mathbf{1} & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \xrightarrow{\textsc{SparseSub}(W_4, U_2')} \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ \beta_{1,1} & 0 & \beta_{1,2} & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ \beta_{2,1} & 0 & \beta_{2,2} & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

In the first representation of W, bold notation is used to highlight in-neighbours of v_1. These fully determine submatrix to be unitarized. The process is initiated with $\textsc{SparseSub}(W_2, U_1')$. Apart from turning the first row into a unit vector, the call removes v_2 from Q. Thus, the second call $\textsc{SparseSub}(W_4, U_2')$ completes the opera and removes v_4. Let us emphasize that, were v_3 to be extracted first, the situation up to this point would be equivalent. The remaining steps to be performed by function Unitarize are left to the reader.

Now, suppose U' to be the identity matrix, *i. e.*, $\beta_{1,1} = \beta_{2,2} = 1$ and $\beta_{1,2} = \beta_{2,1} = 0$. Such choice for U' is clearly troublesome, as the quantum walk W would fail to encode edges $(v_2, v_3), (v_4, v_1) \in E$. Now, assume G to be the line graph of some other graph H instead. Then, Q contains edges of H. For the sake of clarity, let us relabel its elements as $Q = \{e_1, e_2, e_3, e_4, e_5\}$. Since $M(G)_{2,3} = 1$, e_2, e_3 are consecutive edges. However, because $W_{2,3} = \beta_{1,2} = 0$, e_3 may not be traversed right after e_2. Though, because U' is unitary, there must be a non-zero entry on the second column of U' (third of W) ensuring that e_3 may somehow be traversed. Because this holds for any column, it follows that, were G to be a line graph, matrices U, U' may be allowed to contain zero entries.

Newly added edges are off limits As previously stated, function $\textsc{Eulerify}(\mathcal{G}, b)$ may invasively influence the topology of G. Whereas some edges are simply duplicated by Eulerify, the main problem stems from those edges the function creates from scratch. More formally, all edges $(u, v) \in \mathcal{E}_\perp$ such that $(u, v) \notin \mathcal{E}$. As a consequence, the underlying graph $\overrightarrow{\mathcal{G}'}$ of quantum walk W includes vertices that did not originally exist.

Despite seemingly critical, the problem is effectively solved through the use of a projector P_G. Formally,

$$P_{\mathcal{G}} = I - \sum_{e \in \mathcal{E}_\perp} |e\rangle \langle e| . \tag{5.2}$$

Given any superposition of vertices in $\overrightarrow{\mathcal{G}'}$, $P_{\mathcal{G}}$ projects it on the subspace spanned by vertices in $\mathcal{E}$, the orthogonal component of $\mathcal{E}_\perp$. Alternating operators W and $P_{\mathcal{G}}$ gives rise to a quantum walk that respects the adjacencies of the original graph $\mathcal{G}$.

In this regard, the authors of [5] also hint to an alternative solution free of projectors. Under restriction to strongly connected graphs, the problem of editing a graph to a Eulerian one is equivalent to the *Directed Chinese Postman Problem* (DCPP). Solutions to DCPP encode strongly connected graphs to Eulerian ones through mere edge duplication, thus clearing out any reliance on projectors. Moreover a solution is computed in polynomial time.

5.2 Reversible graphs with self-loops to regular multigraphs

Section 4.3 covered part of the work proposed by Montanaro in [12], culminating in the proof of Theorem 7. This section completes the job, demonstrating all reversible graphs with self-loops to be amenable to coined quantum walks.

In light of the results given in Chapter 4, it should be of no surprise that, in order to define a coined quantum walk on a reversible graph with self-loops, this needs be encoded. Briefly justifying the statement, let us emphasize that reversibility does not provide enough structure to define a quantum walk on either the given graph or its line graph.

Before introducing the encoding, a couple of preliminary notions are due.

Definition 5.1 (Weak 1-factorization)**.** Let $G = (V, E)$ be a graph. A *weak 1-factorization* of G is a set $F = \{P_1, P_2, \ldots, P_k\}$, where, for any $1 \leq i, j \leq k$, P_i is a 1-factor of G, and, if $i \neq j$, P_i, P_j are edge disjoint. In a weak 1-factorization, each $(u, v) \in E$ occurs at least once.

A 1-Factorization and a *weak* 1-factorization differ in that the latter allows for edges to occur in more than one 1-factor. Whereas 1-factorizations provided with a convenient decomposition of regular multigraphs, *weak* 1-factorizations do so with respect to reversible graphs with self-loops.

Lemma 5.1. *Let $G = (V, E)$ be a reversible graph with self-loops. Then G admits a weak 1-factorization.*

Proof. Because G is reversible, for any edge $(u, v) \in E$, there exists a path from v to u. Concatenating the path with edge (u, v) gives a cycle. Obviously, the cycle may not span all vertices of G. However, all other vertices w are always spanned by at least one cycle, *i.e.,* (w, w). Combining the cycle to the self-loops gives a 1-factor.

Repeating the process for all $(u, v) \in E$ provides a weak 1-factorization. □

The following remark aids the illustration of the encoding.

Remark 5.1. A 1-factor is a mapping from vertices to edges. Because a 1-factor is a 1-regular spanning subgraph, each vertex is mapped onto its unique outgoing edge. However, for a given weak 1-factorization, there may be two distinct 1-factors mapping a vertex to the same edge.

Let us introduce the encoding procedure which is here framed as proof of the following theorem.

Theorem 10. *[12] Let $G = (V, E)$ be a reversible graph with self-loops. Then it is possible to define a coined quantum walk on G.*

Proof. As usual, to the position of the particle is associated Hilbert space $\mathbb{C}^n$, with $n = |V|$.

As for the coin, let us first observe that, by Lemma 5.1, G admits weak 1-factorization $\mathcal{C}_G = \{P_1, P_2, \ldots, P_k\}$. The idea is to assign each permutation a face/state of the coin. To this end, the coin is associated Hilbert space $\mathbb{C}^k$.

Let C be an arbitrary unitary operator on $\mathbb{C}^k$ chosen as the coin. Then, shift operator T should, ideally, apply the permutation determined by the state of the coin. That is,

$$T \left|P_i\right\rangle \left|u\right\rangle \equiv \left|P_i\right\rangle \left|v\right\rangle ,$$

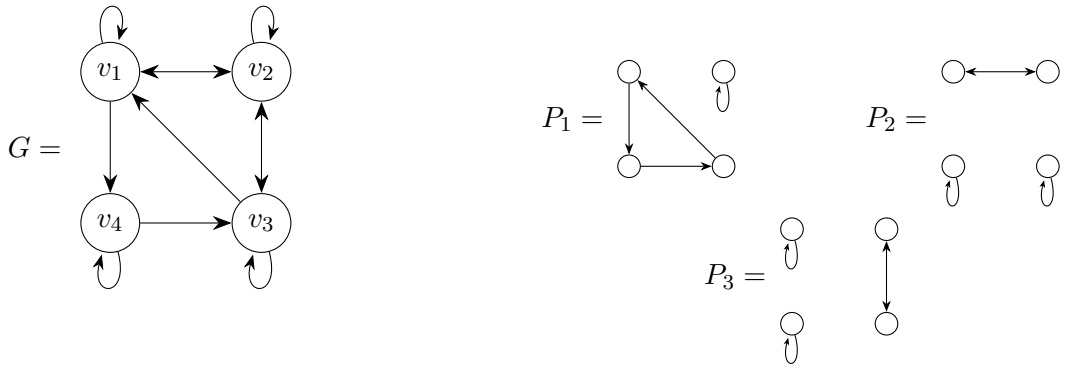


Figure 5.1: Reversible graph with self-loops and its weak 1-factorization.

where $(u, v) \in P_i$. T is a bijective mapping on the orthonormal basis of $\mathbb{C}^k \otimes \mathbb{C}^n$ and, thus, unitary. Moreover, it may be calculated as

$$T = \bigoplus_{i=1}^{k} M(P_i). \tag{5.3}$$

Finally, this allows to define the coined quantum walk $W = T(C \otimes \mathbb{I}_{\mathbb{C}^n})$. □

With the help of an example, let us elaborate on the kind of quantum walk assembled by this procedure. Figure 5.1 displays a reversible graph $G = (V, E)$ with self-loops and its weak 1-factorization $\mathcal{C}_G = \{P_1, P_2, P_3\}$.

To begin with, the coin quantum system is to be defined. According to $\mathcal{C}_G$, to the coin is associated Hilbert space $\mathbb{C}^3$, with orthonormal basis $\{|P_1\rangle, |P_2\rangle, |P_3\rangle\}$.

It is convenient to postpone details over the adopted coin operator C and prioritize the definition of shift operator T instead. Following the instructions provided by Equation (5.3) results in matrix

$$T = \begin{pmatrix} M(P_1) & & \\ & M(P_2) & \\ & & M(P_3) \end{pmatrix}. \tag{5.4}$$

T is a block diagonal matrix, each block being a 1-factor of $\mathcal{C}_G$. Given any state $|P_i\rangle |u\rangle$, T proceeds by applying permutation P_i onto u. In graph theoretical terms, u is mapped to v, such that edge $(u, v) \in P_i$. The resulting state is, thus, $|P_i\rangle |v\rangle$.

Finally, let us elaborate on coin operator C. Given state $|P_i\rangle |u\rangle$, C tosses a coin to determine the permutation states. By Remark 5.1, this is equivalent to a coin toss over the outgoing edges of u.

The CQW is all set, though the title of this section still remains unjustified: no regular multigraph has been involved in the discussion. In this regard, let us consider a weak 1-factorization decomposing a reversible graph. By Lemma 4.7, it immediately follows that summing all k 1-factors gives the adjacency matrix of a k-regular multigraph. More formally, *any weak 1-factorization of cardinality k is a 1-factorization of a k-regular multigraph.*

In a sense, the procedure proving Theorem 9 implicitly encodes a reversible graph with self-loops in a regular multigraph. Figure 5.2 displays the regular multigraph resulting from the encoding on G from Figure 5.1. Edge (v_4, v_4) has been implicitly duplicated.

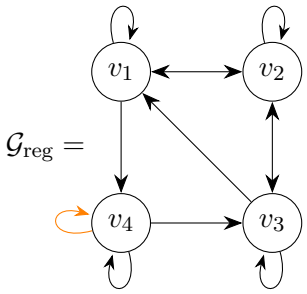


Figure 5.2: Reversible graph encoding to regular multigraph.

Finally, observe that the coined quantum walk defined as proof of Theorem 10 is exactly the same as the one defined as proof of Theorem 9, leading to the following corollary.

Corollary 5.1. *Let G be a reversible graph with self-loops and $\mathcal{G}^{reg}$ be the regular multigraph induced by the weak 1-factorization $\mathcal{C}_G$ on G. The coined quantum walk on G induced by $\mathcal{C}_G$ is performed on $\overrightarrow{\mathcal{G}^{reg}}$.*

5.2.1 Irreversible graphs to reversible

Thus far, our findings have provided us with a procedure to construct CQWs on reversible graphs with self-loops. It has been observed that, behind the assembly of the CQW, lies an encoding of the reversible graph at hand to a regular multigraph. On the other hand, the assumption that the graph be equipped with self-loops may itself be considered an encoding. The encoding treated in this section was also introduced by Montanaro in [12], and somewhat lies one step before these two, as it allows for a transformation of irreversible graphs into reversible ones. Let us provide an overview.

Let $G = (V, E)$ be an irreversible graph. Then, by Definition 4.12, there exists a set $I \subseteq E$ of irreversible edges. Let $G^{\text{rev}} = (V, E \backslash I)$ be the same graph, albeit with all irreversible edges being removed. Removing irreversible edges does not affect reversibility of other edges. By contradiction, were any reversible edge (u, v) to become irreversible after removing irreversible edge $(w, z) \in I$, it would follow that the only path from u to v traversed (w, z). However, this would lead to contradiction as $(w, z) \notin I$. It follows that G^{rev} is reversible.

In turn, the result also ensures a partition of G into reversible components that are connected by irreversible edges. To see why this is the case, let C_i be any connected component of G^{rev}. Because in building G^{rev} no reversible edges were removed, by the previous result, C_i is a reversible - or, equivalently, strongly connected - component of G. Thus, C_i cannot include any irreversible edge (u, v) with both $u, v \in C_i$. It follows that all irreversible edges must connect distinct reversible components.

These two results suggests that one could, in theory, define a separate CQW for each reversible component, albeit leaving uncertainty on how to deal with irreversible edges. Rather pleasantly, irreversible edges shall be simulated by the single irreversible operation Quantum Mechanics provides us with: measurement.

Let us assume all reversible components $\{C_1, C_2, \ldots, C_D\}$ have been found. Their union taking shape into the graph $G^{rev} = (V, E \backslash I)$. Now, consider the irreversible edge $(u, v) \in I$. Because irreversible edges always link different reversible components, $u \in C_i, v \in C_j$ for $i \neq j$. In defining a CQW on C_i,

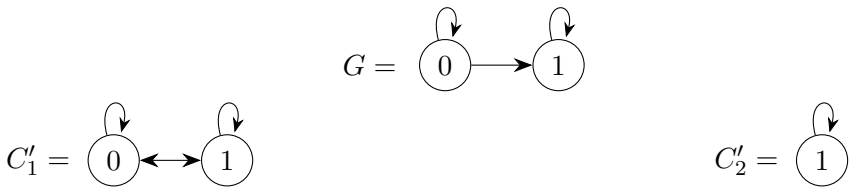


Figure 5.3: Partition of an irreversible graph into its augmented reversible components.

the Hilbert space associated to the position of the particle would exclude $v \in C_j$. Let us then augment C_i into the component C'_i, such that $v \in C'_i$. A consequential issue is then the irreversibility of C'_i: edge (u, v) is irreversible. Let us patch it by adding the opposite edge (v, u). However, because $(v, u) \notin E$, the CQW W_i on C'_i should be prevented from traversing this edge. To this end, a projective measurement operator M is devised, one that, upon superposition between vertices of C_i, C_j, has the particle collapse to one of the components. M would be of the form

$$M = \sum_{i=1}^{D} i\, P_i, \quad \text{where } P_i = \sum_{v \in C_i} |v\rangle \langle v| . \tag{5.5}$$

Through the statements of Postulate 3, to measure i is to measure the particle in the strongly connected component C_i. Thus, were outcome i to occur, the quantum walk would be continued via application of operator W_i. Naturally, the next step could again traverse an irreversible edge. That being the case, CQW operators W_i and measurement M need be alternated.

Example 5.2. Consider the irreversible graph $G = (V, E)$ from Figure 5.3. G presents two reversible components, their augmented form is also visualized. Whereas C'_2 did not bear any alterations, C'_1 has been augmented with edge (v_2, v_1). Even without observing the cycle decomposition of the two components, one can immediately define the CQW they induce via the procedure illustrated in Section 5.2.

Assuming to use Hadamard operator H as the coin for W_1, let us encode its two faces as $|\mathtt{S}\rangle$ (*i.e., stay*) and $|\mathtt{M}\rangle$ (*i.e., move*), as the two cycles of C'_1 encode, respectively, these two actions. Thus, W_1 may be defines as

$$W_1 |\mathtt{S}\rangle |x\rangle = \frac{|\mathtt{S}\rangle |x\rangle + |\mathtt{M}\rangle |x \oplus 1\rangle}{\sqrt{2}}; \qquad W_1 |\mathtt{R}\rangle |x\rangle = \frac{|\mathtt{S}\rangle |x\rangle - |\mathtt{M}\rangle |x \oplus 1\rangle}{\sqrt{2}},$$

where $x \in 0, 1$ and $'\oplus'$ denotes addition modulo 2. On the other hand, clearly, $W_2 = \mathbb{I}$. Finally let $M = 1\,|0\rangle \langle 0| + 2\,|1\rangle \langle 1|$.

Suppose to start the quantum walk on G in state $|\psi(0)\rangle = |\mathtt{S}\rangle |0\rangle$. Measurement M gives outcome 1 with probability one, the first step is does walked via W_1:

$$|\psi(1)\rangle = \frac{|\mathtt{S}\rangle |0\rangle + |\mathtt{M}\rangle |1\rangle}{\sqrt{2}}.$$

There is now probability 1/2 for the particle to collapse at either of the two components. Suppose outcome 2 to occur, the state of the walk thus becomes $|\psi(1)'\rangle = |1\rangle$. Applying W_2, $\mathbb{I}\,|1\rangle = |1\rangle$.

After step 1, the particle from Example 5.2 will forever wander inside C'_2. Indeed, any CQW of this

kind will eventually get stuck inside a sink reversible component. Ideally, once the particle is measured to be in one such component, the projective measurement operator may be safely removed from the discussion. However, there would be no way to know, in general, at which step this happens.

5.3 On edge-addition based encoding procedures

The two encoding procedures reviewed throughout the chapter do not appear too dissimilar. Indeed, both rely on either addition and duplication of edges to meet the requirements introduced at Chapter 4. Although a thorough comparison is out of the scope of this section, it is only fair to provide a few observations on the features that distinguish an encoding from the other.

The encoding procedure to regular multigraphs inherits a main trait of coined quantum walks: the arbitrary choice over the coin operator which, in turn, provides solid control on the global behaviour of the walk. Further studies could attempt at extending the feature to local control through the use of multiple coins. In contrast, via definition of independent full submatrices, the encoding procedure to Eulerian graphs provides local control. On this matter, investigations should be conducted, verifying to which extent this difference is significant. As Chapter 6 shall elucidate, regardless of the adopted procedure, local and global control over the behaviour of the walk are both skewed by phenomena of local bias.

On a different matter, the encoding procedure to Eulerian graphs enjoys the advantage of operating on Hilbert spaces of lower dimensionality. This quality stems from the lower amount of edges required to satisfy Eulericity with respect to regularity.

In conclusion, a paragraph on the fundamental role of projectors is due. In either encoding procedure, use of projectors is inevitable whenever restrictions on strongly connected graphs fall. The restriction seems to be inherent of the reversible nature of quantum computation. Indeed, Lemmata 4.5 and 4.6 hinted to a deeper connection between reversible - and, thus, strongly - connected graphs and the property of reversibility of unitary operators (in the latter case, reversibility is to be understood as given in Postulate 2). Further work could aim at formalizing the relation, integrating the role of projectors.

5.4 A conceptual summary

As the reader might have noticed, the relationship shared by graphs and unitary matrices is an intricate one. Encoding procedures, on the other hand, hardly make it any clearer. In an attempt to break these intricacies down, Figure 5.4 provides a diagram summarizing all results illustrated throughout Chapters 4 and 5. A solid line represents a logical implication, the direction of which is described by an arrow. Dashed lines represent encoding procedures instead.

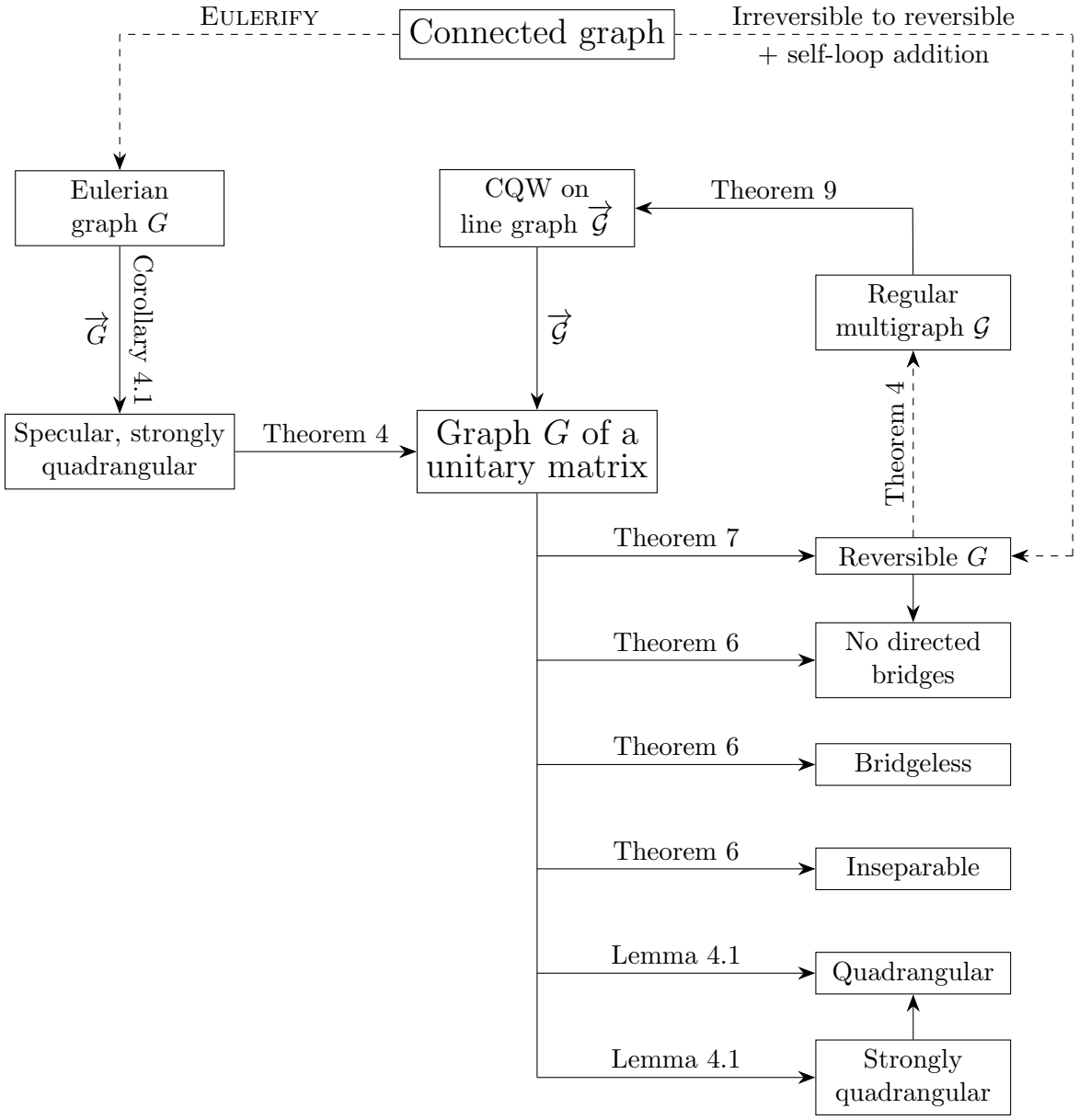


Figure 5.4: Summary of the relationship between graphs and unitary matrices.

6

Encoding bias

Chapter 5 has run through two forms of encoding that allow for the definition of quantum walks on graphs far from those of unitary matrices. Both encoding procedures have been shown to rely on edge-addition and, upon restriction to strongly connected graphs, on mere edge-duplication. Newly added edges are clearly problematic in that they alter the original graph topology. In this chapter however, focus lies on the more subtle impact caused by duplicated edges. Indeed, these appear to affect the resulting quantum walks with effects of local bias. That is, there exist vertices from which an out-neighbour is more likely to be reached than others. This phenomenon is here referred to as *encoding bias*. Which are the conditions that lead to encoding bias? In which way can it be mitigated? These are the questions this chapter attempts to shed light on.

6.1 Defining the problem

Before diving any deeper, let us fully elaborate on what encoding bias is. Figure 6.1 displays an example. A Eulerian graph $\mathcal{G}'$ produced by function EULERIFY (see Algorithm 2) is shown together with its line graph $\overrightarrow{\mathcal{G}'}$. The edge added by EULERIFY is highlighted in orange. Edges have been numbered so to identify them in $\overrightarrow{\mathcal{G}'}$.

Let W be a quantum walk on $\overrightarrow{\mathcal{G}'}$, where

$$W = \begin{pmatrix} & & & \beta_{1,1} & \beta_{1,1} & \beta_{1,1} & \\ & & & \beta_{2,1} & \beta_{2,2} & \beta_{2,3} & \\ \alpha_{1,1} & \alpha_{1,2} & & & & & \\ & & 1 & & & & \\ \alpha_{2,1} & \alpha_{2,2} & & & & & \\ & & & & & & 1 \\ & & & \beta_{3,1} & \beta_{3,2} & \beta_{3,3} & \end{pmatrix}.$$

Now, suppose the particle to lie in state $|i\rangle$, where $i \in \{4, 5, 6\}$. Translated to $\mathcal{G}'$, these states all describe the particle as lying on vertex v_1. In performing a step according to W, the operation is fully determined by the green submatrix. Thus, evolution gives state

$$|\psi\rangle = \beta_{1,i} |1\rangle + \beta_{2,i} |2\rangle + \beta_{3,i} |7\rangle .$$

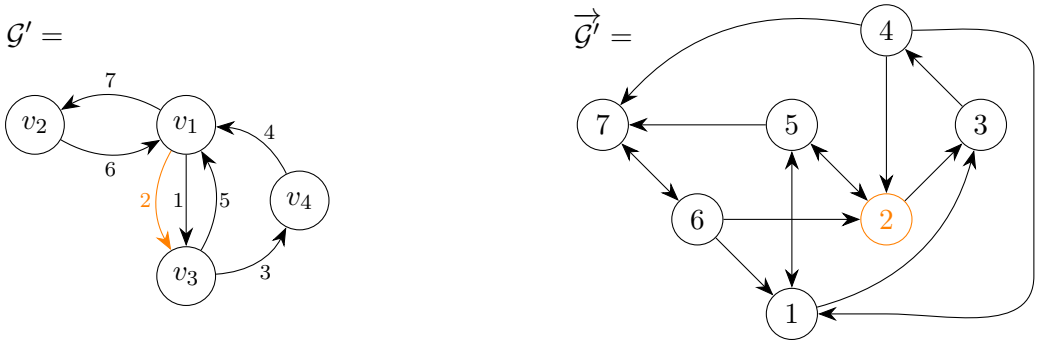


Figure 6.1: Graph encoding to Eulerian and respective line graph.

where states $|1\rangle, |2\rangle$ both represent the particle as laying on vertex v_3, and $|7\rangle$ on v_2. Vertex v_1 was originally connected to both v_2 and v_3 via a single edge. Supposing not to rely on projectors, one would reasonably wish to define the green submatrix so that state $|\psi\rangle$ induced equal probability for the particle to lie at either vertices v_2, v_3. That is, $|\beta_{1,i}|^2 + |\beta_{2,i}|^2 = |\beta_{3,i}|^2$. However, a submatrix of this kind would, clearly, not be unitary. It follows that, independently of the definition of W, steps from vertex v_1 shall be affected by encoding bias. Lemma 6.1 makes this precise in the general case.

Lemma 6.1. *Let $\mathcal{D}$ be a probability distribution on n events different from the uniform distribution. Then, there exists no unitary matrix U operating on $\mathbb{C}^n$ that induces $\mathcal{D}$ independently of the input state to which U is applied.*

Proof. Assume, by contradiction, $n \times n$ unitary matrix U to exist. Because $\mathcal{D}$ differs from the uniform distribution there exists state $|k\rangle$ such that $\mathcal{D}(k) = x > 1/n$. Then, for any state $|i\rangle$ of the canonical basis, $U|i\rangle$ assigns amplitude $\sqrt{x}e^{i\theta_i}$ to state $|k\rangle$. These amplitudes make the k-th row of U. However,

$$\sum_{i=1}^{n} |\sqrt{x}e^{i\theta_i}|^2 = \sum_{i=1}^{n} |\sqrt{x}|^2 |e^{i\theta_i}|^2 = \sum_{i=1}^{n} x > 1$$

That is, the k-th row of U is no unit vector, contradicting unitarity of U. □

Lemma 6.1 implies encoding bias to be independent of the definition of the quantum walk. Instead, it is inherent of the encoding procedure applied to the graph.

Function Eulerify was here taken as a mere example. Indeed, encoding bias appears to affect both edge-addition based encoding procedures introduced so far. Let us recall Figure 5.2 to provide an example as to how encoding bias affects encoding from reversible graphs to regular multigraphs. Turning the attention on vertex v_4 from $\mathcal{G}^{\text{reg}}$, two faces of the coin cause the particle to stay idle. On the other hand, only a single outcome leads the particle to head towards v_3. In turn, Lemma 6.1 implies that, in coined quantum walks, *no biased coin can balance the unfair behaviour emerging from its outcomes.*

6.2 Graphs subject to encoding bias

Section 6.1 has hinted to the fact that, in order to study encoding bias, one should primarily focus on either the encoding procedure or the graph under consideration. This section shall deal with the latter,

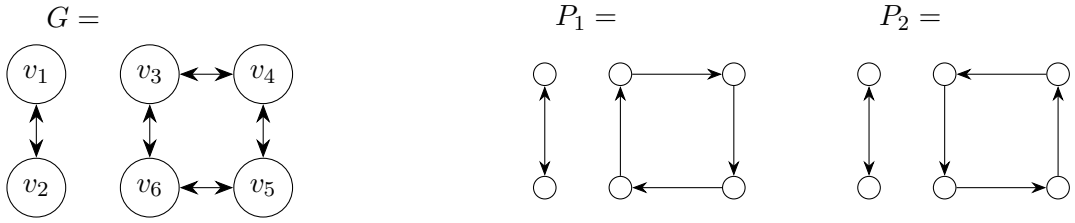


Figure 6.2: Graph with no 1-factorization allowing for the definition of a quantum walk free of encoding bias.

providing an analysis of which graphs inevitably lead to encoding bias, according to the encoding from reversible graphs to regular multigraphs.

Let us approach the problem by first observing which graphs certainly *do not* give rise to encoding bias. As it turns out, our very first definition of coined quantum walks (see Section 3.3) relied on a class of graphs that, indeed, is not subject to the phenomenon: regular graphs. A CQW on a k-regular graph assigns each outgoing edge from a given vertex a single coin face. Thus, it suffices to choose an unbiased coin to construct an unbiased walk. Unsurprisingly, were one to adopt the encoding procedure to regular multigraphs on a regular graph, the resulting CQW would be equivalent. To make this statement more precise, by Lemma 4.7, a regular graph always admits a 1-factorization. That is, a k-regular graph may be decomposed in a set of k directed spanning cycles, where each edge occurs exactly once. Exclusively because of this last observation, can the CQW assign exactly one coin face to each edge.

In light of these considerations, one may reasonably conjecture the presence of a 1-factorization (or equivalently, regularity) to be both a sufficient and necessary condition for a graph to be free of encoding bias. Unfortunately, the following remark immediately shatters our hopes.

Remark 6.1. There are graphs that do not admit 1-factorization over which it is possible to define quantum walks with no encoding bias.

In support of the remark is graph G displayed in Figure 6.2. G is clearly irregular since $d^+(v_1) \neq d^+(v_4)$. However, its weak 1-factorization does not induce encoding bias. Despite edges $(v_1, v_2), (v_2, v_1)$ occurring twice, it is still the case that, for any $v \in V$, the outgoing edges of v all occur the same number of times. It follows that the faces of the coin may be equally assigned among the edges.

Clearly, a condition coarser than that posed by 1-factorizations is required. On the other hand, such loosening process needs be done with care, as weak 1-factorizations have been shown to induce encoding bias. Ideally, such condition would lie in the middle: allowing edges to occur differently in a factorization, though objecting whenever these depart from the same source vertex. Let us introduce the notion of *locally fair, weak 1-factorization.*

Definition 6.1 (Locally fair, weak 1-factorization)**.** Let $G = (V, E)$ be a graph and let $\mathcal{L} = \{P_1, P_2, \ldots, P_k\}$ be a multiset, where, for any $1 \leq i \leq k$, P_i is a 1-factor of G. Then, $\mathcal{L}$ is said to be a *locally fair, weak* (LFW) *1-factorization* if and only if, for any $(u, v) \in E$, (u, v) occurs in $\mathcal{L}$ at least once and, for any $u \in V$, all edges $(u, v) \in E$ occur in $\mathcal{L}$ the same number of times.

Because encoding bias is a local phenomenon, one reasonably demands for local fairness to cancel it. In requiring that, for a given vertex, all outgoing edges be occurring the same number of times, an

LFW 1-factorization fully meets the requirement. Using similar words, one could, in contrast, say that 1-factorizations require *global fairness.*

The following Claim aims at generalizing the case described by the example in Figure 6.2.

Claim 6.1. *Let G be a graph of p disconnected regular connected components $\{C_1, C_2, \ldots, C_p\}$. Then G admits a LFW 1-factorization into $\mathsf{lcm}(\{d(C_i)\}_{i=1}^{p})$ 1-factors, where lcm denotes the least common multiple.*

Proof. By induction on the number of connected components p. If $p = 1$, then G is a k-regular graph with 1-factorization. Because $\mathsf{lcm}(k) = k$ the result follows.

For $p > 1$, let G be a graph of p disconnected components. Removing any single connected component C_p gives the graph G' of connected components $\{C_1, C_2, \ldots, C_{p-1}\}$. By inductive hypothesis, G' has LFW 1-factorization $\mathcal{L}' = \{P_1, P_2, \ldots, P_d\}$, where $d = \mathsf{lcm}(\{d(C_i)\}_{i=1}^{p-1})$.

Let $k = d(C_p)$, then C_p has 1-factorization $\mathcal{C} = \{Q_1, Q_2, \ldots, Q_k\}$. Because any 1-factor $Q_i \in \mathcal{C}$ is vertex-disjoint from any $P_j \in \mathcal{L}'$, it is possible to consider the factorization:

$$\mathcal{F} = \{P_1 \cup Q_1, P_2 \cup Q_2, \ldots, P_d \cup Q_d\},$$

where each edge in C_p occurs d/k times in $\mathcal{F}$.

If $d \equiv 0 \pmod{k}$, then each edge of C_p occurs the same natural number of times, and $\mathcal{F}$ is a LFW 1-factorization of G. Moreover, because k divides d, $d = \mathsf{lcm}(\{d(C_i)\}_{i=1}^{p})$. Otherwise, $\mathcal{L}'$ is duplicated a minimum number of times c, such that $cd \equiv 0 \pmod{k}$. Clearly, the resulting multiset $\{P_1, P_2, \ldots, P_{cd}\}$ is still a LFW 1-factorization of G'. A LFW 1-factorization for G is then

$$\mathcal{L} = \{P_1 \cup Q_1, P_2 \cup Q_2, \ldots, P_{cd} \cup Q_{cd}\}.$$

Because k divides cd, the 1-factors Q_i can be equally distributed among the cd spots. Moreover, by definition of c, $cd = \mathsf{lcm}(\{d(C_i)\}_{i=1}^{p})$. □

Remark 6.1 has quickly disposed of regularity as a necessary condition for graphs to prevent encoding bias. However, both proofs to its support (Figure 6.2 and Claim 6.1) appear to rely on regularity of disconnected components. A question, thus, spontaneously arises: Can a restriction to strongly connected graphs bring regularity back into discussion?[1] The question lends itself to a rephrasing: Are 1-factorizations and LFW 1-factorizations of strongly connected graphs equivalent definitions?

Despite empirical observation suggesting an affirmative answer, we are, for the time being, able to produce formal proof only for the case of strongly connected, Eulerian graphs. Only a single preliminary notion separates us from the result. The following claim also provides a chance to define the *matrix of a LFW 1-factorization.*

Claim 6.2. *Let $\mathcal{L} = \{P_1, P_2, \ldots, P_k\}$ be an LFW 1-factorization of a graph $G = (V, E)$. Then, the matrix of $\mathcal{L}$ is*

$$M(\mathcal{L}) = \sum_{P_i \in \mathcal{L}}^{k} P_i,$$

[1] It is emphasized that, according to the constructions from Sections 5.1 / 5.2, the restriction to strongly connected graphs is reasonable: one merely requires to define a quantum walk on each Eulerian/reversible connected component.

where $M(\mathcal{L})$ is such that all rows and columns sum to k and, for any row $M(\mathcal{L})_i$, all non-zero entries have same values.

Proof. The first result follows from the fact that $M(\mathcal{L})$ is the sum of k permutation matrices. Then, because for any $u \in V$ all outgoing edges from u occur the same number of times, it follows that the non-zero entries of row $M(\mathcal{L})_u$ all present the same value. □

The result is proven by contraposition.

Lemma 6.2. *Let $G = (V, E)$ be an irregular, strongly connected graph, Eulerian graph. Then G admits no LFW 1-factorization.*

Proof. Assume, by contradiction, $\mathcal{L}$ to be an LFW 1-factorization of G into k 1-factors. Let u be the vertex of lowest degree in G, where $d = d^+(u)$. Then, because G is strongly connected, there exists $(v, u) \in E$ such that $d' = d^+(v) > d$. Consider the matrix $M(\mathcal{L})$ of $\mathcal{L}$. By Claim 6.2, both rows $M(\mathcal{L})_u, M(\mathcal{L})_v$ sum up to k. Let α_u and α_v be, respectively, the values of the non-zero entries of rows $M(\mathcal{L})_u, M(\mathcal{L})_v$. Because $d' > d$, it must be the case that $\alpha_u > \alpha_v$. Now, observe column $M(\mathcal{L})_{,u}$. Since $(v, u) \in E$, $M(\mathcal{L})_{v,u} = \alpha_v$. From the fact that u is the vertex of lowest degree, there exists no $w \in V$ with $\alpha_w > \alpha_u$. However, because G is Eulerian, column $M(\mathcal{L})_{,u}$ only has d non-zero entries, one being equal to α_v. It follows that column $M(\mathcal{L})_{,u}$ may sum at most up to $k - 1$, contradicting the definition of $\mathcal{L}$. □

6.3 On the inevitability of encoding bias

Lemma 6.2 guarantees the existence of reversible graphs onto which the encoding procedure to regular multigraphs *necessarily* leads to encoding bias. Sure enough, projectors may again intervene and deal with any unwanted edges. However, were this solution to be adopted, why even bother restricting to edge-duplication in the first place?

In contrast, Lemma 6.2 is silent over the encoding procedure to Eulerian graphs. As previously suggested, one may reasonably conjecture the result to extend to general irregular graphs. At the moment, however, it is unclear how such generalization would reflect on the encoding procedure. To shed light on this matter, further studies should be conducted on the relationship between the encoding procedure to Eulerian graphs and LFW 1-factorizations.

The example given in Figure 6.1 provides a solid starting point for the analysis. Indeed, notice that merely duplicating edges 6 and 7 fixes local bias on vertex v_1. The remedy does so without affecting Eulericity or introducing local bias to other vertices. Further developments should aim at formalizing such process, investigating the existence of conditions that could prevent it from converging.

Finally, were both encoding procedures to be inevitably affected by encoding bias, a further conjecture would spontaneously arise: is encoding bias inevitable for any edge-addition based encoding procedure?

7

Conclusions and future work

Throughout the chapters of this thesis, the relationship between graphs and quantum walks has been investigated at different levels. This conclusive chapter provides a bigger-picture perspective on the topic, hinting to potential future developments.

The restrictions posed by unitarity over the class of quantum walk amenable graphs have been a leitmotif of this manuscript. Via the notion of graphs of unitary matrices, Chapter 4 has made these constraints precise. The relationship between graphs and unitary matrices turned out to be extremely involved, being characterized by a collection of properties that hardly show any connection between each other. Further studies should be conducted on the potential existence of such connections. The apparent equivalence between reversible graphs and graphs without disconnecting sets of directed bridges provides a valid starting point for the investigations. On a related matter, Severini's conjecture also deserves careful scrutiny, that is, all graphs of unitary matrices are Hamiltonian.

With the aim of eluding the aforementioned restrictions, the graph encoding procedures reviewed in Chapter 5 provide a means to transform general connected graphs into those of unitary matrices. Due to their nature, these are categorized as *"edge-addition based"* encoding procedures. On the one hand, the encoding procedure to Eulerian graphs appears to deal with Hilbert spaces of lower dimension. On the other, encoding graphs to regular multigraphs enjoys the convenient structure of coined quantum walks. Regardless of the procedure, projectors appear to be inevitable whenever dealing with non-strongly connected graphs. Such necessity is argued to stem from the reversible nature of quantum computation, as suggested by results such as Lemmata 4.5 and 4.6. Further work on this connection is due. On a related matter, research should be conducted on *non*-edge-addition based encoding procedures.

Finally, Chapter 6 has extended the discussion to the matter of encoding bias, that is, phenomena of local bias over quantum walks induced by encoding procedures. The encoding procedure to regular multigraphs has been shown to inevitably lead to encoding bias when dealing with strongly connected, irregular, Eulerian graphs. It is conjectured that the result may be generalized. Clearly, the encoding procedure to Eulerian graphs performs no action on such class of graphs, implying that, for the two encoding procedures, the classes of graphs leading to bias differ. In this regard, it is yet to be shown whether encoding to Eulerian graphs leads to encoding bias at all. Moving a step further, were both encoding procedures to inevitably induce encoding bias, one would spontaneously question whether such feature belongs any edge-addition based encoding procedure.

Bibliography

[1] Dorit Aharonov, Andris Ambainis, Julia Kempe, and Umesh Vazirani. Quantum walks on graphs. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 50–59, 2001.

[2] Andris Ambainis, Eric Bach, Ashwin Nayak, Ashvin Vishwanath, and John Watrous. One-dimensional quantum walks. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 37–49, 2001.

[3] P. Bocchieri and A. Loinger. Quantum recurrence theorem. *Phys. Rev.*, 107:337–338, Jul 1957.

[4] Andrew M. Childs. Universal computation by quantum walk. *Phys. Rev. Lett.*, 102:180501, 2009.

[5] D. Della Giustina, C. Piazza, B. Riccardi, and R. Romanello. Directed graph encoding in quantum computing supporting edge-failures. In Claudio Antares Mezzina and Krzysztof Podlaski, editors, *Reversible Computation*, pages 75–92, Cham, 2022. Springer International Publishing.

[6] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400:117 – 97, 1985.

[7] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439:553 – 558, 1992.

[8] Richard P Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6/7), 1982.

[9] Denis König. *Theorie der endlichen und unendlichen Graphen*. Springer Vienna, 1 edition, 1936.

[10] David A. Meyer. From quantum cellular automata to quantum lattice gases. *Journal of Statistical Physics*, 85(5-6):551–574, 1996.

[11] Giorgia Minello, Luca Rossi, and Andrea Torsello. Can a quantum walk tell which is which?a study of quantum walk-based graph similarity. *Entropy*, 21(3), 2019.

[12] Ashley Montanaro. Quantum walks on directed graphs. *Quantum Info. Comput.*, 7(1):93–102, jan 2007.

[13] Rajeev Motwani and Prabhakar Raghavan. *Randomized algorithms*. Cambridge university press, 1995.

[14] Ashwin Nayak and Ashvin Vishwanath. Quantum walk on the line. *arXiv preprint quant-ph/0010117*, 2000.

[15] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2011.

[16] Simone Severini. The underlying digraph of a coined quantum random walk, 2002.

[17] Simone Severini. Graphs of unitary matrices, 2003.

[18] Simone Severini. On the digraph of a unitary matrix. *SIAM Journal on Matrix Analysis and Applications*, 25(1):295–300, 2003.

[19] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2):303–332, 1999.

[20] Hasunuma T. and Shibata Y. Isomorphic decomposition and arc-disjoint spanning trees of kautz digraphs. *IPSJ SIG Notes*, pages 63–70, 1996.