Quantum Computing on Cloud-Based Processors

Unathi Skosana

April 2022

Thesis presented in partial fulfilment of the requirements for the degree of Master of Science in the Faculty of Science at Stellenbosch University

DECLARATION

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification

This thesis includes one original paper published in peer-reviewed journals or books and one unpublished publications. The development and writing of the papers (published and unpublished) were the principal responsibility of myself and, for each of the cases where this is not the case, a declaration is included in the thesis indicating the nature and extent of the contributions of co-authors.

Abstract

The noisy intermediate-scale quantum (NISQ) era refers to the current technological epoch permeated with quantum processors that are big enough (50-100 qubits) to be no longer trivially simulatable with digital computers but not yet capable of full fault-tolerant computation. Such processors provide great testbeds to understand the practical issues and resources needed to realize quantum tasks in these processors, such as quantum algorithms. Many pressing issues arise in this context that are a direct consequence of the limitations of these processors (limited number of qubits, low qubit connectivity, and limited coherence times). Hence, for near-term quantum algorithms, there is an overriding imperative to adopt an approach that takes into account, and attempts to mitigate or circumvent some of these limitations.

In this thesis, we examine realizing Grover's quantum search algorithm for four qubits on IBM Q superconducting quantum processors, and potentially scaling up to more qubits. We also investigate non-canonical forms of the quantum search algorithm that trade accuracy for speed in a way that is more suitable for near-term processors. Our contribution to this topic of research is a slight improvement in the accuracy of the solution to a graph problem, solved with a quantum search algorithm implemented on IBM Q quantum processors by Satoh et .al in IEEE Transactions on Quantum Engineering (2020). We also explore the realization of a measurement-based quantum search algorithm for three qubits. Unfortunately, the number of qubits and two-qubit gates required by such an algorithm puts it beyond the reach of current quantum processors.

Based on a recently published work with Professor Mark Tame, we also report a proof-of-concept demonstration of a quantum order-finding algorithm for factoring the integer 21. Our demonstration builds upon a previous demonstration by Martín-López et al. in Nature Photonics 6, 773 (2012). We go beyond this work by implementing the algorithm on IBM Q quantum processors using a configuration of approximate Toffoli gates with residual phase shifts, which preserves its functional correctness and allows us to achieve a complete factoring of $N = 21$ using a quantum circuit with relatively fewer two-qubit gates.

Lastly, we realize a small-scale three-qubit quantum processor based on a spontaneous parametric down-conversion source built to generate a polarization-entangled Bell state. The state is enlarged by using the path degree of freedom of one of the photons to make a 3-qubit GHZ state. The generated state is versatile enough to carry out quantum correlation measurements such as Bell's inequalities and entanglement witnesses. The entire experimental setup is motorized and made automatic allowing remote control of the measurements of each of the qubits, and we design and build a mobile graphical user interface to an provide intuitive and visual way to interact with the experiment.

Abstrak

Die ruiesende intermediêre skaal kwantum (NISQ) era verwys na die huidige tegnologiese epog deurdring met kwantumverwerkers wat groot genoeg is (50-100 qubits) om nie meer doeltreffend gesimuleer te kan word op digitale rekenaars nie, maar nog nie in staat is om volle foutverdraagsame berekening uit te voer nie. Sulke verwerkers bied baie goeie toetsplatforms om die probleme en hulpbronne mee te verstaan wat nodig is om kwantumtake soos kwantumalgoritmes in hierdie verwerkers te verwesenlik. Baie dringende kwessies ontstaan in hierdie konteks wat 'n direkte gevolg is van die beperkings van hierdie verwerkeers (beperkte aantal qubits, lae qubit konnektiwiteit en beperkte samehang tye). Daarom is daar vir naby-termyn kwantum algoritmes 'n oorheersende noodsaaklikheid om 'n benadering aan te neem wat hierdie beperkings in ag neem en pogings aanwend om sommige daarvan te versag of te omseil.

In hierdie handeling het ons ondersoek ingestel na Grover se kwantumsoekalgoritmes vir vier qubits op IBM Q supergeleier kwantumverwerkers en die moontlike opskaal na 'n groter aantal qubits. Ons ondersoek ook nie-kanonieke vorms van die kwantumsoekalgoritmes wat akkuraatheid vir spoed verhandel op 'n manier wat meer geskik is vir naby-termyn verwerkers. Ons bydra tot hierdie navorsingsonderwerp is 'n effense verbetering aan die akkuraatheid van die oplossing vir 'n grafiekprobleem opgelos met 'n soekalgoritme wat op IBM Q kwantumverwerkers geïmplimenteer is deur Satoh et al. In IEEE Transactions on Quantum Engineering (2020). Ons ondersoek ook die verwesenliking van 'n waarneming-gebaseerde kwantumsoekalgoritme vir drie qubits. Die aantal qubits en twee-qubit logikahekke wat deur so 'n algoritme vereis word plaas dit buite die bereik van huidige kwantumverwerkers.

Gebaseer op 'n onlangs-gepubliseerde navorsingsstuk saam met professor Mark Tame rapporteer ons ook 'n bewys-van-konsep demonstrasie van 'n kwantum volgordebepaling algoritme vir die faktorisering van die heelgetal 21. Ons demonstrasie bou voort op 'n vorige demonstrasie deur Martín López et al. In Nature Photonics 6,773 (2012). Ons brei uit op hierdie navorsing deur die die algoritme op IBM Q kwantumverwerkers te implimenteer met gebruik van benaderde Toffoli logikahekke met oorblywende faseverskuiwings – wat sy funksionele integriteit behou en ons instaat stel om 'n volledige faktoriseering van N = 21 te bereik met behulp van 'n kwantumstroombaan met 'n kleiner aantal twee-qubit logikahekke.

Laastens bewerkstellig ons 'n kleinskaalse drie-qubit kwantumverwerker gebaseer op 'n spontane parametriese fluoressensie ("spontaneous parametric down-conversion") bron wat gebou is om 'n polarisasie-verstrengelde Bell staat te genereer. Hierdie staat word vergroot deur die baanvryheidsgraad van een van die fotone te gebruik om kwantumkorrelasie metings soos Bell se ongelykhede en verstrengelingsgetuies uit te voer. Die hele eksperimentele opstelling word gemotoriseer en geautomatiseer sodat waarnemings van elk van die qubits deur middel van afstandbeheer gemaak kan word, en ons ontwerp en ontwikkel 'n mobile grafiese gebruikerskoppelvlak om 'n intuïtiewe en visuele manier te bied om met die eksperiment te kommunikeer.

COLOPHON

This document was typeset using XeTeX, with tufte-latex [1] which is based on Edward Tufte's *Beautiful Evidence*, and the bibliography was processed by Biblatex [2]. All visualizations in this document was done through Matplotlib [3], Inkscape [4], TikZit [5] and Yquant [6]. Robert Slimbach's Jenson Pro acts as the main font. Sans-serif text is typeset in Hermann Zapf's URW Classico and sometimes Volker Schnebel's URW DIN; monospaced text uses Raph Levien's Inconsolata.

[1] https://tufte-latex.github.io/tufte-latex/
[2] https://ctan.org/pkg/biblatex
[3] https://matplotlib.org/
[4] https://inkscape.org/
[5] https://tikzit.github.io/
[6] https://ctan.org/pkg/yquant?lang=en

"Le mieux est l'ennemi du bien."

— Voltaire, Dictionnaire philosophique

Acknowledgements

"No act of kindness, no matter how small, is ever wasted."

— Aesop, Aesop's Fables

It is to my supervisor, Mark Tame, whom I owe my deepest gratitude. I am greatly indebted for his continuous support, patience and advice, overseeing my research for the past three years. Words have a tendency to debase what their author intends to convey, be it expressions of gratitude, so I will altogether avoid undertaking such an endeavor altogether.

I would like to thank Mueletshedzi for her Herculean resolve of proof-reading an early version of the front matter of this document, companionship and all the coffee breaks, Olivia and Jacques for their charitable acts of kindness, Hjalmar for translating the abstract of this document, and listening to my ramblings down in the lab, Andre for diagnosing an interference filter used in one of the experiments here, Mr Botha for technical support down in the lab, and Khilly for being a great companion.

I would also like to extend my thanks to Taariq Surtee and Barry Dwolatzky at the University of the Witwatersrand and Ismail Akhalwaya at IBM Research Africa for access to the IBM processors through the Q Network and African Research Universities Alliance. Half of this thesis would not have come to fruition if it were not for them. This research was supported by the South African National Research Foundation, the South African Council for Scientific and Industrial Research, and the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

Most importantly, I would like to especially thank my family for their support and encouragement to pursue whatever it was I happened to be interested in, and granting me an opportunity to do so.

Contents

List of Figures

List of Tables

List of Acronyms

API application programming interface. xiv, 128, 129, 131

BBO β-barium borate. xii–xiv, 84, 85, 88, 89, 92, 93, 95, 96, 98, 100

CHSH Clauser-Horne-Shimony-Holt. xiv, 17, 86, 89

CW continuous wave. xiv, 84–86

DFT discrete Fourier transform. xiv

DOF degree of freedom. xiv, 5, 82, 83, 93–96, 109

DOFS degrees of freedom. xiv, 94, 96

ELC edge local complementation. xiii, xiv, 104, 120, 122

FPGA field-programmable gate array. xiv, 85, 104

FWHM full width at half maximum. xiv, 85, 91, 92

GHZ Greenberger–Horne–Zeilinger. xiii, xiv, 16–18, 83, 88, 97, 98, 101–103, 106, 109

GRK Grover-Radhakrishnan-Korepin. xi, xiv, 34, 35, 37, 38

GUI graphical user interface. xiii, xiv, 104, 105

HWP half-wave plate. xi, xiv, 21–23, 84–86, 88, 98–100

IF interference filter. xiv, 84, 85, 98

LG Laguerre-Gaussian. xiv, 95

LU local unitary. xiii, xiv, 52, 53, 104, 108, 119, 120

MAX-CUT maximum cut. xi, xii, xiv, 43–50, 56, 108, 112

MBQC measurement-based quantum computing. xiv, 4, 51, 52

MEF modular exponentiation function. xiv

MZI Mach-Zehnder interferometer. xiii, xiv, 5, 97–101

NISQ noisy intermediate-scale quantum. xiv, 3, 25, 26, 30, 35–37, 41–43, 50, 53, 55–57, 66, 70, 108, 109

NMR nuclear magnetic resonance. xiv, 24

NPBS non-polarizing beam splitter. xiv, 22, 84, 98

OAM orbital angular momentum. xiv, 95, 96

PBS polarizing beam splitter. xi, xiv, 22, 23, 84, 85, 97, 98

QAOA quantum approximate optimization algorithm. xiv, 50

QFT quantum Fourier transform. xii, xiv, 63, 65, 67, 69, 71, 74, 75, 80

QPE quantum phase estimation. xii, xiv, 58, 61–63, 65, 109

QST quantum state tomography. xiv, 83, 93, 100, 101, 113

QWP quarter-wave plate. xi, xiv, 22, 23, 84, 85, 98

SMF single-mode fiber. xiv, 84, 85, 98

SPDC spontaneous parametric down conversion. xiii, xiv, 82–84, 86–89, 91–99, 103

VQE variational quantum eigensolver. xiv, 50

List of Symbols

Γ Adjacency matrix.

$(a^\dagger, a)$ Photon creation and annihilation operators.

$\{\cdot,\cdot\}$ Anticommutator $\{X, Y\} = X \cdot Y + Y \cdot X$.

$d(\cdot)$ Circuit depth of argument.

$[\cdot,\cdot]$ Commutator $[X, Y] = X \cdot Y - Y \cdot X$.

$*$ Complex conjugate $(x - iy)^* = x + iy$.

$\mathbb{C}$ Field of complex numbers.

CNOT Controlled Not gate.

CPHASE Controlled Phase gate.

E Edge set of a graph.

$G = (V, E)$ Graph.

$|G\rangle$ Graph state.

$\mathcal{H}$ Hilbert space.

$\mathbb{1}$ Identity matrix.

η_i Neighborhood set of vertex i .

X, Y, Z Pauli matrices for a spin 1/2 particle..

$\mathbb{R}$ Field of real numbers.

V Vertex set of a graph.

0

Prelude

0.1 Historical footnote

"Begin at the beginning," the King said, very gravely, "and go on till you come to the end: then stop."

— Lewis Carroll, Alice in Wonderland

Two score years have passed since Richard Feynman conceived the idea of simulating quantum mechanical phenomena with a fundamentally "new kind of computer" [1]. He argued for the necessity of such a new kind of computer on the account that conventional digital computing machines were inadept at such a task; reasons being that any classical description of the quantum state of a many-particle system needed to keep track of a large number of variables, far greater in number than the size of the system:

> *"But the full description of quantum mechanics for a large system with R particles is given by a function which we call the amplitude to find the particles at $x_1, x_2, \ldots, x_R$ and therefore, because it has too many variables, it cannot be simulated with a normal computer with a number of elements proportional to R."*

He also put forth the point that the predictions of quantum mechanics, supported by numerous experimental validations to remarkable levels of accuracy[1], were incompatible with any interpretation that attempted to reconcile them within classical physics, *i.e.*, by interpreting the probabilities arising in quantum mechanics as a reflection of the observer's ignorance of the full degrees of freedom of a quantum system:

> *"If you take the computer to be the classical kind I've described so far (not the quantum kind described in the last section) and there're no changes in any laws, and there's no hocus-pocus, the answer is certainly, No! This is called the hidden variable problem: It is impossible to represent the results of quantum mechanics with a classical universal device."*

Thus it seemed to Feynman that any inquiry directed towards quantum mechanical phenomena by way of simulation, classical in its foundations, in one way or another would miss out on a full understanding of these phenomena, and that a possible way of circumvention was the full acceptance of quantum mechanics, that is, any such simulation needed to be quantum mechanical from the outset.

[1] The prediction of the value of the anomalous magnetic moment of the electron by quantum electrodynamics agrees with the experimentally measured value to more than **10** decimal figures; *i.e.* the error in the prediction is less than the ratio of the width of a human hair strand to the height of Mount Everest.

What he meant by this, was that the new kind of computer he envisaged would "itself be built of quantum mechanical elements which obey quantum mechanical laws", and he would call such a computer, a *quantum computer*[2]. To Feynman this was a *condicio sine qua non*, and to this end he said these epoch-making words:

> *"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."*

[2] Aptly named; uncharacteristically good nomenclature by a physicist.

Notwithstanding, the boldness of such an enterprise, Feynman's ideas grew in influence, and in the same decade they would reach a new zenith. In 1985, David Deutsch formulated a fully quantum mechanical model of computation [2, 3], which formalized many of the ideas that had been floating around up until that point. In particular, he showed that the operations of such a computing device subsume the operations of a conventional digital computer, but would further admit a class of operations, which exploit quantum phenomena such as superposition, interference, entanglement, and non-determinism, with no classical analogues. Deutsch's ideas on this subject had taken a slightly different trajectory; he sought for a general purpose quantum computing machine, which could be used for, but was not entirely limited to, simulating physics[3]; which meant the aforementioned phenomena would be exploited in a programmable way, analogous to the operation of a conventional digital computer. To this end, Deutsch and Josza [4] formulated a problem[4], which in principle could be solved more efficiently by quantum computation than by any classical computation, deterministic or otherwise. Thence, endeavors in this direction escalated rapidly, and soon culminated in Peter Shor's discovery of an efficient way to perform the discrete Fourier transform on a quantum computer, which he applied in his *chef-d'œuvre* [5], showing that quantum computers were, in principle, capable of efficiently computing discrete logarithms, and subsequently prime factorization of large numbers, which are both considered to be difficult problems for a classical computer.[5]

[3] Such as an analogue quantum simulator.

[4] Putting utility aside for the moment.

[5] Difficult as in, there is no known classical algorithm that can give an answer to the problem in algorithmic time that scales polynomially with the problem size.

The discoveries of Peter Shor, and their implications were a significant milestone for quantum computing as a field of study. Notwithstanding the progress that had been made thus far, there were questions yet to be answered, particularly those of a practical kind. All of the considerations hitherto were in *abstracto*, based on the hypothetical premise that such a quantum device would be operating under ideal conditions, that is, its operations would be fully coherent quantum mechanical processes, free from any errors, or, in the least negligible. In fact, the presupposition that the device would have the ability to be prepared in a coherent superposition of input states, and be kept in such a state for the duration of a computation, had been the crux in its efficiency gains. In practice this entailed precise control over the device's means, among other practical issues, which had not been addressed yet, and few things are so fatal to an ideal as its realization. One preeminent stumbling block that stood in the path towards realizing this ideal was that of decoherence, which can arise as a consequence of a quantum system, however isolated, coupling to unwanted and external degrees of freedom such as those of its surrounding environment. As a result of this external influence, over time the ability of the system to be in a coherent superposition of states is lost[6]. This is often attributed to the interaction having a preferred subset of "classical" (statistical mixtures of) states in the full Hilbert space of the system together with its environment, with the vast of majority of states effectively excluded by the interaction, in a phenomena known as environment-induced superselection [6, 7].

[6] Relaxation noise , where a system in an excited state spontaneously relaxes to its ground state, can also affect its coherence.

The time scale over which the computer remains quantum-mechanically coherent (coherence time), is of great practical importance, since it dictates the length of the longest possible quantum computation. Candidate quantum systems then (*e.g.* quantum optical systems) had relatively short-lived coherence times[7], if the effects of decoherence were left unchecked, a large-scale quantum device of such a kind would not be viable for the foreseeable future, or ever!

[7] Coherence times have much improved since then. For instance, the coherence times for superconducting qubits ranges between 50 µs to 100 µs,while for trapped-ion qubits the coherence times range between 0.2 s to 600 s [8, 9].

"There will always be rocks in the road ahead of us. They will be stumbling blocks or stepping stones; it all depends on how you use them."

— *Friedrich Nietzsche*

The advent of theoretical developments surrounding appropriate extensions of classical fault-tolerant methods, led to the discovery of quantum analogs of error detection and correction, which could, under reasonable assumptions, reduce errors introduced during a computation by the inimical effects of decoherence. These discoveries, in conjunction with the threshold theorem [10, 11] meant that, in principle, it is possible to perform a quantum computation reliably on imperfect hardware, at the cost of an overhead incurred from its fault-tolerant design (fault-tolerantly encoded states and elementary operations) in the computation, which grows polylogarithmically with the length of the computation [12]. As a result there was renewed optimism in that building a scalable and fault-tolerant quantum computer should be possible in practice. However, the overheads in the fault-tolerant methods have unforeseeably put their use far beyond reach, even for modern-day quantum computers [13].

The noisy intermediate-scale quantum (NISQ) era refers to the interregnum permeated with quantum computers that are big enough in size (50-100 qubits) to be no longer trivially simulatable with digital computers but not yet capable of full fault-tolerant computation [13]. Due to their non fault-tolerant operation and other hardware-related limitations such as inaccurate control and size, their capabilities will be limited in scope. Despite these apparent limitations, such devices have a utility that is peculiar to them. John Preskill in Ref. [13] mentions that they make for great testbeds for the investigation of many practical issues brought about by their non-ideal behaviour in a bottom-up manner. In the near-term, many algorithms with a provable quantum advantage will continue to elude realization due to their great costs in resources (number of qubits, number of two-qubit gates). As a result, there is emphasis in designing near-term algorithms in a way that is aware, and attempts to circumvent some of the limitations of near-term devices. One approach, in the way of this emphasis, is one that seeks reduction of the aforementioned resources in near-term quantum algorithms. It is in this light with which this thesis deals.

0.2 Organization

"Sometimes a scream is better than a thesis."

— *Ralph Waldo Emerson*

In broad terms, the content of this thesis is divided in two as dictated by its initial aims and objectives. The first of which, is to investigate some of the practical issues of, and study in detail, the realization of quantum algorithms on cloud-based quantum processors.

We confine our scope of study to two kinds of quantum algorithms, namely quantum search [14] and quantum factoring [5] algorithms, and their realization on IBM's quantum experience platform [15]. Here, superconducting quantum processors will be used and their performance under non-ideal operation will be quantified. Even to such a seemingly confined scope, there remains much to be studied, and this thesis comprises nothing more than a mere dint on the surface of a volumeous subject. The other half of the thesis turns towards experimental physics, with the aim of understanding how to build and optimally access a remote small-scale quantum processor. Such a small-scale quantum processor is one based on the use of photons, prepared in a state that falls under a special class of states exhibited by two-state systems called graph states, which serve as a substratum for one-way quantum computing [16]. Thus the structure of this document will be of the form[8]:

[8] This document has as its contents the Masters thesis under the title 'Quantum Computing on Cloud-Based Processors', written for the Department of Physics, Faculty of Natural sciences, Stellenbosch University, solely with the intention of earning its author a Masters degree. In effect, the author seeks to only convey the main results of his study with minimal meanderings, and does not seek to write a full-blown textbook-style thesis. Thus where ever possible the author omits some of the details, though not unnecessary per se, but simply because they have been written elsewhere with commendable diligence and erudition.

Part I: Realizing quantum algorithms on the cloud

Chapter 1 will be a preliminary chapter, partly with the aim of providing necessary background, however brief. The chief aim of this chapter will be for the sake of completeness of the document in its entirety; for a thorough introduction, many a textbook and lecture notes have been written [17–19], this chapter will be mainly comprised of their spoils. Fundamental notions of quantum mechanics such as state space, evolution and measurements will be revisited, and their relation to quantum computation summarized.

Chapter 2 transitions towards the main matter of the thesis and introduces the problem of finding a needle in a haystack *via* quantum search algorithms. This topic is first treated within the theoretical machinery of the quantum circuit model, where we review and study two instances of quantum search algorithms; Grover's search [14] and partial search [20] quantum algorithms along with related results in this regard and their implementations (and their viability thereof) on current quantum hardware. The topic is treated in a similar manner within framework of measurement-based quantum computing (MBQC), by first revisiting the simplest scenario; that of when the needle is in a four-element haystack, which naturally arises as a measurement procedure on a four-qubit graph state. Next, we consider the scenario of an eight-element search space, which contrary to the aforementioned scenario, does not arise as a measurement procedure on a well known graph state. Thence one has to work backwards from its quantum circuit model implementation; by constructing graph states for its various components, of which the most resourceful (in terms of number of qubits and two-qubit gates) is the diffusion operator, which is equivalent to a Toffoli gate (modulo single qubit gates). Thus, the graph state implementations of a Toffoli gate are explored, and their performances assessed on quantum hardware (and thus their viability thereof).

Chapter 3 presents the crown jewel of quantum computation in the form of Shor's algorithm for prime factorization [5]. We follow the path of least action, and adopt the standard textbook *modus operandi*, by first introducing the quantum phase estimation algorithm; which seeks to estimate an eigenvalue corresponding to an eigenvector of a unitary matrix, and the theoretical machinery thereof. Thereafter, we reduce prime factorization into an isomorphic problem; that of order-finding, which can be reformulated as a phase estimation problem, and thereby treated with the theoretical machinery of quantum phase estimation.

Similar to the previous chapters, we mention a selection of relatively recent realizations of Shor's algorithm. Finally, we present the main contribution of the thesis; which is a proof-of-concept demonstration of the complete prime factorization of $N = 21$, which builds upon a recent demonstration in this regard, that of Martín-López et al. in Nature Photonics 6, 773 (2012), and goes beyond this demonstration in fully factorizing $N = 21$, aided by a great reduction in resources (number of two-qubit gates) compared to the original demonstration.

Part II: Building a three-qubit one-way quantum computer

Chapter 4 endeavors towards experimentally realizing and characterizing a photonic source of entanglement which takes the form of a two-qubit Bell state where the two qubits are encoded in the polarization degree of freedom (DOF) of two photons; a nonlinear optical process that converts a single photon of higher energy, incident on a nonlinear crystal to a pair of lower energy photons, such that the total momenta and energy of the entire process is conserved. One of the consequences of the aforementioned conversation laws is that the joint polarization state of the generated pair is non-separable or entangled; it is no longer possible to describe the polarization state of one photon (qubit 1) without making reference to the state of the other photon (qubit 2), the manifestation of such an effect is the appearance of non-classical correlations for the polarization measurements of each photon [21]. An experiment that generates photons in this way is set up in the laboratory, and appropriately characterized as dictated by our aims.

Chapter 5 is dedicated to the expansion of the two qubit state from the previous chapter to three qubits, with the additional qubit encoded on the path DOF of one of the down-converted photons. The additional qubits are realized by having each photon go through a Mach-Zehnder interferometer (MZI). Effectively, the full joint state after this expansion is a linear graph state of three-qubits; a versatile source of entanglement. Once the aforementioned state is characterized, automatic wave plates and translatable mirrors are incorporated into the experimental setup, providing remote control of the measurements of each of the qubits. With accessibility in mind, we designed and built a small mobile graphical user interface (android mobile "app"), providing an interactive and visual way to remotely control our experimental setup. Through the app, one can conduct experiments of a similar nature in this thesis by the specifying measurement basis for each qubit, and subsequently retrieve the experiment data for analysis *via* the app.

Lastly, the thesis concludes with Chapter 6, which summarizes the entire body of work, and the author gives an outlook towards related future research.

0.3 Contributions

This thesis draws a significant portion of its material from earlier work in the following papers jointly written with Mark Tame:

- U.Skosana, M.Tame. "Demonstration of Shor's factoring algorithm for N=21 on IBM quantum processors". *Scientific Reports* 11, 16599 (2021).
- U. Skosana and M. Tame. "On the advantages of relative-phase Toffolis". *The Proceedings of SAIP2021, the 65th Annual Conference of the South African Institute of Physics*. (Accepted for publication)

PART I

REALIZING QUANTUM ALGORITHMS ON THE CLOUD

1

Preliminaries

"Throughout the narrative you will find many statements that are obviously nonsensical and quite at variance with common sense. For the most part these are true."

— *Robert Gilmore, Alice in Quantumland: An Allegory of Quantum Physics*

Readers acquainted with one of the main background texts [17, 18] may skip this chapter without a great reduction in their entropy; this chapter is primarily included for the sake of completeness and mainly bound up with spoils from the aforementioned texts.

1.1 Notation

We begin by introducing some notation that we will repeatedly make use of throughout this thesis. The first piece of notation is the bra-ket notation, which provides a convenient way to notationally represent vectors in a complex vector space equipped with an inner product. An element of a d-dimensional complex vector space $V = \mathbb{C}^d$, in conventional notation is typically denoted as $\vec{v}$; in bra-ket notation such an element is denoted as $|v\rangle$. The symbol $|\cdot\rangle$ denotes a ket vector, called a ket for brevity. The notation generalizes to infinite dimensional vector spaces, however, for our purposes we will only consider the former case. Sometimes, we will write $|v\rangle$ explicitly, similar to conventional vector notation as

$$|v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix}, \tag{1.1}$$

where $v_i \in \mathbb{C}$. Associated with the complex vector space V, there is a complex vector space called the dual vector space of V, and denoted by V^*. Elements of the dual vector space V^* are linear maps ϕ that associate each element in V to a number in $\mathbb{C}$, $\phi : V \to \mathbb{C}$. In bra-ket notation, the linear function ϕ is associated another symbol, which is denoted by $\langle\cdot|$, called a bra vector, or simply called a bra. The action of the linear function on a element $v \in V$, in this notation is denoted as

$$\phi_w(v) \to \langle w|\,(|v\rangle) \equiv \langle w|v\rangle\,, \tag{1.2}$$

where $\langle w|v\rangle \in \mathbb{C}$. In the case of $w \in \mathbb{C}^d$, a bra $\langle w|$ is uniquely associated with the complex conjugate transpose of the element w,

$$\langle w| = \left(|w^*\rangle\right)^\mathsf{T} = \begin{pmatrix} \bar{w}_1 \\ \vdots \\ \bar{w}_d \end{pmatrix}^\mathsf{T} = \begin{pmatrix} \bar{w}_1 & \dots & \bar{w}_d \end{pmatrix}, \tag{1.3}$$

where $*$ is element-wise complex conjugation, *i.e.* for a complex $\alpha = a + ib \in \mathbb{C}$ with $a, b \in \mathbb{R}$, and $i = \sqrt{-1}$; the complex conjugate of c is denoted by $\bar{c} = a - ib$. The symbol $(\cdot)^\mathsf{T}$ denotes the transpose, which transforms a column vector to row vector and *vice versa* with the same entries. Often, we shall write the complex conjugate transpose with a dagger $\dagger$, that is,

$$\langle \cdot| = |\cdot^*\rangle^\mathsf{T} \equiv |\cdot\rangle^\dagger . \tag{1.4}$$

Thus, for the finite-dimensional vector space $\mathbb{C}^d$, the linear map ϕ_w can take the form

$$\phi_w(v) = w^\dagger v = \langle w|v\rangle = \bar{w}_1 v_1 + \bar{w}_2 v_2 + \cdots + \bar{w}_d v_d , \tag{1.5}$$

that is, ϕ is a linear function of the components of the vector v. Since we can associate a ket $|v\rangle$, uniquely with a bra $\langle v|$, we can define an inner product on the vector space V. The inner product of two vectors $v, w \in V$ is a function that maps two vectors to a number in $\mathbb{C}$, $(\cdot, \cdot) : V \times V \to \mathbb{C}$

$$(|w\rangle , |v\rangle) = \phi_w(v) = \langle w|v\rangle = \bar{w}_1 v_1 + \bar{w}_2 v_2 + \cdots + \bar{w}_d v_d . \tag{1.6}$$

The inner product imparts the notion of orthogonality on the vector space; two vectors $v, w \in V$ are said to be orthogonal if $\langle w|v\rangle = 0$. Furthermore, the inner product imparts a notion of length on the vector space by inducing a norm $\|\cdot\| : V \to [0, \infty)$ on V. For a $v \in V$, the norm is defined in terms of the inner product as

$$\|v\| = \sqrt{\langle v|v\rangle}. \tag{1.7}$$

Subsequently, the norm imparts a notion of distance on the vector space; a distance metric $d : V \times V \to [0, \infty)$

$$\|v - w\| = \sqrt{\langle v - w|v - w\rangle}, \tag{1.8}$$

for $v, w \in V$. A vector space V equipped an inner product $(\cdot, \cdot)$ is called a Hilbert space, specially denoted by $\mathcal{H}$. The Hilbert space is where quantum states live.

1.2 Quantum mechanics

Max Planck's postulates about then mysterious spectrum of black body radiation in terms of discrete energy quanta, was the cock's crow of the physical theory we know today as quantum mechanics. Since then, quantum mechanics has achieved acclaimed status as one of the most successful physical theories in accounting for phenomena at the atomic and subatomic scales. Unsurprisingly, the theory of quantum mechanics is at the foundation of quantum computation. This sections describes the necessary and minimal background from the theory of quantum mechanics relevant for quantum computing.

1.2.1 States

The state of a physical quantum system, isolated from its immediate environment, is mathematically described by a unit vector in a Hilbert space $\mathcal{H}$[17]. The simplest non-trivial physical quantum system is a two-state quantum system, the state of such a system can preoccupy two distinct states. The state of a two-state quantum system is described by a unit vector in a two-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^2$, often, the two distinct states are denoted as $|0\rangle$ and $|1\rangle$. The states $|0\rangle, |1\rangle$ form an orthonormal basis for the Hilbert space, hence a general state $|\psi\rangle$ in such a vector space be written as,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha\begin{pmatrix}1 & 0\end{pmatrix}^{\mathsf{T}} + \beta\begin{pmatrix}0 & 1\end{pmatrix}^{\mathsf{T}}. \tag{1.9}$$

where $\alpha, \beta \in \mathbb{C}$, and we enforce the condition $|\alpha|^2 + |\beta|^2 = 1$, such that $\langle\psi|\psi\rangle = 1$. The spanning coefficients α and β are called amplitudes of states $|0\rangle$ and $|1\rangle$, respectively. Such a mathematical abstraction of a two-state quantum system is called a quantum bit or simply "qubit", analogous to the bit, which is the most basic information carrying unit of information in classical computation and can only preoccupy either one of two possible states. Similarly, a qubit is the most basic information carrying unit in quantum computation and information. In the nomenclature of quantum computation and information, the orthonormal basis $\{|0\rangle, |1\rangle\}$ is called the computational basis, and elements of this basis are called computation basis states. One of the peculiarities of a qubit, which makes it distinct from its classical counterpart is a direct consequence of Equation (1.9); which suggests that in addition to the two states $|0\rangle, |1\rangle$, such a two-state system can occupy a continuum of states that are not either $|0\rangle$ nor $|1\rangle$ but a linear combination of these states. This strange, and somehow counterintuitive property is called superposition.

The constraint $\langle\psi|\psi\rangle = 1$, which implies that $|\psi\rangle$ is a unit vector in a two-dimensional Hilbert space, gives a useful way to geometrically visualize the state of a qubit. For real numbers θ and φ, a general pure state of a qubit can be written as

$$|\psi\rangle = e^{i\gamma}\cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle, \quad 0 \le \theta \le \pi, 0 \le \varphi < 2\pi, \gamma \in \mathbb{R}.$$

The parameters θ and φ represent a point on the sphere of a ball in $\mathbb{R}^3$ with unit radius, called a Bloch sphere as shown in Figure 1.1.

The Hilbert space $\mathcal{H} = \mathbb{C}^2$ can be spanned by some other orthonormal basis other than $\{|0\rangle, |1\rangle\}$. Sometimes, it might instructive or convenient to write a general qubit state $|\psi\rangle$ in a different basis. Common bases include the Pauli-X basis denoted by $\{|+\rangle, |-\rangle\}$

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}; \quad |\pm\rangle = \left(1/\sqrt{2}, \pm 1/\sqrt{2}\right)^{\mathsf{T}},$$

and the Pauli-Y basis denoted by $\{|+i\rangle, |-i\rangle\}$

$$|\pm i\rangle = \frac{|0\rangle \pm i\,|1\rangle}{\sqrt{2}}; \quad |\pm i\rangle = \left(1/\sqrt{2}, \pm i/\sqrt{2}\right)^{\mathsf{T}},$$

where $i = \sqrt{-1}$.

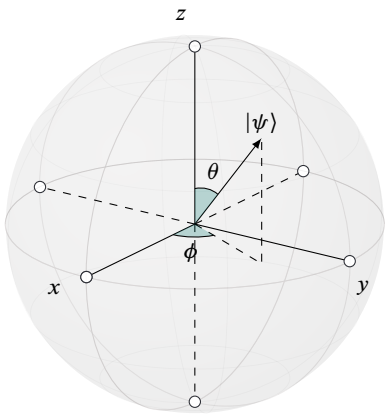


Figure 1.1: Visualization of the state of a qubit as a unit vector in $\mathbb{R}^3$

1.2.2 Evolution

A completely isolated physical quantum system is an idealization, not only that but such a system would be uninteresting, as its state will never change, and an external observer would have no way to access it which *ipso facto* would present a sizeable challenge if we ever to hope do any meaningful information processing. In reality, however, such an idealization does not hold, quantum system have dynamics and evolve over time. Mathematically, the dynamics of an isolated[1] quantum state are described by a special kind of linear operator defined on the Hilbert space of the quantum state. A linear operator $U : V \to V$ defined on the Hilbert space $\mathcal{H}$ is a linear operator such that for a general ket vector $|\psi\rangle = \sum_i \alpha_i |v_i\rangle \in \mathcal{H}$,

[1] Isolated here includes whatever is instigating the dynamics, *i.e.* a laser pulse causing a transition between energy levels of a hydrogen atom.

$$\left|\psi'\right\rangle = U|\psi\rangle = U\left(\sum_i \alpha_i |v_i\rangle\right) = \sum_i U(\alpha_i |v_i\rangle) = \sum_i \alpha_i U |v_i\rangle\,, \tag{1.10}$$

for all $|v_i\rangle \in \mathcal{H}$ and $\alpha_i \in \mathbb{C}$ and $|\psi'\rangle \in \mathcal{H}$. i.e The linear operator acts on a quantum state and maps it to another quantum state.

Hence, formally stated — the evolution of the state of an isolated quantum system over time is described by a unitary transformation [17]. That is, the state of a quantum system at the present time $|\psi\rangle$ and at a later time $|\psi'\rangle$ is described by a linear operator defined on $\mathcal{H}$. Why unitary ? Recall that we imposed the constraint that the quantum states are described by unit vectors in $\mathcal{H}$, hence it must be that $\langle\psi|\psi\rangle = \langle\psi'|\psi'\rangle = 1$ which implies that the linear map U must be preserve the norm defined on the space. Norm-preserving linear operators are called unitary operators. The inverse of a unitary operator U is the same as its complex conjugate transpose $U^\dagger$, *i.e.* $U^\dagger U = U^\dagger U = 1$ since

$$\left\langle\psi'\middle|\psi'\right\rangle = (U|\psi\rangle)^\dagger U|\psi\rangle = |\psi\rangle^\dagger U^\dagger U|\psi\rangle = \langle\psi| U^\dagger U|\psi\rangle \tag{1.11}$$

Since it must be that $\langle\psi|\psi\rangle = \langle\psi'|\psi'\rangle$, the last expression implies $U^\dagger U = \mathbb{1}$. Hence, a unitary operator U always has an inverse and hence the evolution over time of an isolated system is always reversible.

For a single qubit, unitary operators are represented by square complex matrices, and their action on a qubit can be visually presented as rotations on the Bloch sphere shown in Figure 1.1. Perhaps, the most prevalent example of such unitary operators for a single qubit are the Pauli matrices, $\sigma_x, \sigma_y, \sigma_z$ and the identity matrix $\mathbb{1}$

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_1 \equiv X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\sigma_2 \equiv Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 \equiv Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The action of each of the above gates on a general qubit state $|\psi\rangle$ are given by

$$\begin{aligned} X(\alpha\,|0\rangle + \beta\,|1\rangle) &= \alpha\,|1\rangle + \beta\,|0\rangle\,, \\ Y(\alpha\,|0\rangle + \beta\,|1\rangle) &= i(\alpha\,|1\rangle - \beta\,|0\rangle), \\ Z(\alpha\,|0\rangle + \beta\,|1\rangle) &= \alpha\,|0\rangle - \beta\,|1\rangle\,. \end{aligned}$$

Hence, the Pauli-X gate is called a NOT gate analogous to the classical NOT gate since it swaps around $|0\rangle$ and $|1\rangle$, the Pauli-Z gate is called the phase flip gate since it puts a negative phase on $|1\rangle$, and Pauli-Y gate ($Y = ZX$) gate performs both of these operators in sequence. The Pauli matrices have many useful algebraic properties:

$$\begin{aligned} \sigma_i^\dagger = \sigma_i^{-1} = \sigma_i \quad & \text{Hermitian and unitary,} \\ \{\sigma_i, \sigma_j\} = 2\delta_{ij}\mathbb{1} \quad & \text{Mutually anti-commutation,} \\ [\sigma_i, \sigma_j] = 2i\varepsilon_{jkl}\sigma_l \quad & \mathfrak{su}(2) \text{ Lie algebra.} \end{aligned}$$

where ε_{jkl} is the Levi-Civita symbol, $\{A, B\} = AB + BA$ and $[A, B] = AB - BA$ denote anti-commutator and commutator, respectively. Prominently, a single qubit rotation by angle θ around an axis $\hat{n}$ can be written as an exponential of Pauli matrices

$$R_{\hat{n}}(\theta) = e^{-i\frac{\theta}{2}\hat{n}\cdot\vec{\sigma}} = \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}(n_x X + n_y Y + n_z Z), \tag{1.12}$$

where $\hat{n} = (n_x, n_y, n_z)$ and $\vec{\sigma} = (X, Y, Z)$. Common examples of rotations are rotations around the x, y and z axes of the Bloch sphere

$$\begin{aligned} R_x(\theta) &= \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}X = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \\ R_y(\theta) &= \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}Y = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \\ R_z(\theta) &= \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}Z = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}. \end{aligned} \tag{1.13}$$

Similar to three-dimensional Euclidean space, an arbitrary qubit rotation can be decomposed into three successive rotations around two non-parallel axes $\hat{n}$ and $\hat{m}$, $\hat{n}\cdot\hat{m} \neq \pm 1$

$$U = e^{i\alpha}R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta), \quad \alpha, \beta, \gamma, \delta \in \mathbb{R}.$$

In $\mathbb{R}^3$, the angles β, γ, δ are the so-called Euler angles. Other ubiquitous and note-worthy single unitary operators are the Hadamard H, Phase S, and T gates; as matrices they are written as

$$H = R_x(\pi/2)R_z(\pi/2)R_x(\pi/2) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \qquad R_\phi = e^{-i\frac{\pi}{2}}R_z(\phi) = \begin{pmatrix}1 & 0\\ 0 & e^{i\phi}\end{pmatrix},$$
$$T = e^{-i\frac{\pi}{8}}R_{\pi/4} = \begin{pmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{pmatrix}, \qquad S = R_{\pi/2} = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}.$$

Perhaps, the most note-worthy among these is the Hadamard gate H, which operates on the basis states $|0\rangle, |1\rangle$ to give a uniform superposition of the two basis states $|+\rangle, |-\rangle$, respectively (and *vice versa*).

1.2.3 Measurements

"We cannot see the things as they are. What we do see are only the different aspects of a quantum object, the 'quantum shadows' in the sense of Plato's famous parable."

— Ulf Leonhardt, Measuring the Quantum State of Light

In addition to dynamics being a prerequisite for doing any meaningful information processing with physical quantum systems, being able to extract useful information from the system at the end of any information processing task is vital, as such information can be useful in the characterization and assessment of the success of the said information processing task. At the onset, we are confronted with the situation that the very act of measuring a quantum system by observation by however means, implies the system is no longer isolated, making the evolution of a quantum system under measurement no longer unitary.

Formally stated in the standard text [17] — quantum measurements are described by a collection $\{M_m\}$ of Hermitian operators [2], called measurement operators. The set $\{m\}$ is the set of all possible measurement outcomes that may occur in the experiment. Which outcome occurs? We can never determine in advance, but rather each outcome m occurs with a probability $p(m)$. A measurement operator describes the evolution of the system undergoing a measurement, if the state of a quantum system is $|\psi\rangle$ immediately before the measurement, then state after the measurement $|\psi'\rangle$ if the outcome m is obtained is given by

[2] A Hermitian operator $\boldsymbol{H}$ is a linear operator that is equal to its own complex conjugate transpose $\boldsymbol{H}^\dagger = \boldsymbol{H}$.

$$\left|\psi'\right\rangle = \frac{M_m\left|\psi\right\rangle}{\sqrt{p(m)}}, \tag{1.14}$$

where $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$, the denominator ensures that $\langle\psi|\psi\rangle = 1$. The probability that we will obtain an outcome whatever it may be is unity, *i.e.* $\sum_m p(m) = 1$. Hence

$$\sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle,$$
$$= \langle\psi|\sum_m M_m^\dagger M_m|\psi\rangle = 1 = \langle\psi|\psi\rangle \implies \sum_m M_m^\dagger M_m = \mathbb{1}.$$

The measurement operators are therefore said to satisfy a completeness relation. A particular example of a measurement operators we will refer to throughout this thesis, are the measurement operators of the computational basis $\{M_0, M_1\} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, corresponding to the two possible outcomes $\{0, 1\}$. On a general state written in the basis $\{|0\rangle, |1\rangle\}$,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.15}$$

the probabilities that we obtain the outcomes $m = 0$ and $m = 1$ are given by $p(0) = |\alpha|^2$ and $p(1) = |\beta|^2$, respectively. The respective states directly after measurements are given by

$$\frac{M_0|\psi\rangle}{\sqrt{p(0)}} = \frac{\alpha}{|\alpha|}|0\rangle; \quad \frac{M_1|\psi\rangle}{\sqrt{p(1)}} = \frac{\beta}{|\beta|}|1\rangle$$

The numbers $\frac{\alpha}{|\alpha|}, \frac{\beta}{|\beta|}$ corresponding to phases of the form $e^{i\theta}$ with modulus 1, and have no physical significance since they do not influence the measurement probabilities. For instance, if $|\psi'\rangle$ differs from $|\psi\rangle$ by a global phase $e^{i\theta}$, then probability of measuring an outcome m on $|\psi'\rangle$ after a measurement is given by

$$p(m) = \langle\psi'|M_m^\dagger M_m|\psi'\rangle = \langle\psi|e^{-i\theta}M_m^\dagger M_m e^{i\theta}|\psi\rangle = \langle\psi|M_m^\dagger M_m|\psi\rangle. \tag{1.16}$$

Given the ability to perform any arbitrary single qubit unitary operation together with the ability to perform a computational basis measurement, it is possible to perform a measurement in any arbitrary basis. To perform a measurement in an arbitrary basis $\{|v_0\rangle, |v_1\rangle\}$, we can first apply a unitary operator U such that $\{U|v_0\rangle = |1\rangle, U|v_1\rangle = |1\rangle\}$, and perform a measurement in the computational basis. For instance, an X basis $\{|+\rangle, |-\rangle\}$ measurement can be performed in this way by first applying the Hadamard gate H, taking $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$, respectively, then a computational basis measurement.

The measurement operators on $\mathcal{H}$, such as those of the computational basis, belong to a special class of measurement operators called projectors, and the corresponding measurements are called projective measurements [17]. Such measurement are said to be projective because their action is to project a quantum state onto a subspace of the Hilbert space. As we have seen for computational basis measurements, which project a general state onto either $|0\rangle$ or $|1\rangle$. Projective measurements are associated with Hermitian operators or observables on $\mathcal{H} = \mathbb{C}^2$; since a Hermitian operator O is also a normal operator, *i.e.* $[O, O^\dagger] = [O, O] = 0$. Hence O has a spectral decomposition

$$O = \sum_i m|v_m\rangle\langle v_m|, \tag{1.17}$$

where $m \in \mathbb{R}$ are eigenvalues corresponding to the eigenvectors $|v_i\rangle$. For a Hermitian operator O, the eigenvectors can be chosen to form complete orthonormal basis for $\mathcal{H}$, with mutually orthonormal basis states $\langle v_i|v_j\rangle = \delta_{ij}$. The action of the operators $P_m = |v_m\rangle\langle v_m|$ on quantum state is to project onto a eigenspace associated with the eigenvalue m of the Hermitian operator O, hence their name.

Choosing the measurement operators as $M_m \equiv P_m = |v_m\rangle \langle v_m|$ is a valid choice; the projectors P_m are Hermitian and satisfy the completeness relations since the basis $\{|v_m\rangle\}$ forms a complete basis for $\mathcal{H}$. Furthermore, as a consequence of orthonormality of the basis, the projectors P_m are mutually orthogonal, that is, $P_m P_{m'} = \delta_{m,m'} P_m$. The action of a projector P_m on a general state $|\psi\rangle$ is given by,

$$\left|\psi'\right\rangle = \frac{P_m |\psi\rangle}{p(m)}, \tag{1.18}$$

where $p(m) = \langle\psi|P_m|\psi\rangle$. The computational basis measurement $\{|0\rangle \langle 0|, |1\rangle \langle 1|\}$ is an example of a projective measurement, and the corresponding observable is the Pauli Z matrix. Similarly, for the X basis measurement $\{|+\rangle \langle +|, |-\rangle \langle -|\}$, the corresponding observable is the Pauli X matrix. In summary,

$$Z = 1 |0\rangle \langle 0| - 1 |1\rangle \langle 1|, \tag{1.19}$$
$$X = 1 |+\rangle \langle +| - 1 |-\rangle \langle -|. \tag{1.20}$$

Projective measurements have properties that make them appealing in an experimental scenario, for instance, we can easily calculate the expected value or mean value of the projective measurements with respect to a general state $|\psi\rangle$,

$$\begin{aligned}\mathbb{E}[O] \equiv \langle O\rangle &= \sum_m m p(m), \\ &= \sum_m m \langle\psi|P_m|\psi\rangle, \\ &= \langle\psi|\sum_m m P_m|\psi\rangle, \\ &= \langle\psi|O|\psi\rangle. \end{aligned} \tag{1.21}$$

Similarly, the statistical spread of the projective measurement or variance can be written in terms of $\langle O\rangle$ as

$$\sigma(O)^2 = \left\langle (O - \langle O\rangle)^2 \right\rangle = \left\langle O^2 \right\rangle - \langle O\rangle^2. \tag{1.22}$$

1.2.4 Multiple systems

Hitherto, in everything we have discussed we only made reference to a single quantum system, in the case of a two-state system, its state belongs to a two-dimensional Hilbert space $\mathcal{H}$. In some scenarios, we may be interested in a collective quantum system made up of n distinct physical systems with the state of each in a distinct Hilbert space $\mathcal{H}_i$, for instance the collective quantum system of multiple distinct qubits interacting amongst each other. How do we describe the collective state of a such a system? The tensor product provides a way to construct a new Hilbert space composed up of two other Hilbert spaces in a natural way [17].

If the state space of system A is the Hilbert space $\mathcal{H}_1$ and the state space of system B is the Hilbert space $\mathcal{H}_2$, then joint state space of system AB is the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$.

This Hilbert space is formed by all possible pairs of basis elements of each space of the form $\{|v_i\rangle \otimes |w_j\rangle\}$, where $\{v_i\}$ and $\{w_j\}$ is an orthonormal basis for $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Hence, the dimension of the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ is the product of the dimensions of the individual Hilbert spaces. An element of the collective Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$ is written as

$$|\psi\rangle = \sum_{i,j} \alpha_{i,j} |v_i\rangle \otimes |v_j\rangle, \tag{1.23}$$

and inner product on $\mathcal{H}_1 \otimes \mathcal{H}_2$ is defined by

$$(|v\rangle \otimes |w\rangle, |p\rangle \otimes |q\rangle) = \langle v| \otimes \langle w| (|p\rangle \otimes |q\rangle) \equiv \langle v|p\rangle \langle w|q\rangle, \tag{1.24}$$

the product of the inner products defined on each Hilbert space. For the sake of brevity whenever there is no risk of ambiguity we will write $|v\rangle \otimes |w\rangle$ as $|v\rangle |w\rangle$ or $|v, w\rangle$. The notion of constructing a larger Hilbert space to describe the state of a collective quantum system by taking the tensor product of the Hilbert spaces of each constituent system generalizes to an arbitrary number of systems. The joint state of a collective system made up of n constituent systems in the state $|\psi_i\rangle$ is given by $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

Again, returning to the two-state quantum system, consider an example of two-qubit state $|\phi\rangle \in \mathbb{C}^4$, composed of system A in the state $|\psi_1\rangle \in \mathbb{C}^2$ and system B in the state $|\psi_2\rangle \in \mathbb{C}^2$, with

$$\begin{aligned} |\psi_1\rangle &= \alpha_1 |0\rangle_1 + \beta_1 |1\rangle_1, \\ |\psi_2\rangle &= \alpha_2 |0\rangle_2 + \beta_2 |1\rangle_2. \end{aligned}$$

The joint state $|\theta\rangle$ can be constructed by taking the Kronecker product of the two states of the individual systems

$$\begin{aligned} |\theta\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle, \\ &= \alpha_1 |0\rangle_1 \otimes (\alpha_2 |0\rangle_2 + \beta_2 |1\rangle_2) + \beta_1 |1\rangle_1 \otimes (\alpha_2 |0\rangle_2 + \beta_2 |1\rangle_2), \\ &= \alpha_1\alpha_2 |0\rangle_1 \otimes |0\rangle_2 + \alpha_1\beta_2 |0\rangle_1 \otimes |1\rangle_2 + \alpha_2\beta_1 |1\rangle_1 \otimes |0\rangle_2 + \beta_1\beta_2 |1\rangle_1 \otimes |1\rangle_2, \\ &= \alpha_1\alpha_2 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \alpha_1\beta_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \alpha_2\beta_1 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \beta_1\beta_2 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \end{aligned} \tag{1.25}$$

Linear operators defined on a single Hilbert space can be extended in a similar manner; if the operators $O_1, \cdots, O_n$ are defined on $\mathcal{H}_1, \cdots, \mathcal{H}_n$ respectively, then the operator $O_1 \otimes \cdots \otimes O_n$ is defined on $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ as

$$O_1 \otimes \cdots \otimes O_n(|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle) \equiv (O_1 |\psi\rangle) \otimes \cdots \otimes (O_n |\psi_n\rangle). \tag{1.26}$$

Additionally, an operator O_i acting on a $\mathcal{H}_i$ can be extended to act on a joint Hilbert space $\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n$ by defining it as

$$\begin{aligned} O_i(|\psi_1\rangle \otimes \cdots \otimes |\psi_i\rangle \otimes \cdots \otimes |\psi_n\rangle) \equiv \\ (\mathbb{1}_1 |\psi_1\rangle) \otimes \cdots \otimes (O_i |\psi_i\rangle) \otimes \cdots \otimes (\mathbb{1}_n |\psi_n\rangle), \end{aligned} \tag{1.27}$$

which acts on the joint Hilbert space, but has a non-trivial effect only on the respective Hilbert space $\mathcal{H}_i$. Whenever there is a possibility of ambiguity, such as with single qubit rotations with a subscript, *i.e.* $R_n(\theta)$, the subscript used to denote separate Hilbert spaces will be upgraded to a superscript denoted as $R_n^{(i)}(\theta)$.

1.2.5 Quantum non-separability

In addition to the phenomena of superposition, another phenomena inherently quantum mechanical and associated with composite quantum systems is the phenomena of entanglement, and a staple of quantum advantage in many quantum information processing tasks. A joint quantum system is said to possess entanglement if its quantum state cannot be written as a product state of the states of its individual subsystems, *i.e.* non-separable — the individual subsystems are do not have a definite state, but only collectively when describe it by referencing to the state of the other subsystem.

Consider a joint Hilbert space $\mathcal{H} = \mathcal{H}_a \otimes \mathcal{H}_b$. A pure state $|\psi\rangle$ is said to be separable if it can be written as a product state of the form $|\psi\rangle = |\psi\rangle_a \otimes |\psi\rangle_b$ for $|\psi\rangle_a \in \mathcal{H}_a$ and $|\psi\rangle_b \in \mathcal{H}_b$. Similarly, a density matrix ϱ is separable if it can be written as a convex sum of product states $\varrho = \sum_j p_j \varrho_j \otimes \varrho_j$, where $p_j \geq 0$ and $\sum_j p_j = 1$ [23]. If a quantum system is not separable under the above criteria, it is said to be entangled or non-separable. A two-qubit system is the smallest system that is capable of exhibiting entanglement; the Bell states are the only maximally entangled two-qubit states.

$$\begin{aligned} \left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}\left(|0,0\rangle + |1,1\rangle\right), \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}\left(|0,0\rangle - |1,1\rangle\right), \\ \left|\Psi^+\right\rangle &= \frac{1}{\sqrt{2}}\left(|0,1\rangle + |1,0\rangle\right), \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}\left(|0,1\rangle - |1,0\rangle\right). \end{aligned} \tag{1.28}$$

Another important example of a maximally-entangled state is the three-qubit GHZ state

$$|\psi_{\text{GHZ}}\rangle = \frac{1}{\sqrt{2}}(|0,0,0\rangle + |1,1,1\rangle). \tag{1.29}$$

The above states are said to be maximally-entangled with respect to some entanglement measure. Unfortunately, there is no general-purpose measure of entanglement that fits all the sundry scenarios. We briefly outline a few ways used to characterized the presence of entanglement (albeit not true entanglement measures) in a quantum system in this thesis and refer the interested reader to the Refs. [24, 25] for a detailed treatment of this subject.

Bell-CHSH violations

Formulated by Clauser-Horne-Shimony-Holt (CHSH), the Bell-CHSH inequality imposes necessary conditions on the measured correlations from an arbitrary two-qubit state, under the local realism of classical local hidden variable theories, and shows that quantum mechanics can violate such conditions [26]. The canonical Bell-CHSH inequality asserts that, for any local hidden variable theory $|S| \leq 2$ where

$$S = E(x, y) - E(x, y') + E(x', y) + E(x', y'), \tag{1.30}$$

where x, y, x' and y' are different measurement bases and $E(x, y)$ is the corresponding correlation measurement in the joint basis x, y. If the $E(x, y)$ are quantum correlations, then quantum mechanics violates the aforesaid condition achieving a possible maximum of $|S| = 2\sqrt{2}$. The description in Ref. [27] et al. derives sufficient and necessary conditions on quantities derived from an arbitrary two-qubit state for a violation of a Bell-CHSH inequality, such conditions are derived by way of measuring correlations of this kind on the density matrix ϱ:

$$T_{nm} = \mathrm{Tr}(\varrho\sigma_n \otimes \sigma_m). \tag{1.31}$$

The two largest singular values (λ_1, λ_2) of the resulting matrix T, give the maximum expectation value of the operator associated with Bell-CHSH inequality achievable by the density matrix ϱ

$$\langle S \rangle = 2\sqrt{\lambda_1^2 + \lambda_2^2}, \tag{1.32}$$

the maximum value for the above expression is achieved when $\langle S \rangle = 2\sqrt{2}$, which occurs when the absolute values of singular values of T attain their maximum value of 1. Under local realism, the maximum value attainable is $\langle S \rangle = 2$. A violation of Bell-type inequality is often considered an excellence indicator of the presence of entanglement in a pure two-qubit system; alas, despite its experimental convenience, it is not a true measure of entanglement[3].

[3] Ref. [28] shows that in general, it is not possible to discern the degree of entanglement (a quantifiable measure) in a state *via* an inference from a violation of a Bell-type inequality.

Bell-Mermin operator

A similar condition to the Bell-CHSH can be derived for a N-qubit GHZ state (and any state locally equivalent to it) and the existence of non-local quantum correlations can be verified by a measurement of the Bell-Mermin operator [29]:

$$\mathcal{M}_N = \frac{1}{2i}\left(\prod_{j=1}^{N}(X_j + iY_j) - \prod_{j=1}^{N}(X_j - iY_j)\right), \tag{1.33}$$

where X_j, Y_j denote the Pauli matrices, acting on the qubit j. One can show that permutations of the terms of the form $Y_1 Y_2 \cdots Y_{2m} \cdots X_n$ where $m \in 1, 2, \ldots, \lfloor \frac{N}{2} \rfloor$ vanish. Such a term will have a coefficient of $i^{2m} = -1$ from the first product and a coefficient of $-(-1)^{2m} i^{2m} = 1$ from the second product. Hence, only permutations of terms with an odd number of Y's are non-vanishing.

Permutations of a term where the number of Y's is $k = 2l + 1$ have a coefficient $+1$, where l is in the set of all even numbers less than N (including 0), otherwise having -1. The number of such distinct permutations is given by $\sum_{j\,\text{odd}} \binom{N}{j} = 2^{N-1}$.

Furthermore, the GHZ state is an eigenstate with eigenvalue 2^{N-1} of the Bell-Mermin operator, which implies that the GHZ state is an eigenstate with eigenvalue $+1$ of each of the non-vanishing terms[4], and attains the maximum expectation value with respect to the Bell-Mermin operators *i.e.* $\langle \mathcal{M}_N \rangle_{\text{GHZ}} = 2^{N-1}$. While local hidden-variable theories under local realism [30] predict an expectation value of $\langle \mathcal{M}_N \rangle < 2^{N/2}$ for even N, and $\langle \mathcal{M}_N \rangle < 2^{(N-1)/2}$ for odd N [29] — which for $n \geq 3$ are both less than the maximum expectation value for the quantum analog, thus leading to a violation of both inequalities that grows exponentially in N. For the three-qubit case, the Bell-Mermin operator of Equation (1.33) takes the form:

[4] Self-adjoint operators with this property with respect to some state, are said to be stabilizing operators of that state. More on this a few lines down the text.

$$\mathcal{M} = X_1 X_2 X_3 - X_1 Y_2 Y_3 - Y_1 X_2 Y_3 - Y_1 Y_2 X_3. \tag{1.34}$$

Entanglement witnesses

A way to detect genuine multi-particle entanglement[5] around the expected state is by means of a so-called entanglement witness operator $\mathcal{W}$. An entanglement witness operator $\mathcal{W}$ is a self-adjoint operator, which has a positive or zero expectation value for all product states (fully separable states) and negative for some non-separable states [32]; that is:

[5] A pure state is genuinely multipartite entangled if it cannot be written as tensor product of two states in any bipartition [31].

$$\text{Tr}(\mathcal{W}\varrho) = \begin{cases} \geq 0 & \text{for all product states } \varrho_s, \\ < 0 & \text{for some entangled states } \varrho_e \end{cases}. \tag{1.35}$$

In general, finding such an entanglement witness operator is not a trivial matter[6], however for a certain class of states, called stabilizer states, finding a witness operator can be reduced to finding the so-called stabilizing operators. A stabilizing operator $S^{(k)}$ for some state N-qubit $|\psi\rangle$, satisfies the following:

[6] See Refs. [33, 34] for a thorough exposition on this.

$$S^{(k)} |\psi\rangle = |\psi\rangle\,, \tag{1.36}$$

i.e. it is an eigenstate of $S^{(k)}$ with eigenvalue $+1$ [35]. Stabilizer states can be uniquely defined in terms of their stabilizing operators, thus it is possible to construct entanglement witnesses, detecting entanglement around the ideal state. An entanglement witness operator detecting genuine multi-partite entanglement around the ideal state $|\psi\rangle$ has a noise threshold p_{limit}, that is, it will detect a mixed state of the form $\varrho(p_{\text{noise}}) = p_{\text{noise}} \mathbb{1}/2^N + (1 - p_{\text{noise}}) |\psi\rangle\langle\psi|$ as genuinely entangled if p_{noise} is below the positive-valued threshold $0 < p_{\text{limit}} < 1$ [35].

1.3 Quantum circuit model

The quantum circuit model (or quantum network model) [3] has many parallels with the classical model of Boolean logic circuits, and in fact it is a quantum generalization of the latter. In the classical model of Boolean logic circuits, the smallest information carrying unit is the bit and information processing proceeds temporally *via* computations.

A computation is an abstraction of any operation that takes as input a set of given input values (bits in this instance) to give a set of output values (bits in this instance). A basic computation is abstracted as a Boolean logic gate, which given a fixed length Boolean input of n bits computes some Boolean function of the form $f : \{0,1\}^n \to \{0,1\}$. Hence, at the very basic level, a Boolean logic circuit consists of a set of n inputs and m outputs, and intermediary between the inputs and outputs is a network of logic gates that perform Boolean functions of the aforesaid form for various fixed length input sizes, with the outputs of some gates serving as input to other logic gates in the network.

In the quantum circuit model of computation, the qubit is the corresponding smallest information carrying unit and information processing proceeds temporally in a similar fashion to the classical case, *via* computations. The quantum analog of a Boolean logic gate is a quantum logic gate, and a quantum circuit consists of quantum logic gates acting on a set of input n qubits, which at the end of the computation are subsequently measured in some basis to produce m output bits. At each time step, a quantum logic gate performs some unitary (reversible) operation U, hence the quantum circuit model of computation is a reversible model of computation (before measurement).

When visualizing in a quantum circuit, represented as wires, qubits start in some initial state and evolve temporally from left to right, with the inputs on the left of the diagram and the outputs on the right. At the right end of the circuit after measurement, classical bits are indicated with double wires. Common quantum logic gates we will frequently refer to throughout this thesis are shown in Table 1.1.

Figure 1.2 shows a simple quantum circuit that prepares one of the maximally entangled Bell states, $|\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$ shown in Equation (1.37) and measures the two qubits in the computational basis,

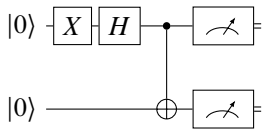


Figure 1.2: A quantum circuit preparing one of the Bell state $|\Phi^-\rangle$ and measures it in the computational basis states.

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \tag{1.37}$$

Initially, the state $|\psi\rangle$ begins as

$$\begin{aligned} |\psi\rangle &= HX \otimes \mathbb{1} \, |00\rangle \, , \\ &= |-\rangle \, |0\rangle \, . \end{aligned} \tag{1.38}$$

Applying a controlled-NOT gate on the above gives

$$\begin{aligned} \mathrm{CX} \, |-\rangle \, |0\rangle &= \frac{1}{\sqrt{2}} \mathrm{CX}(|0\rangle \, |0\rangle - |1\rangle \, |0\rangle), \\ &= \frac{1}{\sqrt{2}}(|0\rangle \, |0\rangle - |1\rangle \, |1\rangle). \end{aligned} \tag{1.39}$$

Measuring the above state in the computational basis states will yield the measurement outcome $o = 00$ or $o = 11$ with equal probability.

Gate	Nomenclature	Circuit symbol	Matrix representation
NOT/X	Pauli-X		$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Y	Pauli-Y		$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Z	Pauli-Z/Phase flip		$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
H	Hadamard		$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
T	T Gate		$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
S	Phase Gate		$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
R_ϕ	Phase-Shift		$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$
CNOT/CX	Controlled-NOT		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
CPHASE/CZ	Controlled-Z		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
SWAP	Swap Gate		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
CCNOT/CCX/$C^2[X]$	Toffoli/Controlled-Controlled-NOT		$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$
CCPHASE/CCZ/$C^2[Z]$	Controlled-controlled-Z/Controlled-Controlled-Phase		$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$
C-SWAP	Fredkin/Controlled-SWAP		$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

Table 1.1: Common quantum logic gate with their names, circuit symbol and matrix presentation

In later chapters we will make plenty of references to circuit depth; circuit depth is defined as the number of consecutive parallel operations in a circuit from its input to output. Circuit depth is taken to be a good proxy for algorithmic time, since each such parallel operations can be counted as a single step. Consider the circuit Figure 1.3, the circuit has 8 quantum logic gates and a circuit depth of 6. This is because the operations in a given column can be executed in parallel, take for instance the set of operations $H \otimes \mathbb{1} \otimes \mathbb{1}$, $\mathbb{1} \otimes H \otimes \mathbb{1}$, and $\mathbb{1} \otimes \mathbb{1} \otimes H$; these operations are equivalent to the single operation $H \otimes H \otimes H$, and thus can executed in parallel without temporal racing conditions.

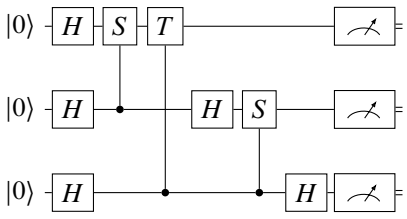


Figure 1.3: A quantum circuit with 8 quantum logic gates and circuit depth of 6.

1.3.1 Universal gate sets

In classical computation the gate set {AND, OR and NOT} defines a universal gate set as every Boolean can be decomposed into a finite sequence of the gates in the set, and in classical reversible computation the reversible the Boolean Toffoli gate is a universal logic gate. This implies that any logic circuit L which computes a Boolean function of the form $f : \{0,1\}^n \rightarrow \{0,1\}$ can be decomposed into a logic circuit L', equivalent in operation, made up of only a combination of gates in the universal gate set. Similarly in quantum information processing, a quantum logic gate set is said to be a universal gate set if any unitary operation U can be decomposed into a finite sequence of the gates in that set. A commonly used universal gate set is $\{H, S, \text{CNOT}, T\}$, in terms of the Hadamard H, phase S, CNOT and T gates. A controlled-controlled-NOT gate with such a universal gate set can be decomposed into seven $T/T^\dagger$, two H and six controlled-NOT gates. A physical realization may implement a different gate from the aforesaid set to the convenience of the physical implementation, *i.e.* the universal gate set for IBM Q processors is $\{\text{CNOT}, R_z(\theta), \sqrt{X}, X\}$ and same gate may not necessarily decompose into the same number of gates across universal gate sets, which may raise concerns over the efficiency of a particular gate set. However, any two universal gate sets can simulate one another efficiently [36] and a particular choice of universal gate set does not the effect the asymptotic efficiency of a physical realization implementing a particular gate set.

1.4 Polarization measurements

In the experiments we will describe in later chapters we shall make plenty of references to performing polarization measurements on a quantum state of light. Hence, I have endeavored to outline in passing what is essential in this regard, that is the mathematical description of the operations of optical elements that alter and measure the polarization of single photons.

1.4.1 Wave plates

Perhaps, the most wide-spread of such optical elements are wave plates. Wave plates are optical elements made up of birefringent material and alter the polarization of light normally incident on it by introducing a phase-shift between its polarization components along the ordinary and extraordinary axes[7] of the material. For light normally incident on a wave plate, the polarization component along the ordinary axis[8] experiences a different refractive index than the polarization component along the extraordinary axis, hence the polarization state of the transmitted light exits the wave plate out of phase by φ.

[7] Sometimes called slow-axis and fast-axis, respectively

[8] The material is often cut such that the ordinary axis is normal to the plane of the wave plate's front face.

For a phase shift of $\varphi = \pi$, the corresponding wave plate is called a half-wave plate (HWP). The action of a HWP on the two perpendicular polarization modes $\hat{a}_H, \hat{a}_V$ (typically horizontal and vertical axis of the lab frame) of a single photon[9] is given by [37]

[9] Here, $\hat{a}_H^\dagger |\text{vac}\rangle = |H\rangle = |0\rangle$ and $\hat{a}_V^\dagger |\text{vac}\rangle = |V\rangle = |1\rangle$

$$U_{\text{HWP}}(\theta) = \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ -\sin(2\theta) & -\cos(2\theta) \end{pmatrix}, \tag{1.40}$$

where θ is the angle between the extraordinary axis and the vertical axis of the lab fame. Similarly, when $\varphi = \pi/2$ the corresponding wave plate is called a quarter wave plate.

The action of a QWP on the two perpendicular polarization modes $\hat{a}_H, \hat{a}_V$ (typically horizontal and vertical axis of the lab frame) of a single photon is given by [37]

$$U_{\text{QWP}}(\theta) = \frac{1}{\sqrt{2}}\begin{pmatrix} i - \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & i + \cos(2\theta) \end{pmatrix}, \tag{1.41}$$

where θ is similarly defined as before.

Similar to Equation (1.12), any polarization rotation $R \in \text{SU}(2)$ can be decomposed as a combination of the action of two QWPs and one HWP, coaxially aligned [38]. Furthermore, the said components can be in any arrangement, *i.e.* a HWP sandwiched between two QWPs.

1.4.2 Beam splitters

A polarizing beam splitter (PBS) acts as a polarization filter; a photon polarized along the transmission axis of a PBS is transmitted, and one polarized perpendicular to the transmission axis of a PBS is reflected at a right angle to the transmission axis. Hence, in an experimental setting a PBS can be taken to be measurement device performing projective measurements of polarization and thus the computational basis $\{|H = 0\rangle, |V = 1\rangle\}$. Typically, whenever a PBS is designated as measurement device its transmission axis is parallel with the horizontal plane in the lab frame (hence transmitting horizontally polarized light and reflecting vertically polarized light) and the transmitted light is sent to a detection stage. The action of a PBS when its transmission axis is parallel with the horizontal, or vertical plane in the lab frame respectively are given by,

$$P_H = |H\rangle\langle H| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{1.42}$$

$$P_V = |V\rangle\langle V| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.43}$$

A non-polarizing beam splitter (NPBS) has almost an similar action to wave plates, however not on the polarization of the light but instead on the spatial path modes of the light. The action of a NPBS on the input modes on each side (at right-angles to one another) of the beam splitter cube $\hat{a}_{\text{in}}$ and $\hat{b}_{\text{in}}$ is given by[10]

[10] Similarly, $\hat{a}^\dagger_{\text{in}}|\text{vac}\rangle = |l\rangle = |\mathbf{0}\rangle$ and $\hat{b}^\dagger_{\text{out}}|\text{vac}\rangle = |r\rangle = |\mathbf{1}\rangle$

$$U(\varphi, \theta)_{\text{NPBS}} = \begin{pmatrix} \cos(\theta) & ie^{-i\varphi}\sin(\theta) \\ ie^{i\varphi}\sin\theta & \cos(\theta) \end{pmatrix} \tag{1.44}$$

The angle θ parameterizes the probability amplitudes of transmission and reflection, and the relative phase $e^{i\varphi}$ ensures that the above action is unitary. A 50:50 beam splitter corresponds to the choice $\varphi = \pi/2$ and $\theta = \pi/4$ and its action is given by

$$U(\varphi, \theta)_{\text{NPBS}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \tag{1.45}$$

which is equivalent to the action of the Pauli-Z and Hadamard gate H, $U(\pi/2, \pi/4) = ZH$.

The combination of a HWP, QWP, PBS and detector can be used to perform any polarization projective measurement, the polarization analyser is shown in Figure 1.4.

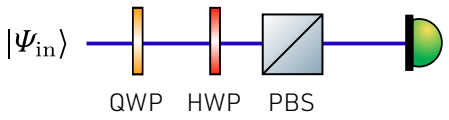


Figure 1.4: A sketch of polarization analyser consisting of a HWP, QWP, PBS, and a detector.

Table 1.2 shows examples of wave plate settings for projecting out a target state, in the case when the PBS transmits horizontally polarized light.

Target state	QWP(θ)	HWP(θ)
$\|H\rangle$	0°	0°
$\|V\rangle$	0°	45°
$\|D\rangle$	45°	22.5°
$\|A\rangle$	45°	−22.5°
$\|R\rangle$	90°	22.5°
$\|L\rangle$	0°	22.5°

Table 1.2: Examples of wave plates settings for the polarization analyser in Figure 1.4 to project out a target state. Here, $|D\rangle := (|H\rangle + |V\rangle)/\sqrt{2}$, $|A\rangle \equiv (|H\rangle - |V\rangle)/\sqrt{2}$, $|L\rangle := (|H\rangle + i\,|V\rangle)/\sqrt{2}$ and $|R\rangle := (|H\rangle - i\,|V\rangle)/\sqrt{2}$.

2

Unstructured Quantum Search

2.1 Introduction

The canonical quantum search algorithm due to Grover [14] provides a way to find a unique target element in an unstructured list of size N, provided that the specified target element exists, with high probability after $\mathcal{O}(\sqrt{N})$ search queries, giving a quadratic advantage over a classical exhaustive search over all possible target elements, which requires $\mathcal{O}(N)$ search queries. Grover's algorithm is phrased as solving the problem of searching an unstructured list of a particular size, its applications are broad and wide-ranging, encompassing combinatorial search and optimization problems such as graph coloring problems and Boolean satisfiability problems [17, 18]. At the heart of Grover's algorithm is a quantum routine called amplitude amplification [39, 40] that amplifies the amplitudes of the so-called target elements[1] while suppressing amplitudes associated with non-target elements, thus in effect increasing the probability of measuring the target elements at end of the subroutine. It is typically phrased as follows [39]: Given a Boolean function $\chi : \mathbb{Z} \to \{0, 1\}$ such that one or more x satisfy $\chi(x) = 1$, there exists a quantum subroutine $\mathcal{A}$ that makes no use of intermediate measurements and has probability p of finding a $|x\rangle$, when applied to $|\mathbf{0}\rangle$. Then $\mathcal{O}(1/p)$ applications of $\mathcal{A}$ and $\mathcal{A}^{-1}$ suffice to produce the measurement outcome(s) x with probability greater than half, if the applications of $\mathcal{A}$ and $\mathcal{A}^{-1}$ are followed by an appropriate measurement[2].

[1] In general, there could be more than one target element or no target element at all.

[2] As we will see later that the canonical quantum search algorithm due to Grover may be taken to be the special case of quantum amplitude amplification, where $\mathcal{A} = \boldsymbol{H}^{\otimes n}$, such that $p = 1/\sqrt{N}$ (*i.e.* $\mathcal{A}$ prepares an equal superposition of all possible outcomes), and the promise that there is one unique target element s, where $\chi(s) = 1$.

There is a large body of experimental work that exists demonstrating the realization of instances of Grover's algorithm for $N = 4$ on two qubits on sundry quantum architectures. The pioneering work was demonstrated on a liquid-state nuclear magnetic resonance (NMR) based quantum architecture, successfully verifying that the algorithm can find a specified target item with near-certainty in a single step of the algorithm, although in a non-programmable and non-scalable manner [41]. One of the very first instances of Grover's algorithm was done on a trapped-ion system [42], with the ability to arbitrary specify any of the $N = 4$ as a target element, and subsequently find it with one single step of the algorithm. Technological improvements over the years made similar programmable demonstrations (promises of scalability) possible [43]. The next instance of Grover's algorithm is on three qubits for a search space of $N = 8$ elements; the only three-qubit experimental demonstrations of Grover's algorithm are due to Vandersypen et al. [44] on a liquid NMR architecture and a complete implementation (with the ability to find arbitrarily specified target elements in a programmable way) is due to Figgat et al. [45] on a trapped-ion system. At the time that the author writes this thesis, there is no complete four-qubit experimental demonstration of Grover's algorithm in its canonical form.

The standard construction of the algorithm has been proven to be optimal in the number of search queries (steps) [40, 46, 47]. However, in actuality, each of these steps are broken down into intermediary subroutines. In particular, for NISQ processors, the intermediary subroutines are further broken down into atomic operations. Such atomic (unitary) operations constitute a finite gate set called a universal gate set [36] for which any unitary operation can be approximated in terms of a finite set of gates from a universal gate set. In the instance of superconducting qubit based architectures, the universal gate set is realized with a set of single-qubit gates along with a high-fidelity two-qubit entangling gate [8]. NISQ processors are severely limited by the debilitating effects of decoherence, that limit the time over which a computation can remain fully coherent, thus there is an upper limit on the number of operations over a set of qubits that can be in a circuit mapped to a physical processor and guarantee a reliable result at the end of the computation. As it stands, standard constructions of the algorithm on four or more qubits present a sizeable challenge on NISQ processors.

One of the intermediary subroutines of the algorithm is the so-called global Grover iterate, which constitutes the most resource intensive part of the algorithm in terms of two-qubit gate count. The global Grover iterate for the standard algorithm on n-qubits consists of one or more n-qubit Toffoli gate (modulo single gates). For $n \geq 4$ the exact controlled-NOT count for a n-qubit Toffoli without auxiliary of qubits is unknown [48]. Additionally, to guarantee close to sure success of finding the target element(s), the global Grover iterate is repeated roughly $\left\lfloor c\sqrt{N} \right\rfloor$ times (for some positive constant c), which presents a considerable handicap for its physical implementation. In our preliminary tests of the standard construction of Grover's algorithm on four qubits, we found that the output probability distribution is indistinguishable from a uniform noise on the IBM quantum processors.

Apart from the standard construction, there are other variants of Grover's algorithm that trade accuracy in various ways for a reduction in the number of search queries, making them suitable for small-scale implementation on NISQ processors. For instance, it has been shown that one may stop short of $\left\lfloor c\sqrt{N} \right\rfloor$ search queries and still guarantee a high probability of success [40], with the downside that we may have to repeat the algorithm in case of failure. Other variants, the canonical variant being due to Grover and Radhakrishnan [20, 49], modifies the Grover iterates to search for a subspace of possible elements to which the target element belongs, rather than the target element itself. This may be thought of as finding the first $n - m$ bits, for some m, of the target element instead of all the bits of the target element. By way of combining local and/or global Grover iterates, it is possible to reduce the number of search queries at the expense of accuracy. Here, the choice of the sequence of local and/or global Grover iterates, and the size of the local Grover iterates $(n - m)$ is of practical interest in maximizing the success probability with the least number of search queries, and hence a reduced two-qubit gate count. In particular instances, local Grover iterates can be applied to the full search problem with appropriate choices for m. There is a large corpus of work studying the optimal sequences of local and/or global Grover iterates [49–53], and a configuration that has with several local Grover iterates sandwiched between one global iterate on one side and several global iterates on another has been shown to be optimal.

During the period over which this part of the thesis was conducted, several important results were published in succession [54–59] that addressed many of the questions, aims and objectives we initially had towards this particular research topic, which had the overriding imperative of reducing the resources used by algorithm, making it suitable for implementation on NISQ devices, hence this chapter will mainly consist of a survey of these results. We also present two marginal results of our own in this chapter, the first of which is an improvement in the success probabilities of the implementation in [54] by way of a further iteration using a local Grover iterate. Alas, the improvements in the results are most probably indicative of the improvement in the quality of the devices used rather than anything particular to our construction as it uses more controlled-NOT gates in comparison. The second result is related to a measurement-based three-qubit implementation of Grover's algorithm, and we also present results of implementing a measurement-based controlled-controlled-Z (equivalent to three-qubit Toffoli gate), which is an important subroutine in the algorithm. The results are unfortunately negative, as the measurement-based controlled-controlled-Z necessarily requires a graph state of ten qubits with twelve edge connections (controlled-Z gates between nodes), which cannot be further reduced by edge local complementation. For these reasons, it is out of reach for current NISQ devices.

2.2 Background

2.2.1 Canonical construction of Grover's algorithm

We begin by reviewing the standard construction of the algorithm in the circuit model of quantum computation, closely following Refs. [14, 17, 18]. The Grover's algorithm provides a way to solve the following dilemma:

On one faithful day, you happen to have locked yourself out of the laboratory and for some reason urgently need to access to your laboratory[3]. To worsen your woes, you realize that you completely forgot the lock combination, but luckily you happen to recall that the lock in question uses a lock-mechanism as the one shown in Figure 2.1; it has n-switches each of which has an "on" and "off" setting, and the lock combination that unlocks your laboratory is some unique configuration s of the n switches, with each being either set to either "on" or "off".

[3] Based on a true story.

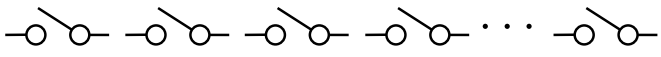


Figure 2.1: A configuration of n binary switches where some configuration of the switches is denoted a winning configuration, as an example to illustrate the search problem Grover's algorithm tries to solve.

If you don't have any prior knowledge of the configuration s, the best you can do is to simply employ a random guess and check strategy, *i.e.* you might try the combination shown in Figure 2.2 and check if the lock opens.

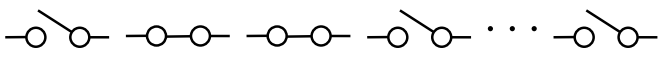


Figure 2.2: An example configuration of the n binary switches where two of the switches are in the on state and rest are in the off state.

If this is the best you can do, in the worst-case scenario you should expect to try all possible combinations, of which there are $N = 2^n$, until you find s, thus the worst-case behaviour scales linearly with N, $\mathcal{O}(N)$.

We can rephrase the above problem more concretely; assume we have the Boolean function $\chi : \{0, 1, \ldots, N-1\} \to \{0, 1\}$ such that

$$\chi(x) = \begin{cases} 1 & x = s \\ 0 & x \neq s \end{cases}, \tag{2.1}$$

for some unknown s. We refer to s as a target element. The above problem can be phrased as finding the unknown s by querying the above Boolean function, with some input x and check if $\chi(x) = 1$.

On a quantum computer, we can do slightly better than $\mathcal{O}(N)$ for the above. We assume here that the size of the search problem is a power of 2, $N = 2^n$ for $n \in \mathbb{N}$. We can thus realize the entire search space for a particular N on $n = \log(N)$ qubits [4]. One of the first clever tricks is to represent the effect of the Boolean function χ to indicate whether a particular input is a target element as a unitary transformation U_χ, which acts on basis states $|x\rangle$ like so,

[4] All logarithms $\log(\cdot)$ are taken base 2 unless state otherwise. $\ln(\cdot)$ is reserved for $\log_e$

$$U_\chi : |x\rangle \to (-1)^{\chi(x)} |x\rangle . \tag{2.2}$$

Observe for all $x \neq s$, the above unitary transformation acts trivially on the corresponding basis state $|x\rangle$, and for $x = s$, the corresponding basis state acquires a negative phase; the unitary U_χ is often called a phase oracle. U_χ may be written explicitly as,

$$U_\chi = \mathbb{1} - 2 |s\rangle\langle s| . \tag{2.3}$$

The algorithm starts with an n-qubit state $|0\rangle^{\otimes n}$ and prepares an equal superposition of all basis states, by applying a Hadamard transformation on each qubit, $H^{\otimes n}$

$$|\psi\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle . \tag{2.4}$$

It is useful to write the above state in a different basis. If there are t target elements (and $N - t$ non-target elements), then define $|x_\perp\rangle$ and $|x_{//}\rangle$ as such

$$\begin{aligned} |x_\perp\rangle &= \frac{1}{\sqrt{N-t}} \sum_{x \neq s} |x\rangle , \\ |x_{//}\rangle &= \frac{1}{\sqrt{t}} \sum_{x=s} |x\rangle , \end{aligned} \tag{2.5}$$

we can rewrite $|\psi\rangle$ as

$$|\psi\rangle = \frac{\sqrt{N-t}}{\sqrt{N}} |x_\perp\rangle + \frac{\sqrt{t}}{\sqrt{N}} |x_{//}\rangle , \tag{2.6}$$

We can further adopt the parametrization

$$\begin{aligned} \theta &= \arcsin \sqrt{\frac{t}{N}}, \\ \cos(\theta) &= \sqrt{\frac{N-t}{N}}, \\ \sin(\theta) &= \sqrt{\frac{t}{N}}, \end{aligned} \tag{2.7}$$

for which we can further rewrite Equation (2.6) as

$$|\psi\rangle = \cos(\theta)\,|x_\perp\rangle + \sin(\theta)\,\left|x_{//}\right\rangle. \tag{2.8}$$

Applying U_f to the above state yields

$$U_\chi\,|\psi\rangle = \cos(\theta)\,|x_\perp\rangle - \sin(\theta)\,\left|x_{//}\right\rangle. \tag{2.9}$$

Another clever trick in Grover's algorithm is an application of another unitary transformation D; defined similarly to Equation (2.3)

$$\begin{aligned} D &= H^{\otimes n}(2\,|0\rangle\langle 0|^{\otimes n} - \mathbb{1})H^{\otimes n}, \\ D &= 2\,|\psi\rangle\langle\psi| - \mathbb{1}. \end{aligned} \tag{2.10}$$

The above unitary transformation is often called a global diffuser operator. Expanding D in terms of the basis $\{|x_\perp\rangle\,,\left|x_{//}\right\rangle\}$, we get to the expression

$$\begin{aligned} D = {} & 2\cos^2(\theta)\,|x_\perp\rangle\langle x_\perp| + 2\sin^2(\theta)\,\left|x_{//}\right\rangle\left\langle x_{//}\right| \\ & + \sin(2\theta)\,|x_\perp\rangle\left\langle x_{//}\right| + \sin(2\theta)\,\left|x_{//}\right\rangle\langle x_\perp| - \mathbb{1}. \end{aligned} \tag{2.11}$$

We apply D to Equation (2.9), after trigonometric and algebraic gymnastics we arrive at

$$\begin{aligned} DU_\chi\,|\psi\rangle &= (\cos 2\theta\cos\theta - \sin 2\theta\sin\theta)\,|x_\perp\rangle \\ &\quad + (\sin 2\theta\cos\theta + \cos 2\theta\sin\theta)\,\left|x_{//}\right\rangle, \\ &= \cos 3\theta\,|x_\perp\rangle + \sin 3\theta\,\left|x_{//}\right\rangle. \end{aligned} \tag{2.12}$$

The full DU_χ has a geometric interpretation; the state $|\psi\rangle$ is a vector in a 2-dimensional Euclidean space spanned by $|x_\perp\rangle$ and $\left|x_{//}\right\rangle$, initially angled at θ with respect to $|x_\perp\rangle$. U_χ reflects the vector $|\psi\rangle$ about the $|x_\perp\rangle$ axis, *i.e.* $\theta \mapsto -\theta$; the angle between $|\psi\rangle$ and $U_\chi\,|\psi\rangle$ at this point is 2θ. D finally reflects $U_\chi\,|\psi\rangle$ about the $|\psi\rangle$ axis; the angle between $|x_\perp\rangle$ and $DU_\chi\,|\psi\rangle$ is 3θ; see figure below.

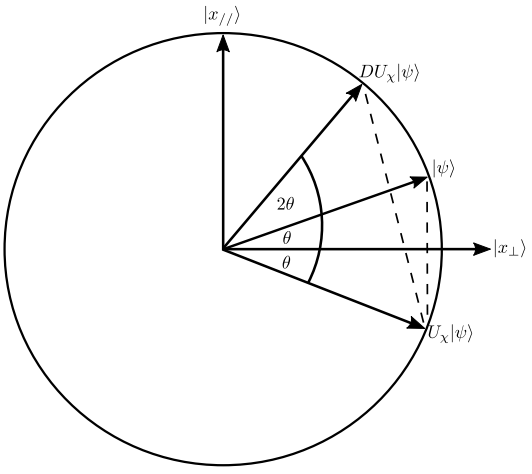


Figure 2.3: The geometric interpretation of a single Grover iterate; the uniform superposition state $|\psi\rangle$ starts at an angle θ with respect to the axis $|x_\perp\rangle$, the action of the phase oracle U_χ reflects $|\psi\rangle$ about the axis $|x_\perp\rangle$. Likewise, the action of the diffuser operator is to reflect $U_\chi\,|x_\perp\rangle$ about the axis $|\psi\rangle$ to get $DU_\chi\,|x_\perp\rangle$.

Looking at Equation (2.12), we can conveniently write the action of DU_χ on the basis states $\{|x_\perp\rangle, |x_{//}\rangle\}$ as

$$DU_\chi = \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix}, \tag{2.13}$$

that is, DU_χ is an element of the special orthogonal group $SO(2)$, the group of rotations in two dimensions. The unitary operator $G = DU_\chi$ is called the global Grover iterate. Rotating by an angle θ around a point k times is equivalent to a single rotation by an angle $k\theta$. From this, it is easy to see that k applications of G give

$$G^k |\psi\rangle = \cos((2k+1)\theta) |x_\perp\rangle + \sin((2k+1)\theta) |x_{//}\rangle. \tag{2.14}$$

Another useful visualization aid for gaining intuition about the Grover iterate is look to at its effect at the level of the amplitudes of the state in Equation (2.4). Consider the case where there is one unique target element; as we have seen the amplitude of the target element $|s\rangle$ acquires a negative phase under the action of unitary operator U_χ while the other amplitudes are left unaltered, hence applying U_χ to Equation (2.4) gives

$$U_\chi |\psi\rangle = \frac{1}{\sqrt{N}} \left(-|s\rangle + \sum_{x \neq s} |x\rangle \right). \tag{2.15}$$

It is not to hard to show that the action of the diffuser operator D on a general n-qubit state $|\varphi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle$ is given by

$$D |\varphi\rangle = \sum_{x=0}^{N-1} (2\langle\alpha\rangle - \alpha_x) |x\rangle, \tag{2.16}$$

where $\langle\alpha\rangle = \sum_{x=0}^{N-1} \alpha_x / N$ is the average value of the amplitudes [5]. Hence, when we apply D to $U_\chi |\psi\rangle$ in Equation (2.15) we obtain the following expression

$$\begin{aligned} DU_\chi |\psi\rangle &= \left(\frac{2(N-2)}{\sqrt{N}N} + \frac{1}{\sqrt{N}} \right) |s\rangle + \left(\frac{2(N-2)}{\sqrt{N}N} - \frac{1}{\sqrt{N}} \right) \sum_{x \neq s} |x\rangle, \\ &= \frac{3N-4}{\sqrt{N}N} |s\rangle + \frac{N-4}{\sqrt{N}N} \sum_{x \neq s} |x\rangle, \end{aligned} \tag{2.17}$$

since $\langle\alpha\rangle = (N-2)/\sqrt{N}N$; clearly, $3N-4 > N-4$. We see that the action of DU_χ is to increase the amplitude associated with the target element $|s\rangle$ while decreasing the amplitudes of the non-target elements (see Figure 2.4). For this reason, the process bears the name amplitude amplification.

How many applications k of the global Grover iterate should be applied to guarantee close to unity probability of observing the target element(s) $|x_{//}\rangle$ when we perform an appropriate measurement? Looking at Figure 2.3, we see that if we do not perform enough iterates we might undershoot and fall short of reaching $|x_{//}\rangle$. More worryingly, we might overshoot past $|x_{//}\rangle$, running the risk of having additional iterations for a clockwise round trip to cycle back close to $|x_{//}\rangle$.

[5] The action of the diffuser operator D on the amplitudes of a general state is often called inversion about the average for this reason, since $\alpha_x \to 2\langle\alpha\rangle - \alpha_x$ for each amplitude α_x associated with a computational basis state $|x\rangle$.

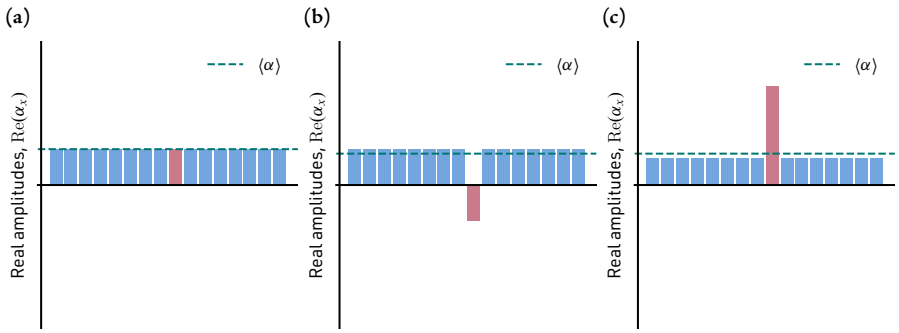


Figure 2.4: The action of a single Grover iterate on the level of the amplitudes for a search space of size $N = 2^4 = 16$, when we guaranteed that there is a unique target element. **(a)** We begin with the uniform superposition state $|\psi\rangle$, the amplitude of the target state is indicated in red while the non-target elements are indicated in blue. **(b)** After applying the phase oracle, the amplitude of the target element (indicated in red) acquires a relative negative sign. **(c)** The action of the diffuser operator is to invert all amplitudes about the average amplitude $\langle\alpha\rangle$. Hence, non-negative amplitudes decrease while negative amplitudes increase; amplifying the amplitude of the target element.

The probability of measuring $|x_{//}\rangle$ is given by

$$P_k = \left|\langle x_{//}| G^k |\psi\rangle\right|^2 = \sin((2k+1)\theta)^2. \tag{2.18}$$

For a particular $\tilde{k}$, we want $P_{\tilde{k}}$ to be close to 1, that is $\sin((2\tilde{k}+1)\theta)^2 \simeq 1$. From elementary trigonometry, we know that $\sin(\phi) = 1$ if $\phi = \pi/2$, then it must be that $(2\tilde{k}+1)\theta = \pi/2$, giving $\tilde{k} = \pi/4\theta - \frac{1}{2}$. In instances where $\tilde{k}$ is not integer, if we chose the number of iterations k to be the closest integer to $\tilde{k}$, we will still measure $|x_{//}\rangle$ with high probability. If we pick $\tilde{k}$ as $k = \lfloor \pi/4\theta \rfloor$, we have a probability of failure that is less than t/N [40], as shown below

$$\begin{aligned}
1 - P_k &= 1 - \sin((2k+1)\theta)^2 = \cos((2k+1)\theta)^2, \\
&= \cos[(2k+1)\theta + (2\tilde{k}+1)\theta - (2\tilde{k}+1)\theta]^2, \\
&= \cos[(2\tilde{k}+1) + (2(k-\tilde{k}))\theta]^2, \\
&= \cos(\pi/2 + 2(k-\tilde{k})\theta)^2, \\
&= \sin(2(k-\tilde{k})\theta)^2, \\
&\leq \sin(\theta)^2 = \frac{t}{N},
\end{aligned} \tag{2.19}$$

here we used $\left|k - \tilde{k}\right| \leq 1/2$ and $(2\tilde{k}+1)\theta = \pi/2$. The asymptotic behaviour of the number of global Grover iterates k when $t \ll N$ is

$$k \leq \frac{\pi}{4\theta} = \frac{\pi}{4\arcsin\sqrt{\frac{t}{N}}} \leq \frac{\pi}{4}\sqrt{\frac{N}{t}}, \tag{2.20}$$

since $\sqrt{t/N} = \arcsin(\phi) \geq \phi$. Hence, the algorithm asymptotically requires $\mathcal{O}(\sqrt{N/t})$ iterations to achieve a probability of success close to one. It is clear that for a given θ, Equation (2.18) does not scale linearly with number of iterations k in reaching its maximum value. Noticing this behaviour, Refs. [40, 60] suggest that if we seek to be frugal in the number of global Grover iterates (steps) — which is often an overriding imperative in practical considerations particularly for NISQ processors with short coherence times — then we may stop short of $\lfloor \pi/4\theta \rfloor$ and still find the target element(s) with reasonably high probability. How do we decide when to stop in such a scenario?

The expected number of times we will have to repeat the algorithm until we find a target element, if we stop it every time after m iterations and restart in case of failure is

$$\begin{aligned}
\mathbb{E}[X] &= \sum_{j=1}^{\infty} (mj)\, P_m (1-P_m)^{j-1}, \\
&= \sum_{j=1}^{\infty} (mj)\, \sin\left((2m+1)\theta\right)^2 \cos\left((2m+1)\theta\right)^{(2j-2)}, \\
&= m \tan\left((2m+1)\theta\right)^2 \sum_{j=1}^{\infty} j \cos\left((2m+1)\theta\right)^{2j}, \qquad (2.21) \\
&= \frac{m}{\sin\left((2m+1)\theta\right)^2} = \frac{m}{P_m}, \\
&= \frac{2m}{1-\cos\left(2(2m+1)\theta\right)}. \qquad (2.22)
\end{aligned}$$

Here we used $\sum_j^{\infty} j \cos(\phi)^{2j} = \cot(\phi)^2 \csc(\phi)^2$, and $\sin(\phi)^2 = 1/2(1 - \cos(2\phi))$. Taking the derivative of the above expression with respect to m and setting it to zero, we get an expression for m that minimizes the above expression. In the asymptotic limit $t \ll N$, the above expression is minimized when $4m\theta = \tan(2m\theta)$, numerically giving $4m\theta \approx 2.33112$. This gives the number of iterations as $m \approx 0.58278\sqrt{N/t}$, and the probability of finding a target element as $P_m = \sin\left((2m+1)\theta\right)^2 \approx \sin(2m\theta)^2 \approx 0.84458$ and $\mathbb{E}[X] \approx 0.69003/\theta \approx 0.8785\pi/4\theta < \pi/4\theta$.

Grover's algorithm has been proved to be asymptotically optimal (no quantum algorithm can achieve the same success with a fewer number of steps) in the number of search queries (iterates) [40, 47, 61], with proofs of this kind finally culminating in Ref. [46], which shows that the algorithm is not only asymptotically but exactly optimal in the number of search queries. For the sake of brevity, we omit the proofs here and refer the interested reader to the aforementioned references.

A seemingly problematic scenario may arise when we are interested in finding multiple target elements, and we are oblivious to how many are there. That is, we don't know the value of t, hence θ. In such a scenario, there is seemingly no way to know how many global Grover iterates we should apply to maximize the probability of finding a target element, $P_k = \sin\left((2k+1)\theta\right)^2$. Fortunately, it turns out it is still possible to preserve the asymptotic optimality of the algorithm, $\mathcal{O}(\sqrt{Nt})$, if we adopt a method that continuously tries and updates informed guesses for k, and restarting the algorithm in case of failure, with the assumption that t is bounded above by $\lceil 3N/4 \rceil$, the interested reader may refer to Ref. [40] for more details. We show the schematic circuit diagram of Grover's algorithm in Figure 2.5, and conclude this subsection by summarizing the steps of Grover's quantum search algorithm when the number of target elements t is known.

1. *Initialization*

   Prepare $|0\rangle^{\otimes n}$ and apply $H^{\otimes n}$ on all the qubits, creating a uniform superposition of $N = 2^n$ basis states:

$$|0\rangle^{\otimes n} \to \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle .$$

2. *Global Grover iterates*

   Apply the global Grover iterates k times, where $k = \left\lfloor \sqrt{N/t}\,\pi/4 \right\rfloor$ for close to unity success and $k = 0.58278\sqrt{N/t}$ for a success probability of $\simeq 0.8446$:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} G^k |x\rangle .$$

3. *Measurements*

   Measure all qubits in the computational basis, yielding a target element in with high probability if $k = \left\lfloor \sqrt{N/t}\,\pi/4 \right\rfloor$. In case of failure for $k = 0.58278\sqrt{N/t}$, go back to step 1; the average number of times we will have to repeat the algorithm is at least $\simeq 0.8785\sqrt{N/t}\,\pi/4$ times before success.

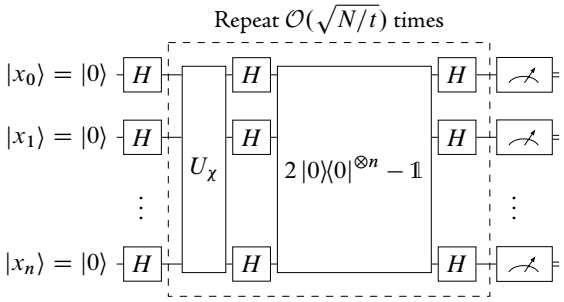


Figure 2.5: A schematic circuit diagram of Grover's algorithm; which begins with all n qubits in the state $|0\rangle$, after which a Hadamard gate H is applied to all qubits to create a uniform superposition of 2^n basis states. Grover iterates, with each consisting of a phase oracle and diffuser operators are repeated $\mathcal{O}(\sqrt{N})$. Measuring the qubits in the computational basis, with high probability we obtain the outcome corresponding to the target element.

2.2.2 Partial search quantum algorithm

The partial search quantum algorithm due to Grover and Radhakrishnan [20] offers another way we might trade accuracy for fewer elementary operations. Rather than searching for a target element[6], the partial search quantum algorithm instead partitions the search space into $K = 2^{n-m}$ blocks of size $b = 2^m$, *i.e.* $N = bK = 2^n$, and searches on the level of blocks, that is, it seeks find the block to which a target element belongs rather than the target element itself. Intuitively, this can be understood as performing the canonical quantum search algorithm on the first $(n - m)$ bits of the target element s. The analysis proceeds in a similar way to the canonical quantum search of the previous section; we begin with $|0\rangle^{\otimes n}$ and prepare a uniform superposition, by applying Hadamard gates to every qubit, preparing the state in Equation (2.4). In the case of a single and unique target element[7], we introduce the basis

$$\begin{aligned} |s\rangle &= |s_1\rangle \otimes |s_2\rangle\,, \\ |ns\rangle &= \frac{1}{\sqrt{b-1}} \sum_{x \neq x_1} |x_1\rangle \otimes |x\rangle\,, \\ |u\rangle &= \frac{1}{\sqrt{N-b}} (\sqrt{N}\,|\psi\rangle - |s\rangle - \sqrt{b-1}\,|ns\rangle), \end{aligned} \tag{2.23}$$

here $|s\rangle$ is the target element, bipartitioned into a product state of $|s_1\rangle$ and $|s_2\rangle$, where we seek to find $|s_1\rangle$, $|ns\rangle$ is the normalized sum of all non-target elements in the block containing the target element$|s\rangle$, $|u\rangle$ is the normalized sum of all the elements belong to blocks not containing $|s\rangle$, and $|\psi\rangle$ is the uniform superposition in Equation (2.4).

[6] In the case where we are assured this is one unique target element, *i.e.* $t = 1$.

[7] The algorithm has been generalized to accommodate multiple target elements across the blocks [62, 63]. In such a scenario optimality is achieved when the target elements are evenly distributed across the blocks [62]. We do not consider such cases here. The interested reader may refer to the aforementioned references.

In this new basis, we can write Equation (2.4) as

$$|\psi\rangle = \frac{1}{\sqrt{N}}|s\rangle + \frac{\sqrt{b-1}}{\sqrt{N}}|ns\rangle + \frac{\sqrt{N-b}}{\sqrt{N}}|u\rangle . \tag{2.24}$$

We adopt the following parametrization

$$\begin{aligned}
\sin(\theta) &= \frac{1}{\sqrt{K}}, \\
\cos(\theta) &= \frac{\sqrt{K-1}}{\sqrt{K}}, \\
\sin(\phi) &= \frac{1}{\sqrt{b}}, \\
\cos(\phi) &= \frac{\sqrt{b-1}}{\sqrt{b}},
\end{aligned} \tag{2.25}$$

and arrive at

$$|\psi\rangle = \sin(\theta)\sin(\phi)|s\rangle + \cos(\phi)\sin(\theta)|ns\rangle + \cos(\theta)|u\rangle . \tag{2.26}$$

We see that $|\psi\rangle$ may be taken to be a vector in a spherical coordinate system with coordinates (1 (radius), θ (inclination), ϕ (azimuth)) where the x-axis is defined by $|ns\rangle$, y-axis by $|s\rangle$ and the z-axis by $|u\rangle$. We proceed in a similar fashion and apply the phase oracle U_χ to Equation (2.26), giving the amplitude of the target element $|s\rangle$ a negative sign. The crucial distinction between the canonical and partial search quantum algorithm is the introduction of a local diffuser operator $D_{n,m}$, which acts in the same way the global diffuser operator D does but on a subspace of m qubits rather than all the qubits, $m < n$. That is,

$$D_{n,m} = \mathbb{1}_{2^{n-m}} \otimes (2|\phi\rangle\langle\phi| - \mathbb{1}_{2^m}), \tag{2.27}$$

where $|\phi\rangle = H^{\otimes m}|0\rangle^{\otimes m}$ is a uniform superposition of m qubits in such a subspace. The unitary operator $D_{n,m}$ has a similar effect on the amplitudes as D does, that is, it inverts about the average in each block simultaneously. The unitary operator $G_{n,m} = D_{n,m}U_\chi$ is called the local Grover iterate[8]; we can similarly trace its effects on Equation (2.26) as before by looking at the evolution of the amplitudes after each step, as shown in Figure 2.6.

[8] From now on, we will denote to global Grover iterates with a with a single subscript G_n, instead of $G_{n,n}$. Similarly, we will indicated a global diffuser operator D_n instead of $D_{n,n}$.

A feature worth noting is that for some choice of the block size b, the local Grover iterate can amplify the amplitude of the target element to a moderately high value relative to the rest of the amplitudes. Grover and Radhakrishnan noticed this too, and in Ref. [20] suggested that we can use local Grover iterates in conjunction with global Grover iterates to guarantee a high probability of measuring the target element.

The order in which global and local Grover iterates are applied is important, since the two operators share non-trivial commutation relations, Figure 2.7 shows the amplitudes after applying two local Grover iterates $G_{n,m}$ and one global Grover iterate G_n in different orders. Ref. [20] proves that it is possible to guarantee a high probability of measuring the target if l_1 sequences of the global Grover iterates G_n are applied first followed by l_2 sequences of local Grover iterates $G_{n,m}$, and lastly a single global Grover iterate G_n, that is, $G_n G_{n,m}^{l_2} G_n^{l_1}$.

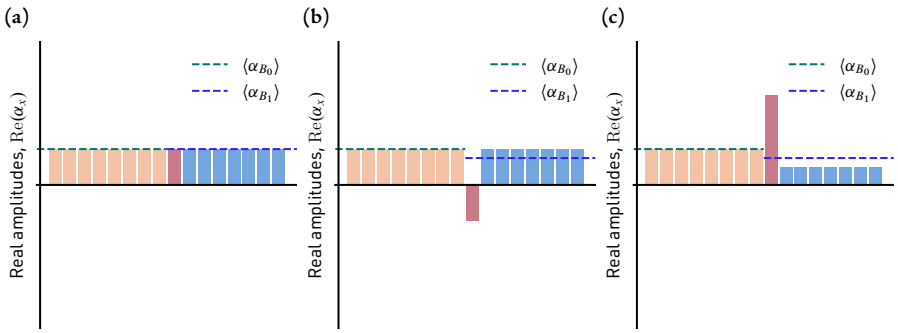


Figure 2.6: The action of a single local Grover iterate on the level of the amplitudes for a search space of size $N = 2^4$ and a block size $b = 2^3$, which divides the search into $K = 2$ blocks. $\langle\alpha_{B_0}\rangle$ and $\langle\alpha_{B_1}\rangle$ represent the block average for each block. **(a)** We begin with the uniform superposition state $|\psi\rangle$, the amplitude of target element is indicated in red and the rest of amplitudes in the target block is indicated in blue, while all the amplitudes in the non-target block indicated in orange. **(b)** After applying the phase oracle the amplitude of the target state acquires a relative minus sign. **(c)** The action of local diffuser operator $D_{4,3}$ is to invert the amplitudes in each block about the block's average amplitude, thus non-negative amplitudes decrease while negative amplitudes increase in each block; amplifying the amplitude of the target element.

They further show that the number of iterates (both local and global) for large values of K scales like $\pi/4\sqrt{N} - c\sqrt{b}$ for a positive constant c. Refs. [49–53] study various sequence and application orders of $G_{n,m}$ and G_n with the aim of reducing the constant c, culminating in Ref. [51] showing that sequences of the kind $G_n G_{n,m}^{l_1} G_n^{l_2}$ are optimal among different classes of sequences. The values of l_1, l_2 can be found by minimizing $S = l_1 + l_2 + 1 \simeq \pi/4\sqrt{N} - c\sqrt{b}$ for a certain probability threshold value and number of blocks K. Ref. [50] adopts the parametrization $l_1 = \pi/4\sqrt{N} - \eta_K\sqrt{b}$ and $l_2 = \alpha_K\sqrt{b}$ and numerically minimizes $c = (\alpha_K - \eta_K)$; Table 2.1 shows some values for α_K and η_K from the aforementioned reference. The quantum partial search with this sequence of local and global is called the Grover-Radhakrishnan-Korepin (GRK) algorithm. Equation (2.26) is suggestive that the partial quantum search algorithm has a similar geometric interpretation as the canonical quantum search. Indeed, $G_{\mathrm{GRK}} = G_n G_{n,m}^{l_1} G_n^{l_2}$ is an element of the orthogonal group $O(3)$ [52].

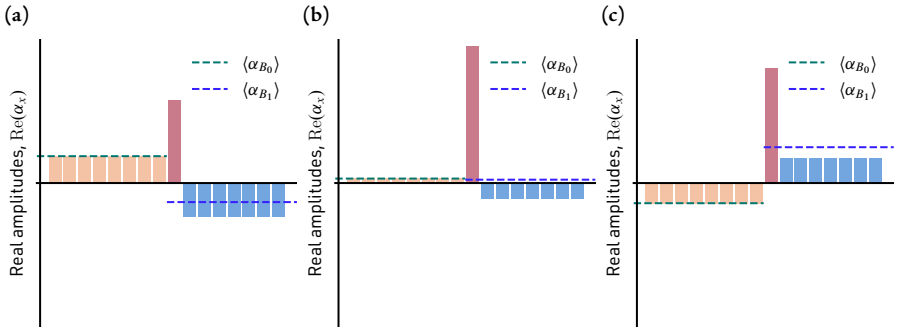


Figure 2.7: The actions of different application order of a global and two local Grover iterates on the level of the amplitudes for $N = 2^4$, $b = 2^3$, and $K = 2$. $\langle\alpha_{B_0}\rangle$ and $\langle\alpha_{B_1}\rangle$ represent the block average for each block. Action of the application order **(a)** $G_{4,3}G_{4,3}G_4$, **(b)** $G_{4,3}G_4G_{4,3}$, and **(c)** $G_4G_{4,3}G_{4,3}$. The order of operators is important since the local and global Grover operators have non-trivial commutation relations, in all three scenarios we end up with different probabilities for the target element.

We summarize the GRK algorithm to conclude the subsection and show its schematic in Figure 2.8.

K	α_K	η_K
2	0.7854	1.1107
3	0.65906	0.9961
4	0.6155	0.9553
5	0.6155	0.9341
∞	0.5236	0.866

Table 2.1: Numeric values for α_K and η_K for different values of the number of blocks K for the GRK algorithm, adopted from Ref. [50].

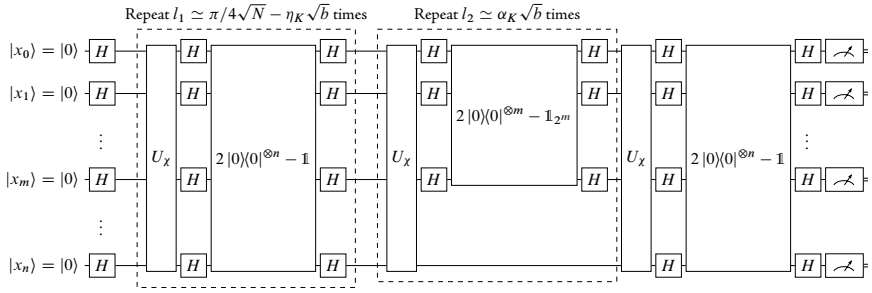


Figure 2.8: A schematic circuit diagram of the GRK algorithm; which begins with all n qubits in the state $|0\rangle$, after which a Hadamard gate H is applied to all qubits to create a uniform superposition of 2^n basis states. A sequence of l_1 global Grover operators, followed by a sequence of l_2 local Grover iterates, and lastly a single global Grover operator is applied to the uniform superposition. Measuring in the computational basis, the target element will be found with high probability.

1. *Initialization*

   Prepare $|0\rangle^{\otimes n}$ and apply $H^{\otimes n}$ on all the qubits, creating a uniform superposition of $N = 2^n$ basis states:

$$|0\rangle^{\otimes n} \to \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

2. *Global Grover iterates*

   Apply the global Grover iterates $l_1 \simeq \pi/4\sqrt{N} - \eta_K\sqrt{b}$ times:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \to \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} G_n^{l_1} |x\rangle$$

3. *Local Grover iterates*

   Apply local Grover iterates $l_2 \simeq \alpha_K\sqrt{b}$ times:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} G_n^{l_1} |x\rangle \to \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} G_{n,m}^{l_2} G_n^{l_1} |x\rangle$$

4. *Single global Grover iterate*

   Apply a single global Grover iterate:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} G_{n,m}^{l_2} G_n^{l_1} |x\rangle \to \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} G_n G_{n,m}^{l_2} G_n^{l_1} |x\rangle$$

5. *Measurements*

   Measure all qubits in the computational basis yielding a target element with high probability. In case of failure, go back to step 1.

2.3 Survey of recent results relating to NISQ processors

As we have seen in sections § 2.2.1 and § 2.2.2, both the canonical and partial quantum search algorithms in various scenarios have been proven to be optimal in the number of steps they undertake to solve the search problem. However, as I briefly alluded to in the opening of this chapter, in physical implementations (emphasis on NISQ processors) of any quantum algorithm, each of these steps are broken down into intermediary subroutines and further into physically realizable atomic operations in the universal gate set of a particular physical implementation.

For physical realizations of quantum search algorithms, the Grover iterates constitute the most resource intensive parts of the algorithm in terms of such atomic operations. The phase oracle U_χ in the Grover iterate is equivalent to an n-qubit controlled-Z gate (modulo single qubit gates). Suppose our unique target element is the computational basis state $|b_0 b_1 b_2 \cdots b_{n-1}\rangle$, then following circuit composed of Pauli X gate and n-qubit controlled-Z, $C^{n-1}[Z]$ gates, implements a phase oracle U_χ that gives the state $|b_0 b_1 b_2 \cdots b_{n-1}\rangle$ a relative negative amplitude [9].

[9] For $n = 2$, it is equivalent to a controlled-Z and for $n = 3$ it is equivalent to a controlled-controlled-Z gate.

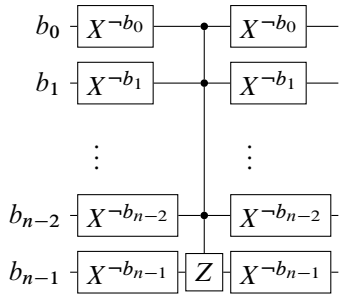


Figure 2.9: A circuit diagram that realizes a general phase oracle in Grover's algorithm; the circuit maps $|b_0 b_1 b_2 \cdots b_{n-1}\rangle \to -|b_0 b_1 b_2 \cdots b_{n-1}\rangle$, where $(X_a)^{b_a}$ applies a Pauli X gate to qubit a if $b_a = 1$ and applies the identity if b_0. Z denotes the Pauli Z gate

where $\neg 0 = 1$ and $\neg 1 = 0$. The diffuser operator G_n is implemented similarly

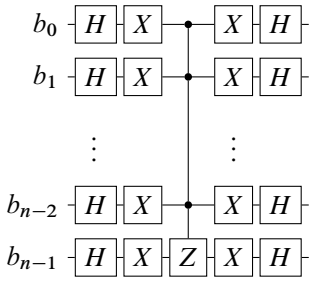


Figure 2.10: A circuit diagram that realizes a global diffuser operator in Grover's algorithm, where X, Z, H are the Pauli X, Z and H is the Hadamard gate respectively.

As we have seen, these two operators (the Grover iterate $D_n U_\chi$) must be repeated several times to guarantee some threshold for the probability of success. For NISQ processors, the n-qubit controlled-Z gate for more than two qubits is not an atomic operation. The n-qubit controlled-Z gate is equivalent to a generalized n-qubit Toffoli gate, $C^{n-1}[X]$, by applying a Hadamard gate H to the target qubit just before and after the gate (*i.e.* $HZH = X$). The generalized n-qubit Toffoli gate itself is also not an atomic operation on NISQ processors, but instead decomposed into atomic operations (controlled-NOT and single qubits). The two-qubit gate such as the controlled-NOT gate are physically realized through two-qubit interactions that induce conditional dependence of the state of one qubit to the other, for instance a cross-resonance interaction for superconducting qubits [8] and Mølmer-Sørensen interaction for trapped ions qubits [9]. The commonality across NISQ architectures is that such two-qubit interactions are non-trivial, making them experimentally expensive and much more prone to errors than single-qubit gates. Hence, for reasons motivated by practicality, the analysis of circuit complexity is done usually in terms of the two-qubit gate count in a circuit.

For $n = 3$, the controlled-controlled-Z (hence the controlled-controlled-NOT gate) gate cannot be implemented with less than five two-qubit gates [64]; the traditional three-qubit decomposition shown in Figure 2.11, uses six controlled-NOT and seven $T/T^\dagger$ gates, has shown to be optimal in terms of controlled-NOT count [48]. However, for $n \geq 4$ the exact controlled-NOT count of its decomposition without the use auxiliary of qubits is not known [48]. He et al. [65] have shown that if a single auxiliary qubit is provided $24n-72$ controlled-NOT gates suffice.

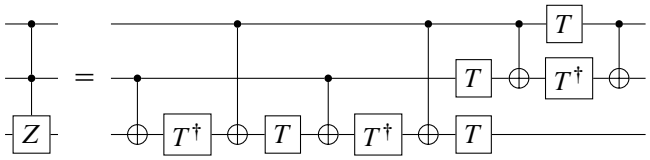


Figure 2.11: A circuit diagram showing the decomposition of a controlled-controlled-Z gate in terms of elementary gates; six controlled-NOT and seven $T/T^\dagger$ gates.

Additionally, they show that if $n-1$ auxiliary qubits are provided, then $4n-7$ controlled-NOT gates suffice. With such a decomposition it is possible to trade for a great reduction of controlled-NOT gates at the expensive of using more qubits. The unavoidable consequence for physical implementations is that, it becomes much harder to maintain quantum coherence as the relevant Hilbert space is much larger (from 2^n to 2^{2n-1} possible states). Furthermore, NISQ processors have limited connectivity among the qubits on the physical device hence multi-qubit gates cannot be performed directly on qubits that are not directly connected, and instead must be done by way of appropriate SWAP gates; a single SWAP gate costs three controlled-NOT gates, as shown in Figure 2.12

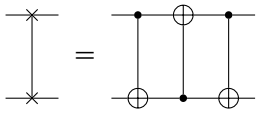


Figure 2.12: A circuit diagram showing the decomposition of a SWAP gate in terms of elementary gates; three controlled-NOT gates.

The theoretical reduction of the controlled-NOT gate count gained by the use of auxiliary qubits in practice may be lost depending on the connectivity of the physical device. Besides, the two-qubit gate count, another way circuit complexity is examined is in terms of its circuit depth. Circuit depth is the number of consecutive parallel operations in a circuit from its input to output. Each such parallel operation can be counted as a single step, and thus circuit depth can be taken to be a good proxy for algorithmic time. Analysis in terms of circuit depth is also motivated by practicality, since NISQ processors have short-lived coherence times, over which a computation can remain fully coherent, and thus limited to realizing shallow depth circuits [13]. The aforementioned decomposition of an n-qubit Toffoli due to He et al. [65] has a linear depth $\mathcal{O}(n)$ and logarithmic depth $\mathcal{O}(\log n)$ for a single auxiliary qubit and $n-1$ auxiliary qubits, respectively.

2.3.1 Depth optimization of the quantum search

On the account of the limitations of NISQ processors, *i.e.* the short-lived coherence time, limited number of qubits and limited connectivity among qubits, an analysis by Zhang and Korepin [55] emphasizes the imperative of designing algorithms in such a way that is aware of these limitations. Inspired by the GRK algorithm, and these practical considerations, they proposed a modification of the quantum search algorithm that is optimal in circuit depth, not necessarily optimal in the number of steps with respect to achieving some probability threshold. To facilitate this optimization, they define a figure of merit α, that is a ratio of the depth of the phase oracle depth and depth of the diffuser operator D_n

$$\alpha = \frac{d(U_\chi)}{d(D_n)}, \tag{2.28}$$

for single-target oracle implementations of the kind in Figure 2.9 and global diffuser operator of the kind in Figure 2.10, since the dominating circuit depth arises from the n-qubit controlled-Z gate, it is expected that $\alpha = 1$.

Recall that the local diffuser operators $D_{n,m}$ act on a small subspace $m < n$, thus in theory require fewer elementary operators and have lower depth than the global diffuser operators, at the cost of reducing the success probability[10]; hence their optimization method is based on the replacement of global diffuser operators with local diffuser operators to minimize the depth of Grover's algorithm, while taking into account the trade-off in the probability of success. Similar to the GRK algorithm, they consider a general sequence of local (G_m) and global Grover iterate operators (G_n) of the form

[10] This is clear from the perspective of Figure 2.10, we expect an m-qubit controlled-Z gate will decomposed into fewer elementary gates than n-qubit controlled-Z gate if $m < n$.

$$S_{n,m}(\bar{l}) = G_n^{l_1} G_m^{l_2} \cdots G_n^{l_{q-1}} G_m^{l_q}, \tag{2.29}$$

here $\bar{l} = (l_1, l_2, \ldots, l_q)$ is a tuple of natural numbers, $l_{\text{tot}} = \sum_{p=1}^{q} l_p$ is the total number of Grover iterates (both local and global). For instance, $S_n(l, 0) = G_n^l$ is the canonical Grover algorithm. The notational convention is that last number l_q is always the number of local Grover iterate operators, thus in this notation the Grover iterate for the GRK is denoted by $S_{n,m}(1, l_2, l_1, 0) = G_n^1 G_m^{l_2} G_n^{l_1} G_m^0$. Furthermore, the above notation only considers local Grover iterate operators acting on the same qubit subspace with the same block size m. For such a sequence of Grover iterates, the probability of measuring the target element $|s\rangle$ is given by

$$P_{n,m}(\bar{l}) = \left| \langle s | S_{n,m}(\bar{l}) H^{\otimes n} |0\rangle^{\otimes n} \right|^2. \tag{2.30}$$

From this, they define the ratio of the expected depth for the Grover iterate sequence $S_{n,m}$ and its probability of success as

$$\tilde{d}(\alpha) = \frac{d(S_{n,m}(\bar{l}))}{P_{n,m}(\bar{l})}, \tag{2.31}$$

and minimize the above quantity with respect both $m \geq 2$ and the tuple of natural numbers $\bar{l}$.

$$\tilde{d}(\alpha) = \underset{m,\bar{l}}{\text{minimize}} \frac{d(S_{n,m}(\bar{l}))}{P_{n,m}(\bar{l})}. \tag{2.32}$$

The study in Ref. [55] report that below certain threshold values of α for $n \geq 4$, their algorithm gives rise to sequences that have lower expected depth than the canonical algorithm, that is, the canonical algorithm is not optimal in depth[11]. Ref. [55] gives examples of depth-optimal sequences $S_{n,m}(\bar{l})$ for $\alpha = 1, n \in 3, 4, \ldots, 10$, in comparison with the canonical sequence with only global Grover iterates S_n; shown in Table 2.2 and Table 2.3, respectively.

[11] $S_n(l, 0) = G_n^l$, for $l = \left\lfloor 0.583\sqrt{N} \right\rfloor$. Recall from § 2.3.1 this value of l gives the least expected number of iterations, and thus the minimal expected depth, for a $P_n(l) \simeq 0.845$ probability of success.

n	$S_n(\bar{l})$	$P_n(\bar{l})$	$d\left(S_n(\bar{l})\right)$	$\tilde{d}(\alpha = 1)$
4	$S_4(1, 0)$	0.473	30	64.47
5	$S_5(2, 0)$	0.602	124	205.83
6	$S_6(4, 0)$	0.816	504	617.36
7	$S_7(6, 0)$	0.833	1446	1756.35
8	$S_8(9, 0)$	0.861	2916	3388.03
9	$S_9(12, 0)$	0.798	4848	6071.76
10	$S_{10}(18, 0)$	0.838	8712	10397.28

Table 2.2: The minimum expected depth for the quantum search algorithm for the sequence of the kind $S_n(l, 0) = G_n^l$, where $l = \left\lfloor 0.583\sqrt{N} \right\rfloor$ from Equation (2.29), where the ratio in Equation (2.28) is set to $\alpha = 1$; adopted from Ref. [55].

n	$S_{n,m}(\bar{l})$	$P_{n,m}(\bar{l})$	$d\left(S_{n,m}(\bar{l})\right)$	$\tilde{d}(\alpha=1)$
4	$S_{4,3}(1,1)$	0.821	52	63.32
5	$S_{5,4}(1,1,1)$	0.849	154	181.48
6	$S_{6,4}(1,1,2)$	0.755	360	475.97
7	$S_{7,4}(1,1,2,1,2)$	0.887	1173	1322.75
8	$S_{8,4}(1,1,2,1,2,1,2)$	0.875	2211	2527.43
9	$S_{9,5}(1,1,2,1,2,1,2,1,2)$	0.831	3713	4470.20
10	$S_{10,5}(1,1,2,1,2,1,2,1,2,1,2)$	0.847	6453	7614.56

Table 2.3: The minimum expected depth for the quantum search algorithm for the sequence of the kind $S_{n,m}(\bar{l}) = G_n^{l_1} G_m^{l_2} \cdots G_n^{l_{q-1}} G_m^{l_q}$ from Equation (2.29), where the ratio in Equation (2.28) is set to $\alpha = 1$; adopted from Ref. [55].

2.3.2 Multi-stage strategy for quantum search

Another significant contribution from Ref. [55] is a multi-stage quantum search algorithm that divides the quantum search algorithm into separate circuits (with reinitializations and measurements) that each find the m bits of the target element $|s\rangle$ (similar to the partial search). Each subsequent stage is dependent on the results of the preceding stage to reinitialize the subsequent circuit such that the first m_1 bits of the target are those found from the preceding, then find another m_2 of the target element. This process is repeated until we have all the bits of the target element are recovered. In each subsequent stage, the diffuser operators no longer act on the reinitialized subspace from the preceding stage. This greatly reduces the number of elementary operations (hence circuit depth) in each subsequent stage. The great advantage of such a multi-stage algorithm is mostly due to the reinitializations, since coherence no longer has tp be maintained over one long circuit, and is renewed on each reinitialization, preventing the effects of noise from accumulating. The steps for a two-stage quantum search from Ref. [55] are given below and the circuit diagram schematic is shown in Figure 2.13

1. *Initialization*

   Prepare $|0\rangle^{\otimes n}$ and apply $H^{\otimes n}$ on all the qubits, creating a uniform superposition of $N = 2^n$ basis states:

   $$|0\rangle^{\otimes n} \to \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \,.$$

   The target element is $|s\rangle$ is bipartitioned into $|s\rangle = |s_1\rangle \otimes |s_2\rangle$, where s_1 is m_1 bits long and s_2 is m_2 bits long such that $m_1 + m_2 = n$.

2. *Finding* $|s_1\rangle$

   Apply the sequence of Grover iterates $S_{n,m_2}(\bar{l}) = G_n^{l_1} G_{m_2}^{l_2} \cdots G_n^{l_{q-1}} G_{m_2}^{l_q}$:

   $$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \to \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} S_{n,m_2}(\bar{l}) \, |x\rangle \,,$$

   where the local Grover operator G_{m_2} are acting on the m_2 qubit subspace.

3. *First round of measurements*

   Measure the on the m_1 qubit subspace in the computational basis; Suppose we obtain the bit string outcome $b = b_0 b_1 \cdots b_{m_1-1}$; the probability for obtaining this outcome is denoted by $P^{(1)}_{n,m_2}(\bar{l})$.

4. *Reinitialization*

   Restart the computation to $|0\rangle^{\otimes n}$ and prepare the state $|b_0 b_1 \cdots b_{m_1}\rangle$ on the first m_1 qubits by applying $X^{b_0} \otimes X^{b_1} \otimes \cdots \otimes X^{b_m}$ on $|0\rangle^{\otimes n}$. Apply $H^{\otimes m_2}$ on the m_2 qubit subspace, creating a uniform superposition of $M = 2^{m_2}$ basis states on this subspace:

$$X^{b_0} \otimes X^{b_1} \otimes \cdots \otimes X^{b_m} H^{\otimes m_2} |0\rangle^{\otimes n} \rightarrow \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |b_0 b_1 \cdots b_{m_1-1}\rangle \otimes |x\rangle .$$

5. *Finding* $|s_2\rangle$

   Apply the sequence of Grover iterates $S_{m_2,m'}(\bar{l}') = G_{m_2}^{l'_1} G_{m_2,m'}^{l'_2} \cdots G_{m_2}^{l'_{q-1}} G_{m_2,m'}^{l'_q}$:

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |b_0 b_1 \cdots b_{m_1-1}\rangle \otimes |x\rangle \rightarrow \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |b_0 b_1 \cdots b_{m_1-1}\rangle \otimes S_{m_2,m'}(\bar{l}') |x\rangle .$$

6. *Second round of measurements*

   Measure the on the m_2 qubit subspace in the computational basis; Suppose we obtain the bit string outcome $b' = b'_0 b'_1 \cdots b'_{m_2-1}$, the probability for obtaining this outcome is denoted by $P^{(2)}_{m_2,m'}(\bar{l}')$.

7. *Verify solution*

   We verify the solution $s = b_1 b_2 \cdots b_{m_1-1} b'_{m_1} b'_{m_1+1} \cdots b'_n$ by simply checking the boolean function χ in Equation (2.1) if $\chi(s) = 1$. If it happens that $\chi(s) = 0$, then we go back to step 1.

Similarly, as they define the expected depth for the two-stage algorithm for the different sequences in the algorithm

$$\tilde{d}(\alpha) = \frac{d(S^{(1)}_{n,m_2}(\bar{l})) + S^{(2)}_{m_2,m'}(\bar{l}'))}{P^{(1)}_{n,m_2}(\bar{l}) P^{(2)}_{m2,m'}(\bar{l}')}, \tag{2.33}$$

and minimize the above quantity with respect to m_2, m' and $\bar{l}, \bar{l}'$

$$\tilde{d}(\alpha) = \underset{m_2,m',\bar{l},\bar{l}'}{\text{minimize}} \frac{d(S^{(1)}_{n,m_2}(\bar{l})) + S^{(2)}_{m_2,m'}(\bar{l}'))}{P^{(1)}_{n,m_2}(\bar{l}) P^{(2)}_{m2,m'}(\bar{l}')}. \tag{2.34}$$

The optimal two-stage quantum search sequences for $\alpha = 1, n \in \{3, 4, \ldots, 10\}$ are shown in Table 2.4.

	$S_{n,m}(\bar{l})$		$P_{n,m}(\bar{l})$		$d(S_{n,m}(\bar{l}))$		
n	Stage 1	Stage 2	Stage 1	Stage 2	Stage 1	Stage 2	$d(\alpha = 1)$
4	$S_{4,2}(1,1)$	$S_{2,0}(1,0)$	0.953	1	48	18	69.25
5	$S_{5,2}(1,1)$	$S_{2,0}(1,0)$	0.658	1	96	34	197.51
6	$S_{6,2}(1,1,1,1)$	$S_{2,0}(1,0)$	0.791	1	384	66	569.22
7	$S_{7,4}(1,4)$	$S_{2,0}(2,0)$	0.739	0.908	792	274	1587.09
8	$S_{8,5}(1,4,1,2)$	$S_{5,4}(1,1,2)$	0.882	0.998	1806	724	2876.40
9	$S_{9,5}(1,4,1,3,1,3)$	$S_{5,4}(1,1,2)$	0.096	0.998	3542	884	4898.88
10	$S_{10,5}(1,4,1,3,1,3,1,3)$	$S_{5,4}(1,1,2)$	0.810	0.998	5485	1044	8081.89

Table 2.4: The minimum expected depth for the two-stage quantum search algorithm where the ratio in Equation (2.28) is set to $\alpha = 1$; adopted from Ref. [55].

The multi-stage quantum search algorithm also lends itself to a natural way to parallelization, that is, having each stage run on a different quantum processor [55].

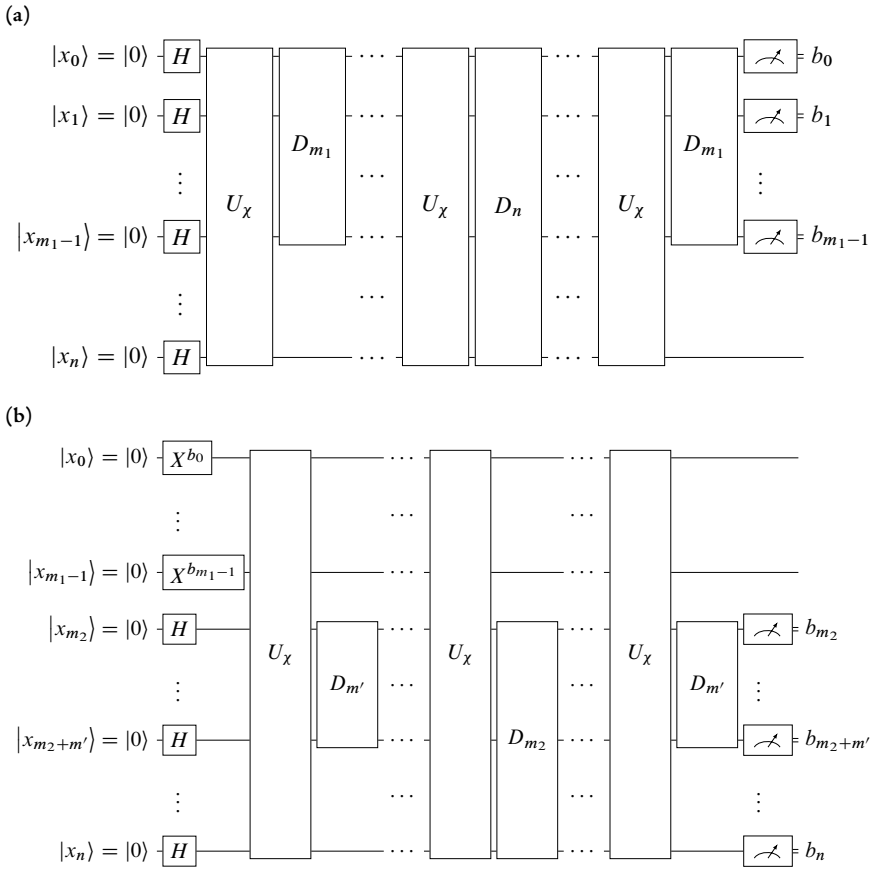


Figure 2.13: A schematic circuit diagrams for the two-stage quantum search algorithm; **(a)** In the first stage a sequence of local and global diffuser operators are used in conjunction to search for the first m_1 bits of the target element, where the local diffuser operators act on the first subspace of m_1 qubits, at the end of this stage, these qubits are measured in computational basis. **(b)** The second stage begins by first preparing the measured outcome from the first stage in the first m_1. Then a sequence of local diffuser operators are applied on the m_2 qubit space and on a smaller subspace of m' qubits. At end of this stage we measure all m_2 in the computational basis to recover the last m_2 bits of the target element.

However, unlike a parallelized classical unstructured search, it is not clear that such a parallelization would offer significant improvements in performance (in terms of number of steps) over the multi-stage quantum search algorithm on a single processor; for the canonical algorithm, the performance of such parallelization and multi-stage quantum search (not necessarily depth-optimal) are asymptotically equivalent [46].

2.3.3 Implementations on NISQ processors

The first (of great value) of the results of implementations of quantum search algorithms on NISQ processors is due to Wang and Kristic [56], who provided a thorough analysis of the performance of the quantum search algorithms presented here under different sources of errors and decoherence afflicting NISQ processors. By way of simulation, they consider the effects of gate errors such as phase, bit flips and depolarizing noise, and dissipative decoherence mechanisms such as amplitude and phase damping, with an increasing number of qubits used. To facilitate their analysis, they define a metric S they call selectivity

$$S = 10 \log_{10} (P_s / P_{hn}), \tag{2.35}$$

that quantifies the signal-to-noise of the measured probability of the target element (signal) P_s, in comparison to the highest measured probability among the non-target states (noise) P_{hn}. A negative value for the selectivity is deemed to indicate the search was unsuccessful as the measured probability of the target state is indistinguishable from the noise, *i.e.* $P_{hn} > P_s$.

In this way, the analysis is of how much of the various sources of noise can afflict a quantum search algorithm before the selectivity goes below a certain threshold, above which they consider the search to be successful, and defines the greatest strength of the afflicting noise source tolerated by the algorithm [56].

The results in the aforementioned reference show that the depth-optimized quantum search algorithm of Ref. [55], particularly the two-stage variant has better tolerance than the canonical algorithm under the various noise sources. Additionally, if one incorporates the use of n-qubit controlled-NOT gates that use one auxiliary qubit of the form in Ref. [66], the noise resilience of both the canonical and depth-optimized quantum search algorithms can be improved. This improvement is cited as due to the reduction in the number of elementary gates in comparison to using n-qubit controlled-NOT gates without auxiliary qubits[12].

[12] The n-qubit controlled-NOT gate synthesis due to Barenco et al. [66] uses $48n - 208$ controlled-NOT gates with a linear depth; a much more economical synthesis is due to He et al. [65], which uses $24n - 72$.

The first experimental demonstration to this topic of research of a four-qubit quantum search algorithm on a real NISQ processor is due to Gwinner et al. [57]. Distinct from the schemes presented here thus far, both constructions of the phase oracle and diffuser operators in Ref. [57] are tailored towards the connectivity of the NISQ processors. Their circuit for the four-qubit case of Grover's algorithm uses local diffuser operators with controlled-controlled-Z gates aided by a single auxiliary qubit. They are able to construct the diffuser operators in a way that mitigates the limits of qubit connectivity on a physical device. For instance, the standard decomposition of a three-qubit controlled-Z gate shown in Figure 2.11 is modified to the form shown in Figure 2.14. The great advantage of the latter circuit is that the controlled-NOT gates in the circuit are only acting between successive qubits, *i.e.* qubits connected in a line. Thus, the circuit can be transpiled to a physical NISQ processor with such a topology without incurring additional SWAP gates.

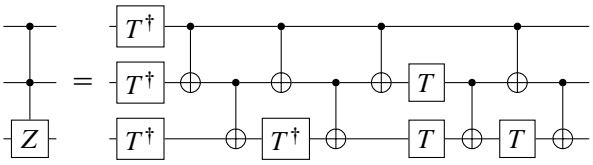


Figure 2.14: A circuit diagram showing the decomposition of a controlled-controlled-Z gate in terms of elementary gates such that it can realized on a set of qubits that are connected in a line; six controlled-NOT and seven $T/T^\dagger$ gates.

The modified gate is used to construct the four-qubit controlled-Z used in the phase oracle in a way that is suitable for NISQ devices with low connectivity, with the aid of one auxiliary qubit. To aid with the construction, they make use of a three-qubit controlled-Y gate ($ZX = Y$) shown in Figure 2.15.

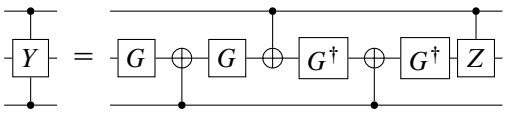


Figure 2.15: A circuit diagram showing the decomposition of a controlled-controlled-Y gate in terms of elementary gates such that it can realized on a set of qubits that are connected in a line; three controlled-NOT, one controlled-Z and seven $G/G^\dagger$ gates, where $G = R_y(\pi/4)$.

The above gate, due to Margolus [67], is also suitable for a line topology, since the controlled-NOT gates are between successive qubits. Hence, in Ref. [57] a four-qubit controlled-Z shown in Figure 2.16. With above multi-qubit gates adapted for NISQ devices with low connectivity among their physical qubits, Gwinner et al. [57] were able to successfully conduct a four-qubit quantum search algorithm on IBM Q processors.

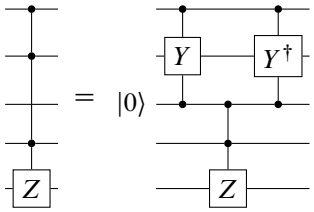


Figure 2.16: A circuit diagram showing the decomposition of a four-qubit controlled-Z gate with the help of one auxiliary qubit in terms of the controlled-Z construction in Figure 2.14 and the controlled-controlled-Y construction in Figure 2.15.

The four-qubit quantum search algorithm in Ref. [57] finds the target element with probability $> 21\%$ with a global diffuser operator (*i.e.* D_4) only and with a probability of 25% for a three qubit local diffuser operator (*i.e.* $D_{4,3}$). An additional significant contribution from Ref. [57] is another metric, similar to the selectivity from Ref. [56], that benchmarks the success of a quantum search algorithm on NISQ hardware. The so-called degraded ratio is defined as

$$R = \frac{P_{\text{exp}}}{P_{\text{theo}}}, \tag{2.36}$$

where P_{theo} is the theoretical probability of finding the target element and P_{exp} is the measured probability of finding the target element. A value close to one for the degraded ratio R indicates a good agreement between the theoretical and measured probabilities for finding the target element, and value close to zero is indicative of the reverse. The study in Ref. [57] reports that the degraded ratio R decays exponentially with the number of two-qubit gates in a circuit for a quantum search algorithm. For the 5-qubit **ibmq_vigo** processor, the degraded ratio decays drastically when a circuit for a quantum search algorithm is transpiled down to aforesaid physical device and the two-qubit gate count exceeds 30 gates [57].

Recently, Zhang et al. [59] improved over above the demonstration in Ref. [57] by using the connectivity-aware multi-qubit gates in the latter reference, and incorporating them into the depth-optimized and two-stage quantum search algorithms in their earlier work [55]. Their two-stage algorithm with these connectivity-aware multi-qubit gates incorporated, achieves a probability of success above 30%. Similar to Ref. [57] they report that above a 30 two-qubit gate count, the degraded ratio decays sharply. Lastly, they attempted to run a five-qubit quantum search algorithm; due to the increased number of gates, the success of their endeavor is inconclusive as their results are comparable to a classical search, roughly 6.25% probability of finding the target element [59].

2.4 Results

2.4.1 Application of the Grover's algorithm: Maximum cut graph problem

As already alluded to in the introduction of this chapter, Grover's algorithm can applied to a range of combinatorial search and optimization problems such as graph problems. However, as we have seen, their realization on NISQ processors may be unattainable due to the limitations of these devices. As a result, there is growing emphasis on designing and benchmarking the performance of algorithms in a manner that is aware of such limitations. Ref.[54] is another recent result that emphasizes the above point; Satoh et al. [54] propose an adaption of Grover's algorithm suitable for NISQ processors (reduction of two-qubit gate count and a connectivity-aware design), and apply it to solve the five vertex maximum cut (MAX-CUT) problem for a sparse graph.

The MAX-CUT problem is formally stated as follows: For an undirected graph $G = (V, E)$, with $|V|$ vertices and $|E|$ edges, each cut in $G = (V, E)$ is a subset of vertices $S \subset V$. The complement set of the cut S is given denoted by $\bar{S} = V \setminus S$, and $E(S, \bar{S})$ denotes the set of edges with a vertex in S and another in $\bar{S}$. Edges of G that one vertex in S, and other in $\bar{S}$ are referred to as cut edges, and the $E(S, \bar{S})$ is the set of cut edges. Hence, the MAX-CUT problem aims to find a cut S that maximizes the number of cut edges $|E(S, \bar{S})|$. Visually, one can think of the MAX-CUT problem as using two colors palette to color the vertices of G, one color is labeled as S and the other as $\bar{S}$. We begin by assigning each vertex in G a color, either from either S or $\bar{S}$ (repeating colors is allowed). Then we tally up the number of edges that exist between different colored vertices. Once we have exhausted all possible ways to color graph with the two colors, the color combination x with the greatest number of edges between the two colors S and $\bar{S}$ solves the MAX-CUT problem. Figure 2.17 shows an example of a MAX-CUT for a planar graph with five vertices, and the MAX-CUT color combination for this cut is given by $s = 00101$; Here vertices belonging to S are labeled with 0 and the vertices belong to $\bar{S}$ are labeled with 1.

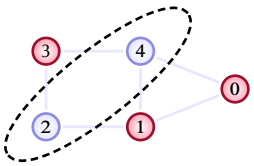


Figure 2.17: MAX-CUT on an example graph with five vertices. The vertices are colored with two different colors, red and purple. The dashed line shows the maximum cut.

The above visual interpretation is suggestive of an unsophisticated way to find such a MAX-CUT of a general graph $G = (V, E)$ by trying all possible $2^{|V|} - 1$ color combinations, that is, for each step we color in the vertices of G with the two colors and count the number of cut edges and continue until we have exhausted all combinations, then the color combination with the maximum number of cut edges is the MAX-CUT solution. Ref. [54] applied Grover's algorithm to solve the MAX-CUT by assigning the colors as $|0\rangle$ and $|1\rangle$, and designed a subdivided phase oracle that assigns a negative sign to the amplitude of the basis corresponding to color combination x with more edge connections than some threshold $t \leq |E|$.

The procedure for MAX-CUT of the graph $G = (V, E)$ is no different from the canonical algorithm; the aforesaid oracle and an appropriate diffuser operator are applied $\mathcal{O}(\sqrt{N})$ times to a uniform superposition $|+\rangle^{|V|}$ of $2^{|V|}$ basis states, with each representing a possible color combination. If the found measurement outcome x is a valid color combination for the current threshold, that is, a color combination with more than t cut edges, then we increase the threshold t and repeat. Otherwise, we decrease the value of t and if the value of t returns to a prior value, then the current measurement outcome is the MAX-CUT solution. The authors in Ref. [54] reason that we expect to repeat such a procedure $\mathcal{O}(\log(E))$ times to get MAX-CUT solution with high probability. This is because we can zone in on the value of t by repeatedly dividing the search interval for t in half and checking whether we get an legal or illegal output at the end of each iteration (binary search).

The proposed design for the oracle for a general graph $G = (V, E)$ in Ref. [54] is by way of subdividing the full oracle operator O into sub-oracles $O_{v,w}$, which checks if an edge $(v, w) \in E$ is a cut edge, that is, if the vertices v and w are colored differently. Thus, such a sub-oracle $O_{v,w}$ performs the following unitary transformation on two qubits $|q_v\rangle$ and $|q_w\rangle$, with each representing the vertices v and w, respectively

$$O_{v,w} |q_v\rangle |q_w\rangle |q_{\text{accum}}\rangle \rightarrow |q_v\rangle |q_w\rangle |q_{\text{accum}} + (q_v \oplus q_w)\rangle , \tag{2.37}$$

where q_{accum} is a register of an appropriate size that accumulates the number of cut edges.

Whenever the vertices v and w are colored differently, then the corresponding qubit states $|q_w\rangle$ and $|q_v\rangle$ will differ, *i.e.* $|q_w\rangle = |0\rangle$ and $|q_v\rangle = |1\rangle$ or $|q_w\rangle = 1$ and $|q_v\rangle = 0$; for such a scenario represents a cut edge and accordingly $q_w \oplus q_v = 1$ is accumulated to the accumulator register (it is a binary half adder from classical digital logic circuits).

The full oracle O for a general graph $G = (V, E)$ is realized by applying above sub-oracle $O_{v,w}$ between all pairs of vertices $(v, w) \in E$. An additional flag register that initially contains the state $|-\rangle$ is required. For a particular data input $|x\rangle$, if value in the accumulator register for the input $|x\rangle$ is equal to or exceeds t after the application of the full oracle O , multi-qubit controlled operations between the flag register and accumulator register are applied such that the flags register acquires a negative amplitude *i.e.* $-|-\rangle$. Effectively the joint state of all three registers acquires a phase, *i.e.* $-|x\rangle\,|q_{\text{accum}}\rangle\,|-\rangle$; see Ref. [54] for details. Their proposed scheme for the MAX-CUT problem was applied to both the four node graph $K_{1,3}$ and five node graph $K_{1,4}$ shown in (a) and (b) of Figure 2.18 as proof-of-concept demonstrations. For both $K_{1,3}$, $K_{1,4}$ graph, Ref. [54] reports that the realization of the full circuit on IBM Q processors was not possible as the circuits requires at least 36 controlled-NOT gates per iteration for even a smaller $K_{1,3}$ graph shown in Figure 2.18 (a), with the bulk of the controlled-NOT gates coming from the half adder that accumulates the number of cut edges, and which additionally adds to the number of qubits used by circuit, since it requires at least $\log(|E| + 1)$ qubits to store the number of possible cut edges [54]

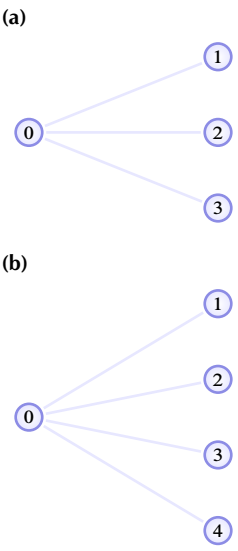


Figure 2.18: Tree graphs where the number of vertices $|V|$ is equal to the number of edges plus 1, $|V| = |E| + 1$. **(a)** $K_{1,3}$ and **(b)** $K_{1,4}$ star graphs, where in each case the vertex with the highest degree is the vertex 0.

To circumvent the above issue, Ref. [54] proposed a design for the above oracle that avoids the need for storing the number of cut edges in binary data, which removes the need for both the accumulator and flag register, and the circuitry between the two registers. The proposed oracle significantly reduces the number of qubits and two-qubit gates in comparison to the original circuit at cost of accuracy. For a two-qubit state $|q_v\rangle\,|q_w\rangle$ with each representing a vertex v and w in a general graph $G = (V, E)$, respectively; the action of the new subdivided phase sub-oracle $O_{v,w}(\theta)$ is given by

$$O_{v,w}(\theta)\,|q_v\rangle\,|q_w\rangle = e^{i\theta}\,|q_v\rangle\,|q_w\rangle\,, \tag{2.38}$$

where $\theta \in (0, \pi]$. Similarly, the full oracle $O(\theta)$ is realized by applying the above sub-oracle $O_{v,w}(\theta)$ to all pairs of vertices $(v, w) \in E$ in $G = (V, E)$. If the basis state $|s\rangle$ represents the color combination s for a vertex in $G = (V, E)$ that gives the MAX-CUT solution, applying the $O_{v,w}(\theta)$ between all pairs of vertices $(v, w) \in E$ on $|s\rangle$ gives

$$O(\theta) \equiv \prod_{(u,w)\in E} O_{u,w}(\theta)\,|s\rangle = e^{ik\theta}\,|s\rangle\,, \tag{2.39}$$

for some value of $k \leq |E|$, such that $k\theta \leq \pi$. The value of k is the number of cut edges for the MAX-CUT color combination s. Hence the above oracle stores the number of cut edges for a particular color combination x in the phase information of the corresponding basis state $|x\rangle$ after the application of the full oracle $O(\theta)$. Clearly, for any other color combination x of the vertices that is not the MAX-CUT solution whose corresponding basis state $|x\rangle$ acquires the phase $e^{i\tilde{k}\theta}$, it must be that $\tilde{k} < k$.

The proposed algorithm then proceeds as usual by applying the above oracle and a global diffuser operator to the uniform superposition $|+\rangle^{|V|}$ of $2^{|V|}$ basis states, with each representing a possible color combination of the vertices in $G = (V, E)$. Recall the action of the diffuser operator on the amplitudes shown in Equation (2.16); the amplitude of the basis state $|x\rangle$ corresponding to the color combination x after the application of the full oracle $O(\theta)$ and global diffuser operator D_n will be

$$\alpha_x(\theta) = \frac{1}{2^{|V|}} \left(2 \langle \alpha(\theta) \rangle - e^{ik\theta} \right), \tag{2.40}$$

where $\langle \alpha(\theta) \rangle$ is the mean amplitude after the application of full oracle $O(\theta)$ on all vertex pairs $(v, w) \in E$ for a graph $G = (V, E)$. The oracle is designed in such a way that the angle θ for the full oracle $O(\theta)$ is by maximizing the probability

$$p(\theta) = \frac{1}{2^{|V|}} \left(\left| 2 \langle \alpha(\theta) \rangle - e^{ik\theta} \right| \right)^2, \tag{2.41}$$

probability of measuring the color combination x after one Grover iterate. Hence, for each iteration of the algorithm, we choose a $k \leq |E|$ and find a θ that maximizes the above probability, and appropriately increase or decrease k as described previously and repeat this process until we cycle back to a prior value of k.

It is worthy to note that each color combination (hence the MAX-CUT color combination) has a redundancy of two, *i.e.* if $x = 01010$ is a color combination then the binary complement (corresponding to swapping the colors) of $s = 10101$ is also a valid color combination. This redundancy can removed by fixing the color of one vertex; a natural choice is one with the most number of edges incident to it [54]. For the graph $K_{1,4}$ shown in Figure 2.18 (b) with $|V| = 5$ and $|E| = 4$ from Ref. [54]. The mean amplitude for such a graph after the full oracle $O(\theta)$ application on the uniform superposition has the form

$$\langle \alpha(\theta) \rangle = \frac{1}{2^{|E|}} \sum_{k=0}^{|E|} \binom{N}{k} e^{ik\theta}. \tag{2.42}$$

Alas, due to the many trials it takes to find a value for k that yields the MAX-CUT outcome with high probability for a general graph $G = (V, E)$, it is not clear whether proposed algorithm in [54] offers any significant improvement over a classical algorithm for the MAX-CUT problem. We suspect that this is the reasons the graphs $K_{1,3}$ and $K_{1,4}$ are chosen, as from their simple structure one can deduce that $k = 3$ and $k = 4$ respectively for $K_{1,3}$ and $K_{1,4}$, which corresponds to the number of edges in the MAX-CUT of each graph (see Figure 2.18). Hence, as a proof-of-concept demonstration for the $K_{1,4}$, the value of k is taken as $k = 4$ *a priori* rather than through iteration as described earlier. For $k = 4$, using Equation (2.42) to maximize $p(\theta)$ in Equation (2.41), one obtains $p(\theta_{\text{opt}}) \simeq 0.212$ with $\theta \simeq 0.323\pi$. The aforementioned probability of success is about half the probability of success given by the complete circuit with the accumulator oracle for $t = 4$ and a single grover iteration, $p \simeq 0.473$. *Caveat emptor*, for the input basis state $|s\rangle$ corresponding to the MAX-CUT color combination s where $k = 4$ and the input basis state $|x\rangle$ corresponding to a color combination x with no cut edges where $k = 0$, the corresponding probabilities for measuring both outcomes after amplitude amplification are equal for the graphs $K_{1,3}$ and $K_{1,4}$ for any θ.

This is because for $k = 0$ and $k = 4$, the absolute value (complex modolus) factors in Equation (2.41) are equal

$$|2\langle\alpha(\theta)\rangle - 1|^2 = \left|2\langle\alpha(\theta)\rangle - e^{i4\theta}\right|^2 \tag{2.43}$$

for any θ, where $\langle\alpha\rangle$ is of the form shown in Equation (2.42). Hence, we correctly detect the MAX-CUT and no-cut outcomes with equal probability; this is the trade-off in accuracy the algorithm suffers by encoding the number of cut edges in this way. The sub-oracle operation in Equation (2.38) for an edge $(v, w) \in E$ with the vertices v and w, represented by qubits $|q_v\rangle$ and $|q_w\rangle$, respectively, can be realized by the following circuit [54]

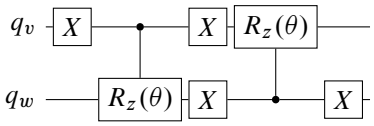


Figure 2.19: A circuit diagram that implements the sub-oracle $O_{v,w}(\theta)$ circuit for a pair of vertices $(v, w) \in E$ for a graph $G = (V, E)$, with each vertex represented by the qubits $|q_w\rangle, |q_v\rangle$ respectively. If $(v, w) \in E$ is a cut edge, then the vertices v, w are colored differently, hence the states $|q_v\rangle, |q_w\rangle$ differ then this circuit applies a $e^{i\theta}$ phase to joint state $|q_v\rangle |q_w\rangle$.

where $R_z(\theta) = \text{diag}(1, e^{i\theta})$ where $R_z(\theta)|0\rangle = |0\rangle$, $R_z(\theta)|1\rangle = e^{i\theta}|1\rangle$. In Ref. [54] for the graph $K_{1,4}$, to remove the redundancy of the MAX-CUT problem as described earlier in the passage, the color of vertex 0 in $K_{1,4}$ is fixed as 0 and corresponding qubit is set to $|0\rangle$. The vertex 0 is chosen because it has the highest degree and every other vertex in $K_{1,4}$ is connected to it. After this modification, the full oracle $O(\theta)$ is given by

$$O(\theta) = \prod_{(u,w)\in E} O_{u,w} = R_z^{(1)}(\theta) \otimes R_z^{(2)}(\theta) \otimes R_z^{(3)}(\theta) \otimes R_z^{(4)}(\theta). \tag{2.44}$$

Setting the qubit corresponding to vertex 0 as $|0\rangle$ removes the need of the controlled-$R_z(\theta)$ gates in since it is fixed at $|0\rangle$ and the sub-oracle $O_{0,w}(\theta)$ of the form in Figure 2.19 will always apply a $R_z(\theta)$ for any other vertex w connected to the vertex 0, and $O_{w,0}(\theta)$ will have no effect since $R_z(\theta)|0\rangle = |0\rangle$. Hence, for this reason the full oracle can be implemented with only single qubit gates on four qubits[13]. In Ref. [54], the global diffuser is implemented with a 4-qubit Toffoli gate with one auxiliary qubit. Thus, their proposed algorithm is implemented on five qubits with a total of 13 controlled-NOT gates (before transpiling it down to the physical device), and the $K_{1,4}$ graph is mapped onto the physical qubits of an IBM Q processor with the topology as shown in Figure 2.21 (a) (see Ref. [54] for more details).

[13] The qubit corresponding to the vertex **0** can thus be removed from the circuit, and taken to be a virtual vertex [54]. Thus, whenever we obtain the measurement outcome four-bit $x_1x_2x_3x_4$ on four qubits, it corresponds to the five-bit outcome $\mathbf{0}x_1x_2x_3x_4$ for the original MAX-CUT for the graph $K_{1,4}$.

The first of our marginal contributions to this topic of research is an improvement in the success probabilities of the MAX-CUT implementation for the $K_{1,4}$ graph in [54] by way of a further iteration using an additional local diffuser operator. Before we present our results, for comparison we implemented their scheme on the four-qubits without the use of an auxiliary qubit for the four-qubit Toffoli gate. The circuit is shown in Figure 2.20 and mapping of vertices (qubits) onto the physical device is shown in Figure 2.21 (b). The angle θ is taken to be $\theta \simeq 0.323\pi$, which maximizes the probability of measuring the MAX-CUT solution. With the mapping shown in Figure 2.21 (b), the circuit is transpiled to a physical device that contains 19 controlled-NOT gates in total, and has a circuit depth of 15. Figure 2.22 shows the measurement outcomes from two processors **ibmq_montreal** and **ibm_hanoi**, where measurement error mitigation has been applied to results, which mitigates the effect of readout errors on the raw results (see section § A.1 of technical Appendix A for details).

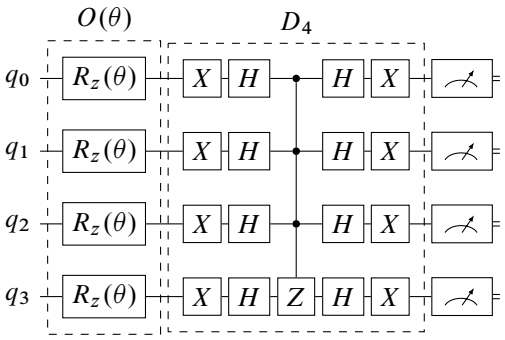
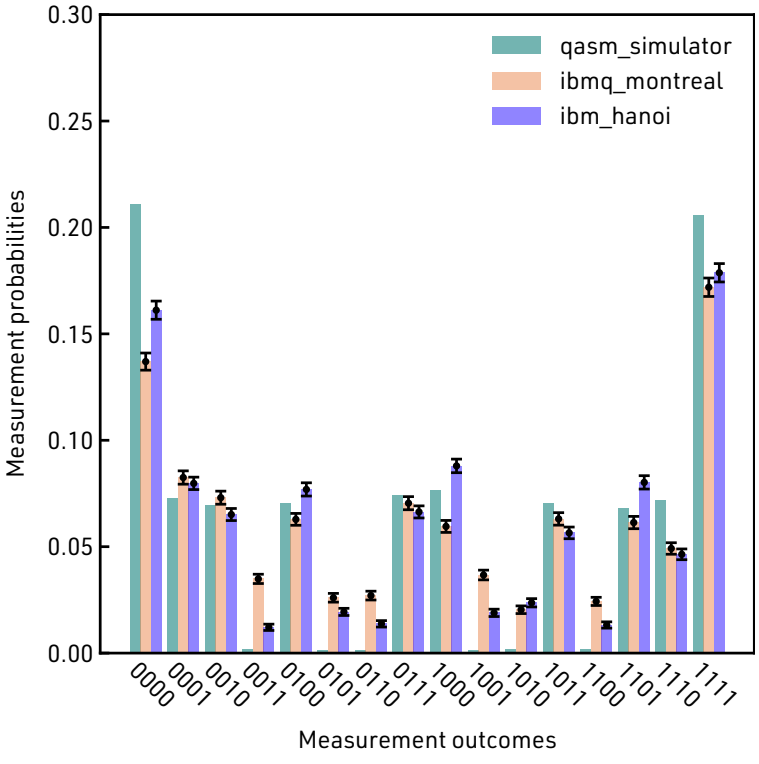


Figure 2.20: A circuit diagram for the MAX-CUT problem for the star graph $K_{1,4}$ in the study [54] realized on four-qubits. Here, one Grover iterate is used where $\theta \simeq 0.323\pi$ yields an ideal probability of observing the MAX-CUT outcome close to 0.212 upon measuring all the qubits in the computational basis.

The outcomes $x = 1111$, corresponding to the MAX-CUT solution and $x = 0000$, where no edge is cut. Recall since the qubit corresponding to vertex 0 of $K_{1,4}$ is set to 0, hence the outcome $x = 1111$ corresponds to the $x = 01111$, likewise the outcome $x = 0000$ corresponds to $x = 00000$ for original MAX-CUT problem for the graph $K_{1,4}$. The aforesaid outcomes occur with probability close to 0.14 and 0.17, respectively on the **ibmq_montreal** processor. And occur with probability close to 0.16 and 0.18, respectively on the **ibm_hanoi** processor. The ideal probability is close to 0.21.

We compare the experimental and ideal probability distributions via the Kolmogorov distance [17], which measures the closeness of two discrete probability distributions P and Q and is defined by the equation $D(P, Q) \equiv \sum_{x \in \mathcal{X}} |P(x) - Q(x)|/2$, where $\mathcal{X}$ represents all possible outcomes. The Kolmogorov distance between the measured distribution and the ideal distribution is close to 0.1289 and 0.1730 for **ibmq_montreal** and **ibm_hanoi**, respectively. This is indicative that there is good agreement between measured and ideal probability distributions.



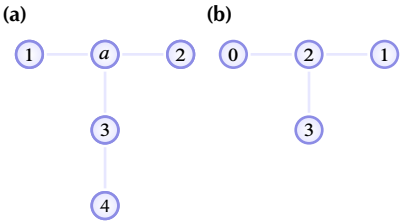


Figure 2.21: A T-shaped physical device mapping for the MAX-CUT algorithm for the $K_{1,4}$ star graph shown in Figure 2.18 (b) from the study [54]; The physical device mapping **(a)** uses an auxiliary qubit for the three-qubit Toffoli, indicated by the node a and the rest of the vertex of $K_{1,4}$ corresponds to a qubit with the same label on the device. While the mapping **(b)** uses no auxiliary qubits and each vertex of $K_{1,4}$ corresponds to a qubit with the same label on the device.

Figure 2.22: Results of the MAX-CUT problem for the star graph $K_{1,4}$ on IBM Q processors. The four-qubit circuit in Figure 2.20 is used where the qubit for vertex 0 is not included as described in the main text. On each processor, the circuit was executed 8192×900 times with measurement error mitigation. The error bars represent 95% confidence intervals around the mean value of each histogram bin (See § A.2 of technical Appendix A for details). The simulator probabilities show the ideal case.

Compared to the results in the study [54], they represent an improvement as they exceed 0.11 for the MAX-CUT solution. However, the comparison is a bit unfair, as the improvement of the results is probably indicative of the improvement of the capabilities of the IBM Q processors more than anything else, as the study [54] used earlier processors that could only tolerate lower two-qubit gates in a circuit than the currently reported 30 two-qubit gate limit for current IBM Q processors [57, 59]. More importantly, our transpiled circuit uses 6 more controlled-NOT gates.

We now improve the maximum ideal probability for measuring the MAX-CUT by using a further Grover iterate that uses a local diffuser operator as shown in Figure 2.23. The circuit is mapped to a physical device using the same mapping as in Figure 2.21 (b) as before, with the controlled-NOT gates in the transpiled circuit tallying to 33.

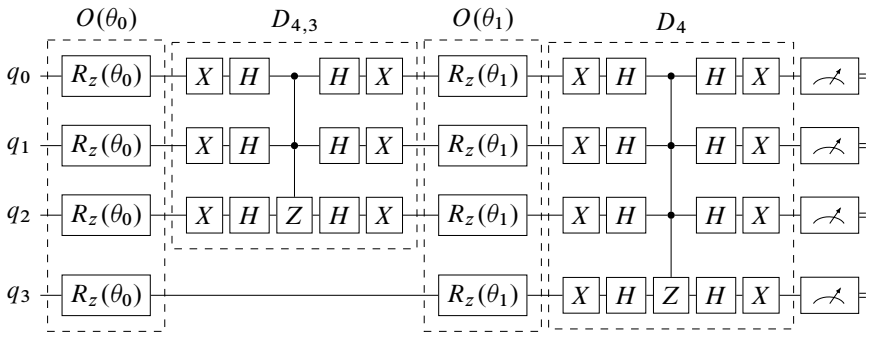


Figure 2.23: A circuit diagram for the MAX-CUT problem for the star graph $K_{1,4}$ realized on four qubits that uses two Grover iterates improves over the ideal probability of MAX-CUT in the study [54]. Here, one local Grover iterate $G_{4,3}(\theta_0)$ where $\theta_0 \simeq 0.323\pi$ and a global Grover iterate $G_4(\theta_1)$ where $\theta_1 \simeq 0.322\pi$ yield an ideal probability of observing the MAX-CUT outcome close to 0.25 upon measuring all the qubits in the computational basis.

We choose the values $\theta_0 = \theta_1 \simeq 0.323\pi$ (more on this choice later), for this choice the ideal probability of measuring the MAX-CUT is close to 0.25. Figure 2.24 shows the readout error mitigated results of measurement outcomes from the two processors.

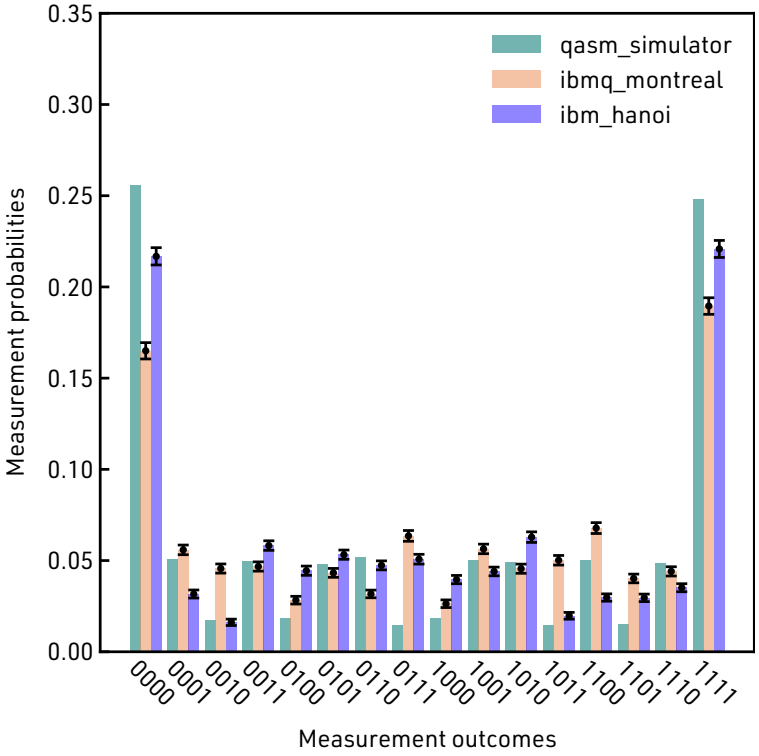


Figure 2.24: Results of the MAX-CUT problem with two Grover iterates for the star graph $K_{1,4}$ on IBM Q processors. The four-qubit circuit in Figure 2.23 is used where the qubit for vertex 0 is not included as described in the main text. On each processor, the circuit was executed 8192×900 times with measurement error mitigation. The error bars represent 95% confidence intervals around the mean value of each histogram bin (See § A.2 of technical Appendix A for details). The simulator probabilities show the ideal case.

The MAX-CUT outcome 1111, and the no-cut outcome 0000 (00000 and 01111 respectively since virtual vertex 0 is set to 0), occur with probability close to 0.16 and 0.19, respectively on the **ibmq_montreal** processor. And occur with probability close to 0.22 and 0.22, respectively on the **ibm_hanoi** processor. The Kolmogorov distance between the measured distribution and the ideal distribution is 0.1308 and 0.1844 for **ibmq_montreal** and **ibm_hanoi**, respectively. With an additional local diffuser operator, we have slightly improved over the results in Figure 2.22. At the time of writing this thesis, it dawned on the author that the choice of angles θ_0 and θ_1 as 0.323π for the circuit Figure 2.23 do not necessarily achieve the maximum possible ideal probability of measuring the MAX-CUT any more. The choice $\theta_0 \simeq 0.301\pi$ and $\theta_1 \simeq 0.541\pi$ for the circuit shown in Figure 2.23 yields a maximum ideal probability for measuring the MAX-CUT close to 0.311. Interestingly, another revelation that occurred to the author is that the local diffuser operator $D_{4,3}$ in Figure 2.23 can be replaced with a smaller local diffuser operator $D_{4,2}$ as shown in Figure 2.25. Choosing the angles θ_0 and θ_1 as 0.359π and 0.814π, respectively yields a probability of measuring the MAX-CUT close to 0.2482.

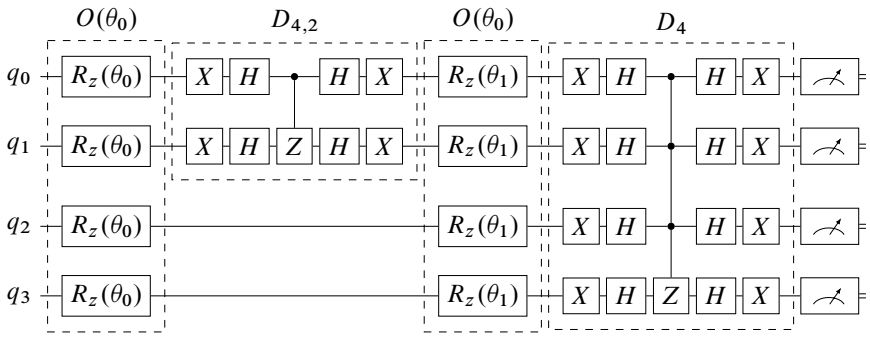


Figure 2.25: A circuit diagram for the MAX-CUT problem for the star graph $K_{1,4}$ realized on four qubits that uses two Grover iterates improves over the ideal probability of MAX-CUT in the study [54] even with a smaller local diffuser operator compared to Figure 2.20. Here one local Grover iterate $G_{4,2}(\theta_0)$ where $\theta_0 \simeq 0.359\pi$ and global Grover iterate $G_4(\theta_1)$ where $\theta_1 \simeq 0.814\pi$ yields an ideal probability of observing the MAX-CUT outcome close to 0.2482 upon measuring all the qubits in the computational basis.

Unfortunately, the author realized the aforementioned possibilities quite late in their thesis writing when they returned to the MAX-CUT problem and could not test the two circuits in shown Figure 2.23 and Figure 2.25 on the IBM Q processors in time. However, it is not too far-fetched to think that the results would slightly improve over the ones presented here, even more so, for the circuit in Figure 2.23, since it would be transpiled to a circuit with fewer two-qubit gates. This combination of local and global diffuser operators together with a subdivided oracle $O(\theta)$, where the θ are optimized at each stage to maximize the probability of observing the MAX-CUT solution, is an interesting direction for future work in realizing the MAX-CUT problem on NISQ processors.

However, it is unlikely that such an algorithm can be still considered as Grover's algorithm because we modify the angles of the oracle at each step by classically finding the optimal angles θ_i for the oracle $O(\theta_i)$ that achieve maximum probability of observing the desired outcome at that step. Such an algorithm is comparable to hybrid quantum/classical algorithms such as the variational quantum eigensolver (VQE) [68] and quantum approximate optimization algorithm (QAOA) [69]. In a similar fashion, the aforesaid algorithms seek to prepare some desired n-qubit state $|\psi\rangle$ that maximizes/minimizes some objective cost function. In the case of VQE, the desired state $|\psi\rangle$ is one that minimizes the expectation value $\langle\psi|H|\psi\rangle \,/\, \langle\psi|\psi\rangle$ with respect to some Hamiltonian H. For QAOA, $|\psi\rangle$ maximizes some cost function for an optimization problem such as the MAX-CUT (see Ref. [69] details).

For both algorithms at each step, a sequence of gates $U_1(\theta_1)U_2(\theta_2)\cdots U(\theta_n)$ parameterized with tunable parameter(s) $\vec{\theta}$ is applied to the current best approximation of $|\psi\rangle$ after which, a quantum computer evaluates the objective function and the classical computer aids by optimizing the parameters $\vec{\theta}$ for the next evaluation step. For the previously described scheme, the oracle $O(\theta)$ can be viewed as the $U_1(\theta)U_2(\theta)\cdots U(\theta)$ and the objective cost function is $p(\theta)$ from Equation (2.41). Recently, such a hybrid quantum/classical approach to Grover's canonical search algorithm has been considered in the study [70]. For a parametrized phase oracle and non-parametrized diffuser (and other), such a hybrid approach achieves a better success probability than Grover's algorithm canonical quantum search for small search space size N, asymptotically both algorithms have the same performance [70].

2.4.2 Quantum search in measurement-based quantum computing

The experimental demonstrations of Grover's algorithm have also been realized in the context of MBQC on graph states. The canonical quantum search algorithm on two qubits has been experimentally realized by different studies thus far [16, 71–73] on a four-qubit graph state. Common among the aforementioned references, is the realization that the canonical quantum search algorithm on two qubits naturally arises as a measurement procedure on a four-qubit box graph state shown in Figure 2.26.

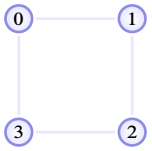


Figure 2.26: Four qubit box graph state realized by first preparing all qubits in the $|+\rangle$, and then applying controlled-Z gates between qubits with edges connecting them.

Recall that in MBQC, gates are simulated by performing measurements on an initially prepared graph state in the equatorial measurement basis $B(\alpha) = \{|+\alpha\rangle, |-\alpha\rangle\}$, where $|\pm\alpha\rangle_j = (|0\rangle_j \pm e^{i\alpha}|1\rangle)$. Thus if we measure qubits 0 and 3 in the basis $B_0(\alpha)$ and $B_3(\beta)$, respectively. This set of measurements effectively applies the $(X^{m_0}HR_z(\alpha))^{(q_0)} \otimes (X^{m_3}HR_z(\beta))^{(q_3)}CZ_{q_0q_3}$ on qubits $|q_0\rangle$ and qubit $|q_3\rangle$ of graph state shown in Figure 2.26 [14]. The values $m_0, m_3 \in \{0, 1\}$ denote measurement outcomes of the preceding measurements outcomes where a value of $m_i = 0$ or $m_i = 1$ indicates that we measured the $|+\alpha\rangle$ or $|-\alpha\rangle$ state, respectively, on qubit i. Lastly, we perform the measurement $B(\pi)$ on both qubits 1 and 2.

[14] See Ref.[74–76] for detailed descriptions of MBQC.

It is useful to write $X^{m_a}HR_z(\theta)$ as $HZ^{m_a}R_z(\theta)$ where we use the identity $XH = HZ$. From this, the effective two-qubit state after the above measurement procedure that resides on qubits 2 and 3 is equivalent to the circuit diagram shown in Figure 2.27 in the quantum circuit model. The aforementioned circuit realizes Grover quantum search algorithm on two qubits for an appropriate choice of the angles α and β, in the case where $m_0 = m_3 = 0$. For the choice of angles $(\alpha, \beta) = (-\pi, -\pi), (-\pi, 0), (0, -\pi)$ and $(0, 0)$, the phase oracle puts a negative sign on the amplitude of the state $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$, respectively. For any combination of m_0, m_3, the above circuit still realizes Grover's algorithm with an appropriate reinterpretation of the measurement outcomes. The interested reader may refer to section § B.1 of the technical Appendix B for more details.

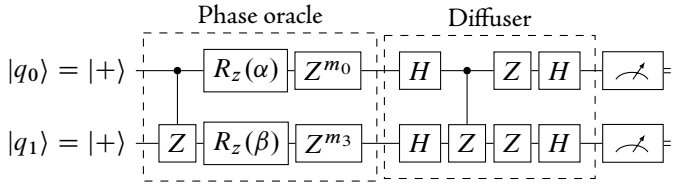


Figure 2.27: A circuit diagram equivalent of the remaining two qubit after the four-qubit measurement procedure described in the main text; the resultant circuit realizes Grover's algorithm for two qubits with the appropriate choice of angles α and β. For $(\alpha, \beta) = (-\pi, -\pi), (-\pi, 0), (0, -\pi)$ and $(0, 0)$ the circuit finds the target $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$ respectively.

In my honours studies, we realized the above measurement-based Grover's algorithm for two qubits successfully on IBM Q processors. Additionally, we were able to realize a measurement-based Grover's algorithm for two qubits on a graph state with one fewer edge, thus one less two-qubit gate in its state preparation. The original four-qubit graph state and the latter graph state belong to the same LU-equivalence class [77, 78]. The local unitaries relating the two states can be derived by successive applications of the edge local complementation rule [77, 78]. For the interested reader, the missing details are filled in sections § B.1 and § B.2 of the technical Appendix B.

Hence, we considered the next natural step; whether it would be possible to realize a measurement-based Grover's algorithm for three qubits. The initial hurdle was that the quantum circuit model equivalent of Grover's algorithm on three qubits does not naturally arise as a measurement procedure on any well known graph state unlike the case for two qubits, as far as we are aware. An unsophisticated way to circumvent this hurdle is to look for measurement-based implementations of the various gates in the quantum circuit model of Grover's algorithm for three qubits, and thus by constructing the measurement-based equivalent of each gate in the circuit and linking them together, one can realize the entire circuit as a measurement-based procedure. As we have seen earlier, the n-qubit $C^{n-1}[Z]$, in this case, a controlled-controlled-Z gate constitutes the most resourceful part in Grover's algorithm, appearing in both the phase oracle and diffuser operators. The canonical measurement-based controlled-controlled-Z due to Browne and Briegel [74] can be realized on a graph state of ten qubits. The measurement-based controlled-controlled-Z gate is a special case of a general result from the aforementioned reference, any n-qubit unitary operator diagonal in the computational basis of the form [74]

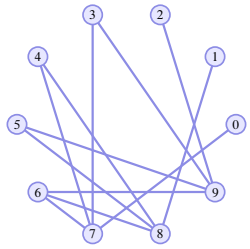


Figure 2.28: Ten-qubit graph state used as a resource for realizing a measurement-based three-qubit Toffoli gate. Qubits $0, 1, 2, 6$ are measured in the $HB(\pi/4)$ basis and qubits $3, 4, 5$ in the $HB(\pi/4)$ basis, which realizes a controlled-controlled-Z gate up to measurement outcome byproducts acting on the inputs in qubits $7, 8$ and 9 as two control and target qubits, respectively.

$$\begin{aligned} U_n &= \prod_{\vec{m}} \exp\left(i \frac{\theta_{\vec{m}}}{2} (Z_1)^{m_1} \otimes (Z_2)^{m_2} \otimes \cdots \otimes (Z_n)^{m_n} \right), \\ &= \exp\left(\frac{i}{2} \sum_{\vec{m}} \theta_{\vec{m}} (Z_1)^{m_1} \otimes (Z_2)^{m_2} \otimes \cdots \otimes (Z_n)^{m_n} \right), \end{aligned} \tag{2.45}$$

where $m_j \in \{0, 1\}$ and Z_j is the Pauli Z operator acting on qubit j. The sum is performed over all possible bit strings of length n. From the above form, the controlled-controlled-Z gate is realized by the following choice of angles

$$\begin{aligned} \theta_{000} = 0, \theta_{001} = -\frac{\pi}{4}, \theta_{010} = -\frac{\pi}{4}, \theta_{011} = \frac{\pi}{4}, \\ \theta_{100} = -\frac{\pi}{4}, \theta_{101} = \frac{\pi}{4}, \theta_{110} = \frac{\pi}{4}, \theta_{111} = -\frac{\pi}{4}. \end{aligned} \tag{2.46}$$

The ten-qubit graph state that realizes the three-qubit Toffoli gate is shown in Figure 2.28. The input qubits 7, 8 and 9 can be prepared in any single-qubit state rather than strictly $|+\rangle$ since qubits 7, 8 and 9 are designated as input controls and target qubits, respectively, for the MBQC controlled-controlled-Z gate. Thus, the procedure to realize a controlled-controlled-Z gate with input qubits $|c_1\rangle, |c_2\rangle, |t\rangle$ as follows: (i) Prepare inputs $|c_1\rangle, |c_2\rangle, |t\rangle$ to any state of our choosing, the rest of the qubits are prepared in the $|+\rangle$, and we perform controlled-Z gates on qubits connected by an edge in Figure 2.28. (ii) perform the projective measurements of the $HB(\theta) = \cos\theta/2\,|0\rangle \pm \sin\theta/2\,|1\rangle$, with $\theta = \pi/4$ for qubits $0, 1, 2, 6$ and $\theta = -\pi/4$ for qubits $3, 4, 5$, respectively [74].

The above measurement procedure realizes a three qubit controlled-controlled-Z gates acting on the inputs c_1, c_2, t and output of the gate residing on qubits 7, 8 and 9, up to the byproduct Pauli operators that arise from the measurement outcomes.

$$(Z^{m_0+m_3+m_4+m_6})^{(7)} \otimes (Z^{m_1+m_4+m_5+m_6})^{(8)} \otimes (Z^{m_2} Z^{m_3} Z^{m_5} Z^{m_6})^{(8)}, \tag{2.47}$$

where $m_i \in \{0, 1\}$ is an outcome from the aforementioned measurement procedure on qubit i, and the byproducts act on qubits 7, 8 and 9, respectively.

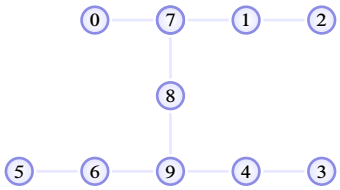


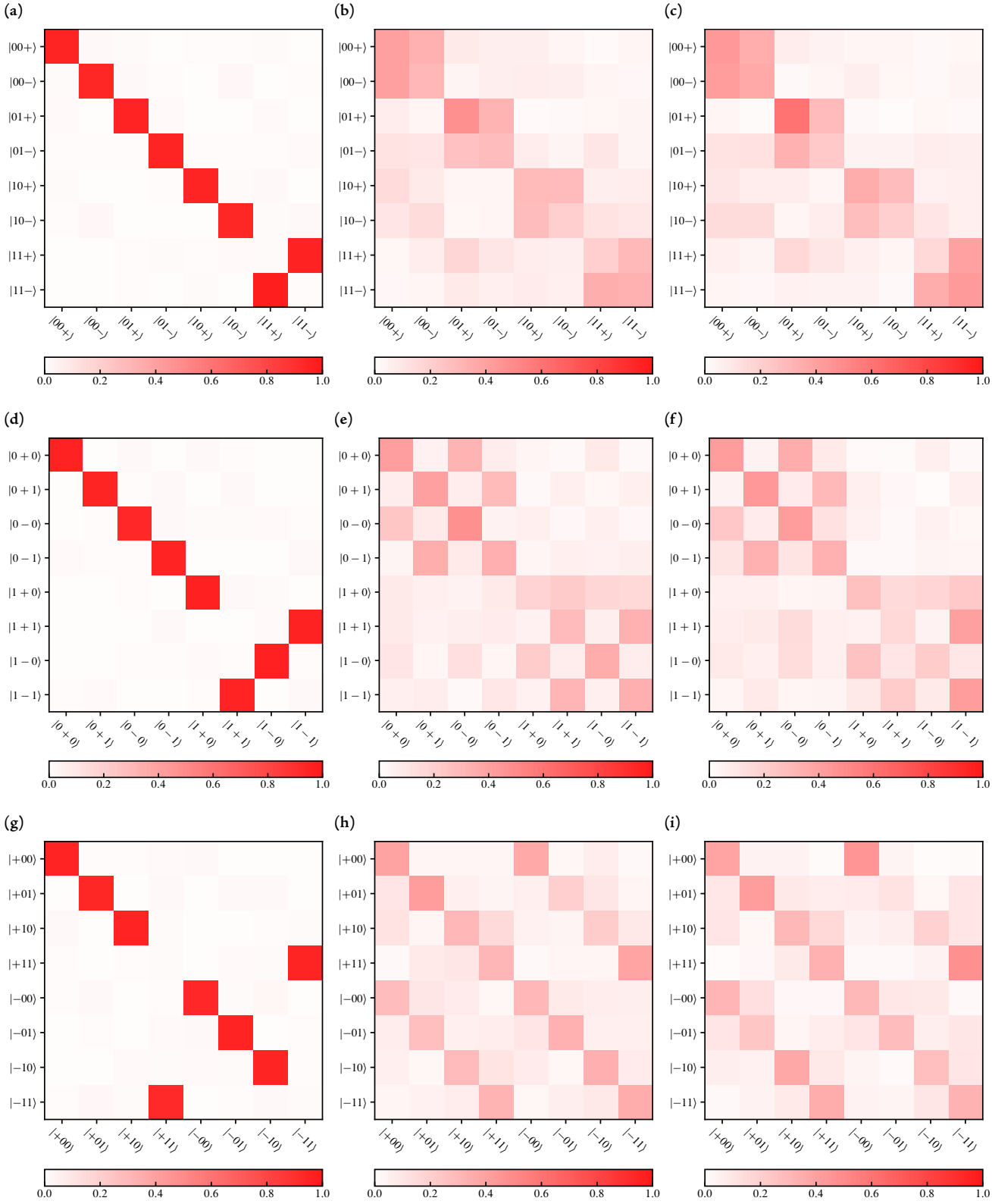
Figure 2.29: Physical device ten-qubit mapping for the ten-qubit graph state in Figure 2.28; each labeled node in the aforesaid is mapped to the corresponding labeled qubit in this figure.

In implementing the described measurement-based controlled-controlled-Z gate on IBM Q, we begin by mapping the graph state to the qubits of a physical device. The graph state in Figure 2.28 is highly connected, and no physical device exists with such a topology. Thus, we choose to map qubits that have the most connections to the physical qubits that have most connections on the physical device; in Figure 2.28 the qubits 7, 8 and 9 have the most edges. We show a physical device mapping in Figure 2.29, which results in 60 controlled-NOT gates for the transpiled circuit. Such a number of two-qubits gates in circuit is well-beyond the 30 two-qubit gate count limit [57], nonetheless we tested the measurement-based controlled-controlled-Z gate by preparing the qubits 7, 8 and 9 in various input states, and subsequently performed quantum state tomography to recover the corresponding output states, and then measured the state fidelity of each of the recovered output states against a set of expected output states. From these measurements, we are able to construct a truth table for the controlled-controlled-Z gate for various input and output states, this is shown in Figure 2.30. As seen can be seen by the naked eye, the discrepancies between the ideal truth tables and measured truth tables on the **ibmq_montreal** and **ibmq_mumbai** are quite conspicuous. We show the greatest element difference between the ideal and the measured truth tables for both processors in Table 2.5. The fourth truth table shows the smallest value among the truth tables, which corroborates with the visual representation of the fourth truth table in Figure 2.30, as it bears somewhat of an resemblance to the corresponding ideal truth table.

Figures	$\mathcal{E}_{\text{mumbai}} - \mathcal{E}_{\text{ideal}}$	$\mathcal{E}_{\text{montreal}} - \mathcal{E}_{\text{ideal}}$
(b) and (c)	0.427	0.395
(e) and (f)	0.401	0.336
(h) and (i)	0.435	0.353
(k) and (l)	0.308	0.268

Table 2.5: The maximum element difference between a measured truth table and corresponding ideal truth table for the truth tables of measurement-based controlled-controlled-Z in Figure 2.30.

Similar to the case for the four-qubit graph realizing Grover's algorithm for two qubits, we can hope to reduce the number of controlled-Z operations we have to apply to create the ten-qubit graph state shown in Figure 2.28 by finding an LU-equivalent graph state with fewer edges. However, it turns out that the graph state in Figure 2.28 corresponds to the one with the least number of edges in its LU-equivalence class. See the technical appendix Appendix B for details. Thus at the present moment a measurement-based implementation of a controlled-controlled-Z is beyond the reach of current NISQ processors. Which subsequently also puts realization of a measurement-based Grover's algorithm for three qubits beyond reach, since at least two controlled-controlled-Z and a few single qubit gates are required to realize Grover's quantum search algorithm for three qubits.


(a)
(b)
(c)
(d)
(e)
(f)
(g)
(h)
(i)
0.0
0.2
0.4
0.6
0.8
1.0

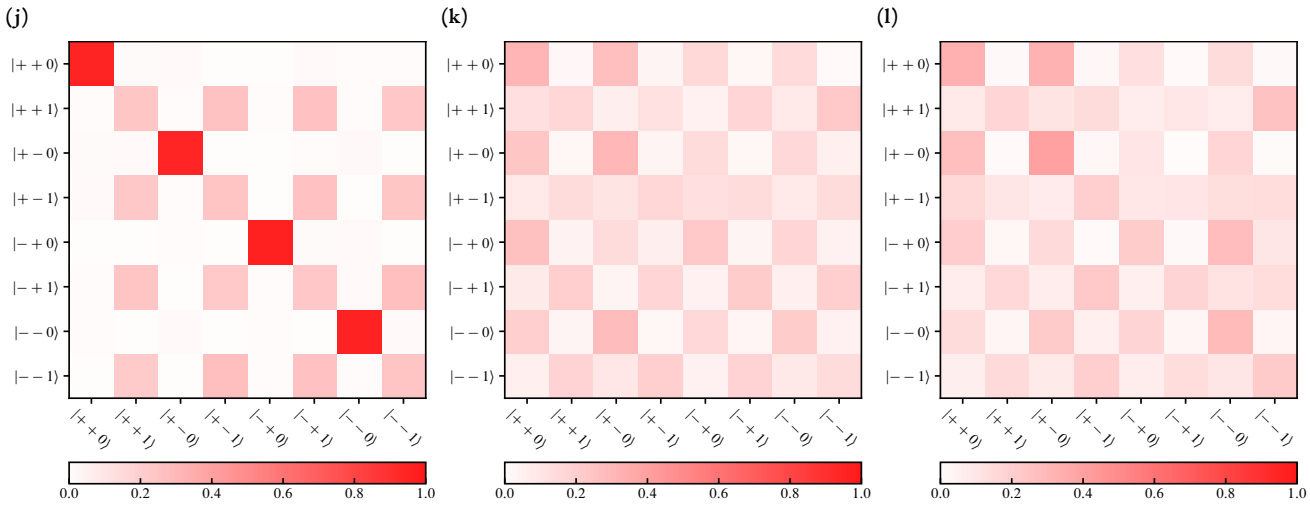


Figure 2.30: Various truth tables for the measurement-based three-qubit controlled-controlled-Z gate. Three figures in each row show a single truth table showing the ideal truth table and measured truth tables from the **ibmq_montreal** processor and the measured truth tables from **ibmq_mumbai** processor, respectively. When performing the state tomography on the outputs of the gate, we only consider where all the outcomes on the measured qubits are 0, resulting in no byproducts. **(a, d, g, j)** Ideal truth tables. **(b,e,h,k)** Measured truth tables from the processor **ibmq_montreal**. **(c, f, i, l)** Measured truth tables from the processor **ibmq_mumbai**.

2.5 Concluding remarks

In this chapter, we first began by describing the canonical quantum search algorithm, which assumes no *a priori* knowledge about the structure of the search problem. Such a quantum search algorithm achieves a quadratic speedup over an exhaustive classical search [14]. We also described a variant of the quantum search algorithm called the partial search quantum algorithm, which trades accuracy for speed by finding a partial bit string or target block to which the target element belongs rather than the target element itself [20]. With regards to practicality, especially on NISQ processors, the appealing feature of the quantum partial search algorithms in comparison to the canonical quantum search is that they are economical in the number of elementary gates and algorithmic steps they use, albeit the above advantage comes at the expense of accuracy. This realization prompted a large corpus of work interested in realizing small-scale demonstrations of the quantum search algorithm for four qubits and beyond, by reducing the number of elementary operations, particularly two-qubit gates, in quantum search algorithms.

Two important theoretical results along these lines were the depth-optimization of the quantum search algorithm, and multi-stage quantum search [55], which both place an emphasis on and try to circumvent one of the foremost pressing limitations of NISQ processors; short periods of time over which NISQ can maintain quantum coherence. The depth-optimized quantum search algorithm optimizes circuit depth of the quantum search algorithm, and hence the algorithmic (proxy) time spent on the processor. The multi-stage quantum search takes this a further step, by breaking up the quantum search algorithm into smaller stages. Each stage performs a smaller quantum search for a substring of the target element at a time, and is executed by a reinitialized circuit. The great advantage of the multi-stage quantum search is that it splits circuits (which would require long coherence times for reliable execution) into smaller circuits that perform the quantum search stage by stage, recovering the target element substring by string, which then reduces the time over which the qubits in each circuit must remain coherent for a reliable execution of the quantum search algorithm, since these qubits are reinitialized at each stage.

Studies in such a direction, eventually led to the first realization of a four-qubit quantum search algorithm on IBM Q processors [57]. The aforesaid study follows suite in finding ways to circumvent the limitations of NISQ processors; by designing multi-qubit gates such as the controlled-Z and controlled-controlled-Z in a manner that is suitable for physical quantum processors with limited connectivity between their physical qubits. Similarly, Ref. [59] experimentally realized an improved a four-qubit quantum search algorithm through incorporating the methods in [55] on IBM Q processors. The study in Ref. [59] also reported an inconclusive five-qubit quantum search algorithm with a success probability comparable to a classical search. Lastly, an application of Grover's algorithm to the MAX-CUT problem was studied by Ref. [54] successfully implementing a proof-of-concept demonstration on IBM Q processors for sparse graphs by proposing a design for a low-depth subdivided phase oracle that assigns a large phase shift to target outcomes and compared to non-target elements. Alas, the advantage for such a demonstration over a classical algorithm was not proved. Nonetheless, our marginal contribution is an adaptation that improves over the theoretical and measured success probability for the MAX-CUT by way of an additional shallow depth iteration of the proposed algorithm. Furthermore, we found that if we vary and optimize the phases imparted by the oracle to between iterations to maximize the probability of obtaining the MAX-CUT outcome, we can further increase the theoretical success probability for our contributed adaptation. However, it is not clear whether such an adaptation can be still considered as Grover's algorithm; it is comparable to hybrid quantum classical algorithms [68–70].

Prompted by the success during my Honours studies of a measurement-based Grover's quantum algorithm for two-qubits, we attempted to realize a measurement-based Grover's algorithm for three qubits. We found that, due to the large number of qubits (10) and controlled-NOT gates (>60) required for simulating a measurement-based controlled-controlled-Z gate on IBM Q processors, the output of the controlled-controlled-Z gate for various truth tables is comparable to uniform noise. Hence, the realization of a three-qubit measurement-based Grover's algorithm is somewhat out of reach for these processors; the situation is even more bleak when we consider that Grover's algorithm for three-qubits requires at least two such gates (one for the phase oracle and another for a diffuser operator) and a few single qubits, which must linked together somehow to realize the full measurement-based quantum search algorithm for three qubits.

Another measurement-based implementation of a controlled-controlled-Z (or controlled-controlled-NOT) gate is due to Tame et al. [79], which realizes a controlled-controlled-Z gate on a graph state of 8 qubits. For the eight-qubit graph state in Ref. [79], some edges between the qubits are created in the usual way by applying a controlled-Z gate between qubits connected by an edge. While other edges are created with a controlled-$R_z(\theta)$ gate for a particular choice of θ, the standard controlled-Z gate corresponds to $\theta = \pi$. Edges created in this way are called weighted edges, and the angle θ for such an edge is said to be the weight of that edge. A graph state with edges is said to be a weighted graph [79]. The eight-qubit weighted graph state that realizes a measurement-based controlled-controlled-Z in Ref. [79] has one weighted edge, with a weight $\theta = \pi/2$ and the rest of edges have weight $\theta = \pi$ (corresponds to controlled-Z gate). However, such a measurement-based gate is not yet suitable for IBM Q processors as it requires real-time adaptive measurements for the realized controlled-controlled-Z gate to be deterministic.

As of Nov 2020, IBM's quantum processors do not yet support real-time classical conditionals necessary for the implementation of the adaptive measurements. Alas, in the future once the capability of performing real-time classical conditionals is added, it is not fully clear whether such a measurement-based controlled-controlled-Z gate would offer a significant improvement on NISQ processors over the one in Ref. [74], since the number of qubits and two-qubit gates for the two gates are comparable (8 *versus* 10 qubits , 11 *versus* 12 two-qubits gates, respectively).

3

Quantum prime factorization

3.1 Preface

This chapter is based on the work reported in Ref. [80], originally appearing in Nature Scientific Reports. It was co-authored by Professor Mark Tame and the author of this thesis. Both Professor Mark Tame and the author of this thesis conceived the idea and designed the experiments, with the author of this thesis performing the experiments. Both authors analyzed the results, contributed to the discussions and interpretations.

3.2 Introduction

HOR's algorithm [5] is a quantum algorithm that provides a way of finding the nontrivial factors of an L-bit odd composite integer $N = pq$ in polynomial time with high probability. There is no known classical algorithm that can solve the same problem in polynomial time [17, 18]. The crux of Shor's algorithm rests upon quantum phase estimation (QPE) [17], which is a quantum routine that estimates the phase φ_u of an eigenvalue $e^{2\pi i\varphi_u}$ corresponding to an eigenvector $|u\rangle$ for some unitary matrix $\hat{U}$. QPE efficiently solves a problem related to factoring, known as the order-finding problem, in polynomial time in the number of bits needed to specify the problem, which in this case is $L = \lceil \log_2 N \rceil$. By solving the order-finding problem using QPE and carrying out a few extra steps, one can factor the integer N.

A large corpus of work has been done with regards to the experimental realization of Shor's algorithm over the years. Similar to the experimental realization of Grover's algorithm discussed in the previous chapter, the pioneering work was performed with liquid-state nuclear magnetic resonance, factoring 15 on a 7-qubit computer [81]. The considerable resource demands of Shor's original algorithm were circumvented by using various approaches, including adiabatic quantum computing [82] and in the standard network model using techniques of compilation [83] that reduced the demands to within the reach of single-photon architectures [84–86] and a superconducting phase qubit system [87].

In 2012, a proof-of-concept demonstration of the order-finding algorithm for the integer 21 was carried out with photonic qubits using, in addition to the aforementioned compilation technique, an iterative scheme [88], where the control register is reduced to one qubit and this qubit is reset and reused [89]. However, factoring was not possible in this demonstration due to the low number of iterations. Later, the iterative scheme was demonstrated for factoring 15, 21 and 35 on an IBM quantum processor by splitting up the iterations and combining the outcomes [90]. Recently, building on previous schemes of hybrid factorization [91, 92], a quantum-classical hybrid scheme has been implemented on IBM's quantum processors for the prime factorization of 35. This hybrid scheme of factorization alleviates the resource requirements of the algorithm at the expense of performing part of the factoring classically [93].

The main result of this chapter builds on the order-finding routine of Ref. [88] and implements a version of Shor's algorithm for factoring 21 using only 5 qubits – the work register contains 2 qubits and the control register contains 3 qubits, each providing 1-bit of accuracy in the resolution of the peaks in the output probability distribution used to find the order. This approach is in contrast to the iterative version [94] used in Refs. [88] and [90], which employs a single qubit that is recycled through measurement and feed-forward, giving 1-bit of accuracy each time it is recycled. The advantage of the iterative approach lies in this very reason; through mid-circuit measurement and real-time conditional feed-forward operations, the total number of qubits required by the algorithm is significantly reduced. At the time of writing, IBM's quantum processors do not yet support real-time conditionals necessary for the implementation of the iterative approach, so we use 3 qubits for the control register, one for each effective iteration. Thus, our compact approach is completely equivalent to the iterative approach. In future, once the capability of performing real-time conditionals is added, a further reduction in resources will be possible for our implementation, potentially improving the quality of the results even more and opening up the possibility of factoring larger integers.

As it stands, the controlled-NOT gate count of the standard algorithm for $N = 21$ [95] exceeds 40. In our preliminary tests we found that the output probability distribution is indistinguishable from a uniform probability distribution (noise) on the IBM quantum processors. Our improved version reduces the controlled-NOT gate count through the use of relative phase Toffoli gates, reducing the controlled-NOT gate count by half while leaving the overall operation of the circuit unchanged and we suspect this technique may extend beyond the case considered here. We have gone further than the work in Ref. [88], where full factorization of 21 was not achieved as with only two bits of accuracy for the peaks of the output probability distribution, the final step of continued fractions would fail to extract the correct order. On the other hand, in the work in Ref. [90], where 21 was factored on an IBM processor, a larger number of 6 qubits was required and the iterations were split into three separate circuits, with the need to re-initialise the work register into specific quantum states for each iteration. Our approach is thus more efficient and compact, enabling algorithm outcomes with reduced noise. To support our claims, we successfully carry out continued fractions and evaluate the performance of the algorithm by (i) quantitatively comparing the measured probability distribution with the ideal distribution and noise *via* the Kolmogorov distance, (ii) performing state tomography experiments on the control register, and (iii) verifying the presence of entanglement across both registers.

3.3 Background

3.3.1 Order-finding

The order-finding problem is intimately related to that of finding prime factors[1] of a composite integer. The two problems are tied together with a few number and group theoretic results, we will follow [17, 18] and mention these in passing here.

[1] A prime number is any integer greater than 1, which only is divisible by 1 and itself.

Two positive integers N and $x \leq N-1$ are relatively prime to each other if they share no common factor, that is, the largest positive integer c that divides both N and x is 1. The integer c is called the greatest common divisor of the integers N and x, and denoted by $\gcd(x, N) = c$; for relatively prime integers N and x, $\gcd(x, N) = 1$. The set of positive integers x that are relatively prime to N, form a finite Abelian group [2] with the group operation being multiplication mod N, this group is denoted by $\mathbb{Z}_N^*$. Consider an arbitrary element x of $\mathbb{Z}_N^*$, the sequence

[2] Multiplication of elements in the group are also in the group (closure), multiplication under the group operation is associative and commutative, the group contains a multiplicative identity with respect to the group operation and every element in the group has a unique multiplicative inverse with respect to the group operation.

$$x^0 \bmod N = 1, x^1 \bmod N, x^2 \bmod N, x^3 \bmod N, \ldots, \tag{3.1}$$

this sequence of elements forms a subgroup (finite) of $\mathbb{Z}_N^*$. For the subgroup to be finite implies that the above sequence will not carry on indefinitely but repeat after several iterations, that is, there exists a positive integer r for which

$$x^r \bmod N = 1, \tag{3.2}$$

for positive integers greater than r, the sequence in Equation (3.1) will cycle again, restarting at integer multiples of r. Thus the size of the subgroup is given by the smallest integer r satisfying Equation (3.2), evidently $r \leq N$. Such an integer is called the order of element x in $\mathbb{Z}_N^*$. The order-finding problem may be stated as follows. Given two relatively prime positive integers N and $x \in \{0, 1, \ldots, N-1\}$, we seek to find the smallest positive integer $r \in \{0, 1, \ldots N\}$ such that $x^r \bmod N = 1$.

It is not immediately clear how the solution to the above problem has anything at all to do with prime factorization of composite integers. To see this, suppose we were able to find an even order r for two integers N and x,

$$\begin{aligned} x^r \bmod N &= 1, \\ x^r - 1 \bmod N &= 0, \\ (x^{r/2})^2 - 1 \bmod N &= 0, \\ (x^{r/2} - 1)(x^{r/2} + 1) \bmod N &= 0. \end{aligned} \tag{3.3}$$

The case where the solution to the last expression excludes both $x^{r/2} = 1$ and $x^{r/2} = N - 1$ (collectively, $x^{r/2} \bmod N \neq \pm 1$) is of particular interest, since this would mean that at least one of the factors $(x^{r/2} - 1)$ and $(x^{r/2} + 1)$, which are both greater than 0 and less than N, divides N. Computing the greatest common divisor $\gcd(x^{r/2} \pm 1, N)$, we can possibly learn at least one non-trivial prime factor of N, that is a factor of N is only divisible by 1 and itself only. The reasons why $\gcd(x^{r/2} \pm 1, N)$ is not always guaranteed to be a non-trivial prime factor of N are the crucial assumptions leading to the result; that the found order r is even so that for the chosen x relatively prime to N, $x^{r/2} \bmod N \neq \pm 1$, these two assumptions are not always true. However, they are true half of the time, it can be shown that the probability that the order r is even and a randomly chosen element x in $\mathbb{Z}_N^*$, satisfies $x^{r/2} \bmod N \neq \pm 1$ is greater than one half[3].

[3] The interested reader may refer for a proof of this statement in Theorem A4.13 of Ref. [17]

Thus we may find a prime factorization of a composite integer N with high probability, by finding the order of the group $\mathbb{Z}_N^*$. If we can efficiently compute the order of $\mathbb{Z}_N^*$, we can find an efficient algorithm to successfully compute the factors of N with high probability since the preliminary steps can be also be computed efficiently[4]. For a chosen N, (i) we can check easily check if it is even and return 2. (ii) We also can always check if $N = p^m$ is a prime power, and find p efficiently. (iii) To check if a chosen x is relatively prime to N, we compute $\gcd(x, N) = 1$ if not, then $\gcd(x, N)$ is a factor of N and the $\gcd(x, N)$ may be computed efficiently as well. (iv) Lastly, we compute the order of $x \bmod N$ and check if $\gcd(x^{r/2} \pm 1, N)$ yields a non-trivial factor of N, succeeding most of the time.

[4] An efficient algorithm is one that computes a solution to a problem in steps/elementary operations that scale polynomially with the intrinsic size of the problem. For prime factorization, the size of problem is the number of bits needed to specify N, $L \equiv \lceil \log_N \rceil$.

Classically, such an algorithm that solves the order-finding problem with steps that scale polynomially in the number of bits $L \equiv \lceil \log N \rceil$ needed to specify N is yet to be found [17, 18]. Here enters Shor's algorithm which efficiently solves the order-finding problem with a number of elementary operations that scale polynomially with $\lceil \log N \rceil$.

3.3.2 Shor's quantum algorithm for order-finding

Peter Shor's insight was the realization that the order-finding problem can reduced into another related problem, for which quantum computers were known to solve efficiently, that is, with a number of elementary operations (quantum gates) that scales polynomially. The latter problem is the finding an eigenvalue λ corresponding to an eigenvector $|u\rangle$ of a unitary matrix U, that is $U|u\rangle = \lambda|u\rangle$. Since U is unitary ($U^{-1} = U^\dagger$), its eigenvalues are complex numbers with unit modulus, since

$$1 = \langle u|u\rangle = \langle u|U^\dagger U|u\rangle = \lambda^*\lambda \langle u|\mathbb{1}|u\rangle = |\lambda|^2, \tag{3.4}$$

therefore λ may be parametrized by $\lambda = e^{2\pi i\varphi}$ with $\varphi \in [0, 1)$. The canonical QPE is due to Kitaev [96] (and later by Cleve et al. [97] in its current form) and provides an efficient way to estimate the value of φ. The quantum algorithm for order-finding is an instance of the QPE for the following unitary U_x. For two relatively prime positive integers x and N, and for $y \in \{0, 1, 2, \ldots, N-1\}$, the action of U_x on a computational basis element $|y\rangle$ is defined by:

$$U_x|y\rangle = |xy \bmod N\rangle. \tag{3.5}$$

The matrix U_x is unitary since $\langle y|y'\rangle = \delta_{y,y'}$ and

$$\begin{aligned}\langle y|U_x^\dagger U_x|y'\rangle &= \langle xy \bmod N|xy' \bmod N\rangle, \\ &= \langle xy|xy'\rangle, \\ &= \delta_{xy,xy'}, \\ &= \delta_{y,y'}.\end{aligned} \tag{3.6}$$

This because if $xy = xy' \implies x^{-1}xy = x^{-1}xy' \implies y = y'$, similarly $xy \neq xy' \implies y \neq y'$.

Since x is relatively prime to N, the multiplicative inverse $\bmod N$ of x exists. Recall from Equation (3.2) that if r is the order of $x \bmod N$, then $x^r \bmod N = 1$, for our unitary matrix U_x this means that for any computational basis state $|y\rangle$

$$(U_x)^r |y\rangle = |x^r y \bmod N\rangle = |y\rangle \implies (U_x)^r = \mathbb{1} \tag{3.7}$$

From the above fact, if $|u_k\rangle$ is an eigenstate of U_x, then the corresponding eigenvalues are r-th roots of unity,

$$\begin{aligned} \langle u_k|I|u_k\rangle = \langle u_k|(U_x)^r|u_k\rangle = \lambda_k^r = 1, \\ \lambda_k = e^{2\pi i k/r}, \quad k \in \{0, 1, 2, \ldots, r-1\}. \end{aligned} \tag{3.8}$$

With a little of bit algebraic deadlifting one can show that the corresponding mutually orthonormal eigenvectors are given by [17]:

$$|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{q=0}^{r-1} e^{2\pi i q k/r} \left| x^k y \bmod N \right\rangle, \tag{3.9}$$

for any y in $\{0, 1, 2, \ldots, N-1\}$ (for convenience, typically $y = 1$). Thus, in this instance for a given eigenstate $|u_k\rangle$ of U_x, the QPE algorithm provides an estimate of k/r, which if we are clever enough we may extract the order r.

Next, we summarize the QPE algorithm; given the unitary matrix U and an efficient way to apply the controlled-U^{2^j} operations in terms of other elementary gates, estimate φ for the eigenstate $|u_s\rangle$ of U with eigenvalue $e^{2\pi i\varphi}$. In the case of order-finding, each of the unitaries U^{2^j} carry out *modular exponentiation* on a basis state:

$$U_x^{2^j} |y\rangle = \left| x^{2^j} y \bmod N \right\rangle. \tag{3.10}$$

The QPE algorithm initially proceeds by preparing a set of n qubits in the state $|0\rangle$ and a Hadamard H gate is applied on each of the n qubits; preparing an equal superposition state of all the possible 2^n computational basis states

$$H^{\otimes n} |0\rangle^{\otimes n} = |+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle . \tag{3.11}$$

An eigenstate $|u_s\rangle$ of the unitary matrix U is prepared by another set of m qubits, resulting in the joint state at beginning of the algorithm.

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle \otimes |u_s\rangle . \tag{3.12}$$

This is then followed by repeated applications of the controlled-U operations, raised to successive powers of two as shown in Figure 3.1.

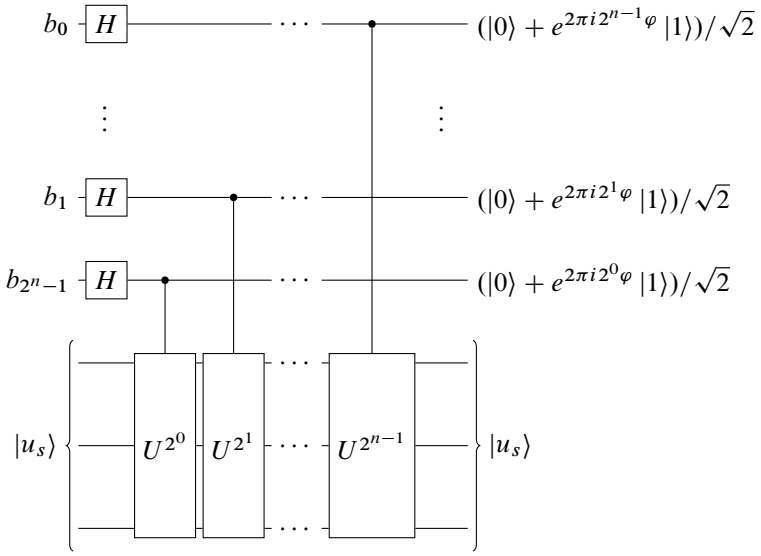


Figure 3.1: Part of the QPE routine.

To see the action of this step, we consider a particular computational basis state $|j\rangle$ in the above superposition, which we can write as a bitstring $|j\rangle = |b_0 b_1 b_2 \cdots b_{n-1}\rangle$, *i.e.* $j = b_0 2^{n-1} + b_1 2^{n-2} + \cdots + b_{n-2} 2^1 + b_{n-1} 2^0$ (in little endian). The application of a U^{2^i} is conditioned on the i-th (i-th qubit from the right most qubit) qubit being in the state $|1\rangle$, or equivalently the corresponding bit b_{n-i} being 1, otherwise it acts trivially. Thus, the action of the above step on a state $|j\rangle \otimes |u_s\rangle = |b_0 b_1 b_2 \cdots b_{n-1}\rangle \otimes |u_s\rangle$ is

$$\begin{aligned} |j\rangle \otimes |u_s\rangle &\mapsto |j\rangle \otimes U^{b_0 2^{n-1} + b_1 2^{n-2} + \cdots + b_{n-2} 2^1 + b_{n-1} 2^0} |u_s\rangle\,, \\ &= |j\rangle \otimes U^j |u_s\rangle\,, \\ &= |j\rangle \otimes e^{2\pi i s j / r} |u_s\rangle\,. \end{aligned} \tag{3.13}$$

By the linearity of the controlled unitaries, Equation (3.12) becomes,

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2\pi i s j / r} |j\rangle \otimes |u_s\rangle\,. \tag{3.14}$$

In general, modular exponentiation implemented by the controlled-U^{2^j} for order-finding may be realized with a number of elementary operations that scale polynomially in L, $\mathcal{O}(L^3)$ [17, 97]. The next crucial step in the QPE algorithm is the QFT, which is defined by its action on a computational basis state [17, 18],

$$|j\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle \tag{3.15}$$

The inverse QFT inverts the above operation. Applying the inverse QFT on the first set of n-qubits on the state in Equation (3.14), we arrive at the following state,

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2\pi i s j / r} |j\rangle \otimes |u_s\rangle \mapsto |2^n s / r\rangle \otimes |u_s\rangle\,. \tag{3.16}$$

The QFT (and its inverse) can be realized with two-qubit gates that asymptotically scale like $\mathcal{O}(L^2)$ [17, 18].

If s/r can be written exactly with n bits and we proceed to measure the state above in the appropriate measurement basis, we recover the bitstring of s/r with a probability of 1, and we can subsequently extract the value of r *via* a continued fractions expansion. Whenever this isn't the case (*i.e.* when s/r is not a fraction of a power of two), the algorithm still yields an n-bit approximation of s/r with high probability[5].

[5] The interested reader may refer to Ref. [17] and Ref. [97] for a thorough treatment of this case.

An assumption of the algorithm described above is that we can prepare one of the eigenstates of U in Equation (3.9), however this would require knowledge of r. Despite this, the algorithm still guarantees a high probability for obtaining an approximation of s/r. Recall that the eigenstates of U form an orthonormal basis, thus any general state $|\psi\rangle$ may be expressed as

$$|\psi\rangle = \sum_{q=0}^{r-1} \alpha_q \left|u_q\right\rangle. \tag{3.17}$$

Thus for a general $|\psi\rangle$, the probability to recover an approximation of s/r for a particular $|u_s\rangle$ is simply scaled with the probability to measure that particular $|u_s\rangle$, which is $|\alpha_s|^2$. For the case of order-finding it turns out that

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{q=0}^{r-1} \left|u_q\right\rangle, \tag{3.18}$$

and $|1\rangle$ is easy to prepare! Thus we use $|1\rangle$ in place of the $|u_s\rangle$, and when we perform a measurement at the end of the algorithm, the values of s are now randomly sampled from a uniform distribution of values in $\{0, 1, 2, \ldots r-1\}$. *Caveat emptor*, in such a scenario it might happen a particular s shares a common factor with r such that $s/r = p/q$, in which case continued fractions would incorrectly yield q, which we always check in constant time ($a^q \bmod N = 1$). Fortunately, with enough trials, we can successfully extract r in a constant number of steps. This is because for two independent trials of the algorithm yield that s_1/r_1 and s_2/r_1, respectively; if $\gcd(s_1, s_2) = 1$ then the candidate value of r is the least common multiple of r_1 and r_2, and the probability that $\gcd(s_1, s_2) = 1$ for two independent trials is greater than 0.25 [17].

The total cost of the order-finding quantum algorithm scales polynomially with L, with most of the cost being due to the modular exponentiation operation which requires $\mathcal{O}(L^3)$ quantum gates [17]. The continued fractions is classically realized with atomic steps that scale similarly. We conclude this section by summarizing Shor's quantum algorithm for order-finding:

Shor's algorithm for order-finding uses two quantum registers; a control register and a work register. The control register contains n qubits, each for one bit of precision in the algorithmic output. The work register contains $m = \lceil \log N \rceil$ qubits where m is the number of qubits to encode N. The measurement of the control register outputs a probability distribution peaked at approximately the values of $2^n s/r$, where s is associated with the outcome of the measurement and thus randomly assigned. The details of how the peaked probability distribution comes about are given in the order-finding routine outlined below. One can determine the order r from the peak values of the distribution using continued fractions, with a number of steps that scales polynomially in $\lceil \log N \rceil$, $\mathcal{O}(L^3)$.

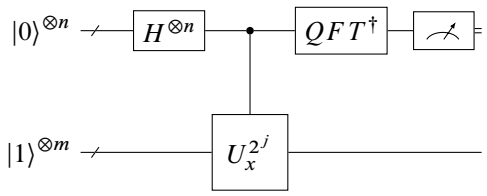


Figure 3.2: Circuit diagram schematic of the routine used for the period finding part of Shor's algorithm. The first (control) register has n qubits. The number of qubits in the control register determines the bit-accuracy of the value of $2^n s/r$. The bottom (work) register has the m qubits required to encode N. First, the control and work registers are initialized, then conditional modular exponentiation is performed, indicated by the controlled unitary and an inverse quantum Fourier transform is applied to the control register followed by a standard computational basis measurement. The circuit is essentially the QPE algorithm applied to the unitary matrix $\hat{U}_x$ – see text for details.

The procedure, or routine, for order finding is summarized below.

1. *Initialization*

   Prepare $|0\rangle^{\otimes n}\,|0\rangle^{\otimes m}$ and apply $H^{\otimes n}$ on the control register and $X^{\otimes m}$ on the m^{th} qubit in the work register to create a superposition of 2^n states in the control register and $|1\rangle^{\otimes m}$ in the work register:

   $$|0\rangle^{\otimes n}\,|0\rangle^{\otimes m} \to \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} |j\rangle\,|1\rangle^{\otimes m}\,.$$

2. *Modular exponentiation*

   Conditionally apply the unitary operation $\hat{U}$ that implements the modular exponentiation function $x^j \bmod N$ on the work register whenever the control register is in state $|j\rangle$:

   $$\begin{aligned}\frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} |j\rangle\,|1\rangle &\to \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} |j\rangle\,\left|x^j \bmod N\right\rangle \\ &= \frac{1}{\sqrt{r2^n}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^n-1} e^{2\pi i s j/r}\,|j\rangle\,|u_s\rangle\,.\end{aligned}$$

   In the second line, $|u_s\rangle$ is the eigenstate of $\hat{U}$: $\hat{U}\,|u_s\rangle = e^{2\pi i s/r}\,|u_s\rangle$ and $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$ has been used for the work register. This provides an alternative way to write the output state and allows a connection between the modular exponentiation operation and the QPE algorithm for the unitary operation $\hat{U}$.

3. *Inverse Quantum Fourier Transform* (QFT)

   Apply the inverse quantum Fourier transform on the control register:

   $$\frac{1}{\sqrt{r2^n}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^n-1} e^{2\pi i s j/r}\,|j\rangle\,|u_s\rangle \to \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\varphi_s\rangle\,|u_s\rangle\,.$$

4. *Measurements*

   Measure the control register in the computational basis, yielding peaks in the probability for states where $\varphi_s \simeq 2^n s/r$ due to the inverse QFT. Thus, the outcome of the algorithm is probabilistic, however, there is a high probability of obtaining the location of the φ_s peaks after only a few runs. The accuracy of φ_s to $2^n s/r$ is determined by the number of qubits in the control register.

5. *Continued fractions*

   Apply continued fractions to $\varphi = \varphi_s/2^n$ (the approximation of s/r) to extract out r from the convergents (see § C.4 of technical Appendix B for details).

3.4 Compiled Shor's quantum algorithm for order-finding

As mentioned in the previous section the most resource intensive part of Shor's quantum algorithm for order-finding is modular exponentiation, which is implemented by the controlled unitaries, thus an analysis of the resource demands for the algorithm are mostly to analyze the resource demands of the modular exponentiation function. We have seen that the controlled unitaries can be implemented with $\mathcal{O}(L^3)$ elementary quantum gates. However, the preceding analysis may take for granted the physical implementations of elementary gates. In Ref. [98], a full-scale implementation of Shor's algorithm to factor an L-bit number would require a quantum circuit with $\mathcal{O}(L^3)$ elementary quantum gates acting on $7L + 1$ qubits for the modular exponentiation. Here, the elementary gates are taken to be a single-qubit Pauli-X operation, a two-qubit controlled-X operation, and a Toffoli gate. Beckman et al. [99] devised a circuit for modular exponentiation that uses $5L + 1$ qubits and $72L^3$ similarly defined elementary gates, *i.e.* factoring $N = 21$ would require 9000 elementary quantum gates acting on 26 qubits. An improvement of both of these schemes is due to Zalka [100], which uses $3L$ qubits and $\mathcal{O}(L^3)$ Toffoli gates. the modular exponentiation circuit due to Beauregard [95] uses $2L + 3$ qubits and $\mathcal{O}(L^3 \log(L))$ elementary gates with a circuit depth of $\mathcal{O}(L^3)$, which represents a slight improvement over the previous schemes[6].

[6] The circuit depth is the number of consecutive parallel operations from input to output (measurement). Each such parallel operation can be counted as a single step, and thus depth is a proxy for algorithmic time.

The overriding assumptions in the analysis of these schemes are (i) the underlying physical implementation of a QC has a high connectivity between its qubits and (ii) that the physical implementations natively implement a Toffoli gate, and thus may be taken to be an elementary gate. However, for modern-day NISQ physical implementations, these two assumptions do not necessarily hold. For instance, superconducting-qubit based architectures implement a set of single-qubit gates along with a high-fidelity single two-qubit entangling gate [8], for which a n-qubit Toffoli gate is then decomposed into single and two-qubits from such a native set [66]. The canonical decomposition of a three-qubit Toffoli gate uses six controlled-NOT (recall Figure 2.11 in the previous chapter) and for a general n-qubit Toffoli gate without the use auxiliary of qubits[7], its exact controlled-NOT count is not known [48, 64]. Taking this into consideration, and while even ignoring the difficulties that arise from compiling such circuits on physical devices with limited connectivity, the cost of implementing these circuits on a near-term devices is significantly increased if the cost analysis of the previous schemes is done in terms of two-qubit gates.

[7] Recall from the previous chapter that if auxiliary qubits are permitted, a n-qubit Toffoli gate can be realized with $\mathcal{O}(n)$ elementary gates.

The overhead in quantum gates comes from the modular exponentiation function part of the algorithm, while the overhead in qubits comes from the level of accuracy needed to successfully carry out the continued fractions part of the algorithm. Such an overhead obviously puts a full-scale implementation beyond the reach of current devices. However, compilation techniques such as the one described in Ref. [99], bridge this gap and allow for small-scale proof-of-concept demonstrations, where the quantum circuit is tailored around properties of the number to be factored. This significantly simplifies the controlled-operations that realize the modular exponentiation operation (see § 3.3.2), which is the most resource-intensive part of the order-finding routine. The resource demands (mostly two-qubit gates) of the compiled quantum circuit are significantly reduced, making it suitable for NISQ quantum devices with low connectivity and moderate two-qubit gate errors.

From Ref. [88], we extend the compiled quantum order-finding routine for the particular case of factoring $N = 21$ with $x = 4$ to accommodate another iteration for better precision in the resolution of the peaks for the value of $2^n s/r$. For the case of $N = 21$, other choices of x give 2, 4 or 6 for r. The cases for $r = 2$ or $r = 4$ have been demonstrated for $N = 15$ [81, 84–87] and would bear a similar circuit structure in the present case. With only three iterations, $r = 6$ would be out of reach as continued fractions would fail. For $x = 4$ we have $r = 3$, which is a choice that does not suffer from the aforementioned reasons. Despite r being an odd integer, the algorithm is successful in finding it from $x = 4$. This is the case for certain choices of perfect square x and odd r, and $x = 4$ and $r = 3$ is such a case[8].

[8] See Ref. [101] and supplementary information of Ref. [88] for more details.

In contrast to Ref. [88], our implementation is not iterative and uses three qubits for the control register rather than one qubit recycled on every iteration. The iterative version is based on the recursive phase estimation, made possible by the use of the semi-classical inverse QFT [89], which replaces two-qubit gates in the circuit with single-qubit rotations classically conditioned on the measurement outcomes, reducing the cost of circuit to $\mathcal{O}(L\log(L))$ single-qubit gates. However, we have used the traditional inverse QFT because mid-circuit measurements with real-time conditionals are not possible yet on IBM's quantum processors. The traditional inverse QFT for 3 qubits is realized by the circuit below [17]

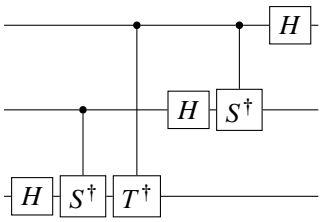


Figure 3.3: Circuit diagram for the three-qubit inverse QFT. Here, up to a global phase, $S^\dagger = R_z(-\frac{\pi}{2})$ and $T^\dagger = R_z(-\frac{\pi}{4})$ are phase and $\pi/8$ gates, respectively.

In the case where the inverse QFT is performed before a set of measurement, we can replace the controlled gates in the above circuit to ones that are classically controlled by a preceding measurement outcome [89], and we are able to reset qubits back to $|0\rangle$ during a computation, then the above circuit can be made to use a single qubit [94]

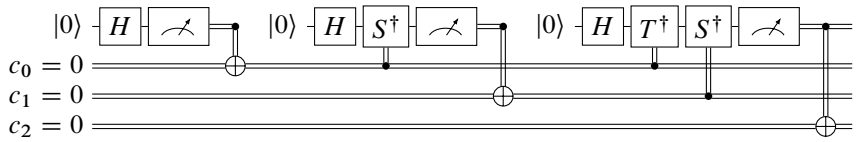


Figure 3.4: Circuit diagram for the three-qubit semi-classical inverse QFT that recycles a single qubit and replaces the two-qubit gates in the fully coherent QFT with classically controlled gates by the preceding measurement outcomes. Here, up to a global phase, $S^\dagger = R_z(-\frac{\pi}{2})$ and $T^\dagger = R_z(-\frac{\pi}{4})$ are phase and $\pi/8$ gates, respectively.

The latter is the semi-classical QFT that makes possible the implementation of the iterative version of Shor. If mid-circuit measurements with real-time conditionals were possible, the 3-qubit semi-classical QFT would be possible and may improve the quality of the results we present here through the use of only 1 qubit for the control register, as in Ref. [88]. IBM has suggested that the behaviour of real-time conditionals can be reproduced through post selection of the mid-circuit measurements. However, in the present case the speed up gained would be lost using this post selection method (see § C.1 of technical Appendix B for details).

A step that is unique to the demonstration in Ref. [88], among the compilation steps of previous demonstrations, and central to their demonstration is mapping the three levels $|1\rangle$, $|4\rangle$ and $|16\rangle$ accessed by the possible $2^L = 2^5$ levels of the work-register to only a single qutrit system.

In our demonstration we also use this step, however IBM processors consist of qubits and so we represent the work register by 3 basis states from a two-qubit system and discard the fourth basis state as a null state. The states encoding the three possible levels of the work register; $|1\rangle$, $|4\rangle$ and $|16\rangle$ are mapped to $|q_0 q_1\rangle$ according to

$$\begin{aligned} |1\rangle &\mapsto |\log_4 1\rangle = |00\rangle\,, \\ |4\rangle &\mapsto |\log_4 4\rangle = |01\rangle\,, \\ |16\rangle &\mapsto |\log_4 16\rangle = |10\rangle\,. \end{aligned} \tag{3.19}$$

Therefore instead of evaluating $4^j \mod 21$ in the work register as described in step 2 of the order-finding routine, the compiled version of Shor's algorithm effectively evaluates $\log_4[4^j \mod 21]$ in its place for $j = 0, 1 \ldots 2^3 - 1$ [99], which reduces the size of the work register to 2 qubits in comparison to the 5 qubits required in the standard construction. Note the ordering of quantum bits in the work register is $|q\rangle = |q_0\rangle\,|q_1\rangle$, where the rightmost qubit is associated with the least significant bit. Similarly, with the control register we have $|c\rangle = |c_0\rangle\,|c_1\rangle\,|c_2\rangle$. In total the algorithm requires 5 qubits: 3 for the control register and 2 for the work register. Implementing the controlled unitaries $\hat{U}^x$ that perform the modular exponentiation $|j\rangle\,|y\rangle \to |j\rangle\,\hat{U}_x^j\,|y\rangle = |j\rangle\,\left|x^j y \mod N\right\rangle$ reduces to effectively swapping around the states $|1\rangle$, $|4\rangle$ and $|16\rangle$ in the work register controlled by the corresponding bit of the integer j in the control register, which is given by $x = c_2 2^0 + c_1 2^1 + c_0 2^2$. In other words, $\hat{U}^j = \hat{U}^{c_0 2^2}\hat{U}^{c_1 2^1}\hat{U}^{c_2 2^0}$. Thus, depending on the control qubit c_i, one of the following maps is applied:

$$\begin{aligned} \hat{U}^1 &: \{|1\rangle \mapsto |4\rangle\,, |4\rangle \mapsto |16\rangle\,, |16\rangle \mapsto |1\rangle\}, \\ \hat{U}^2 &: \{|1\rangle \mapsto |16\rangle\,, |4\rangle \mapsto |1\rangle\,, |16\rangle \mapsto |4\rangle\}, \\ \hat{U}^4 &: \{|1\rangle \mapsto |4\rangle\,, |4\rangle \mapsto |16\rangle\,, |16\rangle \mapsto |1\rangle\}. \end{aligned} \tag{3.20}$$

The next simplification step comes from the fact that these operations on the work register need not be controlled SWAP (Fredkin) gates, they can be as simple as controlled-NOT gates, as we show next.

3.4.1 Modular exponentiation

Implementing $\hat{U}^1$ on the two-qubit work register is simplified considerably by noting that the states $|4\rangle$ and $|16\rangle$ initially have zero amplitude, and thus the operation $|1\rangle \mapsto |4\rangle$ alone is sufficient. This operation can realized with a controlled-NOT gate controlled by $|c_2\rangle$ targeting the second work qubit $|q_1\rangle$, as shown Figure 3.5

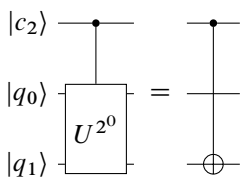


Figure 3.5: Decomposition of the controlled-U^{2^0} unitary as only a single controlled-NOT gate.

Similarly, the implementation of $\hat{U}^2$ can be simplified by noting that the states $|1\rangle$ and $|4\rangle$ are the only non-zero amplitude states in the work register after $\hat{U}^1$ may have been applied, thus prompting us to only consider $|1\rangle \mapsto |16\rangle$ and $|4\rangle \mapsto |1\rangle$. A controlled-NOT gate controlled by $|c_1\rangle$ targeting $|q_1\rangle$ followed by a Fredkin gate, swapping $|q_0\rangle$ and $|q_1\rangle$ realizes this simplified $\hat{U}^2$, as shown in Figure 3.6

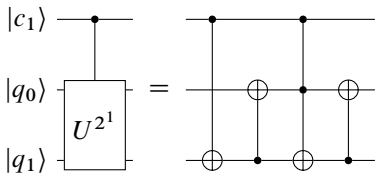


Figure 3.6: Circuit diagram showing the decomposition of the controlled-U^2 unitary in terms of a Toffoli gate and two controlled-NOT gates.

In Figure 3.6, the Fredkin gate has been decomposed into a Toffoli gate and two controlled-NOT gates. The subsequent implementation of $\hat{U}^4$ admits no simplifications as all the possible states in the work register may have non-zero amplitude at this point. This operation is implemented with a Toffoli gate and a Fredkin gate with single-qubit Pauli-X gates, shown in Figure 3.7

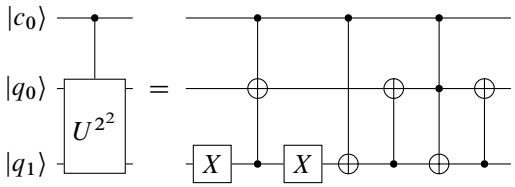


Figure 3.7: Circuit diagram showing the decomposition of the controlled-U^{2^2} unitary in terms of two Toffoli gates, three controlled-NOT gates and two single-qubit gates.

The full circuit diagram is shown in Figure 3.8 – note that before simplification the order of application of the controlled unitaries is interchangeable, $\hat{U}^{2^{(n-1)}}$ or $\hat{U}^{2^1}$ could be applied first. Interchanging the order only has the effect of interchanging the order of the outcome bits at the end of the computation. This is the reason the order of application of the controlled unitaries here is in reverse order to that in Ref. [88].

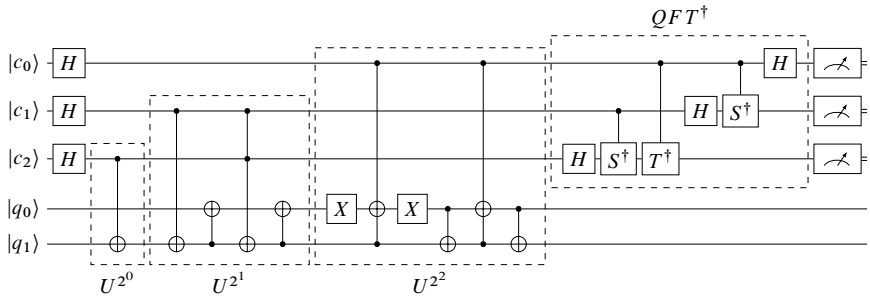


Figure 3.8: Compiled quantum order-finding routine for $N = 21$ and $x = 4$. This circuit uses five qubits in total; 3 for the control register and 2 for the work register. The above circuit determines $2^n s/r$ to three bits of accuracy, from which the order can be extracted. Here, up to a global phase, $S = R_z(\frac{\pi}{2})$ and $T = R_z(\frac{\pi}{4})$ are phase and $\pi/8$ gates, respectively.

3.4.2 Modular exponentiation with relative phase Toffolis

In total, the modular exponentiation routine requires three Toffoli gates; traditionally a single Toffoli gate can be decomposed into six controlled-NOT gates and several single-qubit gates, the decomposition is equivalent to the one shown in Figure 2.11 modulo two single qubit gates ($HZH = X$)

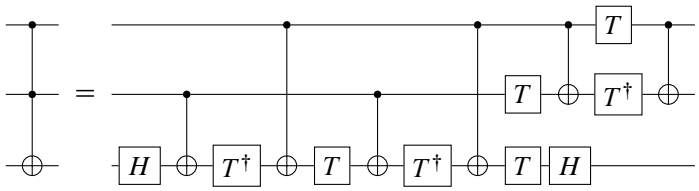


Figure 3.9: Circuit diagram showing the decomposition of a Toffoli gate in terms of elementary gates; six controlled-NOT gate and seven $T/T^\dagger$ gates.

Taking into account a given processor's topology and the constraints it poses, as well as other parts of the circuit (the inverse QFT), further increases the tally of controlled-NOT gates.

This becomes undesirable as it is understood that there is an upper limit on the number of controlled-NOT gates that can be in a circuit with the guarantee of a successful computation on NISQ processors, with current limit is understood to be around 30 controlled-NOT gates for IBM Q processors [57, 59]. The number of controlled-NOT gates from the decomposition of the Toffoli gate can be cut in half if we permit the operation to be correct up to relative phase shifts. Margolus constructed a gate that implements the Toffoli gate up to a relative phase shift of $|101\rangle \mapsto -|101\rangle$ that only uses three controlled-NOT gates and four single qubit gates [67]. This construction has been shown to be optimal [102].

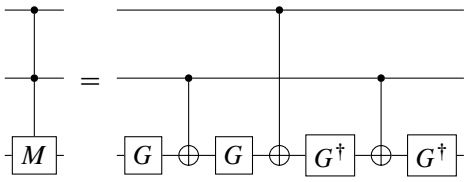


Figure 3.10: Circuit diagram showing the decomposition of a Margolus gate in terms of elementary gates; three controlled-NOT and four $G = R_y(\pi/4)$ single qubit gates, where $R_y(\pi/4) = e^{-i\pi/8}SHTHSZ$, $S = \mathrm{diag}(1, i)$ and $Z = \mathrm{diag}(1, -1)$.

Maslov showed the advantages of using a relative phase Toffoli gate when the gate is applied last or when relative phases do not matter for certain configurations of Toffolis, resulting in no overall change to the functionality in any significant way [103]. The configuration in the circuit shown in Figure 3.8 is one such configuration that permits a replacement of Toffoli gates with Margolus gates without changing the overall functionality. All the Margolus gates in the circuit in Figure 3.11 (which is the circuit in Figure 3.8 with the Toffoli gates replaced by Margolus gates) never encounter the basis state $|101\rangle$, thus leaving the operation of the circuit unchanged. See § C.2 of technical Appendix B for details. This further compacting reduces the number of controlled-NOT gates considerably and puts the algorithm within reach of current IBM processors with a limited number of noisy qubits.

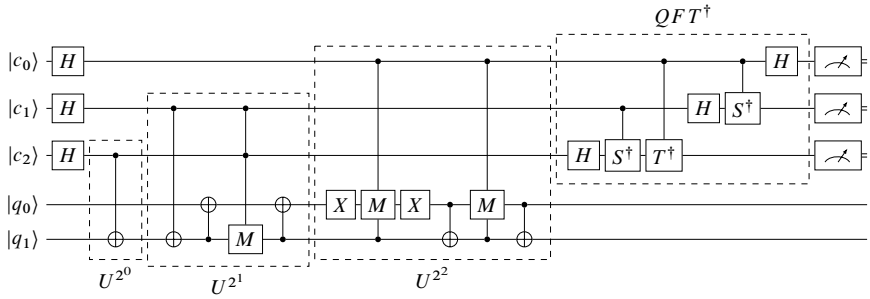


Figure 3.11: Approximate compiled quantum order-finding routine implemented with Margolus gates in place of Toffoli gates in the construction in Figure 3.8.

3.5 Experiments

The proposed compiled circuit in Figure 3.11 was mapped onto 5 physical qubits (3 control qubits and 2 work qubits) and executed on a sub-processor of IBM's 7-qubit quantum processor **ibmq_casablanca** and 27-qubit quantum processor **ibmq_toronto**, which we will refer to as 7Q and 27Q, and whose topologies are shown in Figure 3.12 (a) and (b), respectively. When mapping the compiled circuit a few considerations can be taken into account. First, as can be seen from Figure 3.10, the Margolus gate can be implemented on a collinear set of qubits, as the first control qubit need not be connected to the second control qubit.

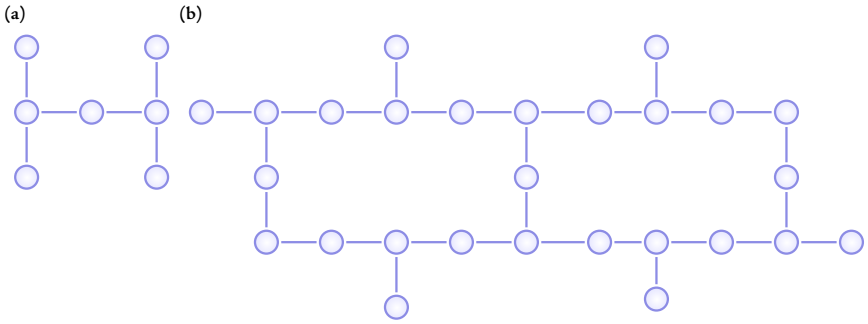


Figure 3.12: Qubit topology of IBM Q experience processors, **(a)** 7-qubit device **ibmq_casablanca**, and **(b)** 27-qubit device **ibmq_toronto**

On the other hand, mapping the three-qubit inverse QFT onto physical qubits without incurring additional SWAP gates is not possible, as the three controlled-phase gates require all three qubits to be interconnected in a triangle and the aforementioned quantum processors do not have such a topology. Additionally, more SWAP gates are introduced to the transpiled circuit, as the processor topologies do not permit the topology required by the compiled circuit, as shown in Figure 3.13.

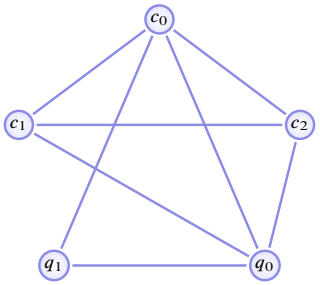


Figure 3.13: Qubit connections required by the compiled circuit Figure 3.11.

The only possible five-qubit mappings on the quantum processors are all isomorphic to either a collinear set of qubits or a T-shaped set of qubits, as shown in Figure 3.14 (a) and (b). Choosing the mapping in (b) over the one in Figure 3.14 (a) is motivated by the fact that the former is slightly more connected than latter and thus in effect would reduce the number of SWAP gates in the mapped and transpiled circuit.

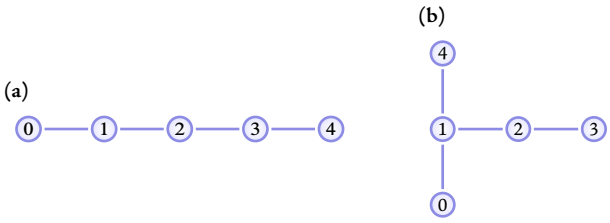


Figure 3.14: The two possible 5-qubit processor mappings on the architectures shown in Figure 3.12, **(a)** A collinear 5-qubit processor mapping, and **(b)** A T-shape 5-qubit processor mapping

3.5.1 Performance

To evaluate the performance of the algorithm, we first transpiled the circuit in Figure 3.11 down to the chosen quantum processor with the mapping below

$$\begin{aligned} 0 &\mapsto c_0, \\ 1 &\mapsto c_2, \\ 4 &\mapsto c_1, \\ 2 &\mapsto q_1, \\ 3 &\mapsto q_0. \end{aligned} \tag{3.21}$$

Through the transpiler's optimization, with the mapping above it is possible to have a circuit that has 25 controlled-NOT gates and a circuit depth of 35. Figure 3.15 shows the results of measurements on the control register qubits from the two processors, where measurement error mitigation has been applied to results and mitigates the effect of measurement errors on the raw results (see § A.1 of technical Appendix B details). The outcomes $|101\rangle$ and $|110\rangle$ occur with probability close to 0.17 and 0.18, respectively on the **ibmq_casablanca** processor. And occur with probability close to 0.19 and 0.16, respectively on the **ibmq_toronto** processor.

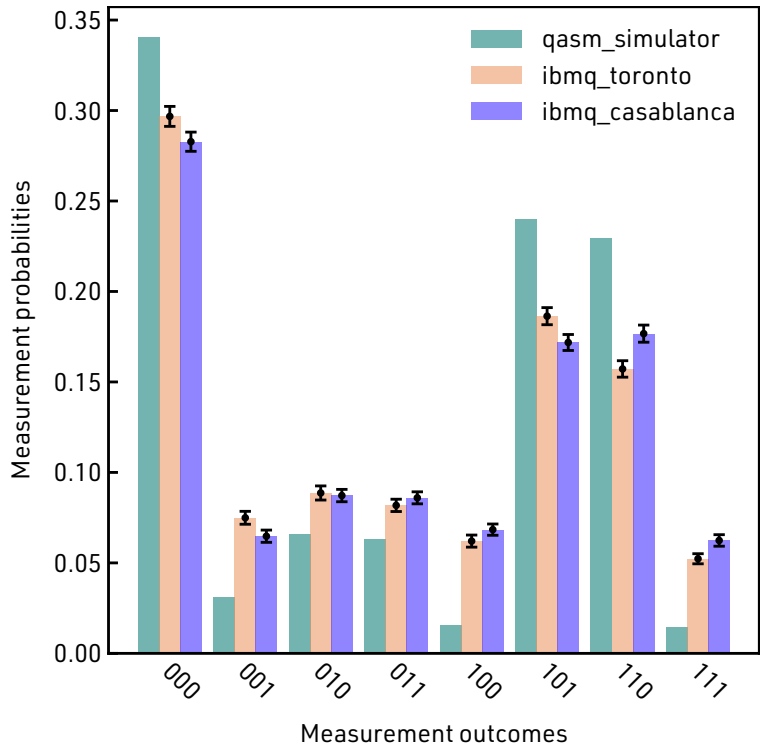
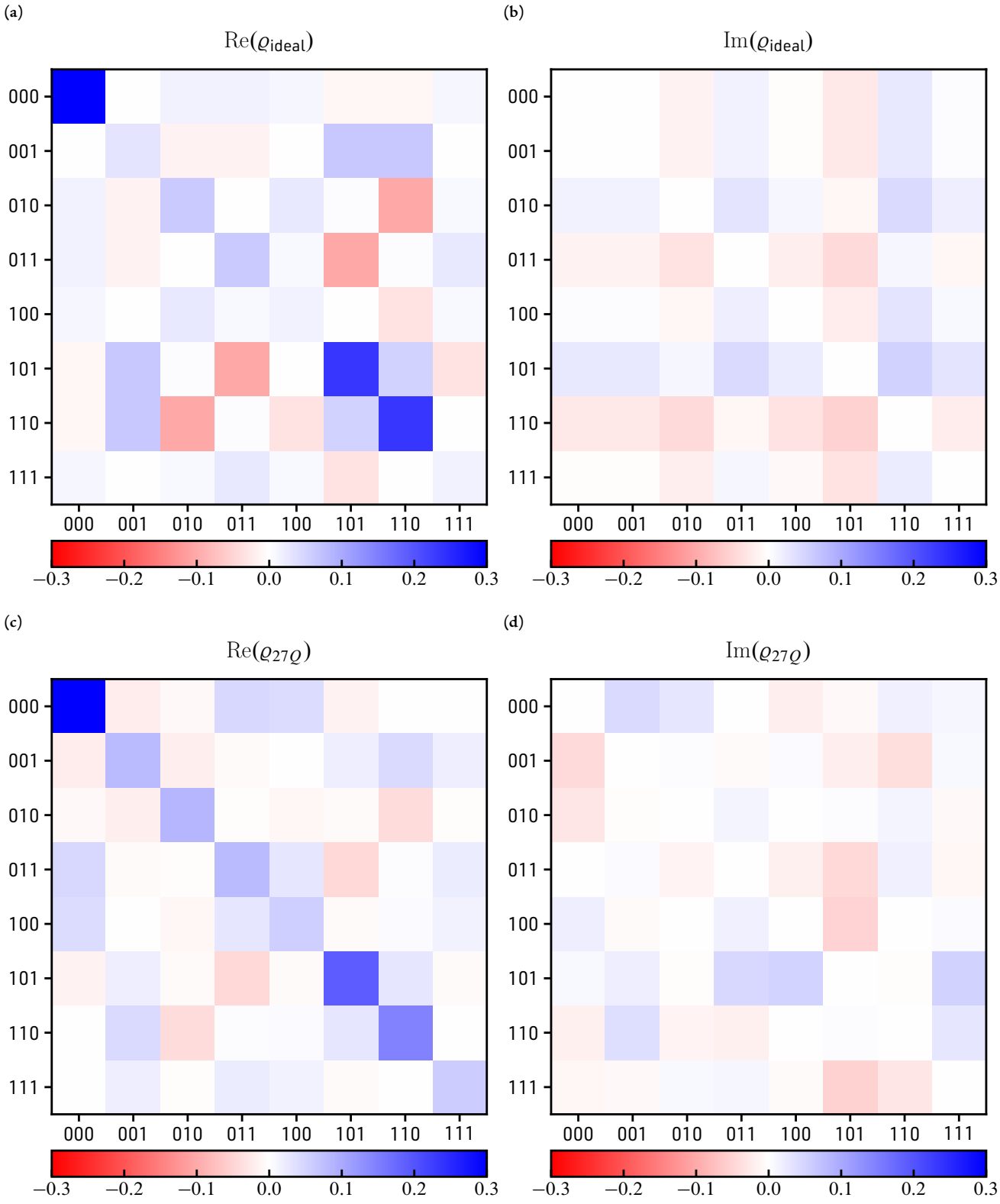


Figure 3.15: Results of the complete quantum order-finding routine for $N = 21$ and $x = 4$. On each processor, the circuit was executed 8192×100 times with measurement error mitigation. The error bars represent 95% confidence intervals around the mean value of each histogram bin (see § A.2 of technical Appendix B details). The simulator probabilities show the ideal case.

The theoretical ideal probability is close to 0.25, as can be seen from the simulator results in Figure 3.15. However, the amplification of the peaks $|000\rangle$, $|101\rangle$ and $|110\rangle$ is clearly visible from the processor outcomes.

We quantify the successful performance of the algorithm by comparing the experimental and ideal probability distributions *via* the trace distance or Kolmogorov distance [17], which measures the closeness of two discrete probability distributions P and Q and is defined by the equation $D(P, Q) \equiv \sum_{x \in \mathcal{X}} |P(x) - Q(x)|/2$, where $\mathcal{X}$ represents all possible outcomes. This measure shows an agreement between measured and ideal results – the trace distance between the measured distribution and the ideal distribution is close to 0.1694 and 0.1784 for **ibmq_toronto** and **ibmq_casablanca**, respectively. On the other hand, the trace distance between the ideal distribution and a candidate random uniform distribution is 0.4347. Furthermore, we evaluate the performance of the algorithm by characterizing the measured output state in the control register, this is achieved *via* state tomography yielding the density matrix of the measured state. The measured state and ideal state on the output register are quantitatively compared using the fidelity for two quantum states ϱ and δ, and is defined to be $F(\varrho, \varsigma) \equiv \mathrm{Tr}\left(\sqrt{\sqrt{\varrho}\varsigma\sqrt{\varrho}}^2\right)$ [17]. We measured a fidelity of $F(\varrho_{\mathrm{id}}, \varrho_{27Q}) = 0.6948 \pm 00650$ and $F(\varrho_{\mathrm{id}}, \varrho_{7Q}) = 0.70 \pm 0.0275$ on the 27 qubit and 7 qubit quantum processors respectively. In Figure 3.16 we show the estimated density matrices in the computational basis for each respective device.


(a)
$\mathrm{Re}(\varrho_{\mathrm{ideal}})$
(b)
$\mathrm{Im}(\varrho_{\mathrm{ideal}})$
(c)
$\mathrm{Re}(\varrho_{27Q})$
(d)
$\mathrm{Im}(\varrho_{27Q})$
000
001
010
011
100
101
110
111
−0.3
−0.2
−0.1
0.0
0.1
0.2
0.3

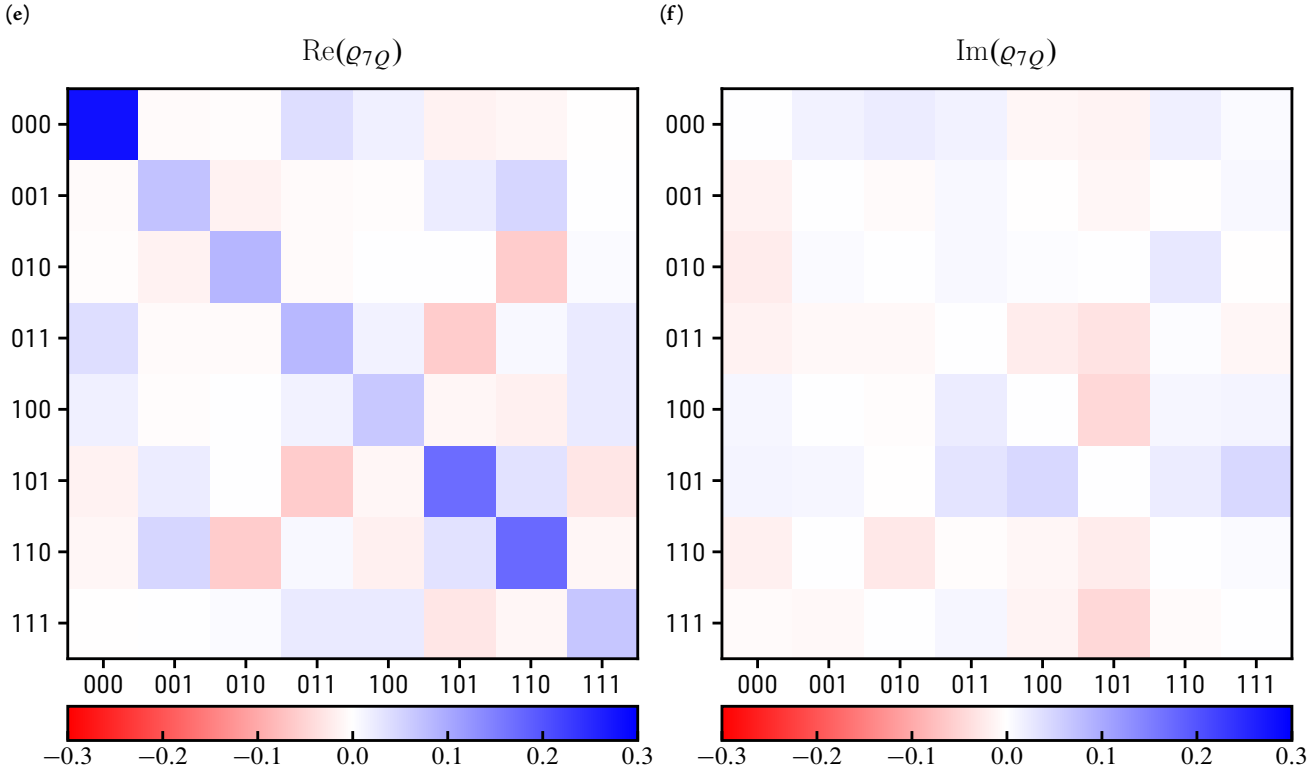


Figure 3.16: Ideal and measured density matrices after the inverse QFT, estimated *via* a maximum-likelihood reconstruction from measurement results in the Pauli-basis. A matrix plot of the **(a)** real and **(b)** imaginary part of the ideal state $|\Psi\rangle\langle\Psi|$. These plots are compared with the measured states ρ_{27Q} and ρ_{7Q} with the corresponding matrix plots of their real parts in panels **(c)** and **(e)**, and imaginary parts in panels **(d)** and **(f)**, respectively. We observe there is a resemblance between the ideal state and the measured states, but noise in both real and imaginary parts is notable. Note that in all figures the color bar has been rescaled to a range between −0.3 and 0.3 for visual clarity.

3.5.2 Factoring $N = 21$

The measured probability distributions in Figure 3.15 are peaked in probability for the outcomes 000 ($\varphi_s = 0$), 101 ($\varphi_s = 5$) and 110 ($\varphi_s = 6$), with ideal probabilities of 0.35, 0.25 and 0.25, respectively. Here we are using the integer representation of the binary outcomes. The outcome 000 corresponds to a failure of the algorithm [88]. For the outcome 101, computing the continued fraction expansion of $\varphi = \varphi_s/2^n = 5/2^3 = 5/8$ gives the convergents $\{0, 1, 1/2, 2/3, 5/8\}$ (see § C.4 of technical Appendix B for details), so that the third convergent $2/3$ in the expansion can be identified as s/r and correctly gives $r = 3$ as the order when tested with the relation $x^r \bmod N = 1$, while the other convergents do not give an r that passes the test. On the other hand, the continued fraction expansion of $\varphi = 6/8$ gives $\{0, 1, 3/4\}$ and incorrectly gives $r = 4$ as the order (see § C.4 of technical Appendix B for details). This failure can be avoided in principle by adding further qubits to the control register so that the peak in the probability distribution becomes narrower and more well defined [88]. Another option is to simply apply continued fractions to all peaked outcomes and test if the value of r found satisfies the order relation for x and N. It is interesting to note that from the results of Ref. [88], successfully finding the order $r = 3$ was not possible to achieve, as with only two bits of accuracy in the experiment the continued fractions would always fail due to the peaked outcomes of 10 (2) and 11 (3) giving the convergents of $\{0, 1/2\}$ and $\{0, 1, 3/4\}$, respectively. In our case, we successfully find $r = 3$, from which we obtain $\gcd(x^{r/2} \pm 1, N) = \gcd(8 \pm 1, 21) = 3$ and 7. Thus, with our demonstration, extending the number of outcome bits to three has allowed us to fully perform the quantum factoring of $N = 21$.

3.5.3 Verification of entanglement

The presence of entanglement between the control and work registers is known to be a requirement for the algorithm to gain any advantageous speedup over its classical counterpart in general [83, 104, 105]. For detecting genuine multipartite entanglement around the vicinity of an ideal state $|\psi\rangle$, one can construct a projector-based witness such as the one below:

$$\hat{\mathcal{W}}_\psi = \alpha \mathbb{1} - |\psi\rangle\langle\psi|\,, \tag{3.22}$$

where α is the square of the maximum overlap between $|\psi\rangle$ and all biseparable states. In other words, $\mathrm{Tr}\left(\hat{\mathcal{W}}_\psi \varrho\right) \geq 0$ for biseparable states and $\mathrm{Tr}\left(\hat{\mathcal{W}}_\psi \varrho\right) < 0$ for states with genuine multipartite entanglement in the vicinity of $|\psi\rangle$ [106]. For the ideal state after modular exponentiation (but before the inverse QFT) in both the control and work registers, $\alpha = 0.75$ was found using the method described in the appendix of Ref. [106]. This was implemented using the software package QUBIT4MATLAB [107]. Therefore ideally the state in both registers after modular exponentiation has genuine multipartite entanglement.

In order to check whether the output state from the IBM processors is close to the ideal state and has genuine multipartite entanglement, full state tomography would normally be needed to characterize the state ϱ_{exp} in both the control and work registers. This would require 3^5 measurements, making it impractical to gather a sufficiently large data set within a meaningful time frame. However, we need not measure the full density matrix, the quantity $\mathrm{Tr}\left(|\Psi\rangle\langle\Psi|\,\varrho_{\mathrm{exp}}\right)$ suffices. To measure this, we can decompose $\varrho = |\Psi\rangle\langle\Psi|$ into 293 Pauli terms as

$$|\Psi\rangle\langle\Psi| = \sum_{ijklm} p_{ijklm} \sigma_i^{(1)} \sigma_j^{(2)} \sigma_k^{(3)} \sigma_l^{(4)} \sigma_m^{(5)}, \tag{3.23}$$

where $\sigma_i = \{I, X, Y, Z\}$ are the usual Pauli matrices plus the identity.

However, the number of measurements needed to obtain all 293 expectation values can be reduced. This is because the measured probabilities from a measurement of a single Pauli expectation value, *i.e.* $\langle ZZZZZ\rangle$, can be summed in various combinations to derive other Pauli expectations values, *i.e.* $\langle ZIZZZ\rangle$, $\langle IZZZZ\rangle$, etc. The values derived are nothing but the marginalization of the measured probabilities over the outcome space of some set of qubits (see § A.3 of technical Appendix B for details). We can do the same for each term in the set of terms from the Pauli decomposition of ϱ, calling it $\mathcal{S}_d$, forming a set of other Pauli terms that can be derived from the same counts. Taking the union of these sets to be $\mathcal{S}_u$, the complement $\mathcal{S}_d \setminus \mathcal{S}_u$ gives the 79 terms we only need to measure (see § A.3 of technical Appendix B for details). We measure the 79 Pauli expectation values of the terms above with respect to the state in both registers after modular exponentiation and from this we compute/derive the 293 terms in $\mathcal{S}_d$ and therefore $\mathrm{Tr}\left(|\Psi\rangle\langle\Psi|\,\varrho_{\mathrm{exp}}\right)$; the measurement outcomes for evaluating some of the Pauli operator expectation values are shown in Figure 3.17.

The measured probabilities for each term result in an expectation value of $\mathrm{Tr}\big(|\Psi\rangle\langle\Psi|\,\varrho_{7\mathcal{Q}}\big) = 0.677 \pm 0.00365$ and $\mathrm{Tr}\big(|\Psi\rangle\langle\Psi|\,\varrho_{27\mathcal{Q}}\big) = 0.626 \pm 0.00304$, which leads to

$$\begin{aligned}\mathrm{Tr}\Big(\hat{\mathcal{W}}_{\Psi}\varrho_{7\mathcal{Q}}\Big) &= 0.0729 \pm 0.00365,\\ \mathrm{Tr}\Big(\hat{\mathcal{W}}_{\Psi}\varrho_{27\mathcal{Q}}\Big) &= 0.124 \pm 0.00304.\end{aligned} \tag{3.24}$$

The results obviously fail to detect genuine multipartite entanglement, however, this does not mean entanglement is entirely absent. Consider the square of the maximum overlap between the ideal state $|\Psi\rangle$ and all pure states $|\theta\rangle$ that are unentangled product states with respect to some bipartite partition (bipartition) $\mathcal{B}$ of the qubits,

$$\max_{\theta\in\mathcal{B}} |\langle\theta|\Psi\rangle|^2 = \beta_{\Psi}. \tag{3.25}$$

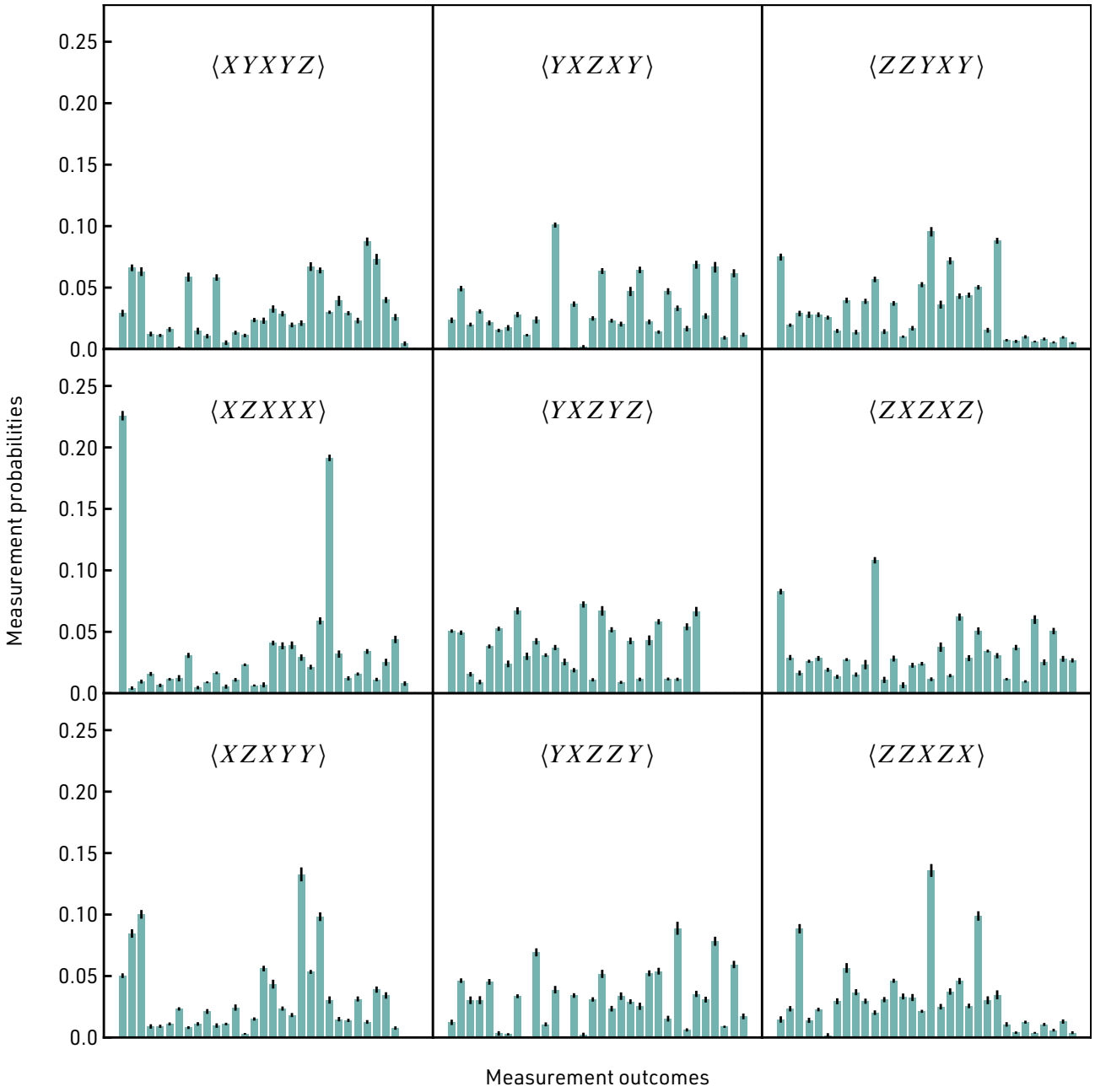
Thus, any other state $|\xi\rangle$ for which

$$|\langle\xi|\Psi\rangle|^2 > \beta_{\Psi}, \tag{3.26}$$

cannot be a product state with respect to the bipartition $\mathcal{B}$, implying that there is non-separability, or entanglement, across this bipartition. The above result extends to mixed states ϱ_{ξ} due to the convex sum nature of mixed quantum states [107]. We compute Equation (3.25) for all possible bipartitions of our ideal state $|\Psi\rangle$ (see § C.3 of technical Appendix B for details).

For the experimental state $\varrho_{7\mathcal{Q}}$ we find, with the exception of the bipartition $\mathcal{B} = (c_0c_1c_2q_1)(q_0)$, that it is non-separable with respect to all other bipartitions, *i.e.* the square of the overlap between $\varrho_{7\mathcal{Q}}$ and $|\Psi\rangle$ (~ 0.677) is greater than the maximal square overlap between $|\Psi\rangle$ and all product states in each of these bipartitions. Similarly for $\varrho_{27\mathcal{Q}}$, with the exception of bipartitions $\mathcal{B} = (c_0c_1c_2q_1)(q_0)$ and $\mathcal{B} = (c_0c_1c_2q_0)(q_1)$, the state is non-separable with respect to all other bipartitions. Most notably, both $\varrho_{7\mathcal{Q}}$ and $\varrho_{27\mathcal{Q}}$ are non-separable with respect to the bipartition $\mathcal{B} = (c_0c_1c_2)(q_0q_1)$, which is a bipartition between the control and work registers.

(a)


⟨XYXYZ⟩
⟨YXZXY⟩
⟨ZZYXY⟩
⟨XZXXX⟩
⟨YXZYZ⟩
⟨ZXZXZ⟩
⟨XZXYY⟩
⟨YXZZY⟩
⟨ZZXZX⟩
0.25
0.20
0.15
0.10
0.05
0.0
Measurement probabilities
Measurement outcomes

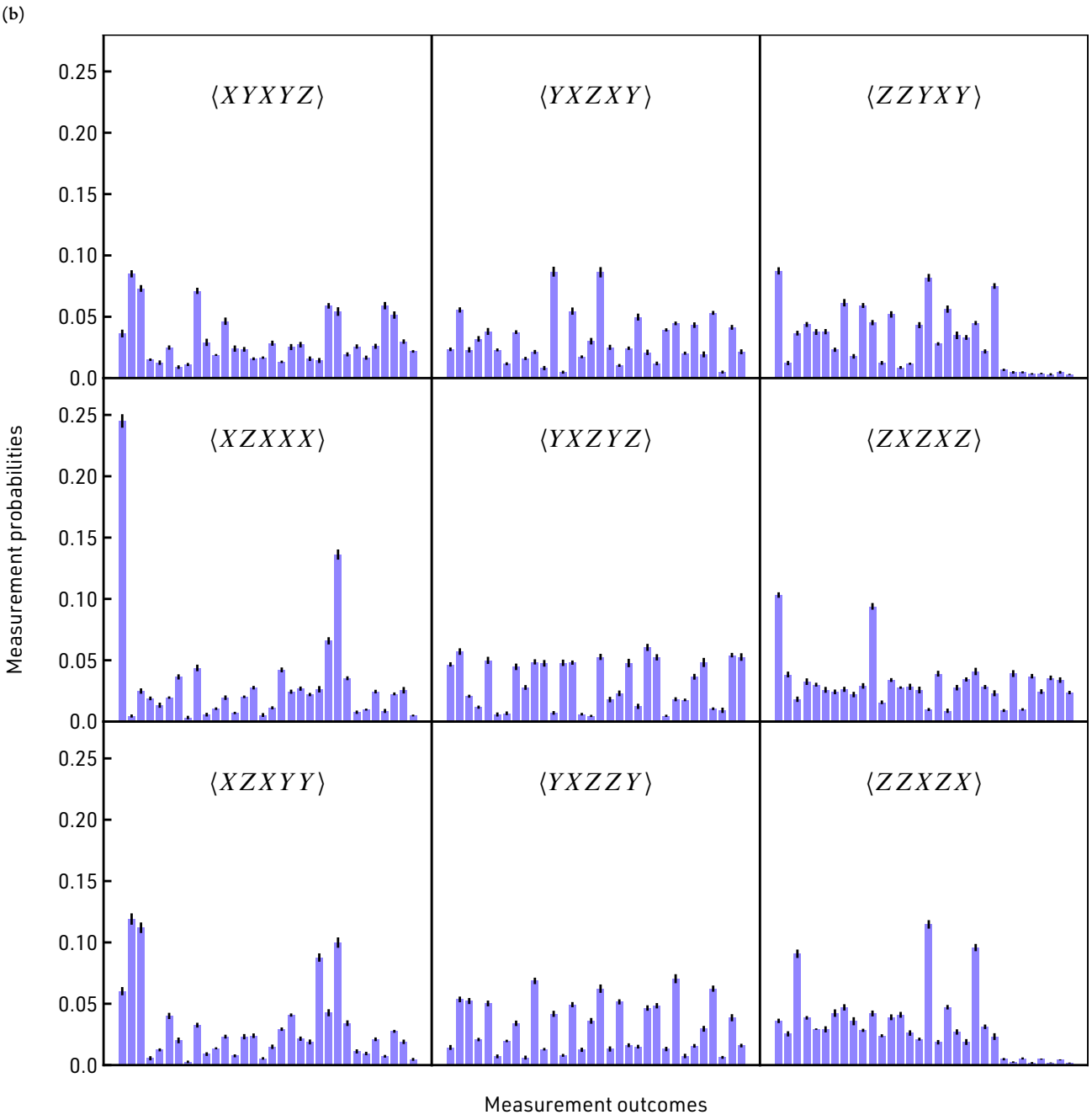


Figure 3.17: A subset of 9 of the 79 measurement settings required for each term in: **(a)** $\mathrm{Tr}\big(|\Psi\rangle\langle\Psi|\,\varrho_{7Q}\big)$ and **(b)** $\mathrm{Tr}\big(|\Psi\rangle\langle\Psi|\,\varrho_{27Q}\big)$. The x-axis from left to right shows the labels from p_{00000} to p_{11111}.

3.6 Concluding remarks

In summary, we have implemented a compiled version of Shor's algorithm on IBM's quantum processors for the prime factorization of 21. By using relative phase shift Toffoli gates, we were able to reduce the resource demands that would have been required in the standard compiled and non-iterative construction of Shor's algorithm (with regular Toffoli gates), and still preserve its functional correctness. The use of relative phase shift Toffoli gates has also allowed us to extend the implementation in Ref. [88] to an increased resolution. Moreover, while the latter implementation used only 1 recycled qubit for the control register, in contrast to our 3 qubits, it falls one iteration short of achieving full factoring for the reasons already mentioned. It is not clear what additional resource overheads (single and two-qubit gates) would be needed in implementing another iteration in their scheme and it is likely that these overheads are what prevented the full factoring of 21 in the photonic setup used. Furthermore, we note that in principle there is no real advantage in using 3 qubits for the control register as we have done here instead of 1 qubit recycled, as in Ref. [88]. However, in practice it is not possible at present to recycle qubits on the IBM processors and so we used 3 qubits instead. In future, once this capability is added, a further reduction in resources will be possible for our implementation, potentially improving the quality of the results even more.

We have verified, *via* state tomography, the output state in the control register for the algorithm, achieving a fidelity of around 0.70. For the verification of entanglement generated during the algorithm's operation, the resource demands of state tomography were circumvented by measuring a much reduced number of Pauli measurements to directly estimate the fidelity of the state. However, this method is quite specialized and cannot be easily generalized to larger systems. In scaling up Shor's algorithm to higher integers beyond 21 using larger quantum systems, other methods of quantum tomography / direct fidelity estimation can be used to characterize the performance. These include compressed sensing [108] and classical shadows [109], which give theoretical guarantees, and improved scaling in the number of Pauli measurements and classical post-processing than standard methods. In the case where one is only interested in a direct estimate of fidelity, the method due to Flammia and Liu [110] provides a fidelity estimate using a constant number of Pauli expectation values.

For states that belong to a class of states with certain symmetries, such as stabilizer states, only a few measurements are required for measuring the fidelity and detecting multipartite entanglement [35]. However, not all entangled states are neatly housed within these well-studied classes. Ref. [111] introduces a device-independent method for multipartite entanglement detection which scales polynomially with the system size by relaxing some constraints. Another scheme constructs witnesses that require a constant number of measurements of the system size at the cost of robustness against white noise. This provides a fast and simple procedure for entanglement detection [112]. Many fundamental questions on the subjects of quantum tomography and multipartite entanglement still remain to be answered [113] and advances will help in efficiently quantifying the performance of algorithms in larger quantum processors.

Our demonstration involves a two-fold reduction of the resource count from the full circuit in Figure 3.8 *via* the replacement of regular Toffoli gates with relative phase variants, which is an approach that is in the spirit of the NISQ era; tailoring quantum circuits to circumvent the shortcomings of noisy quantum processors.

In addition, the resource count of the full QFT in our circuit may be reduced through the use of the approximate QFT [114], while possibly still maintaining a clear resolution of the peaks in the output probability distribution [115]. A possible avenue of future research derived from what we have reported here is the investigation and identification of scenarios where one can replace Toffoli gates with relative phase Toffoli gates while preserving the functional correctness, in a wide range of algorithms including Shor's algorithm, as seen here. In the present case, whether such an approach is special to the case of $N = 21$ or extendable to other N is not known. Ref. [103] has performed some work in this regard, however a proper analysis and systematic composition of relative phase Toffoli gates for such purposes is still an open problem. In future, a similar approach may make possible the factorization of larger numbers with adequate accuracy in resolution of the algorithm's outcomes and their characterization.

PART II

BUILDING A THREE-QUBIT ONE-WAY QUANTUM COMPUTER

4

Polarization-entangled photons

"Quantum phenomena do not occur in a Hilbert space. They occur in a laboratory."

— Asher Peres, Quantum Theory: Concepts and Methods

4.1 Introduction: Non-separability in the laboratory

In the introductory chapter we have described various linear optical elements and how information can be encoded and subsequently measured in the polarization DOF of a single photon. As the avid reader (or by the title of this thesis) might have suspected, much of the appeal of such optical systems comes about from their potential applications to quantum information processing tasks. In this particular chapter, we steer towards this direction and consider this use of polarization-entangled pairs of photons generated *via* a nonlinear process called SPDC, with the polarization of a single-photon as a substrate for a quantum bit. Multi-qubit states that possess non-classical correlations have been realized in a variety of, and often exotic optical systems, but in this regard perhaps, the most readily available and controllable source of entanglement arises from polarization-entangled photons. This is in part attested by their ubiquitous use; for demonstrations of Shor's algorithm from the first half of thesis (see Chapter 3); after the pioneering work on a spin-1/2 nuclei system [81], have been realized on single-photonic architectures making use of polarized-entangled photons [84, 86, 88] and other sundry tasks; including state-preparation in measurement-based/one-way quantum computing [116–120], algorithms [16, 72, 73] and quantum communication protocols [121–124].

Needless to say, the commonality among all these demonstrations is the central role of entanglement, which necessitates the need for a complete characterization of such entangled states in such applications. In earlier pioneering work of this kind, qualitative arguments for the presence of entanglement were made in the way of violation of Bell-type inequalities from fringe visibility measurements being above a certain threshold [125, 126]. Such measurements gave qualitative evidence for the existence of non-classical correlations in a given experiment, not consistent with any local hidden-variable theory [26, 127, 128].

A violation of Bell-type inequalities is often considered an excellence indicator of the presence of entanglement in a pure two-qubit system; alas, despite its experimental convenience, it is not a true measure of entanglement[1].

[1] Ref. [28] shows that in general, it is not possible to discern the degree of entanglement (a quantifiable measure) in a state *via* an inference from a violation of Bell-type inequality

A more thorough characterization of polarization-entangled photons is through quantum state tomography (QST) [129, 130]. From a set of measurements performed on an ensemble of identically prepared quantum states, a maximum likelihood estimate of the density matrix of the polarization-entangled photon state is obtained, and from which physical quantities of interest such as fidelity, purity and concurrence can be derived.

4.2 Experimental design

In the experiment that we will describe in this chapter, we endeavour to generate and characterize a photonic three-qubit maximally entangled state[2] first studied by Greenberger–Horne–Zeilinger (GHZ) and thus bears their name. The experimental procedure is conceptually simple to describe: A two-photon, two-qubit polarized-entangled state is generated from a SPDC and appropriately characterized with quantum state tomography. Once characterized and optimized, this state is enlarged by using the path (momentum) DOF of one of the photons to a three-qubit polarization and path entangled GHZ state, locally equivalent to a graph state [131]. Encoding a quantum bit on a separate DOF on one of the polarization-entangled photons is motivated by two main reasons.

[2] Maximally entangled state has a maximum entropy of entanglement for each of its bipartitions. For a two qubits, the Bell states are examples of maximally-entangled states.

Primo Experimental convenience: Having additional photons (generated by another SPDC process) in an experimental setup of this kind would necessitate additional tabletop linear optical components *i.e.* mirrors, wave plates, beam splitters, filters, polarizers, etc. The end goal of the experiment is to eventually carry out remotely controllable measurements on the generated state, thus it is preferable to have fewer moving parts.

Secondo Practicality: SPDC is a probabilistic process, that is, for every photon incident on the crystal, with some probability p, it will down convert to a polarization-entangled photon-pair, and the probability p is typically low, on the order of $\lesssim 1\%$ [37]. Thus having an additional two photons produced in our experimental setup would occur with even lower probability p^2 (assumption of independence of the two events), and would also alter the coincidence counting electronics; typically one has to allow a long coincidence window to observe multiple low probability events of this kind[3].

[3] In Ref.[119], a six-photon, six-qubit polarized-entangled state was produced with three SPDC processes occurring in succession,and six-fold coincidence events ($\sim p^3$) were accumulated over a three hour coincidence window.

Similarly, once this state is generated, we appropriately characterize it. Reconstructing the density matrix of a three-qubit state would necessitate a full tomographic analysis, which for a three-qubit state would require 64 measurement settings [132]. However, a GHZ state is locally equivalent to another three-qubit state that is a member of a special class of states, called graph states [77, 131]. What is peculiar to graph states is that they are completely described by their so-called stabilizer operators, which provide an experimentally economical way to discern the presence of entanglement and a lower bound for the fidelity of the generated state by way of evaluating their expectation values [35].

Once characterized, we proceed to automate the experimental calibration and measurement procedures. This is achieved by having the relevant linear optical components in our experimental setup, all connected to a centralized and remotely accessible server that mediates the control of the optical components.

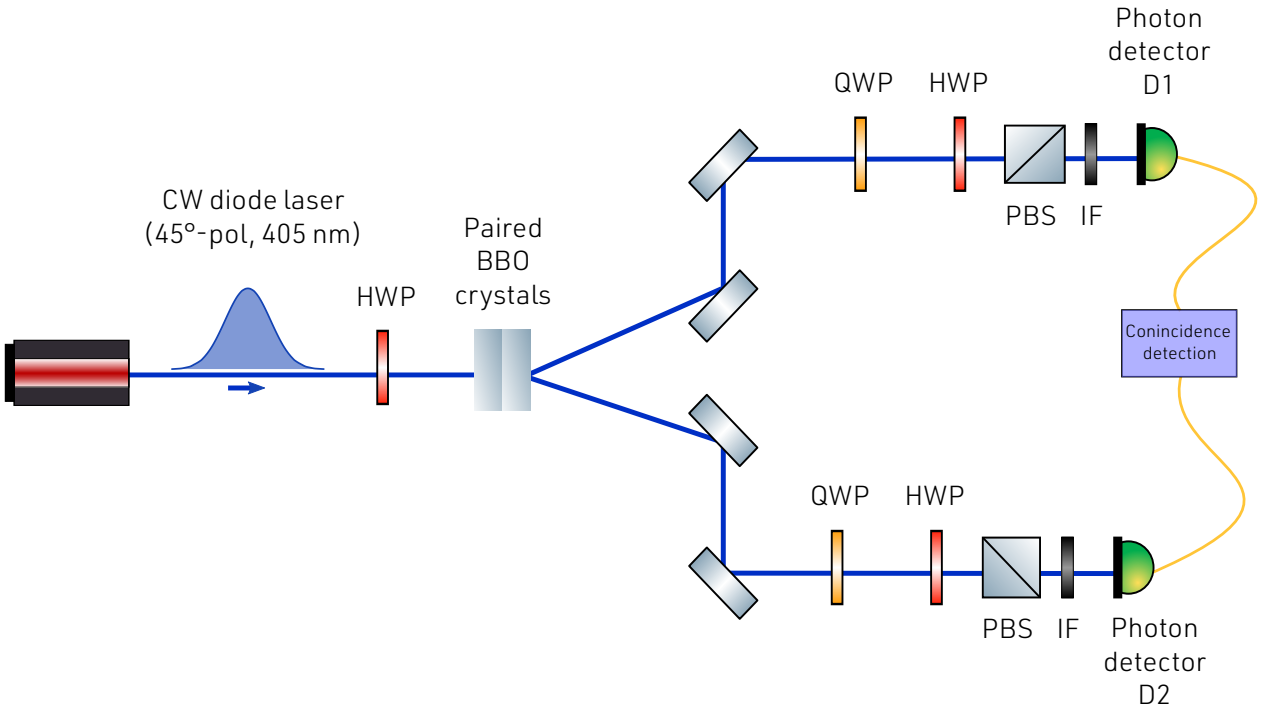


Figure 4.1: Experimental setup for generation and measurement of a two photon two-qubit Bell state. HWP, quarter-wave plate (QWP), β-barium borate (BBO), PBS, NPBS and interference filter (IF). A photon pair is created whenever a laser pump photon with 405 nm wavelength is incident on the paired BBO crystals cut for type-I SPDC, generating photons at 810 nm. Each photon is guided by a set of mirrors to a QWP, HWP, and PBS which are used to perform polarization measurements of the quantum state. Finally, each photon is sent to an IF at 800 nm with a bandwidth of 40 nm and collected by a single-mode fiber (SMF) and sent to a photon detector. Each photon detector produces an electronic signal and sends it to the coincidence counting electronics, which count the signals that arrive simultaneously.

With accessibility in mind, we designed a proof-of-concept mobile app that provides a graphical user interface to communicate with the server, which permits the user to specify an experiment with arbitrary (allowed) measurement settings and retrieve their experimental results. The rest of this chapter is dedicated to the filling in the details and describing the experimental design and subsequently, results from the experiments.

The main goal of the initial stage of the experiment was to characterize the polarization-entangled two-photon two-qubit state from a SPDC source using full quantum state tomography. To perform full quantum state tomography, we used the techniques and tools described in Ref. [129]. We begin by describing the various components of the experimental apparatus shown in Figure 4.1 — A laser and SPDC source, measurement apparatus, photon collection optics, and coincidence detection electronics. The SPDC source used was two concatenated 5 mm × 5 mm × 0.5 mm BBO crystals cut for type-I phase matching, with their two optical axes aligned in perpendicular planes.

When this source is pumped with a vertically polarized pump beam, due to type-I phase-matching, down-conversion will occur in the first crystal producing horizontally polarized energy-degenerate, non-collinear photon pairs. Similarly, a horizontally polarized pump beam will stimulate type-I down-conversion in the second crystal, generating energy-degenerate photon pairs. A diagonally polarized laser is likely to equally stimulate down-conversion in both crystals [126]. Photons in the spatially overlapping regions, diametrically opposed (due to momentum conservation) on the two light cones, will be in the state $(|H_1, H_2\rangle + e^{i\phi}\,|V_1, V_2\rangle)/\sqrt{2}$ as illustrated in Figure 4.2. A main condition here is that the spatial modes of a given pair must have a significant overlap [126]. Our SPDC source is pumped with a continuous wave (CW) blue laser[4], to produce frequency-degenerate photon pairs at a wavelength of 810 nm, emitted onto a light cone with an (full) opening angle of 6°.

[4] We keep our power relatively low, as high power pumps are known to stimulate double pair emissions [133, 134], which degrade the single-photon quality. Our laser pump operates at a power of ∼50 mW) for every experiment we conducted unless stated otherwise.

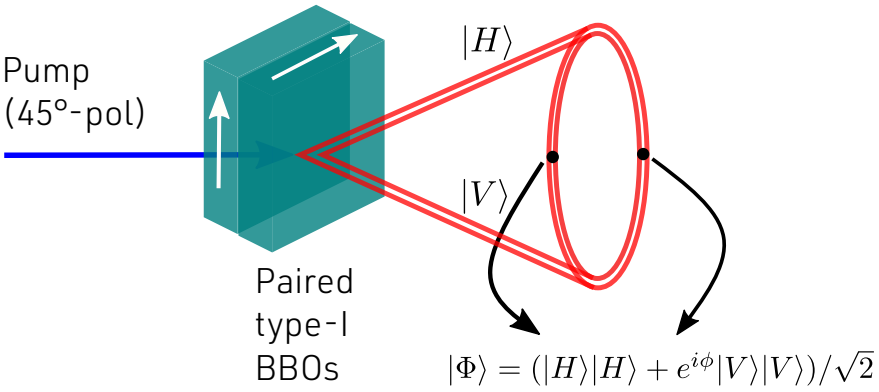


Figure 4.2: Two paired BBO (β-barium borate) crystals cut for type-I phase matching as a source of entangled photons. For every pump photon, the photon pairs emerge from the crystal at a fixed from the pump photon thus creating a cone around the direction of the pump photon. Photon pairs at diametrically-opposed points where the cones intersect represent points of indistinguishability (spatial, temporal and polarizations), and their two-qubit state is an entangled state of the form shown in this figure. The x, y, z axes are formed by the second crystal's optic axis, the pump beam and first crystal's optic axis respectively.

The value of ϕ is determined by the phase-matching, and details and geometry of the two crystals. The laser in our experiment produces vertically polarized light, we use a rotatable HWP[5] to adjust the beam to a desirable linear polarization.

The next stage of the apparatus is dedicated for tomographic analysis of the experimentally generated state and detection. An arrangement of a rotatable QWP and HWP, and PBS[6], allows one to project any arbitrary polarization state. The IFs are centred at 800 nm with a full width at half maximum (FWHM) $\approx$ 40 nm are used for spectral filtering, the photons in each output mode are then sent to a fibre coupler (FC)[7] mounted on a Thorlabs MBT613D/M fibre launch with a FC-connectorized fibre holder with a SMF[8] directly coupled into a single photon detector - built-in silicon avalanche photo-diode (APD)[9]. These last two steps improve the spatial indistinguishability of the collected photons. The detector outputs go to a coincidence counting module described in detail in Ref. [135]. An field-programmable gate array (FPGA) board which takes inputs from the detectors, and outputs the signals and coincidences between the inputs into a computer serial port, accessed by a LABVIEW program, gives the experimenter data processing and storage capabilities. An FPGA also permits a variable time window for n input signals to be detected as an n-fold coincidence. In all the experiments presented, the coincidence window was set to $\sim$7 ns.

4.3 A few practical notes on alignment

The initial alignment stage was done with a lower-power class-1 red laser beam sent from the collection optics (fibre couplers) back towards the crystals. Using the 3-axis dials on the fibre launch and the two target irises[10], we could align the beam path precisely along the plane of the optical table. The beam path in either arm is directed towards a so-called Z-fold laser pattern, two-mirror arrangement. This two-mirror arrangement allows us to precisely get the two beams to be at the correct opening angles of the light cone from the BBO crystals. By having a target with ruler markings at a distance d from the BBO crystals, we could get the two beams to have the correct distance from the CW blue laser beam spot (measured on the target ruler) such that they are incident on the BBO crystals close to the correct half-opening angle of $\theta/2 = 3°$. A simplified schematic of this geometric arrangement is shown in Figure 4.3. The furthest mirror from the BBO crystals in the Z-fold arrangement aligns the red laser beam spot at the ruler target, and the other mirror aligns the red laser beam spot such that it is superimposed with the CW blue laser beam spot on the BBO crystals, the procedure is identical for the two arms.

[5] Thorlabs Ø1/2″ Mounted Zero-Order HWP at 405 nm

[6] Thorlabs Ø1/2″ Mounted Zero-Order QWP/HWP at 808 nm and PBS202 20 mm cube with wavelength range of 620 – 1000 nm, respectively.

[7] With a Thorlabs RMS20X objective with an effective local length of 9 mm and numerical aperture of 0.4.

[8] Thorlabs P1-830A-FC-5 5 m long fibre with cut-off wavelength range of 830 – 980 nm

[9] Excelitas single photon counting modules (SPCM), SPCM-AQRH-15 with efficiencies of 65% and dark count rates of order $50s^{-1}$.

[10] A more convenient, but less precise alignment technique uses two target rulers. Vertical alignment is achieved by directing the beam spot onto a target mark on both rulers. Horizontal alignment is achieved by having the beam spot clipped by the two rulers (which would be aligned by the screw holes on the optical table) equally.

The above alignment procedure is precise enough such that when the two crystals are pumped with the CW blue laser operating at ∼50 mW with the HWP after it set to 22.5° to stimulate both crystals, we can see a few coincidence counts when polarization tomographic analysis optics are set to project out the state $|H_1, H_2\rangle$. The angle is counterclockwise with respect to the fast axis inscribed on the mounted optic, which is aligned perpendicular to the plane of the optical table for the all wave-plates in our experiments. It is also worthy to mention that, all the mounted wave-plates should be oriented to be either front-facing or back-facing, such that a propagating beam is always incident on the optic on the same side. A mismatch of kind between two wave-plates would gives rise to 180° relative difference between their optic axis, and as a consequence the reference frames for the polarization in the optic would be different. A counterclockwise (from the front) tilt on a wave-plate for a beam propagating towards the front-face of the optic, appears as a clockwise tilt for a beam propagating in the opposite direction. Fine adjustments are done with the dials on the fibre couplers to maximize the coincidence counts for both the two-photon state $|H_1, H_2\rangle$ and $|V_1, V_2\rangle$ measurements, first independently then concurrently.

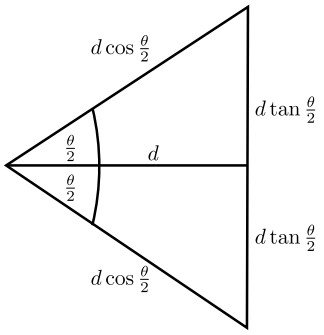


Figure 4.3: Schematic of the geometry due to the opening angle of the light cone from a SPDC source; For a horizontal distance of d from a SPDC source, the two frequency-degenerate photons generated from the source will both be at a distance of $d\tan\frac{\theta}{2}$ from the horizontal axis, defined by the direction of original beam incident on the crystals.

4.4 Results

After we performed the coarse alignment procedure described above to a preliminary and satisfactory level, we performed full quantum state tomography for the two-photon, two-qubit polarization-entangled state with the theoretical machinery described by James et al. [129]. We performed the full set of 16 polarization measurement settings shown in Table 4.1. The coincidence rates were collected over a time interval of 10 s for each measurement setting, with a coincidence window of 7 ns. For the experimentally generated state ϱ, for each measurement setting and corresponding projector in Table 4.1, experimentally we expect to observe the average number of coincidences given by $\nu_v = \langle\varrho|\psi_v|\varrho\rangle$. The set of projectors in the aforesaid table are complete set of measurements, that is, ϱ can be completely and uniquely determined by the said set of measurements. From all 16 projective measurements, it is possible to recover an estimate of ϱ. Recover a valid density matrix estimate of ϱ (Hermitian, positive etc) the estimate of ϱ is recovered *via* maximum likelihood (see [129] for details). Equation (4.1) shows the reconstructed density matrix of the polarization entangled-state and Figure 4.4 shows a graphical representation of this state.

$$\varrho = \begin{pmatrix} 0.43 & -0.044-0.042i & 0.021-0.061i & -0.14+0.32i \\ -0.044+0.042i & 0.013 & 0.016+0.0089i & -0.0071-0.024i \\ 0.021+0.061i & 0.016-0.0892i & 0.045 & 0.020+0.053i \\ -0.14-0.32i & 0.0071+0.024i & 0.020-0.053i & 0.51 \end{pmatrix}. \tag{4.1}$$

The reconstructed state shows a commendable degree of entanglement; It has a fidelity of $F_\varrho = 0.787 \pm 0.0113$ with the maximally entangled state $(|H_1, H_2\rangle - i\,|V_1, V_2\rangle)/\sqrt{2}$. Our measured state also achieves a value of $\langle S\rangle = 2.344 + 0.0228$ for the Bell-CHSH operator, which represents a violation of the inequality, thus confirming that the state possess non-local correlations. Furthermore, from the density matrix, we can derive physical quantities that give an inkling of the statistical properties of the measured state. One such quantity is the linear entropy, which quantifies the statistical "mixedness" of the measured state. We measure it to have a value of $S_L = 4/3(1 - \mathrm{Tr}(\varrho^2)) = 0.387 + 0.0183$.

m	Projector	h_1	q_1	h_2	q_2	$N\ (10s^{-1})$
1	$\|V\rangle\langle V\| \otimes \|V\rangle\langle V\|$	45°	0°	45°	0°	2348
2	$\|V\rangle\langle V\| \otimes \|H\rangle\langle H\|$	45°	0°	0°	0°	24
3	$\|H\rangle\langle H\| \otimes \|H\rangle\langle H\|$	0°	0°	0°	0°	2410
4	$\|H\rangle\langle H\| \otimes \|V\rangle\langle V\|$	0°	0°	45°	0°	206
5	$\|L\rangle\langle L\| \otimes \|V\rangle\langle V\|$	22.5°	0°	45°	0°	720
6	$\|L\rangle\langle L\| \otimes \|H\rangle\langle H\|$	22.5°	0°	0°	0°	1295
7	$\|D\rangle\langle D\| \otimes \|H\rangle\langle H\|$	22.5°	45°	0°	0°	1525
8	$\|D\rangle\langle D\| \otimes \|V\rangle\langle V\|$	22.5°	45°	45°	0°	1346
9	$\|D\rangle\langle D\| \otimes \|L\rangle\langle L\|$	22.5°	45°	22.5°	0°	2350
10	$\|D\rangle\langle D\| \otimes \|D\rangle\langle D\|$	22.5°	45°	22.5°	45°	1005
11	$\|L\rangle\langle L\| \otimes \|D\rangle\langle D\|$	22.5°	0°	22.5°	45°	2132
12	$\|V\rangle\langle V\| \otimes \|D\rangle\langle D\|$	45°	0°	45°	45°	826
13	$\|H\rangle\langle H\| \otimes \|D\rangle\langle D\|$	0°	0°	0°	45°	1705
14	$\|H\rangle\langle H\| \otimes \|R\rangle\langle R\|$	0°	0°	0°	90°	1129
15	$\|V\rangle\langle V\| \otimes \|R\rangle\langle R\|$	45°	0°	45°	90°	1662
16	$\|L\rangle\langle L\| \otimes \|R\rangle\langle R\|$	22.5°	0°	22.5°	90°	626

Table 4.1: Measurement settings and coincidence counts for a preliminary tomography analysis of a two-photon polarization state prior to optimization. Coincidence counts, collected over a ten second intervals, for each of the 16 settings, are sufficient to recover an estimate of the density matrix of the two-qubit polarization state of the two photons. Here, $|D\rangle := (|H\rangle + |V\rangle)/\sqrt{2}$, $|L\rangle := (|H\rangle + i\,|V\rangle)/\sqrt{2}$ and $|R\rangle := (|H\rangle - i\,|V\rangle)/\sqrt{2}$

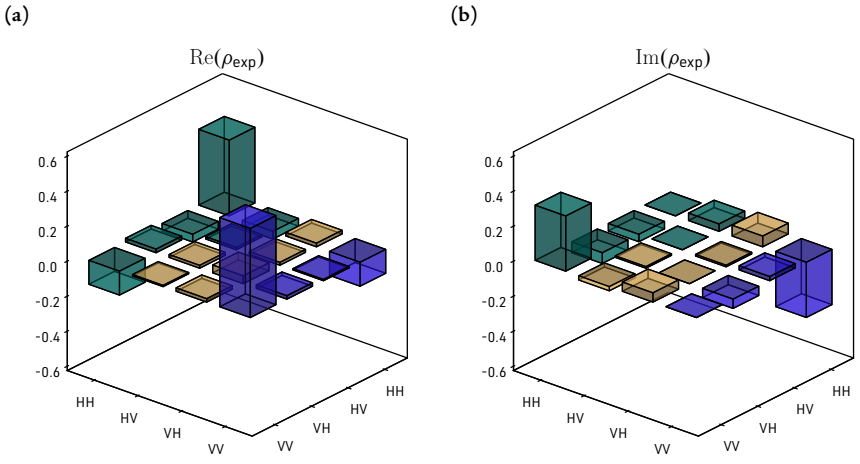


Figure 4.4: Density matrix of a state estimated by maximum likelihood tomography prior to optimization, from the experimental data given in Table 4.1 **(a)** Real part of the estimate of ϱ. **(b)** Imaginary part of the estimate of ϱ.

As also reflected by the graphical representation of the density matrix of this state, this value indicates a considerable amount of mixture present in measured state. The errors of the quantities here were also estimated from a Monte Carlo simulation of 100 samples with Poisson noise. The values for quantities reported above are not necessarily of low quality; the generated state shows a fidelity of commendable quality, and significant degree of entanglement. However, we had to a reason to suspect that the state generated could be improved. An experiment of a similar kind [126], reports over 140 coincidence counts per second per milliwatt of pump power over a 5 nm bandwidth and a value of $\langle S\rangle = 2.700$, thus there is much room for improvement.

Next we will describe the optimization procedure followed to improve the quality of the state generated in the experiment, and the subsequent result. Optimization is with respect to some utility function, and what will be described here is not necessarily a procedure suitable in all circumstances, and definitively imperfect. An imperative of uttermost practical importance to our experiment, was the tuning of the value of ϕ in the state $|H_1, H_2\rangle + e^{i\phi}\,|V_2, V_2\rangle$ generated by the SPDC source.

As it can be inferred from the preliminary results, for that particular state, which has a significant fidelity with the state $|H_1, H_2\rangle - i\,|V_1, V_2\rangle$, the value of ϕ can be crudely inferred to take on a value $\phi = \pi$. We seek to generate one of the four Bell states:

$$\begin{aligned}
\left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}\left(|H_1, H_2\rangle + |V_1, V_2\rangle\right), \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}\left(|H_1, H_2\rangle - |V_1, V_2\rangle\right), \\
\left|\Psi^+\right\rangle &= \frac{1}{\sqrt{2}}\left(|H_1, V_2\rangle + |V_1, H_2\rangle\right), \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}\left(|H_1, V_2\rangle - |V_1, H_2\rangle\right).
\end{aligned} \tag{4.2}$$

This imperative is once again motivated by the end goal of ultimately generating a three qubit GHZ state. Thus, with this end in view, it is more experimentally convenient if we were to generate either one of the first two Bell states in Equation (4.2). In any case, our SPDC source alone is limited to the generation of these two particular Bell states[11]. We chose to optimize for the second Bell state, the optimization procedure for this particular state is guarded by the following observations.

[11] All four Bell states are equivalent up to some local unitary operation, for instance, if our SPDC source generates the states $|H_1, H_2\rangle \pm |V_1, V_2\rangle$, an extra HWP in the second arm that interchanges H and V (rotated 45° counterclockwise to its fast-axis), prepares $|H_1, V_2\rangle \pm |V_1, H_2\rangle$. Similarly, the unitary operator $U = \mathbb{1} \otimes S$, where $S = \mathrm{diag}(1, i)$, acting on $|H, H\rangle \pm i\,|V_1, V_1\rangle$, prepares $|H_1, H_2\rangle \pm |V_1, V_1\rangle$.

Consider one of the projectors from tomography analysis, $P_{DD} = |D_1\rangle\langle D_1| \otimes |D_2\rangle\langle D_2|$ where $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$. Calculating the expectation value of the projector[12] with respect to the state $|\Phi^-\rangle$ in Equation (4.2), we observe that (omitting normalization constants):

$$\begin{aligned}
\langle\Phi^-|P_{DD}|\Phi^-\rangle &= \langle\Phi^-|(|D_1\rangle\langle D_1| \otimes |D_2\rangle\langle D_2|)|\Phi^-\rangle, \\
&= |\langle H|D\rangle|^4 - |\langle D|H\rangle\langle V|D\rangle|^2 - |\langle D|H\rangle\langle V|D\rangle|^2 + |\langle V|D\rangle|^4, \\
&= \left(\frac{1}{\sqrt{2}}\right)^4 - \left(\frac{1}{\sqrt{2}}\right)^4 - \left(\frac{1}{\sqrt{2}}\right)^4 + \left(\frac{1}{\sqrt{2}}\right)^4, \\
&= 0.
\end{aligned} \tag{4.3}$$

[12] This expectation value is related to the probability of a getting an outcome associated with the projector upon performing the projective measurement on $|\Phi^-\rangle$.

Similarly, the projector $P_{LR} = |L_1\rangle\langle L_1| \otimes |R_2\rangle\langle R_2|$, where $|L/R\rangle = (|H\rangle \pm i\,|V\rangle)/\sqrt{2}$ gives:

$$\begin{aligned}
\langle\Phi^-|P_{LR}|\Phi^-\rangle &= \langle\Phi^-|(|L_1\rangle\langle L_1| \otimes |R_2\rangle\langle R_2|)|\Phi^-\rangle, \\
&= |\langle H|L\rangle\langle R|H\rangle|^2 - \langle H|L\rangle\langle L|H\rangle\langle H|R\rangle\langle R|V\rangle, \\
&\quad - \langle V|L\rangle\langle L|H\rangle\langle V|R\rangle\langle R|H\rangle + |\langle V|L\rangle\langle R|V\rangle|^2, \\
&= \left(\frac{1}{\sqrt{2}}\right)^4 - \left(\frac{1}{\sqrt{2}}\right)^4 - \left(\frac{1}{\sqrt{2}}\right)^4 + \left(\frac{1}{\sqrt{2}}\right)^4, \\
&= 0.
\end{aligned} \tag{4.4}$$

Aided by the above observations, we conjure up a procedure to optimize for the state $|\Phi^-\rangle$:

Primo Set the polarization analysis optics to project out $|H_1, H_2\rangle$ and maximize the corresponding coincidence counts, typically achieved by fine adjustments to using the z-dial on the kinematic mount that holds the BBO crystals, which tilts the crystals with respect to the z-x plane (left-handed Cartesian coordinate system). Similarly, maximize the coincidence counts for the projection of $|V_1, V_2\rangle$, achieved by fine adjustments to the dials on the rotation stage at the bottom of the kinematic mount, which rotate the crystals about to the z-axis.

Secondo Set the polarization analysis optics to project out $|D_1, D_2\rangle$ and minimize the corresponding coincidence counts, which we achieved by rotating the crystals with respect to y-axis with the radial dial on the kinematic mount. Similarly, set the polarization analysis optics to project out $|L_1, R_2\rangle$ and minimize the corresponding coincidence counts, by using the x-y axis dials on either side of the kinematic mount.

Terzo We go through several iterations of this process, and roughly equalize the two coincidence counts observed for $|H_1, H_2\rangle$ and $|V_1, V_2\rangle$, while minimizing the ones observed for $|D_1, D_2\rangle$ and $|L_1, R_2\rangle$.

While iterating the steps of the above procedure, one eventually reaches a point where additional iterations have non-desirable results; The coincidence counts for $|D_1, D_2\rangle$ and $|L_1, R_2\rangle$ reach some local minimum (typically around $30s^{-1}$) and start increasing again, or the counts for $|H_1, H_2\rangle$ and $|V_1, V_2\rangle$ are no longer equal. At this point we halt and take the previous iteration to be optimal. Physically, the optimization procedure is changing the opening directions of the two light cones emerging from the BBO crystals such that the collection optics in our experiment can access as much of the light cones as possible, and as close as possible to diametrically-opposed regions of indistinguishability. The measurement results after several iterations of this process are shown in Table 4.2 and the corresponding graphical representation of the reconstructed density matrix shown in Figure 4.5, where the corresponding density matrix for the two-photon state is given by

$$\varrho = \begin{pmatrix} 0.49 & 0.028 + 0.033i & 0.017 - 0.025i & -0.41 + 0.054i \\ 0.028 - 0.033i & 0.0074 & -0.0019 + 0.0017i & 0.0011 + 0.023i \\ 0.017 + 0.025i & -0.0019 - 0.0017i & 0.0074 & -0.034 - 0.042i \\ -0.41 - 0.054i & 0.0011 - 0.023i & -0.034 + 0.042i & 0.49 \end{pmatrix}. \tag{4.5}$$

From the above density matrix and its graphical representation, in comparison to the earlier reconstruction in Figure 4.4, we note a few conspicuous differences. The populations of horizontally-and vertically-polarized photons are equalized in the optimized measured state[13]. Likewise, the coherences[14] between these two populations are equalized, and have a close resemblance to the coherences of the Bell state $|\Phi^-\rangle$; the fidelity between the measured state and the aforementioned state is $F_\varrho = 0.902 \pm 0.00588$. Furthermore, there is an improvement of the other previously reported physical quantities; The measured state a violates a Bell-CHSH inequality, attaining a value of $\langle S \rangle = 2.594 \pm 0.0153$.

Lastly, the linear entropy of the above state has a value of $S_L = 0.211 \pm 0.0134$, which reflects a decrease in the "mixedness" of the state, in comparison to the earlier reconstruction. The errors in these quantities were estimated from a Monte Carlo simulation of 100 samples with Poissonian noise on the count statistics[15].

[13] Represented by the diagonal element on the top-left and diagonal element bottom-right respectively.

[14] Represented by the off-diagonal elements. For this particular instance, the entries on the bottom left and top right.

[15] This is because due to the probabilistic nature of SPDC, the number of n discrete photon pairs that arrive at the detectors for given a collection time interval Δt follows a Poissonian probability distribution Pois$(\lambda = n\Delta t)$.

m	Projector	h_1	q_1	h_2	q_2	N $(10s^{-1})$
1	$\|V\rangle\langle V\| \otimes \|V\rangle\langle V\|$	45°	0°	45°	0°	2738(83)
2	$\|V\rangle\langle V\| \otimes \|H\rangle\langle H\|$	45°	0°	0°	0°	33(5)
3	$\|H\rangle\langle H\| \otimes \|H\rangle\langle H\|$	0°	0°	0°	0°	2718(69)
4	$\|H\rangle\langle H\| \otimes \|V\rangle\langle V\|$	0°	0°	45°	0°	35(2)
5	$\|L\rangle\langle L\| \otimes \|V\rangle\langle V\|$	22.5°	0°	45°	0°	1256(14)
6	$\|L\rangle\langle L\| \otimes \|H\rangle\langle H\|$	22.5°	0°	0°	0°	1492(40)
7	$\|D\rangle\langle D\| \otimes \|H\rangle\langle H\|$	22.5°	45°	0°	0°	1470(23)
8	$\|D\rangle\langle D\| \otimes \|V\rangle\langle V\|$	22.5°	45°	45°	0°	1479(26)
9	$\|D\rangle\langle D\| \otimes \|L\rangle\langle L\|$	22.5°	45°	22.5°	0°	1434(46)
10	$\|D\rangle\langle D\| \otimes \|D\rangle\langle D\|$	22.5°	45°	22.5°	45°	284(15)
11	$\|L\rangle\langle L\| \otimes \|D\rangle\langle D\|$	22.5°	0°	22.5°	45°	1614(31)
12	$\|V\rangle\langle V\| \otimes \|D\rangle\langle D\|$	45°	0°	45°	45°	1549(31)
13	$\|H\rangle\langle H\| \otimes \|D\rangle\langle D\|$	0°	0°	0°	45°	1079(11)
14	$\|H\rangle\langle H\| \otimes \|R\rangle\langle R\|$	0°	0°	0°	90°	1661(46)
15	$\|V\rangle\langle V\| \otimes \|R\rangle\langle R\|$	45°	0°	45°	90°	1159(24)
16	$\|L\rangle\langle L\| \otimes \|R\rangle\langle R\|$	22.5°	0°	22.5°	90°	254(12)

Table 4.2: Measurement settings and coincidence counts for a tomography analysis of a two-photon polarization state after optimization. Coincidence counts, collected over a ten second intervals, for each of the 16 settings, are sufficient to recover an estimate of (reduced) density matrix of the two-qubit polarization state of the two photons. Here, $|D\rangle := (|H\rangle + |V\rangle)/\sqrt{2}$, $|L\rangle := (|H\rangle + i\,|V\rangle)/\sqrt{2}$ and $|R\rangle := (|H\rangle - i\,|V\rangle)/\sqrt{2}$.

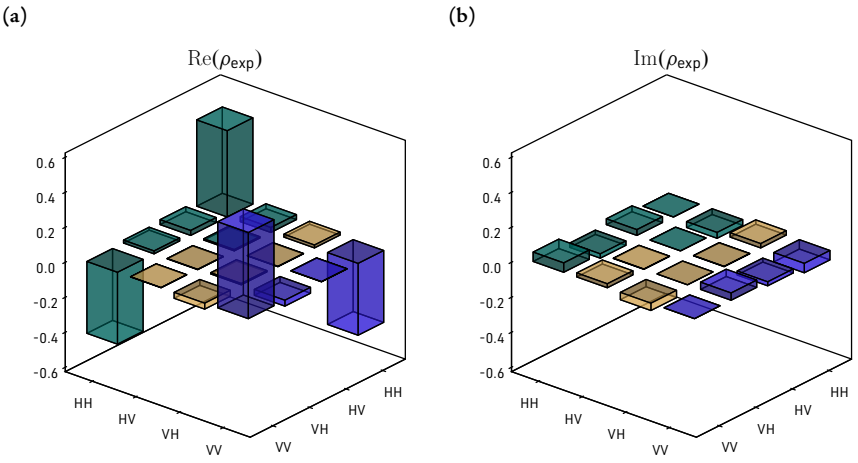


Figure 4.5: Density matrix of a state estimated by maximum likelihood tomography from the experimental data given in Table 4.2 after optimization. **(a)** Real part of the estimate of ϱ. **(b)** Imaginary part of the estimate of ϱ.

Alas, while the above results improve over the preliminary results and are in good agreement with expected state $|H_1, H_2\rangle - |V_1, V_2\rangle$, unwanted artefacts such as the apparent loss in the coherences of the two orthogonal polarizations and a small, non-negligible mixedness of the state, in the reconstructed state still persist. The origins of some of these unwanted artefacts can be attributed to systematic errors, such as those stemming from efficiencies of the various optical components in the experiment[16].

While the origins of the loss of coherences are often attributable to the many decoherence mechanisms of polarization-entangled sources, which vary from source to source and dependent on nature and application of the experiment at hand. We will briefly outline the two decoherence mechanisms that are relevant to our application, following references [136–139].

[16] PBS transmission and reflection efficiencies, photon detector efficiency and their coupling efficiency to optical fibres, collection efficiencies etc.

An ideal process of type-I SPDC has stringent phase matching conditions; for a pump photon incident on a crystal down converts to two photons, a signal and an idler photon, with the same polarization. The entire process must both conserve momentum and energy, which give rise to the aforementioned conditions:

$$\begin{aligned} \vec{k}_i + \vec{k}_s &= \vec{k}_p, \\ \omega_i + \omega_s &= \omega_p, \end{aligned} \tag{4.6}$$

where $\vec{k}$ and ω are the wave vector and frequency of the photon respectively. The subscripts i, s and p refer to the idler, signal and pump photon respectively. For a frequency degenerate type-I SPDC process, the idler and signal photons have half the frequency of the pump photon individually. In an ideal experiment, one expects the phase-matching conditions to be perfectly satisfied, in an actual experiment this is not the case. In reality, there is often a phase mismatch, which enters into Equation (4.6) *via* an additional effective wave vector $\vec{\Delta}$, which has a non-trivial effect on the spectral properties of the process.

$$\vec{k}_i + \vec{k}_s + \vec{\Delta} = \vec{k}_p. \tag{4.7}$$

Ideally, for a type-I non-collinear degenerate SPDC process, only frequency-degenerate photon pairs are emitted at the emission angle of the light cones. However, due to the phase mismatch, it is possible for the process to also produce non-degenerate frequency photons pairs. The emission angles of the non-degenerate pairs will not always be asymmetric around pump beam; the findings in Ref. [139] report the production of non-degenerate pairs at 662.2 nm (signal photon) and 747.3 nm (idler photon) respectively, with the signal photon within the collection angle of their system (around 3°), while the idler photon falls outside this collection angle, hence does not contributing to the single photon rates.

The said effect produces spectral profiles for both signal and idler photons that are asymmetric around the degenerate frequency. The result of this spectral profile asymmetry along with the geometry of a experiment, have a bearing on the two-photon joint spectra which determines the coincidence counts. Baek and Kim [139] show that the joint spectra is significantly reduced in comparison to the spectral profile of the signal/idler photon pairs, and limited by the collection angles in their experiment, $2.95° - 3.17°$; this collection range does not collect one of the photons from a non-degenerate pair. As a result, the two-photon spectra can also have asymmetric spectral profile around the degenerate frequency, which can be significantly altered by small alignment errors.

A way to compensate for this spectral asymmetry is by way of spectral filtering over the bandwidth of a narrow bandwidth filter around the degenerate frequency, the spectral profiles of the idler and signal photons, and consequently two-photon joint spectra are made more similar to one another, by effectively filtering out the unwanted non-degenerate photon pairs. This method of compensation comes at the expense of collection efficiency of the experiment. The spectral filters in our experiment have quite a broad bandwidth, centred at 800 nm with a FWHM of 40 nm, thus it is not far-fetched to suspect the presence of non-degenerate photon pairs, which is by evidenced by the significantly high single count rate in comparison to coincidence rate (by roughly a scale ~ 0.3).

We attempted to use narrow bandwidth filters, centred at 810 nm with a FWHM of 10 nm, which did not improve the results by much, upon inspection, we found that when filtering a white light source[17] the two filters had non-overlapping regions of considerable size in their spectral profiles. One of the interference filters was not centred at 810 nm (as indicated by the manufacturer) but slightly higher, which for the interim explains why the results did not improve by much.

[17] Fianium WhiteLase micro with spectrum <450 nm to >2000 nm with a pulse width of ≈6 ps and a repetition rate of 20 MHz.

Another dominant decoherence mechanism, particularly for a paired-BBO type-I SPDC source, is one that degrades the temporal indistinguishability of the down converted photons. Crudely represented, the two crystals having finite thickness, means the two down-conversion processes in the two crystals will occur at slightly different times (order of femtoseconds). Over the thickness of the crystals, both birefringent and dispersive effects influence the group velocities of both signal and idler photons, and subsequently their emission times from the two crystals. If the assumption is that two down-conversion processes take place at halfway the length of each crystal, then time taken by the signal and idler photons to traverse the length L of the two crystals, can be calculated as follows [138]. For photons down converted in the first crystal:

Primo A pump photon will traverse half of the length of the first crystal where it is extraordinary polarized, after which it down converts resulting in a polarization perpendicular to the original and hence ordinary polarized.

Secondo The resulting signal/idler photon will traverse the second half of the first crystal ordinary polarized.

Terzo After exiting the first crystal, the signal/idler photon will traverse the full length of the second crystal extraordinary polarized.

The time spent by a signal photon in each of the three stages above depends on the refractive-index-dependent group velocities of ordinary and extraordinary photons in the two crystals and the length L:

$$t_s = \frac{L}{2V_g^e(\omega_p)} + \frac{L}{2V_g^o(\omega_s)} + \frac{L}{V^e(\omega_s)}, \tag{4.8}$$

the reasoning is similar for photons down converted in the second crystal, and gives:

$$t_s' = \frac{L}{V_g^o(\omega_p)} + \frac{L}{2V_g^e(\omega_p)} + \frac{L}{2V_g^o(\omega_s)}, \tag{4.9}$$

and the net delay Δt_s between the two down conversion processes is given by

$$\Delta t_s = t_s' - t_s = L\left(\frac{1}{V_g^o(\omega_p)} - \frac{1}{V_g^e(\omega_s)}\right). \tag{4.10}$$

The above time difference leads to the degradation of the temporal indistinguishability between the two light cones; photons belonging to one light cone will be delayed by $\Delta t_{s/i}$ relative to the photons from the other light cone.

Rangarajan et al. [138] derive an expression for the density matrix of the two-photon down converted state with such a delay:

$$\varrho' = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & \nu(\Delta t_s, \Delta t_i) \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \nu^*(\Delta t_s, \Delta t_i) & 0 & 0 & 1 \end{pmatrix}, \tag{4.11}$$

where $\nu(\Delta_s, \Delta_i)$ is dependent on the two-photon joint spectra. As expected, we note that this decoherence mechanism has no effect on the two populations but only affects the coherence between the two polarizations. Refs. [136–138] recommended the use of birefringent crystals, with the same but opposite time delay between extraordinary and ordinary components of the pump photons, to pre(post)compensate for the delay between the emission-times of the two down conversion processes. With use of such techniques, they were able to state fidelities in excess of 0.977.

4.5 Concluding remarks

In this chapter, we described and conducted an experiment based on SPDC, generating a two-photon two-qubit polarization-entangled state. The generated state is fully characterized through QST, recovering its density matrix, from which other physical quantities of interest, such as those quantifying the degree of entanglement possessed by the state can be derived from. The SPDC source is optimized, with a rule of thumb procedure described in the text, to generate one of the Bell states ($|\Phi^-\rangle$). We repeat this process until we achieve a fidelity of 0.90. In comparison to similar demonstrations in the current literature, which can achieve fidelities in access of 0.97, this is a relatively is low fidelity, nevertheless the obtained result is satisfactory to our experimental needs. Lastly, we briefly outlined a description of the two decoherence mechanisms for paired BBO type-I non-collinear SPDC and how these maybe counteracted to improve the fidelity of the generated polarization-entangled state. In the chapter that follows, we will describe how the polarization-entangled state generated by this Bell-state photon pair source may be extended to accommodate an additional qubit through a different DOF.

5

Path-polarization-entangled photons

" Am I a wave? Am I a particle? Am I analog or digital?
The answer surely must be both or none.
My laws say quarks and clocks alike show interference,
That if you watch a state, it never changes,
That two entangled systems act as one."

— Peter Shor, Quantum Poetry Tweet Collection

5.1 Introduction: Multi-degree of freedom entanglement

The preceding chapter describes the generation of a two-photon two-qubit polarization-entangled state *via* the process of SPDC with type-I phase matching. In this chapter, we endeavor to describe and experimentally realize one possible way to enlarge this two-qubit state to a state of more qubits. From the previous chapter, one can at least get an inkling that the generation of entangled photons by way of SPDC is appealing due to its accessibility, in the case of type-I SPDC, ease of alignment and relatively high photon counts in comparison to type-II phase matched SPDC [126]. Thus one could possibly conceive of a way to enlarge the aforesaid two-qubit state *via* the same SPDC process; a string of successive SPDC processes producing a pair of entangled photons at each step, as done in the experiments of Ref. [119, 140, 141]. One potential and sizeable obstacle to such methods is decoherence. As briefly alluded to in the previous chapter, unless one incorporates methods to counteract some of the effects of decoherence on SPDC sources such as phase-compensation [136, 138] to improve the brightness of the source, experiments making use of cascaded SPDC processes typically suffer from low efficiencies [1]

[1] Due to the decoherence mechanisms of SPDC source, but also due to inefficiencies of the optics in the experiment, *e. g.* the collection and detection inefficiencies.

Hitherto, we have only considered the polarization DOF, however photon pairs generated in this way also possess various forms of entanglement. The phase-matching conditions for SPDC give rise to conservation laws for both energy and momenta of the photon pairs, as a result the pairs are entangled in these continuous DOFS as well. The experiments of Rarity et al. [142] and Kwiat et al. [143] were few of the first to demonstrate a violation of a Bell-inequality for a continuous DOFS, energy (and time) and momentum, respectively.

Relatively recent experiments have given evidence that, the process of SPDC conserves the orbital angular momentum [144, 145]; demonstrating the generation and analysis of coherent superposition of Laguerre-Gaussian (LG) transverse spatial modes, and a violation of a Bell-inequality for qutrits. A theoretical justification for this conservation law was later derived by Franke-Arnold et al. [146] from the phase-matching conditions of SPDC. For a LG mode pump beam carrying the quantum number l_{pump} [2], the sum of the corresponding quantum number for signal and idler photons must be the same, *i.e.* $l_{\text{signal}} + l_{\text{idler}} = l_{\text{pump}}$. For a pump beam with $l_{\text{pump}} = 0$, the resultant two-photon orbital angular momentum (OAM) state will be

[2] Every photon in the beam carries an orbital angular momentum of $\hbar l_{\text{pump}}$ [147].

$$|\psi\rangle_{\text{OAM}} = \alpha_{0,0}\,|0_1, 0_2\rangle + \alpha_{1,-1}\,|1_1, -1_2\rangle + \alpha_{-1,1}\,|-1_1, 1_2\rangle + \ldots\ldots, \quad (5.1)$$

with the LG modes spanning a countably-infinite dimensional Hilbert space, where the kets denote OAM states labelled with the indices l and α's denoting their corresponding probability amplitudes; the subscripts 1 and 2 represent the signal and idler photons, respectively.

Photons produced *via* SPDC could result in photons possessing non-classical correlations in degrees of freedom simultaneously, with each DOF independently addressable for such measurements. Such multiply-entangled states are called "hyper-entangled" states, coined by Kwiat [148]. For instance, photon pairs produced by a paired BBO type-I SPDC process, generate a state represented by the product state:

$$|\Psi\rangle \sim (|H_1, H_2\rangle - |V_1, V_2\rangle) \otimes (|-1_1, -1_2\rangle + |1_1, 1_2\rangle). \quad (5.2)$$

For this particular state, each DOF is independently addressable and in a well defined state, that is, measurements of observables on either subsystem, whether of polarization or orbital angular momentum, have no bearing on the other subsystem. Formally, a partial trace over the subsystem in either DOF leaves the other subsystem unaffected.

$$\begin{aligned} \text{Tr}_A(\varrho_{AB}) &= \text{Tr}_A(\varrho_A \otimes \varrho_B), \\ &= \sum_{i=0}^{3} \langle i|\varrho_A|i\rangle \otimes \varrho_B, \\ &= \mathbb{1}_A \otimes \varrho_B, \\ &= \varrho_B, \end{aligned} \quad (5.3)$$

where $\varrho_A = 1/2(|H_1, H_2\rangle - |V_1, V_2\rangle)(\langle H_1, H_2| - \langle V_1, V_2|)$ and $\varrho_B = 1/2(|-1_1, -1_2\rangle + |1_1, 1_2\rangle)(\langle -1_1, -1_2| + \langle 1_1, 1_2|)$, and where $|i\rangle$'s are from the orthonormal basis set $\{|H_1, H_2\rangle, |H_1, V_2\rangle, |V_1, H_2\rangle, |V_1, V_2\rangle\}$ for the polarization subsystem. It is also possible for a SPDC source to generate a state of the kind:

$$|\Psi\rangle \sim (|H_1, H_2, -1_1, -1_2\rangle + |V_1, V_2, 1_1, 1_2\rangle). \quad (5.4)$$

Such a state is a little different from the state of Equation (5.2). The first obvious difference is this state isn't a product state; the state in either DOF can no longer be described separately, we can only collectively describe it by referencing to the state of the other DOF *i.e.* the full joint state is non-separable. For such a state (as we've seen elsewhere), a measurement in one DOF has a bearing on the other DOF. For instance, taking the partial trace over the OAMDOF yields:

$$\begin{aligned}\mathrm{Tr}_{CD}(\varrho_{ABCD}) = \mathrm{Tr}_{AB}(&|H_1, H_2, -1_1, -1_2\rangle \langle H_1, H_2, -1_1, -1_2| \\ &+ |H_1, H_2, -1_1, -1_2\rangle \langle V_1, V_2, 1_1, 1_2| \\ &+ |V_1, V_2, 1_1, 1_2\rangle \langle V_1, V_2, 1_1, 1_2| \\ &+ |V_1, V_2, 1_1, 1_2\rangle \langle H_1, H_2, -1_1, -1_2|) \\ &= |H_1, H_2\rangle \langle H_1, H_2| + |V_1, V_2\rangle \langle V_1, V_2|\,. \end{aligned} \tag{5.5}$$

where the partial trace is performed over the basis set $\{|-1_1, -1_2\rangle, |-1_1, 1_2\rangle, |1_1, -1_2\rangle, |-1_1, -1_2\rangle\}$. Note that the resultant state is one in which coherences between $|HH\rangle$ and $|VV\rangle$ are completely destroyed; the density matrix of the state has no off-diagonal elements. The said states are called "hypoentangled states" [149], their defining feature is that they exhibit simultaneous entanglement, but when one of DOFS is considered independently, the entanglement in that DOF isn't preserved.

The first demonstration and complete characterization of a hyper entangled photonic quantum system was done by Langford [149], generating and completely characterizing a 144-dimensional state, simultaneously and independently entangled in polarization, transverse (OAM) spatial modes and photon emission times (time-bin encoding). The rarity and novelty of such a demonstration would seem to suggest the experimental difficulty/novelty of realizing photonic states of this kind. Indeed, exerting control over different DOFS is not trivial. They often necessitated sophisticated and tricky mode (spatial and/or temporal) matching requirements to implement in practice.

The same partly holds true in practice, for similar experiments that generate hyper(hypo) entangled photonics states through polarization and momentum (directions of the emitted photons) DOFS. Here, a pump beam stimulates a SPDC crystal in both directions resulting in polarization-entangled photon pairs in both directions, which are then appropriately isolated to four optical path modes (l_1, l_2 and r_1, r_2 in Figure 5.1). If the paired path modes, one mode from the backward photon pair and another from the forward photon pair (l_1 and r_1 and l_2 and r_2) are overlapped temporally (and spatially) on the input ports of a 50:50 beam splitter (see Figure 5.2), can they can realize a hyperentangled state of the form [150]:

$$|\Psi\rangle \sim (|H_1, V_2\rangle \pm |H_1, V_2\rangle) \otimes (|r_2, l_2\rangle \pm |l_1, r_1\rangle), \tag{5.6}$$

alternatively if paired path modes belong to the same photon pair (l_1 and l_2 and r_1 and r_2) are similarly overlapped temporally (and spatially) generate the hypoentangled state [72]:

$$|\Psi\rangle \sim (|H_1, H_1\rangle + |V_1, V_2\rangle)\,|l_1, l_2\rangle + (|H_1, H_2\rangle - |V_1, V_2\rangle)\,|r_1, r_2\rangle). \tag{5.7}$$

In this kind of experimental setup, in addition to the spatial and/or temporal mode matching requirements, the generated state depends on the rate of photon pair emissions in both directions.

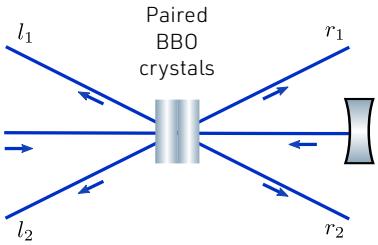


Figure 5.1: A SPDC source with two concatenated BBO crystals stimulated by a pump beam in both directions. The two pairs are emitted in different directions, l_1, l_2 and r_1, r_2 denoting the four spatial modes.

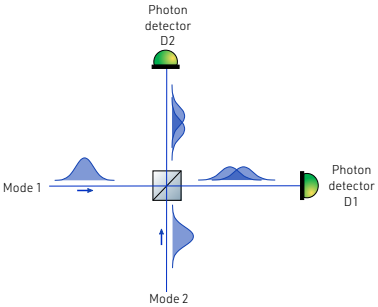


Figure 5.2: Temporal delay between two spatial modes incident on the input ports of a 50:50 beam splitter. The temporal delay leads to temporal indistinguishability, which in an interferometric experiment has a debilitating effect on the observed interference.

For the states described above, the aforesaid rates should be equalized. It is known for a SPDC source, particularly non-collinear non-degenerate SPDC, the resultant (single and joint) spectral profiles, hence the two-photon emission rates and output spatial modes, are dependent on the focus of the pump beam [151]. Hence, the experiments in Refs.[72, 150] equalize the emission rates of the two SPDC processes (backwards and forwards) using an appropriate arrangement of focusing optics (*i.e.* lens). These added complications compel us to consider an experimental scheme for enlarging our two-photon state from the previous chapter that explicitly avoids them. We consider adopt the experimental scheme of Park et al. [116], which uses a single-photon pair source to realize a polarization-path-entangled state. Hence we describe the experimental design next.

5.2 Experimental design

In this experiment, we extend the experimental setup from the previous chapter to accommodate an additional path qubit. The experimental setup is shown in Figure 5.3; conceptually, this experiment is again simple to describe. The experimental design is similar to the design in the previous chapter (see Figure 4.1) with only one minor addition; in one of the arms, arm 1 in the figure, the photon beam is incident on a PBS, transmitting horizontally-polarized photons and reflecting vertically-polarized photons, which effectively defines our path modes (l_1 and r_1). Our SPDC source produces a state close to $(|H_1, H_2\rangle - |V_1, V_2\rangle)/\sqrt{2}$, at the dashed line after the action of the PBS as shown in Figure 5.3 this state becomes:

$$|\Psi_1\rangle = \frac{|H_1, r_1, H_2\rangle - |V_1, l_1, V_2\rangle}{\sqrt{2}}. \tag{5.8}$$

We designate the polarization and path states of the photon in arm 1 as qubit 1 and qubit 2, respectively and the polarization of the photon in arm 2 as qubit 3. Furthermore, relabelling $|H\rangle$ ($|V\rangle$) as $|0\rangle$ ($|1\rangle$), and similarly $|r\rangle$ ($|l\rangle$). The state in Equation (5.8) becomes

$$\left|\Psi_1'\right\rangle = \frac{|0,0,0\rangle - |1,1,1\rangle}{\sqrt{2}} = \frac{|0\rangle^{\otimes 3} - |1\rangle^{\otimes 3}}{\sqrt{2}}. \tag{5.9}$$

The state in Equation (5.9) is locally equivalent to GHZ state [3]. Similarly, if we apply the unitary operator $U = \mathbb{1}Z_2\mathbb{1}_3$ to state in Equation (5.9) and proceed to rotate the coordinate system for all our polarization measurements by $\theta = -22.5°$ ($|H\rangle \mapsto (|H\rangle + |V\rangle)/2, |V\rangle \mapsto (|H\rangle - |V\rangle)/\sqrt{2}$), $|\Psi_1\rangle$ becomes:

$$|\Psi_1\rangle = \frac{|+,0,+\rangle - |-,1,-\rangle}{\sqrt{2}}, \tag{5.10}$$

where $(|\pm\rangle = |0\rangle \pm |1\rangle)/\sqrt{2}$. The above state is a three-qubit linear graph state, which may be generated by applying controlled-Z operations on neighboring qubits ($1-2$ and $2-3$) of the initial resource state $|+\rangle_1 |+\rangle_2 |+\rangle_3$.

[3] Applying the unitary operator $(\mathbb{1}_1 Z_2 \mathbb{1}_3)$ to $|\Psi\rangle$, we recover the GHZ state in its standard form $(|0\rangle^{\otimes 3} + |1\rangle^{\otimes 3})/\sqrt{2}$.

The rest of the optics in arm 1 of the experimental setup are designated for measurement and analysis, consisting of a MZI, which combines the two path modes on the output ports of a 50:50 beam splitter.

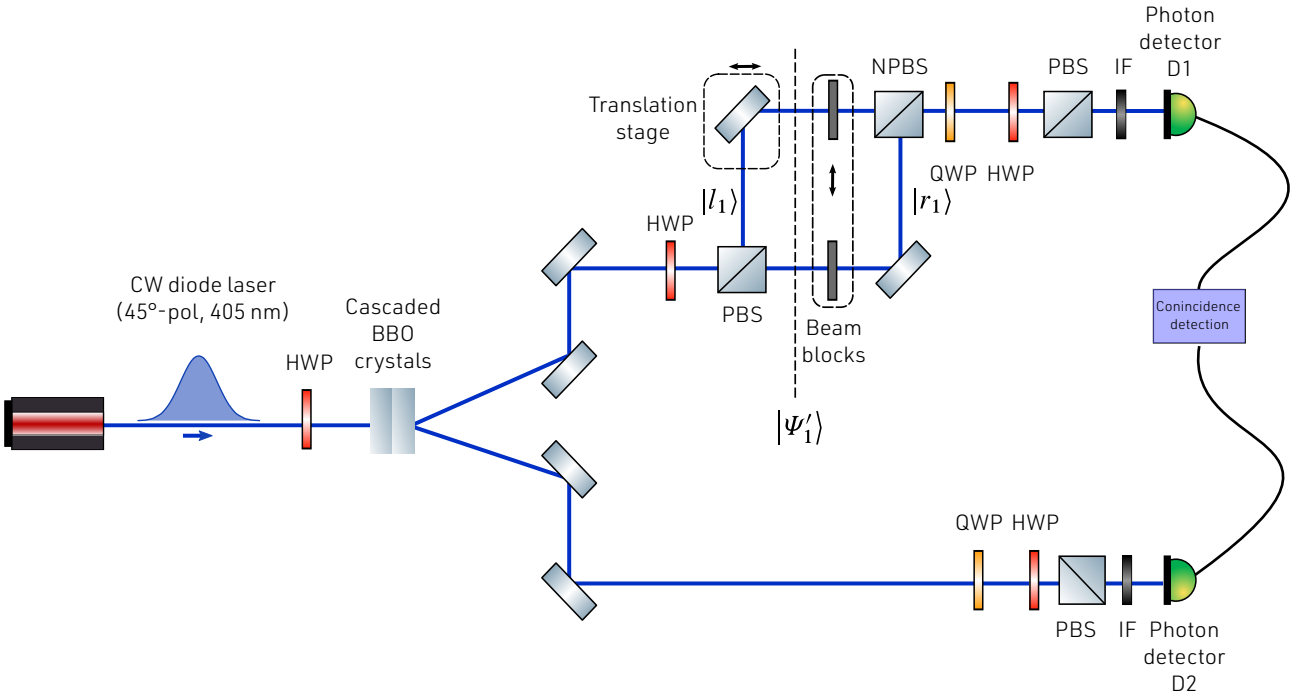


Figure 5.3: Experimental setup for generation and measurement of a two-photon three-qubit path-polarization-entangled state locally equivalent to a GHZ state. HWP, QWP, BBO, PBS, NPBS, translatable mirror, translatable beam blocks, and IF. A photon pair is created whenever a laser pump photon with 405 nm wavelength is incident on the paired BBO crystals cut for type-I SPDC, generating photons at 810 nm. One of the photons enters a MZI where path modes are made to interfer when combined on , at the dashed line the joint state $|\Psi_1'\rangle$ is locally equivalent to a GHZ state. Each photon is guided by a set of mirrors to a QWP, HWP, and PBS which are used to perform polarization measurements of the quantum state. Finally, each photon is sent to an IF at 800 nm with a bandwidth of 40 nm and collected by a SMF and sent to a photon detector. Each photon detector produces an electronic signal and sends it to the coincidence counting electronics, which count the signals that arrive simultaneously.

One of the path modes is reflected off a mirror on an motorized translation stage (MTS25/M-Z8 - 25 mm (0.98") Motorized Translation Stage with a KDC101 K-Cube Motor Controller), which can used to change the relative phase difference between the two path modes, projecting the path qubit to states on the$x$-y plane of the Bloch sphere (on the equator) with the form:

$$|\varphi\rangle = \frac{|0\rangle + e^{i\varphi}|1\rangle}{\sqrt{2}}. \tag{5.11}$$

In both paths, there are beam blocks mounted on an electronically-controlled translation stage, which can either block one of the paths or let them both pass. Whenever we block one of the paths, we project out one of the states ($|0\rangle$, $|1\rangle$) depending on which path is blocked. The combined beam on one of the output ports of the beam splitter is sent to polarization analysis optics and eventually to the photo detector, consisting of a rotatable QWP and HWP, a PBS and an IF at 800 nm with a 40 nm bandwidth. After this stage, the beam goes to a photon detector *via* a fibre launch coupled to the detector with a SMF. The optical path of arm 1 is slightly longer than that of arm 2, for this reason we modify our coincidence counting electronics to add a variable delay to arm 2 to roughly compensate for the delay on arm 1 introduced by the MZI. Through a bit of tinkering, we find that a delay between 0.5 ns to 1.5 ns works well enough; our delay electronics operate in increments of 0.5 ns, the true delay is probably somewhere in between this range.

To match the optical path difference of the two paths to be on the order of the coherence length of the down-conversion photons ($\simeq$ 60 µm) we used a broad spectrum white laser source. The beam from this laser source is guided into the experiment through fibre coupler we previously used to hold the SMF taking the beams to the detectors. It is then sent through the MZI and collected by another fibre coupler near the crystals coupled with a SMF into a spectrometer (Thorlabs CCS200/M with a wavelength range of 200 nm-1000 nm).

We can thus resolve the interference fringes in spectra near our collection bandwidth (800 nm±40 nm) by translating the mirror inside the MZI to obtain optimal matching of the path lengths of two arms of the MZI. Once the MZI is optimized for the coherence length of the down-converted photons, when the two path modes from one of the down-conversion photons combine on the output ports of the 50:50 beam splitter, the state $|\Psi_1\rangle$ of Equation (5.8) then becomes:

$$|\Psi_2\rangle = \frac{1}{2}(e^{\varphi_1}(|H_1, p_1, H_2\rangle + |H_1, q_1, H_2\rangle) \\ -e^{\varphi_2}(|V_1, p_1, V_2\rangle - |V_1, q_1, V_2\rangle)), \tag{5.12}$$

where p_1, q_2 are the path modes of the output ports of the beam splitter and φ_1, φ_2 are the phases acquired by path modes (l_1 and r_1) by the time they are incident on the beam splitter. Here we adopt the convention $|r_1\rangle \mapsto (|p_1\rangle - |q_1\rangle)/\sqrt{2}$ and $|l_1\rangle \mapsto (|p_1\rangle + |q_1\rangle)/\sqrt{2}$ for the 50:50 beam splitter. After a bit of algebraic deadlifting, the preceding equation becomes:

$$|\Psi_2\rangle = \frac{1}{2}(|p_1\rangle (|H_1, H_2\rangle - e^{i(\varphi_2-\varphi_1)} |V_1, V_2\rangle))+ \\ |q_1\rangle (|H_1, H_2\rangle + e^{i(\varphi_2-\varphi_1)} |V_1, V_2\rangle))). \tag{5.13}$$

The mode q_1 goes through the polarization analysis optics and eventually to the photon detector yielding:

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}}(|H_1, H_2\rangle + e^{i\varphi} |V_1, V_2\rangle), \tag{5.14}$$

where $\varphi = \varphi_2 - \varphi_1$. Note that the phase difference between the two path modes influences the state measured by the polarization analysis optics. We can thus infer this phase difference with a similar procedure from our observations in Equation (4.3) and Equation (4.4) to optimize the SPDC source for a particular Bell state. By inserting a HWP in the path mode r_1, and setting it at $\theta = 45°$ ($|H\rangle \leftrightarrow |V\rangle$), Equation (5.14) becomes:

$$\begin{aligned} |\Psi_2'\rangle &= \frac{1}{\sqrt{2}}(|H_1, H_2\rangle + e^{i\varphi} |H_1, V_2\rangle), \\ &= \frac{1}{\sqrt{2}} |H_1\rangle (|H_2\rangle + e^{i\varphi} |V_2\rangle). \end{aligned} \tag{5.15}$$

We infer the value φ by choosing the appropriate projectors, for instance projecting $P_{HR} = |H_1\rangle\langle H_1| \otimes |L_2\rangle\langle L_2|$ on the above state and a bit algebraic deadlifting one obtains the expression for detection probability:

$$\langle\Psi_2'| P_{HR} |\Psi_2'\rangle = \frac{1}{2} - \frac{1}{2}\sin\varphi. \tag{5.16}$$

Thus moving the translation stage mounted with the mirror, we can minimize the observed coincidence counts which would then correspond to $\varphi = \pi/2$, and maximized coincidence counts correspond to the setting $\varphi = -\pi/2$. The aforementioned values of φ project the path qubit in Equation (5.11) to $(|0\rangle + i\,|1\rangle)/\sqrt{2}$ and $(|0\rangle - i\,|1\rangle)/\sqrt{2}$, which are the positive and negative eigenvectors of the Pauli matrix Y. Any value of φ maybe inferred similarly.

Therefore, any equatorial basis measurement of the form:

$$\mathcal{B}(\varphi) = \left\{ \frac{|0\rangle + e^{i\varphi}|1\rangle}{\sqrt{2}}, \frac{|0\rangle - e^{i\varphi}|1\rangle}{\sqrt{2}} \right\}, \tag{5.17}$$

can be performed on the path qubit. Together with the Z basis measurements ($\{|0\rangle, |1\rangle\}$), it is possible to perform measurements, measuring each of the eigenvectors of Pauli matrices; which allows us to independently address each of the three qubits for control and measurements of quantum-mechanical correlations of the generated state.

5.3 Results

To get an inkling of how well the MZI can contrast between constructive and destructive interference of the two path modes, we measure the fringe visibility for down-conversion photons in following configurations: (i) When only one of the BBO crystals, producing the H-polarized light cone is stimulated. (ii) When only one of the BBO crystals, producing the V-polarized light cone. (iii) When both BBO crystals are stimulated. For all three configurations, there is a HWP at the gate of the interferometer (before the PBS) set to 22.5° ($|H\rangle \leftrightarrow |D\rangle$), and the half wave-plate in the path mode r_1 is set to $\theta = 45°$, giving the state in Equation (5.15) and project out $P_{HD} = |H_1\rangle\langle H_1| \otimes |D_2\rangle\langle D_2|$, giving the expression for the detection probability

$$\left\langle \Psi_2' \right| P_{HD} \left| \Psi_2' \right\rangle = \frac{1}{2} + \frac{1}{2}\cos\varphi, \tag{5.18}$$

by translating the mirror in the MZI in increments of 40 nm, we can vary φ. Typical (normalized) coincidence counts when φ is varied for the three aforesaid settings are shown in (a), (b) and (c) of Figure 5.4, respectively[4]. It was worth mentioning that the motor translating the stage can resolve translations down to ∼30 nm, however this may come at the price of accuracy. In a sporadic fashion, the motor sometimes translates the mirror slightly less or slightly more than the set step size, hence the plots in the figure above show a few slightly sparse regions. We observe close-to-unity fringe visibilities (calculated from the minima and maxima of the fit) of 0.940, 0.901 and 0.921, respectively. The non-ideal spatial overlap between the two path modes and less-than-unity fidelity of the Bell state prior to the MZI may explain the less-than-unity fringe visibility. However, we deem these values sufficient and as indicative that the two path modes are indeed interfering with one another and their optical path difference is within the coherence length of the down-conversion photons.

[4] The fitting function used for the plots is of the form $a\cos(bx + c) + d$. The parameters a, b, c, d were found using Mathematica's `NonlinearModelFit` function.

As we have seen elsewhere, to fully characterize an experimentally generated state, one often needs to perform full QST; reconstructing an estimate of the density matrix from which physical quantities of interest may be derived. QST for a general three-qubit state would require at least 64 coincidence measurements. However, if we are only interested in the fidelity of the experimentally generated state and detecting whether the said state possesses genuine multi-particle entanglement around the ideal state we expect to observe, it is possible to circumscribe performing a full tomographic analysis to derive the said quantities, at the cost of generality.

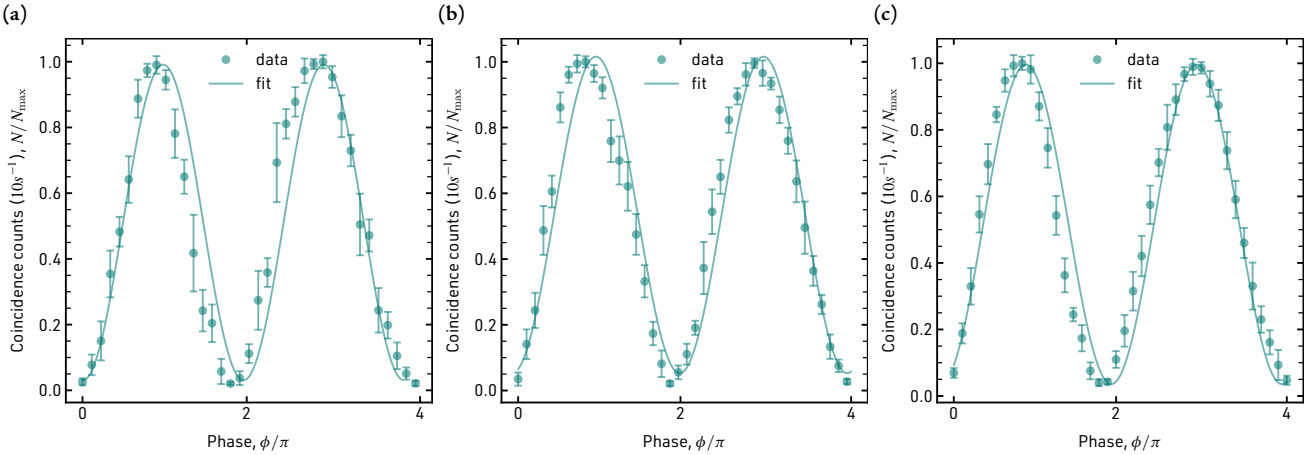


Figure 5.4: Photon coincidence counts traversing the MZI as a function of the relative phase between the two paths in the interferometer: **(a)** coincidence counts vs. ϕ for pairs of only vertically polarized photons **(b)** Coincidence counts vs ϕ for pairs of only horizontally polarized photons **(c)** Coincidences counts vs ϕ for pairs of entangled photons (Bell state). The error bars represent 95% confidence intervals around the mean value (see section § A.2 of technical Appendix A.

Without directly deriving the density matrix of the experimentally generated state, we can derive an estimate of the fidelity of the generated state from a reduced set of Pauli operator expectation value measurements, in comparison to full QST. Recall that the fidelity between a expected ϱ and measure state ς is given by [17]:

$$F(\varrho,\varsigma) = \mathrm{Tr}\left(\sqrt{\sqrt{\varrho}\varsigma\sqrt{\varrho}}^{2}\right) = \mathrm{Tr}(\varrho\varsigma). \tag{5.19}$$

The desired state ρ may be decomposed into a linear combination of N-fold products of $\mathbb{1}, X, Y, Z$. In the case of a three-qubit GHZ state in its standard form, this decomposition is given by:

$$\begin{aligned}\varrho = \frac{1}{8}(&\mathbb{1}_1\mathbb{1}_2\mathbb{1}_3 + \mathbb{1}_1 Z_2 Z_3 + X_1 X_2 X_3 - X_1 Y_2 Y_3 \\ &- Y_1 X_2 Y_3 - Y_1 Y_2 X_3 + Z_1\mathbb{1}_2 Z_3 + Z_1 Z_2 \mathbb{1}_3).\end{aligned} \tag{5.20}$$

Estimating of the fidelity of our measured state ς amounts to the evaluation of the expectation values[5] of above operators with respect to the measured state, and summing them up appropriately. We reduce the number of unique measurements by noting that the expectation value of the terms $\mathbb{1}_1 Z_2 Z_3$, $Z_1\mathbb{1}_2 Z_3$ and $Z_1 Z_2\mathbb{1}_3$ may be derived from the measurement of $Z_1 Z_2 Z_3$ as their distributions are marginal distributions of $Z_1 Z_2 Z_3$ when the outcome of the qubit acted on by the identity is not taken into consideration. Similarly, the expectation value of $\mathbb{1}_1\mathbb{1}_2\mathbb{1}_3$ may derived from any of terms *via* marginalization, it is equal to unity in any case[6]. Thus, we need only evaluate 5 unique measurements: $X_1X_2X_3$, $X_1Y_2Y_3$, $Y_1X_2Y_3$, $Y_1Y_2X_3$, $Z_1Z_2Z_3$. Panels (a), (b), (c), (d) and (e) in Figure 5.5 show the measurement outcomes (8 each) required for the evaluation of the expectation values of the Pauli operators $X_1X_2X_3$, $X_1Y_2Y_3$, $Y_1X_2Y_3$, $Y_1Y_2X_3$ and $Z_1Z_2Z_3$, respectively. The error bars represent 95% confidence intervals around the mean value (see section § A.2 of the technical Appendix A). Table 5.1 shows the measured expectation values from the measurements in Figure 5.5 of each operator. Evaluating the fidelity using Equation (5.19), and the Pauli decomposition of our expected state in Equation (5.9), we obtain a fidelity of $F_\varrho = 0.868 \pm 0.00996$.

[5] For any self-adjoint operator O, the expectation value of O with respect to the general state ς is given by, $\langle O\rangle \equiv \mathrm{Tr}(O\varsigma)$

[6] $\mathrm{Tr}(\mathbb{1}_1\mathbb{1}_2\mathbb{1}_3\varsigma) = \mathrm{Tr}(\varsigma) = 1$ (normalization condition)

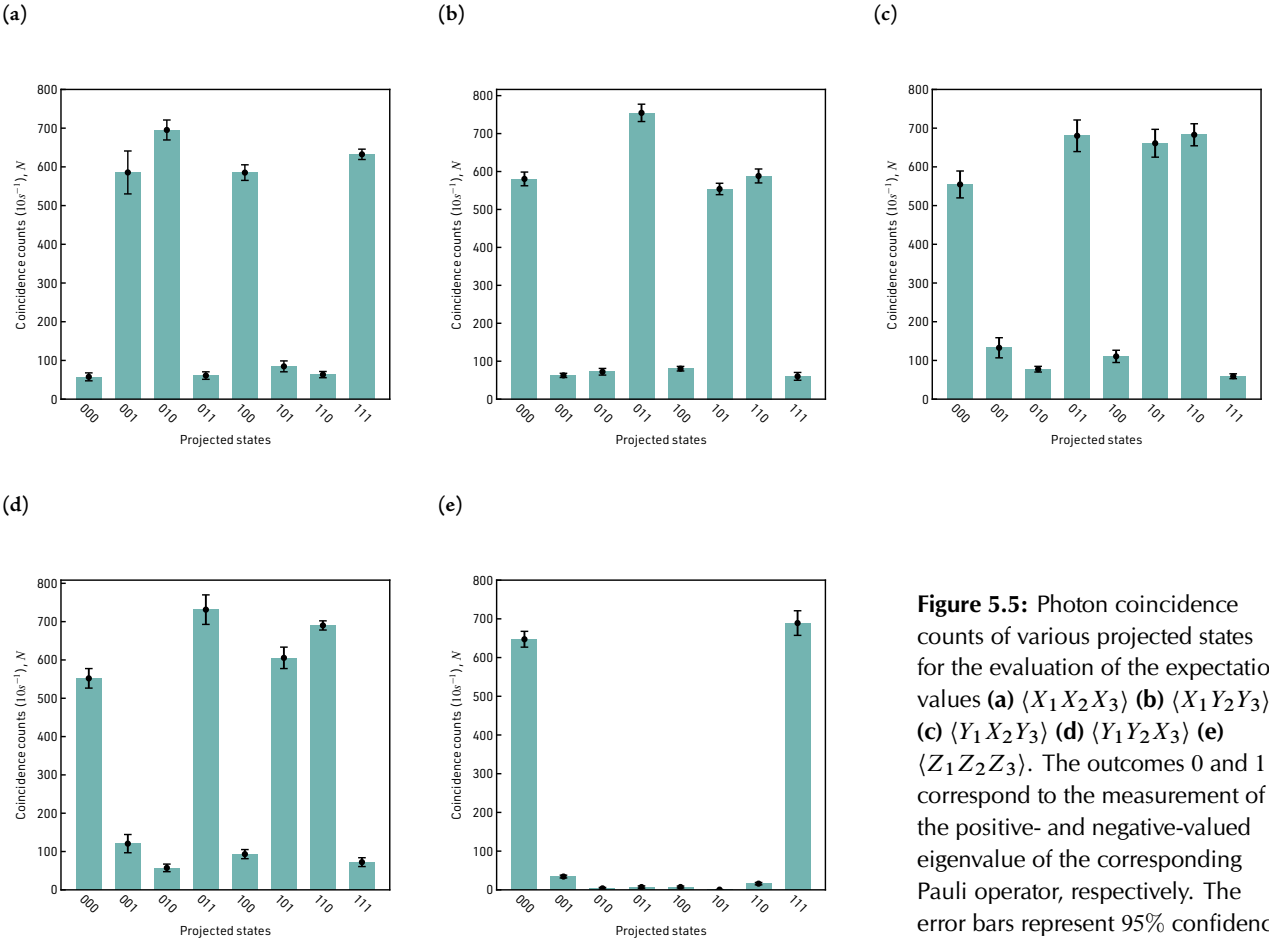


Figure 5.5: Photon coincidence counts of various projected states for the evaluation of the expectation values **(a)** $\langle X_1X_2X_3\rangle$ **(b)** $\langle X_1Y_2Y_3\rangle$ **(c)** $\langle Y_1X_2Y_3\rangle$ **(d)** $\langle Y_1Y_2X_3\rangle$ **(e)** $\langle Z_1Z_2Z_3\rangle$. The outcomes 0 and 1 correspond to the measurement of the positive- and negative-valued eigenvalue of the corresponding Pauli operator, respectively. The error bars represent 95% confidence intervals around the mean value (see section § A.2 of technical Appendix A).

Operator	Expectation value
$Z_1Z_2Z_3$	$-0.0453(0.0329)$
$\mathbb{1}_1Z_2Z_3$	$0.922(0.0329)$
$Z_1\mathbb{1}_2Z_3$	$0.908(0.0329)$
$Z_1Z_2\mathbb{1}_3$	$0.973(0.0329)$
$X_1X_2X_3$	$-0.807(0.0275)$
$X_1Y_2Y_3$	$0.800(0.0163)$
$Y_1Y_2X_3$	$0.765(0.0237)$
$Y_1X_2Y_3$	$0.743(0.0286)$
$\mathbb{1}_1\mathbb{1}_2\mathbb{1}_3$	$1.00(0.0264)$

Table 5.1: Three-qubit operator expectation values for the evaluation of the fidelity and witness of the measured state. The values in parenthesis represent 95% confidence intervals around the mean value and derived from the values in Table 5.1 with appropriate error propagation.

The Bell-Mermin operator (See section § 1.2.5) takes the form:

$$\mathcal{M} = X_1X_2X_3 - X_1Y_2Y_3 - Y_1X_2Y_3 - Y_1Y_2X_3. \tag{5.21}$$

We can evaluate the expectation value of Bell-Mermin from the same expectation values in Table 5.1. Our generated state gives a expectation value of $\langle\mathcal{M}\rangle = 3.137 \pm 0.0490$, clearly violating the bound of $\langle\mathcal{M}\rangle = 2$ under the assumption of local realism [7].

[7] For the case of a state locally equivalent to a GHZ state as in Equation (5.9), the Bell-Mermin for this state is $\mathcal{M} = -X_1X_2X_3 + X_1Y_2Y_3 + Y_1X_2Y_3 + Y_1Y_2X_3$.

Lastly, we may further detect the genuine multi-particle entanglement around the expected state (GHZ) by means of a stabilizer-based entanglement witness operator $\mathcal{W}$. An stabilizer-based entanglement witness operator for a three-qubit GHZ state in its standard form is given by: [35]:

$$\mathcal{W} = \frac{3}{2}\mathbb{1}_1\mathbb{1}_2\mathbb{1}_3 - X_1X_2X_3 - \frac{1}{2}\left(Z_1Z_2\mathbb{1}_3 + \mathbb{1}_1Z_2Z_3 + Z_1\mathbb{1}_2Z_3\right). \quad (5.22)$$

The above entanglement witness operator has an expectation value of -1 with respect to an ideal three-qubit GHZ state, since the GHZ state has an expectation value of $+1$ with respect to the individual stabilizing operator terms[8]. An entanglement witness operator detecting genuine multi-partite entanglement around the ideal state $|\psi\rangle$ has a noise threshold p_{limit}, that is, it will detect a mixed state of the form $\varrho(p_{\text{noise}}) = \mathbb{1}/2^N + (1 - p_{\text{noise}})\,|\psi\rangle\langle\psi|$ as genuinely entangled if p_{noise} is below the positive-valued threshold $0 < p_{\text{limit}} < 1$ [35]; for the above witness $p_{\text{limit}} = 2/5$.

[8] The vigilant reader may notice that Bell-Mermin operator of Equation (5.21) resembles a entanglement witness. In fact, it is a disguised entanglement witness for genuine three-qubit entanglement. See Toth et al. [35].

We evaluate the witness for our experimentally generated state [9] using the expectation values of the stabilizing operators in Table 5.1, we obtain a value of $\mathrm{Tr}(\mathcal{W}\varrho) = -0.709 \pm 0.0560$, confirming that the generated state exhibits genuine three-qubit entanglement. Furthermore, the expectation value of the above entanglement witness gives a lower bound for the fidelity of the measured state ς with respect to the expected state ϱ [35]:

[9] For the three-qubit state in Equation (5.9) is a locally equivalent to the three-qubit standard GHZ state, its entanglement witness operator is given by $\mathcal{W} = 3/2\mathbb{1}_1\mathbb{1}_2\mathbb{1}_3 + X_1X_2X_3 - \frac{1}{2}\left(Z_1Z_2\mathbb{1}_3 + \mathbb{1}_1Z_2Z_3 + Z_1\mathbb{1}_2Z_3\right)$.

$$F(\varrho, \varsigma) = \mathrm{Tr}(\varrho\varsigma) \geq \frac{1}{2}\left(1 - \langle\mathcal{W}\rangle\right). \quad (5.23)$$

As a check for self-consistency, we evaluate the above expression for our experimentally generated state ς and obtain a lower bound of $F(\varrho, \varsigma) \geq 0.854 \pm 0.0280$, which indeed corroborates our measured fidelity from earlier.

In comparison to similar experiments, particularly that in reference [84] where the generation of a three-qubit three-photon GHZ state played a crucial role in an experimental demonstration of Shor's algorithm for the factorization of 15, they achieve a lower fidelity of $F_\varrho = 0.74 \pm 0.02$. Although their full joint state is product state of a GHZ state and $|0\rangle$ (ideally), nonetheless our fidelity results are suggestive of an improvement. Similar reasoning from the previous section may explain the less-than-unity fidelity of our generated state, since this experiment builds upon on it; an improvement of the former will likely improve the latter. Nonetheless, the deviation between the two fidelities is not too great, and the latter result demonstrates that the experimental scheme of Park et al. [116] works well enough in practice, while crucially avoiding the added complications of using two or more SPDC processes to generate moderate hyper(hypo)entangled photonic states.

As noted earlier, a three-qubit GHZ state is locally equivalent to a three-qubit graph state of the form:

$$|\mathcal{G}_3\rangle = \frac{|+,0,+\rangle + |-,1,-\rangle}{\sqrt{2}}, \quad (5.24)$$

which in the circuit model may be generated by an application of controlled-Z (two-qubit gate) operations on neighboring qubits (1-2 and 2-3) of the initial resource state $|+\rangle_1|+\rangle_2|+\rangle_3$.

Interestingly enough, through only the application of local operators (single-qubit gates) we can generate another graph state, that can be otherwise generated from an application of controlled-Z (two-qubit gate) operations on all neighboring qubits (1-2 and 2-3, and 1-3) of the initial resource state $|+\rangle_1 |+\rangle_2 |+\rangle_3$:

$$\begin{aligned} |\mathcal{C}_3'\rangle &= \frac{|0,0,+\rangle + |1,0,-\rangle + |0,1,-\rangle - |1,1,+\rangle}{2}, \\ &= \frac{|\Phi^-,+\rangle + |\Psi^+,-\rangle}{\sqrt{2}}, \end{aligned} \tag{5.25}$$

where $|\Phi^-\rangle$ and $|\Psi^+\rangle$ are two of the Bell states. Thus our experimentally realized state, generated with two non-local gates in the circuit model, is locally equivalent to a graph state, generated with three non-local gates! (See Figure 5.6 for illustration)! A projection of the third qubit (polarization) in either $|+\rangle$ or $|-\rangle$ leaves the qubit 1 (polarization) and qubit 2 (path) in the state $|\Phi^-\rangle$ or $|\Psi^+\rangle$, respectively. graph states with this peculiar property are said to belong to same LU-equivalence class [77, 78].

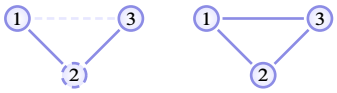


Figure 5.6: LU equivalent graph states through a single application of the ELC rule. A graph state generated with two non-local controlled-Z operations between 1-2 and 2-3 is locally equivalent to a graph state generated with three non-local controlled-Z operations between 1-2, 2-3 and 1-3. The action of an LU operation $U_a(G)$ on the level of the graph, for the chosen vertex a (indicated with a dashed outline) an edge is created between its neighbors (opaque indigo line).

The local unitaries, which may absorbed into our measurement basis, relating the graph state in Equation (5.24) and Equation (5.25) are given by:

$$U = \sqrt{(iZ_1)}\sqrt{(-iX_2)}\sqrt{(iZ_3)}. \tag{5.26}$$

The experimental components that are used in performing the measurements (translation stages and wave plates), had their operations made fully automatic. Thorlabs provides a host-controller communications protocol, which provides a more fine-grained control over their motorized components. Through the programmatic use of this protocol, the operation of each of the aforesaid motorized components was modularized and made accessible through an application programming interface (API), remotely served by a Raspberry Pi 4. Additionally, we designed a simple mobile graphical user interface (GUI) for this API that gives users [10] the ability to remotely perform the same data acquisition experiments in this chapter[11]. A more-detailed explanation of how this was achieved is of very little scientific interest, and thus can be found in the technical Appendix D. Figure 5.7 shows a schematic flow diagram of the various components as described above, and Figure 5.8 shows various demonstrations of the mobile GUI. See Appendix D for details.

[10] At the moment, only the author has access. I will be taking applications for early stage access soon :).

[11] Measurements for witness, fidelity, Bell-Mermin inequality violation, etc

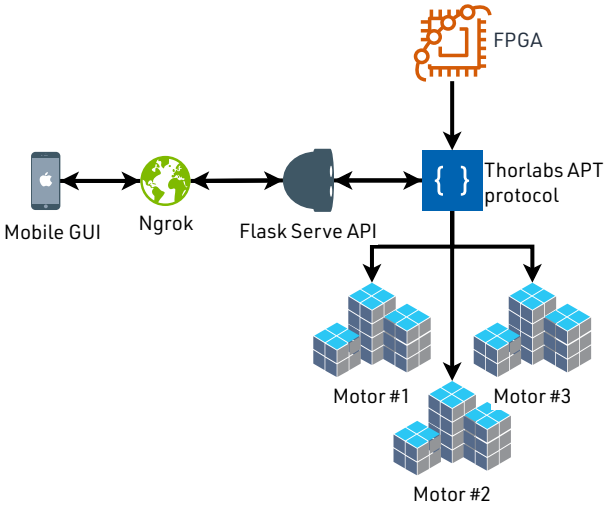


Figure 5.7: Schematic flow diagram showing the various components. Through the GUI one can queue up an experiment through an ngrok endpoint, which serves our locally hosted API on a Raspberry Pi served by a Flask server. Depending on the invoked endpoint, the API using invokes APT protocol to trigger the various motors. In the instance, we invoked endpoint is a move; after this execution, an FPGA collects the coincidence counts from the single photon detectors and sends them back to the mobile GUI.

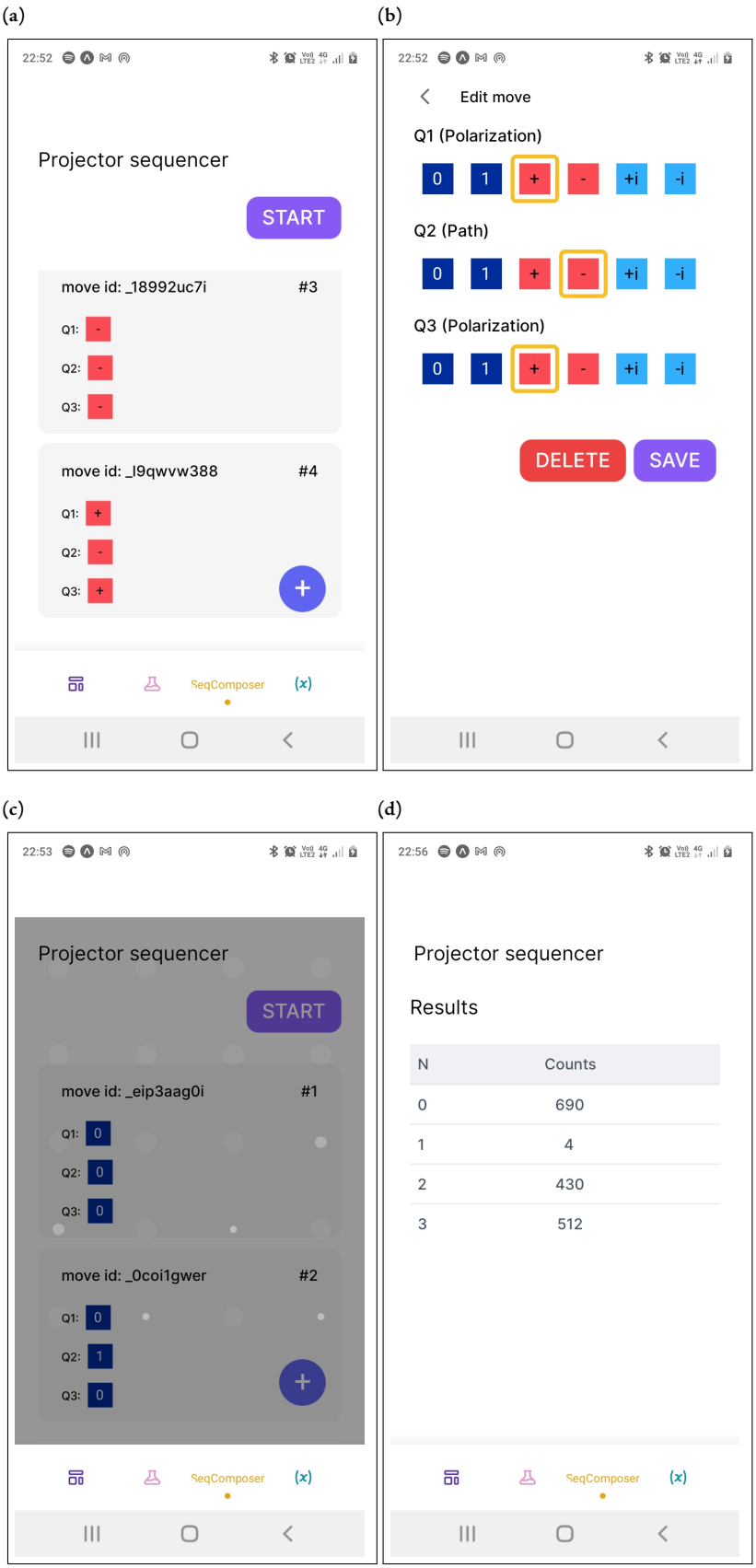


Figure 5.8: Various demo screens for the mobile GUI. See Appendix D for details

5.4 Concluding remarks

In this chapter, we described an experimental scheme due to Park et al. [116] for generating a two-photon three-qubit polarization-path-entangled GHZ state from a Bell-state photon pair source. We experimentally realized this scheme, generating a moderate fidelity state, higher than a previous similar experiment, that is locally equivalent to a three-qubit GHZ state and two graph states. Each of the qubits is addressable by measurement, with the path qubit limited to equatorial basis measurements. We also showed that the generated state possess non-local correlations by showing that it leads to a clear violation of the Bell-Mermin inequality. Furthermore, we verify that the non-local correlations the state possesses are indeed due to genuine three-qubit entanglement, by evaluating an entanglement witness for the generated state. Finally, we proceed to make this entanglement source remotely accessible and designed a simple GUI that allows users the ability to perform data acquisition experiments. A possible avenue of departure from here, would be to extend the three-qubit state to a four-qubit state by similarly encoding a path qubit on the other down-conversion photon, which would realize a four-qubit linear graph state, providing an even more versatile 4-qubit processor on which one can carry out quantum algorithms [72] and other types of quantum protocols, such as quantum games [124].

PART III

EPILOGUE

6

Conclusion

The aim of the project was to investigate the issues that face and study in detail the realisation of quantum algorithms using online cloud-based quantum NISQ processors. The study was not meant to be a comprehensive study of quantum algorithms, and was confined to two kinds of quantum algorithms; quantum search and quantum factoring algorithms. Hence, the first part of the thesis was wholly concerned with realizations of these algorithms on IBM's quantum experience platform, and the difficulties thereof. Most of the discussions concerning the difficulties of realizing quantum algorithms on NISQ processors are phrased in terms of coherence time, or number of two-qubit gates. This is a recurring theme which is emphasized and highlighted with fervent frequency in the first part of the thesis.

We introduced the topic of the thesis in Chapter 0 and began Chapter 1 by providing the necessary background to fundamental notions of quantum mechanics, such as state space, evolution, measurement and entanglement. The main body of the thesis began Chapter 2 by introducing the quantum search algorithm for the problem of finding a needle in a haystack. We explored several contributions in this regard that emphasized the imperative of designing algorithms in such a way to circumvent the limitations of NISQ processors (short coherence, low qubit connectivity etc) using sundry methods, and presented a marginal contribution of our own that improves over an implementation of a MAX-CUT problem using Grover's algorithm [54] with the aforesaid methods. However, the improvement is not clear cut, as it is hard to discern whether it is entirely attributable to the improvement of the capabilities of the IBM Q quantum processors. We also attempted to realize a measurement-based Grover's algorithm for three qubits and found that such a realization is somewhat out of reach for IBM Q processors. Our attempts to reduce the number of resources required to realize such a measurement-based algorithm, were futile as there is no LU-equivalent graph state with fewer than the initial resource graph state for realizing the measurement-based Toffoli gate.

Chapter 3 introduced Shor's algorithm for prime factorization [5] and presented the main contribution of the thesis; which is a proof-of-concept demonstration of the complete prime factorization of $N = 21$, which builds upon a recent demonstration in this regard in Ref. [88], and goes beyond this demonstration in fully factorizing $N = 21$, aided by a great reduction in resources (number of two-qubit gates) compared to the original demonstration [80].

This feat was achieved by a replacement of the Toffoli gates (which decompose into six controlled-NOT each) in the demonstration in Ref. [88] with relative phase Toffoli gates (which decompose into three controlled-NOT each), such a replacement cuts the number of two-qubit gates in half in comparison to the demonstration in Ref. [88]. An interesting point of departure and line of research is whether such a use case of a relative phase Toffoli gates is applicable to instances of Shor's quantum algorithm for a larger number of qubits.

To reiterate, the first part of the thesis comprises nothing more than a mere dint on the surface of a volumeous subject, that is the ongoing effort to use NISQ processors as testbeds for the investigation of many of their practical issues, and the realization of near-term algorithms that are of practical use. The practical issues of NISQ as we have seen throughout the first part of the thesis places an emphasis in designing near-term algorithms in a way that is suitable for NISQ processors (algorithms that use circuits that require low connectivity among qubits, short circuit depth and fewer two-qubit gates). As suggested by Preskill [13] one route towards progress in the near-term is *via* bottom-up experimentation. Most of the material presented in the first part of the thesis represents such bottom-up experimentation; multi-qubit gates with low connectivity in Ref. [57] and divide-and-conquer methods such as the divided QPE routine in Ref. [90] and the depth multi-stage quantum search algorithm in Ref. [55], less than ideal subdivided oracle for an application of Grover's algorithm in Ref. [54] and the replacement of Toffoli gates in a circuit with relative phase Toffoli gates while preserving its functional correctness in Ref. [80]. As NISQ processors grow in hardware (increased coherent times, qubit connectivity, real-time classical conditionals) and software capabilities (error mitigation, transpiling, etc), many existing algorithms with provable advantages may become viable, however, until then experimentation may lend a helping hand.

In the second part, we steered towards experimental physics, and in Chapter 4 we realized and characterized a photonic source of entanglement which takes the form of a polarization-entangled Bell state. In Chapter 5 we expanded of the aforesaid two-qubit polarization-entangled Bell state to a three-qubit path-polarization-entangled GHZ state, with the additional qubit encoded on the momentum DOF of one of the down-converted photons. We designed and built a small mobile graphical user interface, providing an interactive and visual way to remotely control our experimental set up which is the main contribution of the second part of the thesis. Novelty aside, the author believes that such a remotely controlled experimental set up with its ease of access and use can potentially be of some pedagogical worth to future students, particularly undergraduates as such a small-scale experimental setup that contains the some of the core aspects of quantum mechanics are a rarity in the author's department[1]. A possible point of departure from here would be the expansion of the three-qubit state to a four-qubit state [116], providing an even more versatile resource state to remotely control, and on which to carry out quantum algorithms and quantum games. The author would also like to refine the experimental setup and mobile GUI (or a web interface), with the aim of eventually making it publicly accessible to everyone else besides the author and his supervisor.

[1] For the author, the experiments performed in this thesis were the first of their kind (quantum mechanical) they had ever done.

"Je n'ai fait celle-ci plus longue que parce que je n'ai pas eu le loisir de la faire plus courte."

— Blaise Pascal, Lettres Provinciales

PART IV

TECHNICAL APPENDIX

A

Appendix A

A.1 IBM Quantum Experience

The experiments in this thesis were conducted on the IBM Quantum Experience **ibmq_montreal**, **ibmq_mumbai**, **ibm_hanoi**, **ibmq_toronto** and **ibmq_casablanca** processors through the software development kit Qiskit [152]. Each experiment reported was conducted on the date shown in the table below.

Experiment	Date
Compiled quantum order-finding on **ibmq_casablanca**	2020/12/03
State tomography on **ibmq_casablanca**	2020/12/04
Verification of entanglement on **ibmq_casablanca**	2020/12/04
Compiled quantum order-finding on **ibmq_toronto**	2020/12/06
Verification of entanglement on **ibmq_toronto**	2020/12/07
State tomography on **ibmq_toronto**	2020/12/16
Original and improved MAX-CUT problem with on **ibm_hanoi**	2021/08/31
Original and improved MAX-CUT problem with on **ibm_montreal**	2021/11/07
Truth tables for measurement-based controlled-controlled-Z gate on **ibm_montreal**	2021/11/07
Truth tables for measurement-based controlled-controlled-Z gate on **ibm_mumbai**	2021/11/20

Table A.1: Dates of experiments on IBM Q processors.

For instance, when characterizing the compiled quantum order-finding, experiments were submitted in batches of 900 circuits with each circuit having 8192 measurement shots, hence in total, 900×8192 measurement shots. In choosing the qubit device mappings shown in the main text, preference was given to the qubit pairs with relatively small controlled-NOT error rates. Table A.2 and Table A.3 show reported single qubit-error rates for **ibmq_toronto** and **ibmq_casablanca** respectively, where $U2(\phi, \lambda) = R_z(\phi)R_y(\pi/2)R_z(\lambda)$. Table A.4 shows the controlled-NOT error rates for the two processors used in the compiled quantum order-finding. The dates of the experiments are given in the captions. In the rest of the experiments, preference is similarly given to qubits with relatively small controlled-NOT error gates if the choice is between qubits with a similar connectivity, and we override this preference in the cases where one qubit has better connectivity than another.

	U_2 gate error rate (10^{-2})	Readout error rate (10^{-4})
Q0	6.010	4.39
Q1	3.14	2.12
Q2	2.98	1.96
Q3	0.930	5.74
Q4	1.34	2.097

Table A.2: Reported single-qubit gate errors on 16 December 2020.

	U_2 gate error rate (10^{-2})	Readout error rate (10^{-4})
Q0	2.16e-2	2.18
Q1	1.31e-2	4.042
Q2	1.54e-2	2.78
Q3	9.30e-2	2.62
Q4	1.67e-2	4.96

Table A.3: Reported single-qubit gate errors on 06 December 2020.

	ibmq_toronto (10^{-3})	**ibmq_casablanca** (10^{-2})
CX (0,1)	6.620e-3	0.9126
CX (1,4)	8.214e-3	1.114
CX (2,1)	7.152e-3	0.7446
CX (3,2)	6.824e-3	1.337

Table A.4: Reported controlled-NOT gate errors on 06 December (**ibmq_casablanca**) and 16 December (**ibmq_toronto**) 2020.

Qiskit's QST fitter uses a least-squares fitting to find the closest density matrix described by Pauli measurement results [153]. On an n-qubit system, the fitter requires measurement results from executing 3^n circuits. This makes QST on large circuits in impractical. Thus only 30 QST experiments were performed for the three control register qubits and in total $3^3 \times 30 \times 8192$ measurement were made.

In reducing the effect of noise due to final measurement errors, Qiskit recommends a measurement error mitigation approach. The approach starts off by creating circuits that each perform a measurement of the 2^n basis states. The measurement counts of the 2^n basis state measurements are put into a column vector C_{noisy}, arranged in ascending order by the value of their measurement bitstring, *i.e.* $00\ldots00$ is the first element, the next is $00\ldots01$ and so on. The approach assumes that there is a matrix M called the calibration matrix, such that

$$C_{\text{noisy}} = M C_{\text{ideal}}, \tag{A.1}$$

where C_{ideal} is a column vector of measurement counts in the absence of noise. If M is invertible then, then C_{noisy} can transformed into C_{ideal} by finding M^{-1}

$$C_{\text{ideal}} = M^{-1} C_{\text{noisy}}. \tag{A.2}$$

Qiskit [154] uses a least-squares fit to calculate an approximate M^{-1} by some other matrix $\tilde{M}^{-1}$, as in general M is not invertible, giving

$$C_{\text{mitigated}} = \tilde{M}^{-1} C_{\text{noisy}}. \tag{A.3}$$

The entries of the column vector $C_{\text{mitigated}}$ correspond to the mitigated measurement counts in same order as before. The entirety of the results reported in our work make use of this approach.

A.2 Error bars

The bootstrap resampling method is a statistical method dealing with a non-parametric estimation of mean, variances, and measures of error [155, 156]. Suppose we have a sample of n independent random variables from an unknown discrete distribution P

$$X_1, X_2, \cdots X_n \overset{\text{iid}}{\sim} P \tag{A.4}$$

Having observed values $x_1, x_2, \cdots x_n$, we wish to compute some estimate $\hat{\theta}(X)$ and subsequently the variance and error of this estimate. The bootstrap gives a procedure for this, which can be summarized in the following steps [155, 156].

Assign a equal probability to each observed data point $x_i = \frac{1}{n}$, and then proceed to randomly draw with replacement from the observed values to get a new sample

$$X_1^*, X_2^*, \cdots, X_n^* \tag{A.5}$$

Then one computes $\hat{\theta}^* = \hat{\theta}(X_1^*, X_2^*, \cdots, X_n^*)$, then independently repeat the random sampling to a desired number of iterations B. From this we collect a set of B bootstrapped values of the estimate $\hat{\theta}^{*^1}, \hat{\theta}^{*^2}, \cdots, \hat{\theta}^{*^B}$ and the mean of the bootstrapped values is calculated in the standard fashion as $\hat{\theta}^* = B^{-1} \sum_{b=1}^{B} \hat{\theta}^{*^b}$. We are now in a position to calculate the variance of the estimate

$$\hat{\sigma}_{\hat{\theta}}^2 = \frac{1}{B-1} \sum_{b=1}^{B} \{\hat{\theta}^{*^b} - \hat{\theta}^*\}^2. \tag{A.6}$$

The reason why we consider using the bootstrap resampling method to estimate quantities such as the variance and standard error instead of naively calculating the variance from the original observed values is because the sample size is fairly small for statistical inference. The bootstrap resampling method provides a way to account for the some of behavior of the full unknown distribution that may not be represented in a specific sample [155, 156]. All the confidence intervals of the data presented here were established *via* the above non-parametric bootstrap resampling techniques. In order to place the constraint that the measurement counts should sum to the number of experimental shots, a sample contains data as column vectors of outcomes of some experiment. In each round, the resampling draws entire column vectors whose elements respect the aforementioned constraint. For each outcome across the column vectors, mean estimates are obtained and a confidence interval around the estimates can be appropriately constructed.

To elucidate the above, consider the following example. Consider the outcomes of a two-qubit experiment with experimental shots of 8192 repeated 4 times, as shown in Table A.5.

Outcomes	Counts			
	Exp. 1	Exp. 2	Exp. 3	Exp. 4
00	2335	2208	2406	2203
01	665	690	633	656
10	183	100	197	177
11	5009	5192	4956	5156

Table A.5: Example data for a two-qubit experiment repeated 4 times for illustrating how bootstrap resampling was done.

Suppose we resampled the experiments 1, 1, 2, 4 from Table A.5, making a bootstrap sample of size 5.

$$\begin{aligned} B = [&[2335, 665, 183, 5009], \\ &[2335, 665, 183, 5009], \\ &[2208, 690, 100, 5192], \\ &[2203, 656, 177, 5156]]. \end{aligned} \tag{A.7}$$

From this, we can obtain appropriately the bootstrap sample for each outcome (corresponding to an index), *e.g.* the bootstrap sample for the outcomes at index 0 (outcome 00) is

$$B_0 = [2335, 2335, 2208, 2203]. \tag{A.8}$$

The bootstrap mean estimates and confidence intervals can then be performed for each outcome while respecting the constraint of the measurement counts summing up to the total number of experimental shots.

A.3 Pauli measurements

As an example, consider the measurement of the Pauli expectation value $\langle ZZZZZ \rangle$. Let p_{ijklm} denote the probability for a computational basis measurement $\{|0\rangle, |1\rangle\}$ of five qubits to output the binary string $ijklm$, *i.e.* p_{00000} denotes the probability to measure all the qubits in $|0\rangle$ state. To calculate $\langle ZZZZZ \rangle$ we can combine these probabilities as given in the equation below

$$\begin{aligned} \langle ZZZZZ \rangle = &\, p_{00000} - p_{00010} - p_{00100} + p_{00101} + p_{00110} - p_{01000} + p_{01001} \\ &+ p_{01010} + p_{01100} - p_{01101} - p_{01110} + p_{01111} - p_{10000} + p_{10001} \\ &+ p_{10010} - p_{10011} + p_{10100} - p_{10101} - p_{10110} + p_{10111} + p_{11000} \\ &- p_{11001} - p_{11010} + p_{11011} - p_{11100} + p_{11101} + p_{11110} - p_{11111}. \end{aligned} \tag{A.9}$$

Similarly, the expectation $\langle IZIZI \rangle$ is given by

$$\begin{aligned} \langle IZIZI \rangle = &\, p_{00000} - p_{00010} + p_{00100} + p_{00101} - p_{00110} - p_{01000} - p_{01001} \\ &+ p_{01010} - p_{01100} - p_{01101} + p_{01110} + p_{01111} + p_{10000} + p_{10001} \\ &- p_{10010} - p_{10011} + p_{10100} + p_{10101} - p_{10110} - p_{10111} - p_{11000} \\ &- p_{11001} + p_{11010} + p_{11011} - p_{11100} - p_{11101} + p_{11110} + p_{11111}. \end{aligned} \tag{A.10}$$

However, the terms in the equation above are given by the marginalization of the distribution measured in Equation (A.9) across the outcome space of qubits 1, 3 and 5. By considering all such marginalizations of the distribution in Equation (A.9), we obtain the set of Pauli expectation values that can be derived from a measurement of $\langle ZZZZZ \rangle$, namely

$$\begin{aligned}\{\, & ZZZZI, ZZZIZ, ZZZII, ZZIZZ, ZZIZI, ZZIIZ, ZZIII, \\ & ZIZZZ, ZIZZI, ZIZIZ, ZIZII, ZIIZZ, ZIIZI, ZIIIZ, \\ & ZIIII, IZZZZ, IZZZI, IZZIZ, IZZII, IZIZZ, IZIZI, \\ & IZIIZ, IZIII, IIZZZ, IIZZI, IIZIZ, IIZII, IIIZZ, \\ & IIIZI, IIIIZ \,\}. \end{aligned} \tag{A.11}$$

After applying what is described above to the Pauli decomposition of the ideal state $\rho = |\Psi\rangle\langle\Psi|$, we reduce the number of terms that we need to measure from 293 to 79 terms, as given below

$$\begin{aligned}\{\, & XXXXZ, XXXZX, XXXZZ, XXYYZ, XXYZY, XXZXX, XXZXZ, \\ & XXZYY, XXZZX, XYXYZ, XYXZY, XYYXZ, XYYZX, XYYZZ, \\ & XYZXY, XYZYX, XYZYZ, XYZZY, XZXXX, XZXYY, XZXZZ, \\ & XZYXY, XZYYX, XZZXZ, XZZZX, YXXYZ, YXXZY, YXYXZ, \\ & YXYZX, YXYZZ, YXZXY, YXZYX, YXZYZ, YXZZY, YYXXZ, \\ & YYXZX, YYXZZ, YYYYZ, YYYZY, YYZXX, YYZXZ, YYZYY, \\ & YYZZX, YZXXY, YZXYX, YZYXX, YZYYY, YZYZZ, YZZYZ, \\ & YZZZY, ZXXXZ, ZXXZX, ZXXZZ, ZXYYZ, ZXYZY, ZXZXX, \\ & ZXZXZ, ZXZYY, ZXZZX, ZYXYZ, ZYXZY, ZYYXZ, ZYYZX, \\ & ZYYZZ, ZYZXY, ZYZYX, ZYZYZ, ZYZZY, ZZXXX, ZZXXZ, \\ & ZZXYY, ZZXZX, ZZYXY, ZZYYX, ZZYYZ, ZZYZY, ZZZXX, \\ & ZZZYY, ZZZZZ \,\}. \end{aligned} \tag{A.12}$$

B

Appendix B

B.1 The equivalence of Grover's algorithm with a measurement procedure on a four qubit box graph state

In section § 2.4.2 of Chapter 2, we conjectured that Grover's algorithm for two qubits is equivalent to a measurement procedure on a four-qubit box graph state shown in Figure 2.26, which begins by measuring qubits 0 and 3 in basis $B(\alpha)$ and $B(\beta)$, respectively. Followed by a measurement of qubits 1 and 2 in the basis $B(\pi)$.

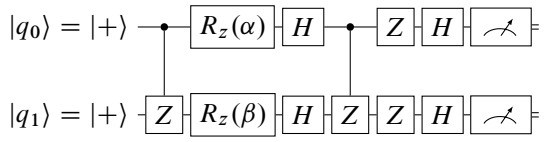


Figure B.1: Effective operations applied to the two remaining qubits after measurement procedure described in § 2.4.2 on a four-qubit box graph state when the measurement outcomes on qubit 2 and 3 are $m_0 = m_3 = 0$. With an appropriate choice of α, β, the circuit diagram is equivalent to Grover's algorithm on two qubits.

After this measurement procedure, on the remaining qubits, originally in the state $|+\rangle|+\rangle$, we have effectively applied the set of operations shown in the circuit diagram in Figure B.1, when the measurement outcomes on qubits 0 and 3 are both $m_0 = m_3 = 0$. Namely,

$$\mathrm{CZ}_{01}\hat{H}^{(0)} \otimes \hat{H}^{(1)}\hat{R}_z^{(0)}(\beta) \otimes \hat{R}_z^{(1)}(\alpha)\mathrm{CZ}_{01}\,|+\rangle_0\,|+\rangle_1\,, \tag{B.1}$$

all the unitary operations in the above equation can be written in matrix notation as

$$\begin{aligned}
\mathrm{CZ}_{01} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \\
\hat{R}_z^{(0)}(\alpha) \otimes \hat{R}_z^{(1)}(\beta) &= \frac{1}{2}\begin{pmatrix} e^{i(\alpha+\beta)/2} & 0 & 0 & 0 \\ 0 & e^{i(\alpha-\beta)/2} & 0 & 0 \\ 0 & 0 & e^{i(\beta-\alpha)/2} & 0 \\ 0 & 0 & 0 & e^{-i(\alpha+\beta)} \end{pmatrix}, \\
\hat{H}^{(0)} \otimes \hat{H}^{(1)} &= \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix},
\end{aligned} \tag{B.2}$$

and the state $|+\rangle_0\,|+\rangle_1$ is written as

$$|\psi_0\rangle = |+\rangle_0 |+\rangle_1 = \frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}. \tag{B.3}$$

Applying the unitary matrices to the state vector $|+\rangle_0 |+\rangle_1$, as in Equation (B.2), after some algebraic deadlifting we arrive at the state vector

$$= \frac{e^{i(\alpha+\beta)/2}}{4}\begin{pmatrix} 1+e^{-i\beta}+e^{-i\alpha}-e^{-i(\alpha+\beta)} \\ 1-e^{-i\beta}+e^{-i\alpha}+e^{-i(\alpha+\beta)} \\ 1+e^{-i\beta}-e^{-i\alpha}+e^{-i(\alpha+\beta)} \\ -1+e^{-i\beta}+e^{-i\alpha}+e^{-i(\alpha+\beta)} \end{pmatrix}. \tag{B.4}$$

The four-qubit box graph state in Figure 2.26 can be realized by applying controlled-Z gates between the qubits connected by edges as depicted in figure.

$$\begin{aligned} &\prod_{(i,j)\in E} \mathrm{CZ}_{ij} |+\rangle_0 |+\rangle_1 |+\rangle_2 |+\rangle_3 , \\ &= \frac{1}{2}(|0\rangle_1 |+\rangle_2 |0\rangle_3 |+\rangle_4 + |0\rangle_1 |-\rangle_2 |1\rangle_3 |-\rangle_4 \\ &+ |1\rangle_1 |-\rangle_2 |0\rangle_3 |-\rangle_4 + |1\rangle_1 |+\rangle_2 |1\rangle_3 |+\rangle_4), \end{aligned} \tag{B.5}$$

where CZ_{ij} is a controlled-Z gate with a control qubit i and target qubit j, and for the graph in Figure 2.26 $E = \{(0,1),(0,3),(1,3),(3,2)\}$. The projectors that correspond to the measurement basis $B(\alpha)$ are given by

$$\Lambda_{\pm\alpha,i} = |\pm\alpha_i\rangle \langle\pm\alpha_i| = \frac{1}{2}(|0\rangle_i + e^{i\alpha_i} |1\rangle_i)(\langle 0|_i + e^{-i\alpha_i} \langle 1|_i). \tag{B.6}$$

For algebraic convenience, and without the loss of generality, we will only consider measurement outcome $m_i = 0$ corresponding to the projector $\Lambda_{+\alpha,i}$. The measurement procedure begins by first measuring qubit 0 in the basis $B(\alpha)$. In the case where we obtain the outcome $m_0 = 0$, the state after the projective measurement is

$$\begin{aligned} \Lambda_{+\alpha,0} |\psi\rangle = \frac{1}{4}(|0\rangle_0 + e^{i\alpha} |1\rangle_0)(|+\rangle_1 |0\rangle_2 |+\rangle_3 + |-\rangle_1 |1\rangle_2) |-\rangle_3 \\ + e^{-i\alpha} |-\rangle_1 |0\rangle_2 |-\rangle_3 + e^{-i\alpha} |+\rangle_1 |1\rangle_2 |+\rangle_3). \end{aligned} \tag{B.7}$$

The above projective measurement is followed by another similar projective measurement in the basis $B(\beta)$ on qubit 3. In the case where we obtain $m_3 = 0$ the state after projective measurement is given by

$$\begin{aligned} \Lambda_{+\beta,3}\Lambda_{+\alpha,0} |\psi\rangle = \frac{1}{8}(|0\rangle_0 + e^{i\alpha} |0\rangle_0)(|0\rangle_3 + e^{i\beta} |1\rangle_3)((1+e^{-i\beta}) |+\rangle_1 |0\rangle_2 \\ + (1-e^{-i\beta}) |-\rangle_1 |1\rangle + (1-e^{-i\beta}) |-\rangle_1 |0\rangle_3 \\ + (1+e^{-i\beta}) |+\rangle_1 |1\rangle_2). \end{aligned} \tag{B.8}$$

Using vector notation, we can write the expression in Equation (B.8) as

$$\begin{aligned}\Lambda_{+\beta,3}\Lambda_{+\alpha,0}\left|\psi\right\rangle &= \frac{1}{8}\begin{pmatrix}(1+e^{-i\beta})+(1-e^{-i\beta})e^{-\beta}\\(1+e^{-i\beta})e^{-i\alpha}+1(1-e^{i\beta})\\(1+e^{-i\beta})-(1-e^{-i\beta})e^{-i\alpha}\\(1+e^{-i\beta})e^{-i\alpha}-(1-e^{-\beta})\end{pmatrix},\\ &= \frac{1}{8}\begin{pmatrix}1+e^{-i\beta}+e^{-i\alpha}-e^{-i(\alpha+\beta)}\\1-e^{-i\beta}+e^{-i\alpha}+e^{-i(\alpha+\beta)}\\1+e^{-i\beta}-e^{-i\alpha}+e^{-i(\alpha+\beta)}\\-1+e^{-i\beta}+e^{-i\alpha}+e^{-i(\alpha+\beta)}\end{pmatrix}.\end{aligned} \tag{B.9}$$

Up to normalization and a global phase, the above state vector is equivalent to the state vector in Equation (B.4) we arrived at *via* the circuit diagram in Figure B.1.

If our choice of the angles α, β is such that $R_z(\alpha) \otimes R_z(\beta)$ puts a negative sign on the amplitude of $|k_0\rangle\,|k_1\rangle$, then the action of the byproduct $Z^{m_0} \otimes Z^{m_3}$ due to the measurement outcomes will be such that the negative sign moves to the amplitude of the state $|k_0 \oplus m_0\rangle\,|k_1 \oplus m_3\rangle$. Thus, depending m_0 and m_3 on qubits 0 and 3, we merely add modulo 2 the measurement outcome of qubit 1 to qubit 0 ($m_0 \oplus m_1$), and of qubit 2 to qubit 3 ($m_2 \oplus m_3$), respectively. In this way, we recover Grover's algorithm for the target element originally determined by our choice of the angles α, β.

B.2 Local unitary equivalence class of the four-qubit box graph states through edge local complementation

Two graph states $|G\rangle, |G'\rangle$ corresponding to the graphs $G = (V, E), G' = (V, E')$ respectively, with the same set of vertices (under a graph isomorphism)[1], *i.e.* $G = (V, E)$ and $G' = (V, E')$, are said to be LU-equivalent if there exists a sequence of unitary operators $U_a(G)$ where $a \in V$ such that

$$\prod_{\vec{a}} U_a(G)\,|G\rangle = \left|G'\right\rangle, \tag{B.10}$$

where $\vec{a}$ is a sequence of vertices in V. The unitary transformation $U_a(G)$ is of the form

$$U_a(G) = \sqrt{iX^{(a)}} \prod_{b\in\eta_a} \sqrt{iZ^{(b)}}. \tag{B.11}$$

Here η_a is the neighborhood of the vertex b, $X^{(a)}$ and $Z^{(a)}$ are Pauli X and Z, respectively, acting on qubit a[2]. The above unitary transformation $U_a(G)$ is independently due to Hein [77] and Nest [78]. Through repeated applications of the $U_a(G)$, it is possible to generate an entire LU-equivalence class of graph states.

On the level of graphs, the unitary transformation $U_a(G)$ has a graph theoretic interpretation, that is, applying $U_a(G)$ to $|G\rangle$, the graph $G = (V, E)$ is transformed to another $G' = (V, E')$ such that the set of edges in the new graph is given by

$$E' = E \cup E(\eta_a, \eta_a) \setminus E \cap E(\eta_a, \eta_a), \tag{B.12}$$

[1] Two graphs G and H are said to be isomorphic if there exists a bijection between their vertex set i.e $f : V(G) \mapsto V(H)$ such that when the two vertices share an edge in one graph, the edge is preserved in the new graph (*i.e.* a relabeling of vertices), such an edge-preserving bijection is called an isomorphism. We write $G \cong H$ to denote that G and H are isomorphic.

[2] For a graph $G = (V, E)$, the neighborhood of a vertex $b \in V$, is the set of all vertices that share an edge with b, that is, $\forall a : (a, b) \in E$.

where $E(\eta_a, \eta_a)$ is the all set of possible edges between the vertices in the neighborhood of a, $\cap$ and $\cup$ are the set interpretation and union operators, respectively, and $\setminus$ denotes the set complement operation. Graphically, the transformation $U_a(G)$ adds new edges between the vertices in the neighborhood of vertex a to E $(E \cup E(\eta_a, \eta_a))$, if they are already present, *i.e.* in $E \cap E(\eta_a, \eta_a)$, the said edges are removed from E. $(\setminus E \cap E(\eta_a, \eta_a))$, such a transformation in graph theory is called edge local complementation (ELC) [157].

One advantageous consequence of the above unitary transformation is the following we may wind up in a scenario where we are interested in realizing some quantum protocol which uses a graph state $|G\rangle$, with the underlying graph $G = (V, E)$, as an initial resource state. For the state initialization procedure of a given protocol, we would have to apply $|E|$ controlled-Z gates between the connected qubits $(v, w) \in E$ to the initial state $|+\rangle^{\otimes|V|}$ to get $|G\rangle$. However, if $|G\rangle$ happens to belong to an LU-equivalence class, and we may be able to find the equivalence class member $|G'\rangle$ with the least of number of edges in that class, such that $|G\rangle = U|G'\rangle$ for some local unitary operator U (tensor product of Pauli matrices and/or their square roots). Thus, in our new state initialization procedure, we can choose to prepare $|G'\rangle$ instead with $|E'| < |E|$ controlled-Z gates. Such a reduction in controlled-Z gates in practice might be of some appeal and advantage, since two-qubit gates are considered non-trivial and expensive in comparison to local (tensor product of single-qubit gates) unitaries.

We now illustrate an example of the scenario described above. The measurement-based equivalent of Grover's algorithm for two qubits can realized on the four-qubit box graph state, which in total has four connections, as we have seen in § 2.4.2. The four-qubit box graph state is LU-equivalent (and up to a graph isomorphism) to a four-qubit linear graph state with one less qubit connection. Starting from the latter graph state, by applying local unitaries $U_2(G)$, $U_1(G)$ and $U_2(G)$ on qubits 2, 1 and 2, respectively, we end up with a four-qubit graph state that is isomorphic to four-qubit box graph state; this is shown in Figure B.2.

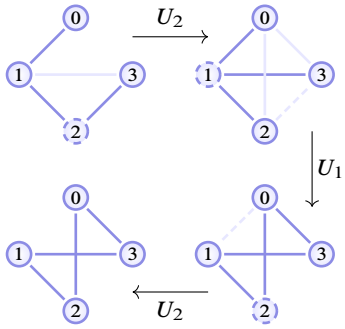


Figure B.2: LU equivalence of a four-qubit graph state with three edges connected with the four-qubit box graph state through repeated applications of edge local complementation. The action of an LU operation $U_a(G)$ on the level of the graph, for the chosen vertex a (indicated with a dashed outline) leads to an edge created between its neighbors (opaque indigo line) and if it already exists is removed (opaque dashed indigo line).

We can find the effective local unitaries that relate the two graph states by successively applying the rule in Equation (B.11), to the initial four-qubit linear graph state as depicted in Figure B.2. Initially, $U_2(G)$ is given by

$$\hat{U}_2(G) = \sqrt{-iX^{(2)}} \prod_{b \in \eta_2} \sqrt{iZ^{(b)}}. \tag{B.13}$$

For the initial graph, the neighbors of vertex 2 are vertices 1 and 3. Thus, the above expression for $U_2(G_0)$ becomes

$$\hat{U}_2(G_0) = \mathbb{1}^{(0)} \otimes \sqrt{iZ^{(1)}} \otimes \sqrt{iZ^{(2)}} \otimes \sqrt{-iX^{(3)}}. \tag{B.14}$$

The action of $U_2(G_0)$ transforms G_0 to new a graph G_1, which has an edge between qubits 1 and 3. For the new graph state $|G_1\rangle$, the local unitary $U_1(G_1)$ that follows is given by

$$\hat{U}_1(G_1) = \sqrt{-iX^{(1)}} \prod_{b \in \eta_1} \sqrt{iZ^{(b)}}. \tag{B.15}$$

In G_1, the neighbors of vertex 1 are vertices 0, 2 and 3. Hence, we have

$$\hat{U}_1(G_1) = \sqrt{iZ^{(0)}} \otimes \sqrt{-iX^{(1)}} \otimes \sqrt{iZ^{(2)}} \otimes \sqrt{iZ^{(3)}}. \tag{B.16}$$

From which, the resultant new graph G_2 has new edges $(0, 3)$ and $(0, 1)$, and the edge between $(2, 3)$ is removed. Lastly, we consider the local unitary $U_2(G_2)$ on the new graph G_2

$$\hat{U}_2(G_2)\sqrt{-iX^{(2)}} \prod_{b\in\eta_2} \sqrt{iZ^{(b)}}, \tag{B.17}$$

where the neighbors of the vertex 2 are now the vertices 0 and 1.

$$\hat{U}_2(G_2) = \sqrt{iZ^{(0)}} \otimes \sqrt{iZ^{(1)}} \otimes \sqrt{-iX^{(2)}} \otimes \mathbb{1}^{(3)}. \tag{B.18}$$

The action of $U_2(G_2)$ is to remove the edge $(0, 1)$ to give the new graph G_3. Looking at Figure B.2, the graph G_3 under the following isomorphism

$$\begin{aligned} f(1) &= 2, \\ f(2) &= 1, \\ f(3) &= 3, \\ f(0) &= 0, \end{aligned} \tag{B.19}$$

is equivalent to the four-qubit box graph state Figure 2.26. Tallying up the all local unitaries and using the identities [158]:

$$\begin{aligned} \sqrt{X} &= e^{i\pi/4} R_x(\pi/2), \\ \sqrt{Z} &= e^{i\pi/4} R_z(\pi/2). \end{aligned} \tag{B.20}$$

The full unitary operation is then given by

$$\begin{aligned} U_2(G_0)U_1(G_1)U_2(G_2) &= iU^{(0)} \otimes U^{(1)} \otimes U^{(2)} \otimes U^{(3)}, \\ U^{(0)} &= R_z^{(0)}(\pi), \\ U^{(1)} &= R_z^{(1)}(\pi/2)R_x^{(1)}(\pi/2)R_z^{(1)}(\pi/2), \\ U^{(2)} &= R_x^{(2)}(\pi/2)R_z^{(2)}(\pi), \\ U^{(3)} &= R_z^{(3)}(\pi/2)R_x^{(3)}(\pi/2). \end{aligned} \tag{B.21}$$

B.3 Edge local complementation equivalence class of a graph state realizing a measurement-based controlled-controlled-Z gate

Starting from the ten-qubit graph state in Figure 2.28 that realizes the measurement-based controlled-controlled-Z gate with an appropriate choice of measurements as described in § 2.4.2. By repeated applications of the ELC rule, which results in the local unitaries of the form in Equation (B.11); using the graph-state compass program [159] from Ref. [160] we expand the equivalence class to which the aforesaid graph state belongs. The representative members of this equivalence class are shown in Figure B.3; in the equivalence class, the member with the least number of edges is the original ten-qubit graph state.

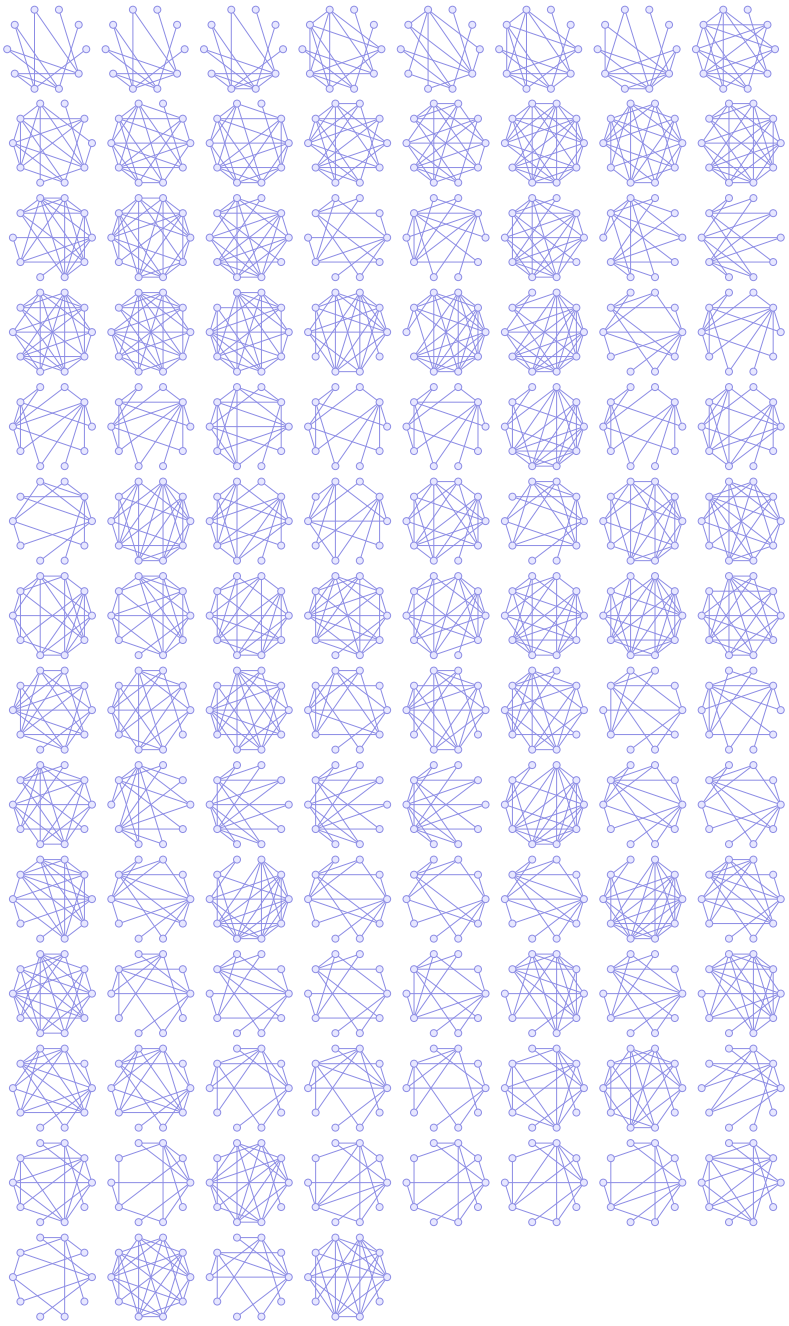


Figure B.3: An equivalence class of ten-qubit graph states that performs a controlled-controlled-Z gate with an appropriate choice of measurements as described in § 2.4.2.

C

Appendix C

C.1 Postselection scaling

In order to do mid-circuit measurements and post select the outcomes, we need to know the basis to measure in for each of the qubits. Looking at Figure 3.11, one would need to measure qubit 1 (or the first iteration in the recycling case) in the $\{|+\rangle, |-\rangle\}$ basis (since there is Hadamard gate H on acting qubit 1 before the Z-basis measurement), then qubit 2 (or the second iteration in the recycling case) in either the $\{S^\dagger |+\rangle, S |-\rangle\}$ (if our measurement outcome on qubit 1 was $|+\rangle$) or $\{|+\rangle, |-\rangle\}$ basis, then qubit 3 in either the $\{T^\dagger S^\dagger |+\rangle, TS |-\rangle\}$, $\{S^\dagger |+\rangle, S |-\rangle\}$ or $\{|+\rangle, |-\rangle\}$ basis. Thus, the number of measurements needed scales as $n!$, which grows faster than an exponential with constant base, e.g. 2^n. So in general the speed up gained would be lost for general factoring using a post selection method, *i.e.* factoring numbers larger than 21.

C.2 Effect of relative phase Toffolis

Below we show the compiled circuit for the period-finding routine and label specific instances during the evolution of the computation. The aim is to show the invariance of the computation when replacing Toffoli gates with relative phase Toffoli gates that use fewer resources.

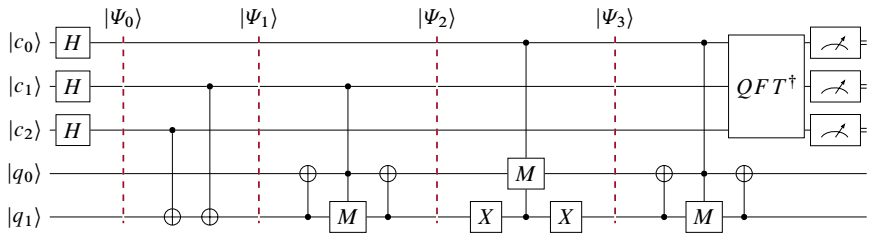


Figure C.1: States in both registers at various points during the execution of the circuit.

The states at various points of the evolution are given explicitly as

$$|\Psi_0\rangle = |+\rangle_{c_0} |+\rangle_{c_1} |+\rangle_{c_2} |0\rangle_{q_0} |0\rangle_{q_1} ,$$

$$\begin{aligned}|\Psi_1\rangle = |+\rangle_{c_0} (&|0\rangle_{c_1} |0\rangle_{c_2} |0\rangle_{q_0} |0\rangle_{q_1} + |0\rangle_{c_1} |1\rangle_{c_2} |0\rangle_{q_0} |1\rangle_{q_1} + \\ &|1\rangle_{c_1} |0\rangle_{c_2} |0\rangle_{q_0} |1\rangle_{q_1} + |1\rangle_{c_1} |1\rangle_{c_2} |0\rangle_{q_0} |0\rangle_{q_1}),\end{aligned}$$

$$\begin{aligned}|\Psi_2\rangle = &|0\rangle_{c_0} |0\rangle_{c_1} |0\rangle_{c_2} |0\rangle_{q_0} |0\rangle_{q_1} + |0\rangle_{c_0} |0\rangle_{c_1} |1\rangle_{c_2} |0\rangle_{q_0} |1\rangle_{q_1} + \\ &|0\rangle_{c_0} |1\rangle_{c_1} |0\rangle_{c_2} |1\rangle_{q_0} |0\rangle_{q_1} + |0\rangle_{c_0} |1\rangle_{c_1} |1\rangle_{c_2} |0\rangle_{q_0} |0\rangle_{q_1} + \\ &|1\rangle_{c_0} |0\rangle_{c_1} |0\rangle_{c_2} |0\rangle_{q_0} |0\rangle_{q_1} + |1\rangle_{c_0} |0\rangle_{c_1} |1\rangle_{c_2} |0\rangle_{q_0} |1\rangle_{q_1} + \\ &|1\rangle_{c_0} |1\rangle_{c_1} |0\rangle_{c_2} |1\rangle_{q_0} |0\rangle_{q_1} + |1\rangle_{c_0} |1\rangle_{c_1} |1\rangle_{c_2} |0\rangle_{q_0} |0\rangle_{q_1} ,\end{aligned}$$

$$\begin{aligned}|\Psi_3\rangle = &|0\rangle_{c_0} |0\rangle_{c_1} |0\rangle_{c_2} |0\rangle_{q_0} |0\rangle_{q_1} + |0\rangle_{c_0} |0\rangle_{c_1} |1\rangle_{c_2} |0\rangle_{q_0} |1\rangle_{q_1} + \\ &|0\rangle_{c_0} |1\rangle_{c_1} |0\rangle_{c_2} |1\rangle_{q_0} |0\rangle_{q_1} + |0\rangle_{c_0} |1\rangle_{c_1} |1\rangle_{c_2} |0\rangle_{q_0} |0\rangle_{q_1} + \\ &|1\rangle_{c_0} |0\rangle_{c_1} |0\rangle_{c_2} |1\rangle_{q_0} |0\rangle_{q_1} + |1\rangle_{c_0} |0\rangle_{c_1} |1\rangle_{c_2} |0\rangle_{q_0} |1\rangle_{q_1} + \\ &|1\rangle_{c_0} |1\rangle_{c_1} |0\rangle_{c_2} |0\rangle_{q_0} |0\rangle_{q_1} + |1\rangle_{c_0} |1\rangle_{c_1} |1\rangle_{c_2} |1\rangle_{q_0} |0\rangle_{q_1} .\end{aligned} \tag{C.1}$$

Looking at the state $|\Psi_1\rangle$, one can see that none of its constituent states is transformed into $|1\rangle_{c_1} |0\rangle_{q_0} |1\rangle_{q_1}$ by the CX gate that follows, since the state $|1\rangle_{c_1} |1\rangle_{q_0} |1\rangle_{q_1}$ that would be transformed to the former is not present in $|\Psi_1\rangle$. Thus the relative phase Toffoli gate does not affect the phase in the registers. Similarly for $|\Psi_2\rangle$, the state $|1\rangle_{c_0} |1\rangle_{q_0} |0\rangle_{q_1}$ is not present when the subsequent relative phase Toffoli gate is applied because the state $|1\rangle_{c_0} |1\rangle_{q_0} |1\rangle_{q_1}$ is absent from the register for $|\Psi_2\rangle$ and this is needed when $\hat{X}$ is applied to qubit q_1. The scenario for $|\Psi_3\rangle$ is the same as that of $|\Psi_1\rangle$, the only difference is the control is now c_0. The Margolus gates in this particular quantum circuit never encounter the basis state $|101\rangle$, thus the operation of the circuit remains unchanged by the replacement of full Toffoli gates with their respective relative phase counterparts.

C.3 Maximum overlap with respect to the bipartitions

The values listed below were obtained using the software package QUBIT4MATLAB [107]. Here, $|\phi\rangle$ is a pure biseparable state in some defined bipartite partition (bipartition), *i.e.* a separable product state with respect to this bipartition, and $|\Psi\rangle$ is the ideal state in both the control and work registers preceding the application of the QFT to the control register.

$$\begin{aligned}
\max_{\phi\in\{(c_1)(c_0c_2q_0q_1)\}} |\langle\phi|\Psi\rangle|^2 &= 0.500,\\
\max_{\phi\in\{(c_2)(c_0c_1q_0q_1)\}} |\langle\phi|\Psi\rangle|^2 &= 0.500,\\
\max_{\phi\in\{(q_0)(c_0c_1c_2q_1)\}} |\langle\phi|\Psi\rangle|^2 &= 0.750,\\
\max_{\phi\in\{(q_1)(c_0c_1c_2q_0)\}} |\langle\phi|\Psi\rangle|^2 &= 0.625,\\
\max_{\phi\in\{(c_0c_1)(c_2q_0q_1)\}} |\langle\phi|\Psi\rangle|^2 &= 0.500,\\
\max_{\phi\in\{(c_0c_2)(c_1q_0q_1)\}} |\langle\phi|\Psi\rangle|^2 &= 0.500,\\
\max_{\phi\in\{(c_0q_0)(c_1c_2q_1)\}} |\langle\phi|\Psi\rangle|^2 &= 0.427,\\
\max_{\phi\in\{(c_0q_1)(c_1c_2q_0)\}} |\langle\phi|\Psi\rangle|^2 &= 0.570,\\
\max_{\phi\in\{(q_0q_1)(c_0c_1c_2)\}} |\langle\phi|\Psi\rangle|^2 &= 0.375,\\
\max_{\phi\in\{(c_0q_1)(c_0c_1q_0)\}} |\langle\phi|\Psi\rangle|^2 &= 0.570,\\
\max_{\phi\in\{(c_1q_1)(c_0c_2q_0)\}} |\langle\phi|\Psi\rangle|^2 &= 0.570,\\
\max_{\phi\in\{(c_1q_0)(c_0c_2q_1)\}} |\langle\phi|\Psi\rangle|^2 &= 0.427,\\
\max_{\phi\in\{(c_2q_0)(c_0c_1q_1)\}} |\langle\phi|\Psi\rangle|^2 &= 0.427,\\
\max_{\phi\in\{(c_1c_2)(c_0q_0q_1)\}} |\langle\phi|\Psi\rangle|^2 &= 0.500. \qquad\qquad (C.2)
\end{aligned}$$

For a given separation of the qubits into two partitions (a bipartition), *e.g.* $(c_1)(c_0c_2q_0q_1)$, there is a pure product state $|\phi\rangle$ with respect to these partitions, *i.e.* no entanglement between the partitions, that maximizes the overlap squared with the ideal state. The value of the overlap squared between this product state and the ideal state, *e.g.* 0.5, is therefore the highest value that can be obtained for an separable state between the partitions. Thus, if a given state has an overlap squared larger than 0.5 it must be an entangled state with respect to the partitions. The value of the maximum overlap squared changes for the different partitions chosen as it depends on the structure of the ideal state. The above results extend to mixed states across the bipartitions due to the convex sum nature of quantum states [107].

C.4 Continued fractions and convergents

A $2L+1$ bit rational number φ is said to have a continued fraction expansion if it can be written as

$$\varphi \equiv [a_0, a_1, \ldots, a_n] \equiv a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}, \tag{C.3}$$

where n is a finite integer and the a_i's are integers. Additionally, if $\varphi < 1$, we have $a_0 = 0$. The convergents of the continued fraction expansion are the rationals,

$$a_0, a_0 + \frac{1}{a_1}, a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}, \cdots \tag{C.4}$$

If a rational number s/r satisfies the following inequality

$$\left| \frac{s}{r} - \varphi \right| \leq \frac{1}{2r^2}, \tag{C.5}$$

then s/r will appear as a convergent in the continued fraction expansion of φ. If φ is an approximation of s/r accurate to $2L+1$ bits, then we have $|s/r - \varphi| \leq 1/2^{2L+1}$. For $r \leq N \leq 2^L$, we have that $1/2^{2L+1} \leq 1/2r^2$. Therefore, since the inequality holds for the approximation φ, there is a classical algorithm that can compute the convergents of φ, and produce integers s', r' such that $\gcd(s', r') = 1$ in $\mathcal{O}(L^3)$ operations [17]. We can then check if r' is the order of x and N by testing whether $x^{r'} \bmod N = 1$. Note that in our approach, $\varphi = \varphi_s/2^n \simeq s/r$ is not an approximation that is accurate to $2L+1$ bits as above, but is a further approximation of s/r depending on the resolution, *i.e.* the number of iterations, or alternatively qubits in the control register.

Consider the following example of the final measurement outcomes from Figure 3.15 in the main text, where the outcomes $|110\rangle = |6\rangle$ and $|101\rangle = |5\rangle$ are peaked in the outcome distribution and we have used the integer representation of the binary outcome. The former outcome gives $\varphi = \frac{6}{2^3}$ and latter gives $\varphi = \frac{5}{2^3}$. Computing the continued fractions of the former gives

$$\begin{aligned} \frac{6}{8} &= \frac{3}{4}, \\ \frac{3}{4} &= 0 + \frac{1}{\frac{4}{3}}, \\ \frac{3}{4} &= 0 + \cfrac{1}{1 + \frac{1}{3}}. \end{aligned} \tag{C.6}$$

Thus

$$\frac{6}{8} = [0, 1, 3]. \tag{C.7}$$

Computing the convergents according to Equation (C.4) gives $0, 1, 3/4$. On the other hand, computing the continued fractions of the latter φ gives

$$\begin{aligned}
\frac{5}{8} &= 0 + \frac{1}{\frac{8}{5}}, \\
\frac{5}{8} &= 0 + \frac{1}{1 + \frac{3}{5}}, \\
\frac{5}{8} &= 0 + \frac{1}{1 + \frac{1}{\frac{5}{3}}}, \\
\frac{5}{8} &= 0 + \frac{1}{1 + \frac{1}{1 + \frac{2}{3}}}, \\
\frac{5}{8} &= 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}}, \\
\frac{5}{8} &= 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}.
\end{aligned} \tag{C.8}$$

The above calculation gives the following continued fractions expansion

$$\frac{5}{8} = [0, 1, 1, 1, 2]. \tag{C.9}$$

Computing the convergents gives $0, 1, 1/2, 2/3, 5/8$. Looking at the former and latter computed convergents, we note that the fourth convergent of the latter correctly gives $r' = 3$ while the convergents of the former do not give the correct order when tested using $x^{r'} \bmod N = 1$.

D

Appendix D

The server architecture we designed for making our entanglement resource remotely accessible for data acquisition experiments was built around Thorlabs' host-controller communications APT protocol [161]. The protocol provides a way to programmatically communicate with almost all Thorlabs motion controllers[1]. The communication protocol is based on a message structure that always starts with a fixed length, 6-byte message header which, in some cases, is followed by a variable length data packet, which specifies the sundry byte sequences for sundry operations, all communicated over a USB port. In the name of simplicity, we do not use the protocol in this form but instead use an open-sourced functional implementation in python made by YAQ [162], which provides modularized functions to invoke sundry operations on motion-controllers such as specifying motors and changing the parameters (speed, acceleration etc) of the motors, hiding the fine-grained implementation details of the APT protocol to the user.

[1] Our experiment uses KDC101 - K-Cube Brushed DC Servo Single-Channel Motor Controllers.

For example, the following code snippet packages the byte sequence to be sent from a source port to a destination source that specifies that an operation that homes a motor to its zero position.

```
def mot_move_home(dest: int, source: int, chan_ident: int) -> bytes:
    return _pack(0x0443, dest, source, param1=chan_ident)
```

Subsequently, the packaged byte sequence can then be communicated over a USB port to execute on some specified motor, with the following prototypical code snippet:

```
import thorlabs_apt_protocol as apt
import serial

# grab motor connected to USB port 0
port = serial.Serial("/dev/ttyUSB0", 115200, rtscts=True, timeout=0.1)
port.rts = True
port.reset_input_buffer()
port.reset_output_buffer()
port.rts = False

# home motor
port.write(apt.mot_move_home(source=source, dest=dest, chan_ident=chan_ident))
```

We used the protocol in a similar manner to the above code snippet, and through an application programming interface (API), we exposed the relevant higher-order

functionalities required to carry out the various projective measurements in our experiment. Our API is served by an HTTP Flask server [163] locally hosted on a Raspberry Pi 4. The HTTP server communicates with clients *via* HTTP requests (GET, POST, PUT); we use GET requests to serve information about the motors, such as the homing parameters, device status, etc to a client that makes such a request. Similarly, PUT requests are used by clients to update the aforesaid parameters on the motors. And lastly, POST requests are used by clients to start the execution of moves, such as homing, jog etc. The code snippet below shows an API endpoint for requests related to the homing move. The GET request here performs the necessary operations to get the homing parameters from a motor specified through the parameters of the request and returns them to the requesting client:

```
@app.route("/home", methods=["GET", "POST", "PUT"])
def home():
    if request.method == "GET":
        device = int(request.args.get("device", 0))
        port = devices[device]

        if port is None:
            return jsonify({"status": "error", "error": "Device unavailable"}), 500

        for i in range(retries):
            port.write(
                apt.mot_req_homeparams(source=source, dest=dest, chan_ident=chan_ident)
            )

            unpacker = apt.Unpacker(port)
            for message in unpacker:
                if hasattr(message, 'msg') and message.msg == "mot_get_homeparams":
                    sem.release()
                    logging.info(message)
                    return jsonify(message), 200

        return (
            jsonify({"status": "error", "error": "Could not get home parameters"}),
            500,
        )
        ...
```

Similarly, all the necessary operations were exposed as an endpoint of the API. Once this was accomplished, the entirety of the locally hosted API was made accessible through a public URL *via* ngrok [164], giving remote access to the API. Lastly, we designed a mobile graphical user interface (GUI) with Expo [165], which provides a simple and intuitive way to use the API for carrying out user-defined experiments and parameter updating operations. We conclude this appendix by showing a demo of the various screens of mobile GUI in Figure D.1, Figure D.2 and Figure D.3.

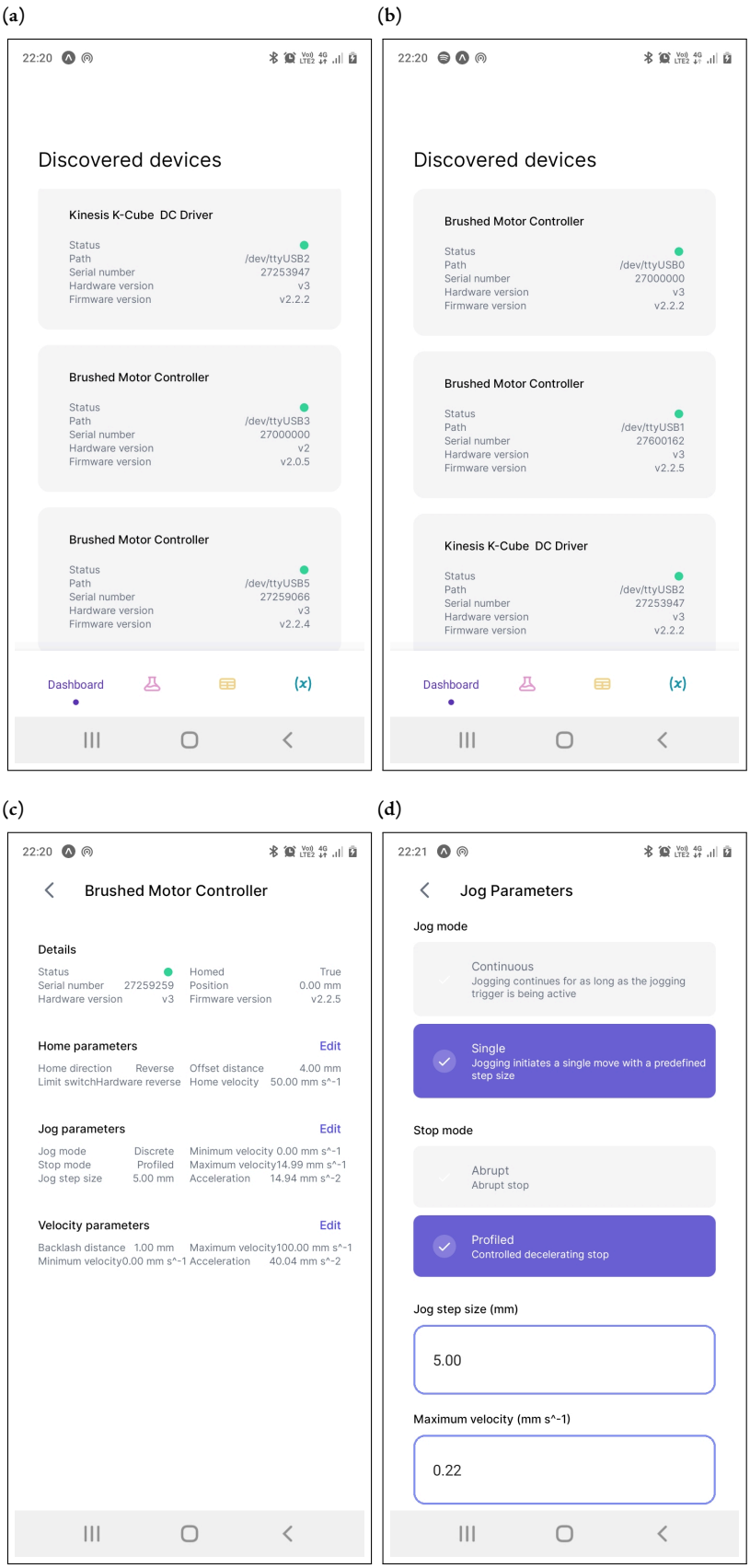


Figure D.1: Various screens for our mobile graphical user interface for controlling our remote source of entanglement: **(a)**, **(b)** On the initial load of the GUI, a user gets directed to the dashboard where they can see all the motorized devices and their meta data (online status, hardware etc) accessible by the API. **(c)** Whenever a user clicks one of the cards, they are directed to a screen with more fine-grained details about that specific device such as jogging parameters, velocity parameters, etc. **(d)** If a user wishes, it possible to edit the parameters by clicking the edit button next to the type of parameters they wish to change. Where they are taken to a screen with text fields of the editable parameters and the ability to save these changes.

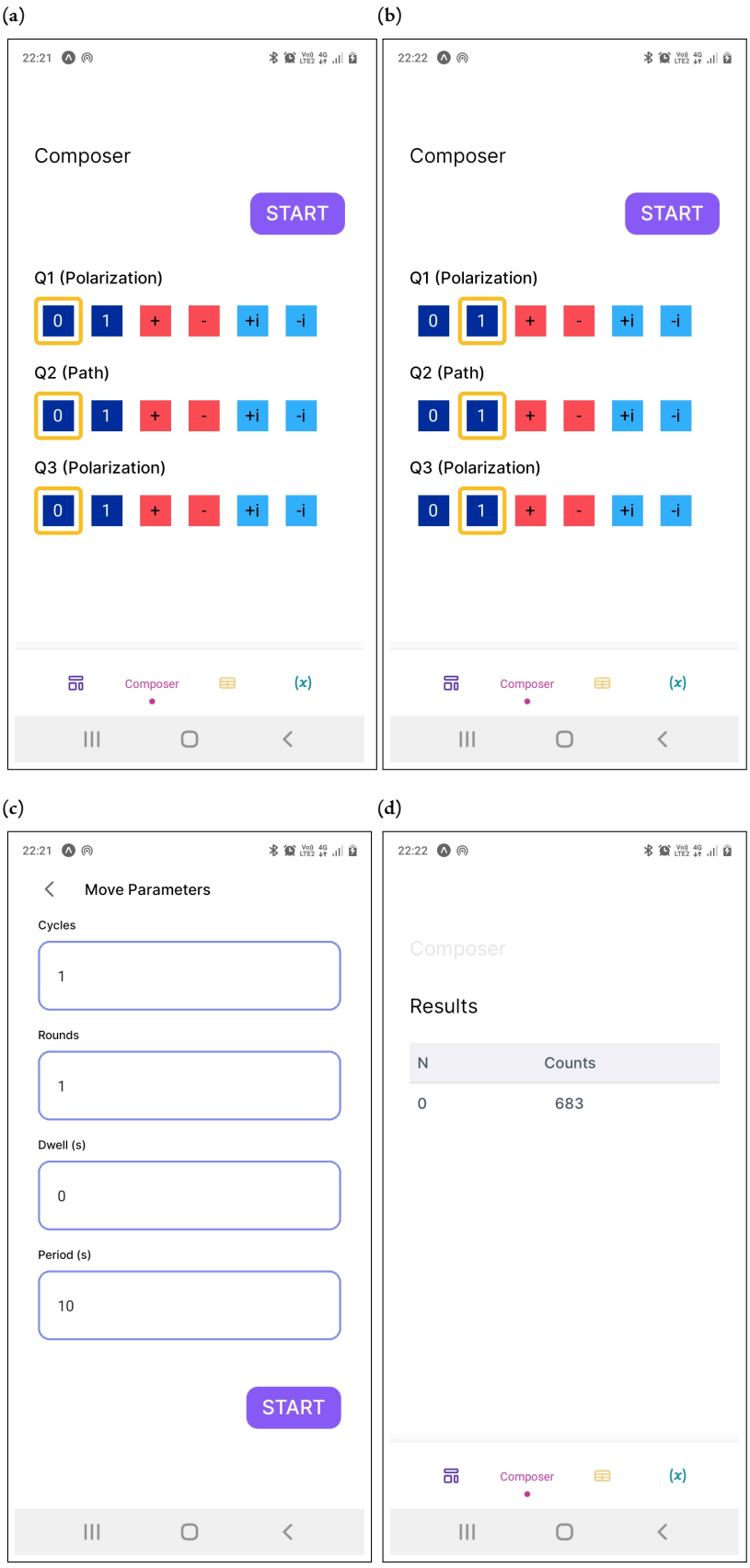


Figure D.2: Various screens for our mobile graphical user interface for controlling our remote source of entanglement. **(a)**, **(b)** The composer screen allows a user to set up a simple experiment by specifying the projective measurements on each qubit, with each of the clickable squares representing the measurement basis indicated on the square $0 = |0\rangle$, $1 = |1\rangle$, $\pm = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and $\pm i = (|0\rangle \pm i\,|1\rangle)/\sqrt{2}$. **(c)** Once a user is happy with their choice of measurement basis, by clicking start button they can set up data acquisition parameters such as the interval of data collection (period), how many data points are collected (rounds) for the collection interval. Furthermore, they can also specify how many times this experiment is to be repeated (cycles) and the paused between these repeated cycles (dwell). **(d)** By clicking the start button on the previous screen, the relevant HTTP requests are made to the API, which are then executed on the motors. Once completed the API returns the collected coincidences counts, which are then shown to the user in table format. In this case, the coincidence counts are for the measurement of $|1,1,1\rangle\langle 1,1,1|$

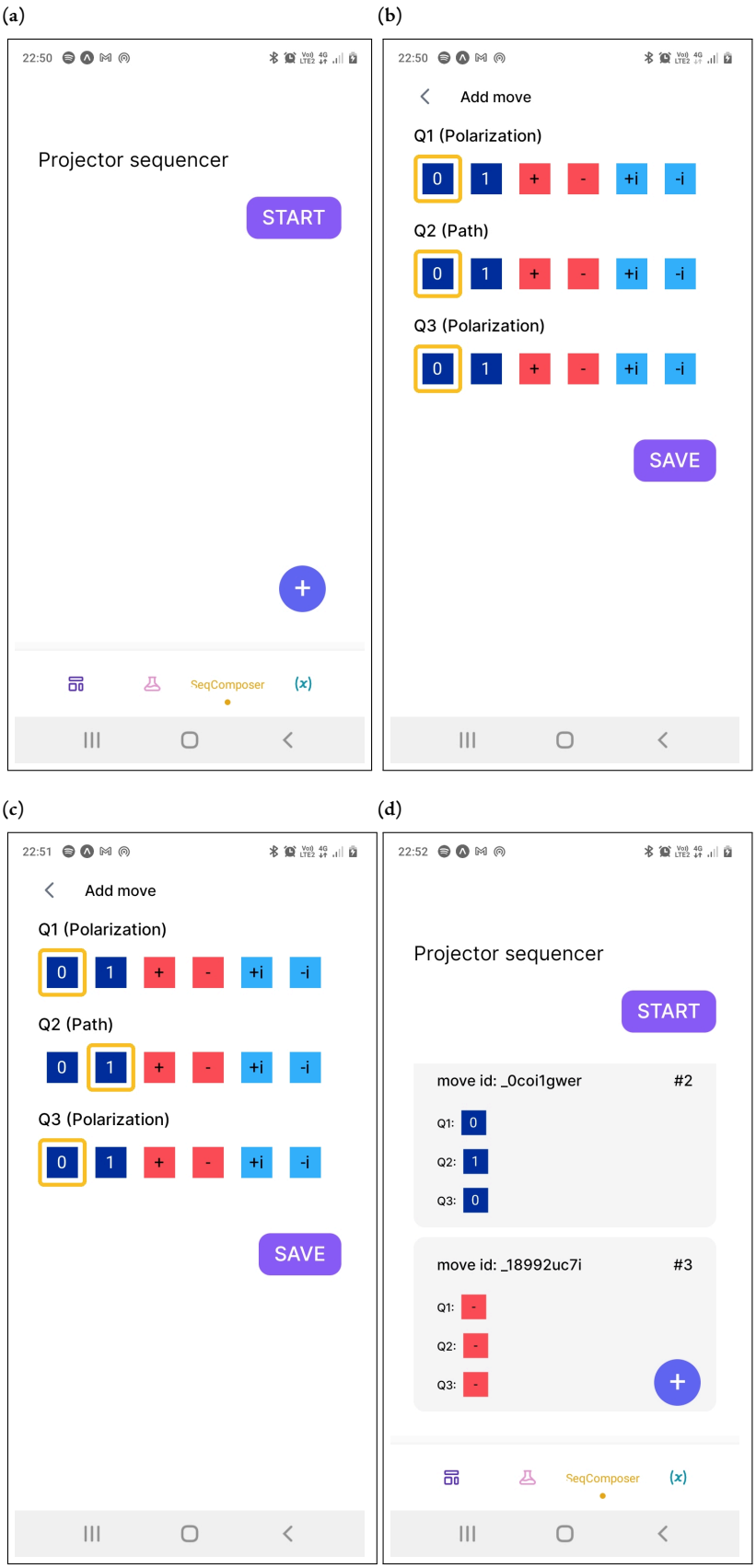


Figure D.3: Various screens for our mobile graphical user interface for queueing up a sequence of projective measurements on our remote source of entanglement. **(a)** This screen allows a user to queue up a sequence of projective measurements in a first in first out (FIFO) queue. **(b)**, **(c)** By clicking the add button on bottom right, a screen similar to the composer pops up for specifying a projective measurement on each qubit and save it on the queue. **(d)** The queued projective measurements populate the screen in (a), where queued measurements can be edited and deleted.

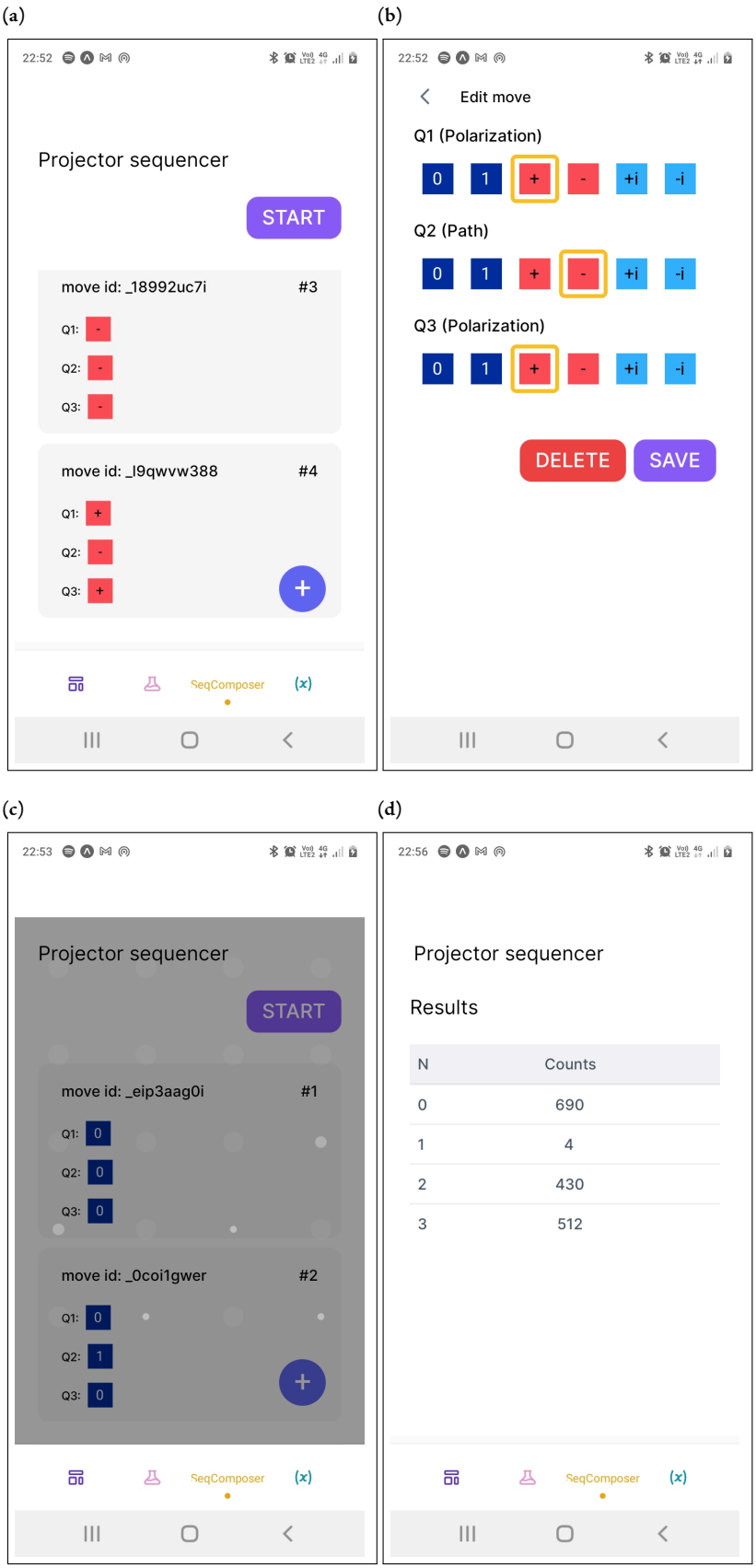


Figure D.4: Various screens for our mobile graphical user interface for editing and executing a sequence of projective measurements on our remote source of entanglement. **(a)** The queued projective measurements are each assigned a unique ID. **(b)** By clicking on a specific card, identified by its ID, a screen similar to the composer pops up where the projective measurements can edited or deleted from the queue. **(d)** Once a user is happy with their queued projective measurements, by clicking the start button screen **(a)**, they can specify move parameters similar to Figure D.2 (c) and start running the queued projective measurements; a loading state is shown. **(d)** Once finished, the collected double coincidences counts are returned, and are shown to the user in table format, in order of in the order of their execution from the FIFO queue.

Bibliography

[1] R. P. Feynman. "Simulating physics with computers". *International Journal of Theoretical Physics* 21 (6 1982), pp. 467–488 (cit. on p. 1).

[2] D. Deutsch. "Quantum theory, the Church-Turing principle and the universal quantum computer". *Proceedings of the Royal Society of London Series A* 400.1818 (July 1985), pp. 97–117 (cit. on p. 2).

[3] D. E. Deutsch and R. Penrose. "Quantum computational networks". *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 425.1868 (1989), pp. 73–90. eprint: https://royalsocietypublishing.org/doi/pdf/10.1098/rspa.1989.0099 (cit. on pp. 2, 18).

[4] D. Deutsch and R. Jozsa. "Rapid solution of problems by quantum computation". *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439.1907 (1992), pp. 553–558 (cit. on p. 2).

[5] P. W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509 (cit. on pp. 2, 4, 58, 108).

[6] W. H. Zurek. "Decoherence, einselection, and the quantum origins of the classical". *Reviews of Modern Physics* 75.3 (May 2003), pp. 715–775 (cit. on p. 2).

[7] W. H. Zurek. "Decoherence and the transition from quantum to classical". *Phys. Today* 44N10 (1991), pp. 36–44 (cit. on p. 2).

[8] M. Kjaergaard et al. "Superconducting Qubits: Current State of Play". *Annual Review of Condensed Matter Physics* 11.1 (Mar. 2020), pp. 369–395 (cit. on pp. 3, 25, 36, 66).

[9] C. D. Bruzewicz et al. "Trapped-ion quantum computing: Progress and challenges". *Applied Physics Reviews* 6.2 (June 2019), p. 021314 (cit. on pp. 3, 36).

[10] D. Aharonov and M. Ben-Or. "Fault-Tolerant Quantum Computation with Constant Error". *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*. New York, NY, USA: Association for Computing Machinery, 1997, pp. 176–188 (cit. on p. 3).

[11] P. W. Shor. "Fault-Tolerant Quantum Computation". *Proceedings of the 37th Annual Symposium on Foundations of Computer Science*. USA: IEEE Computer Society, 1996, p. 56 (cit. on p. 3).

[12] D. Gottesman. *An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation*. 2009. arXiv: 0904.2557 [quant-ph] (cit. on p. 3).

[13] J. Preskill. "Quantum Computing in the NISQ era and beyond". *Quantum* 2 (Aug. 2018), p. 79 (cit. on pp. 3, 37, 109).

[14] L. K. Grover. "Quantum Mechanics Helps in Searching for a Needle in a Haystack". *Phys. Rev. Lett.* 79 (2 July 1997), pp. 325–328 (cit. on pp. 4, 24, 26, 55).

[15] I. Quantum. https://quantum-computing.ibm.com/. 2021 (cit. on p. 4).

[16] P. Walther et al. "Experimental one-way quantum computing". *Nature* 434.7030 (Mar. 2005), pp. 169–176 (cit. on pp. 4, 51, 82).

[17] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 10th. USA: Cambridge University Press, 2011 (cit. on pp. 4, 7, 9, 10, 12, 13, 14, 24, 26, 48, 58, 60, 61, 62, 63, 64, 67, 72, 101, 126).

[18] R. de Wolf. *Quantum Computing: Lecture Notes*. 2019. arXiv: 1907.09415 [quant-ph] (cit. on pp. 4, 7, 24, 26, 58, 60, 61, 63).

[19] J. Preskill. *Lecture Notes for Quantum Computation Course*. 1998. URL: http://theory.caltech.edu/~preskill/ph219/index.html#lecture (visited on 07/26/2021) (cit. on p. 4).

[20] L. K. Grover and J. Radhakrishnan. "Is partial quantum search of a database any easier?" *Proceedings of the 17th annual ACM symposium on Parallelism in algorithms and architectures - SPAA'05*. ACM Press, 2005 (cit. on pp. 4, 25, 32, 33, 55).

[21] P. Hariharan and B. Sanders. "II Quantum Phenomena in Optical Interferometry". Ed. by E. Wolf. Vol. 36. Progress in Optics. Elsevier, 1996, pp. 49–128 (cit. on p. 5).

[22] U. Skosana and M. Tame. "On the advantages of relative-phase Toffolis". *The Proceedings of SAIP2021, the 65th Annual Conference of the South African Institute of Physics*. (Accepted for publication) (cit. on p. 5).

[23] A. Peres. "Separability Criterion for Density Matrices". *Physical Review Letters* 77.8 (Aug. 1996), pp. 1413–14 (cit. on p. 16).

[24] M. B. Plenio and S. Virmani. "An introduction to entanglement measures". *Quant.Inf.Comput.7:1-51,2007* (Apr. 2005). arXiv: quant-ph/0504163 [quant-ph] (cit. on p. 16).

[25] R. Horodecki et al. "Quantum entanglement". 81.2 (June 2009), pp. 865–942 (cit. on p. 16).

[26] J. F. Clauser et al. "Proposed Experiment to Test Local Hidden-Variable Theories". *Phys. Rev. Lett.* 23 (15 Oct. 1969), pp. 880–884 (cit. on pp. 17, 82).

[27] R. Horodecki, P. Horodecki, and M. Horodecki. "Violating Bell inequality by mixed spin-12 states: necessary and sufficient condition". *Physics Letters A* 200.5 (1995), pp. 340–344 (cit. on p. 17).

[28] W. J. Munro, K. Nemoto, and A. G. White. "The bell inequality: A measure of entanglement?" *Journal of Modern Optics* 48.7 (2001), pp. 1239–1246. eprint: https://doi.org/10.1080/09500340108231766 (cit. on pp. 17, 82).

[29] N. D. Mermin. "Extreme quantum entanglement in a superposition of macroscopically distinct states". 65.15 (Oct. 1990), pp. 1838–1840 (cit. on pp. 17, 18).

[30] A. Einstein, B. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" *Phys. Rev.* 47 (10 May 1935), pp. 777–780 (cit. on p. 18).

[31] O. Gühne and G. Toth. "Entanglement detection". *Physics Reports* 474.1-6 (Apr. 2009) (cit. on p. 18).

[32] M. Horodecki, P. Horodecki, and R. Horodecki. "Separability of mixed states: necessary and sufficient conditions". 223.1-2 (Nov. 1996), pp. 1–8 (cit. on p. 18).

[33] S. Gharibian. "Strong NP-hardness of the quantum separability problem". 10.3&4 (Mar. 2010), pp. 343–360 (cit. on p. 18).

[34] L. Gurvits. "Classical deterministic complexity of Edmonds' Problem and quantum entanglement". ACM Press, 2003 (cit. on p. 18).

[35] G. Tóth and O. Gühne. "Entanglement detection in the stabilizer formalism". *Phys. Rev. A* 72 (2 Aug. 2005), p. 022340 (cit. on pp. 18, 79, 83, 103).

[36] C. M. Dawson and M. A. Nielsen. "The Solovay-Kitaev algorithm" (May 2005). arXiv: quant-ph/0505030 [quant-ph] (cit. on pp. 21, 25).

[37] P. Kok et al. "Linear optical quantum computing with photonic qubits". *Reviews of Modern Physics* 79.1 (Jan. 2007), pp. 135–174 (cit. on pp. 21, 22, 83).

[38] R. Simon and N. Mukunda. "Minimal three-component SU(2) gadget for polarization optics". *Physics Letters A* 143.4-5 (Jan. 1990), pp. 165–169 (cit. on p. 22).

[39] G. Brassard et al. *Quantum amplitude amplification and estimation*. 2002 (cit. on p. 24).

[40] M. Boyer et al. "Tight Bounds on Quantum Searching". *Fortschritte der Physik* 46.4-5 (June 1998), pp. 493–505 (cit. on pp. 24, 25, 30, 31).

[41] I. L. Chuang, N. Gershenfeld, and M. Kubinec. "Experimental Implementation of Fast Quantum Searching". *Physical Review Letters* 80.15 (Apr. 1998), pp. 3408–3411 (cit. on p. 24).

[42] K.-A. Brickman et al. "Implementation of Grover's quantum search algorithm in a scalable system". *Physical Review A* 72.5 (Nov. 2005), p. 050306 (cit. on p. 24).

[43] L. DiCarlo et al. "Demonstration of two-qubit algorithms with a superconducting quantum processor". *Nature* 460.7252 (June 2009), pp. 240–244 (cit. on p. 24).

[44] L. M. K. Vandersypen et al. "Implementation of a three-quantum-bit search algorithm". *Applied Physics Letters* 76.5 (Jan. 2000), pp. 646–648 (cit. on p. 24).

[45] C. Figgatt et al. "Complete 3-Qubit Grover search on a programmable quantum computer". *Nature Communications* 8.1 (Dec. 2017) (cit. on p. 24).

[46] C. Zalka. "Grover's quantum searching algorithm is optimal". *Physical Review A* 60.4 (Oct. 1999), pp. 2746–2751 (cit. on pp. 25, 31, 41).

[47] C. H. Bennett et al. "Strengths and Weaknesses of Quantum Computing". *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1510–1523 (cit. on pp. 25, 31).

[48] V. V. Shende and I. L. Markov. "On the CNOT-Cost of TOFFOLI Gates". *Quantum Inf. Comput.* 9.5 (2009), pp. 461–486 (cit. on pp. 25, 36, 66).

[49] V. E. Korepin and L. K. Grover. "Simple Algorithm for Partial Quantum Search". *Quantum Information Processing* 5.1 (Feb. 2006), pp. 5–10 (cit. on pp. 25, 34).

[50] V. E. Korepin. "Optimization of partial search". *Journal of Physics A: Mathematical and General* 38.44 (Oct. 2005), pp. L731–L738 (cit. on pp. 25, 34).

[51] V. E. Korepin and J. Liao. "Quest for Fast Partial Search Algorithm". *Quantum Information Processing* 5.3 (May 2006), pp. 209–226 (cit. on pp. 25, 34).

[52] V. E. Korepin and B. C. Vallilo. "Group Theoretical Formulation of a Quantum Partial Search Algorithm". *Progress of Theoretical Physics* 116.5 (Nov. 2006), pp. 783–793 (cit. on pp. 25, 34).

[53] B.-S. Choi, T. A. Walker, and S. L. Braunstein. "Sure Success Partial Search". *Quantum Information Processing* 6.1 (Nov. 2006), pp. 1–8 (cit. on pp. 25, 34).

[54] T. Satoh, Y. Ohkura, and R. Van Meter. "Subdivided Phase Oracle for NISQ Search Algorithms". *IEEE Transactions on Quantum Engineering* 1 (2020), pp. 1–15 (cit. on pp. 26, 43, 44, 45, 46, 47, 48, 49, 50, 56, 108, 109).

[55] K. Zhang and V. E. Korepin. "Depth optimization of quantum search algorithms beyond Grover 's algorithm". en. *Physical Review A* 101.3 (Mar. 2020), p. 032346 (cit. on pp. 26, 37, 38, 39, 40, 42, 43, 55, 56, 109).

[56] Y. Wang and P. S. Krstic. "Prospect of using Grover's search in the noisy-intermediate-scale quantum-computer era". en. *Phys. Rev. A* 102.4 (Oct. 2020). arXiv: 2006.10037, p. 042609 (cit. on pp. 26, 41, 42, 43).

[57] J. Gwinner et al. "Benchmarking 16-element quantum search algorithms on superconducting quantum processors" (July 2020). arXiv: 2007.06539 [quant-ph] (cit. on pp. 26, 42, 43, 49, 53, 56, 70, 109).

[58] M. Briański et al. "Introducing structure to expedite quantum searching". *Physical Review A* 103.6 (June 2021), p. 062425 (cit. on p. 26).

[59] K. Zhang et al. "Implementation of efficient quantum search algorithms on NISQ computers". *Quantum Information Processing* 20.7 (July 2021) (cit. on pp. 26, 43, 49, 56, 70).

[60] R. M. Gingrich, C. P. Williams, and N. J. Cerf. "Generalized quantum search with parallelism". *Physical Review A* 61.5 (Apr. 2000), p. 052313 (cit. on p. 30).

[61] L. K. Grover. "How fast can a quantum computer search?" (Sept. 1998). arXiv: quant-ph/9809029 [quant-ph] (cit. on p. 31).

[62] K. Zhang and V. Korepin. "Quantum partial search for uneven distribution of multiple target items". *Quantum Information Processing* 17.6 (Apr. 2018) (cit. on p. 32).

[63] B.-S. Choi and V. E. Korepin. "Quantum Partial Search of a Database with Several Target Items". *Quantum Information Processing* 6.4 (Aug. 2007), pp. 243–254 (cit. on p. 32).

[64] N. Yu, R. Duan, and M. Ying. "Five two-qubit gates are necessary for implementing the Toffoli gate". en. *Phys. Rev. A* 88.1 (July 2013), p. 010304 (cit. on pp. 36, 66).

[65] Y. He et al. "Decompositions of n-qubit Toffoli Gates with Linear Circuit Complexity". *Int J Theor Phys* 56.7 (July 2017), pp. 2350–2361 (cit. on pp. 36, 37, 42).

[66] A. Barenco et al. "Elementary gates for quantum computation". *Phys. Rev. A* 52.5 (Nov. 1995), pp. 3457–3467 (cit. on pp. 42, 66).

[67] N. Margolus. "Simple quantum gates". *Unpublished manuscript (circa 1994)* (1994) (cit. on pp. 42, 70).

[68] A. Peruzzo et al. "A variational eigenvalue solver on a photonic quantum processor". *Nature Communications* 5.1 (July 2014) (cit. on pp. 50, 56).

[69] E. Farhi, J. Goldstone, and S. Gutmann. *A Quantum Approximate Optimization Algorithm*. 2014. arXiv: 1411.4028 [quant-ph] (cit. on pp. 50, 56).

[70] M. E. S. Morales, T. Tlyachev, and J. Biamonte. "Variational learning of Grover's quantum search algorithm". *Physical Review A* 98.6 (Dec. 2018), p. 062333 (cit. on pp. 51, 56).

[71] S. Barz et al. "Demonstration of Blind Quantum Computing". *Science* 335.6066 (Jan. 2012), pp. 303–308 (cit. on p. 51).

[72] K. Chen et al. "Experimental Realization of One-Way Quantum Computing with Two-Photon Four-Qubit Cluster States". *Physical Review Letters* 99.12 (Sept. 2007) (cit. on pp. 51, 82, 96, 97, 106).

[73] R. Prevedel et al. "High-speed linear optics quantum computing using active feed-forward". *Nature* 445.7123 (Jan. 2007), pp. 65–69 (cit. on pp. 51, 82).

[74] D. Browne and H. Briegel. "One-way Quantum Computation". *Quantum Information: From Foundations to Quantum Technology Applications* (2016), pp. 449–473 (cit. on pp. 51, 52, 57).

[75] M. A. Nielsen. "Cluster-state quantum computation". *Reports on Mathematical Physics* 57.1 (Feb. 2006), pp. 147–161 (cit. on p. 51).

[76] R. Jozsa. "An introduction to measurement based quantum computation" (Aug. 2005). arXiv: quant-ph/0508124 [quant-ph] (cit. on p. 51).

[77] M. Hein, J. Eisert, and H. J. Briegel. "Multiparty entanglement in graph states". 69.6 (June 2004), p. 062311 (cit. on pp. 52, 83, 104, 119).

[78] M. V. den Nest, J. Dehaene, and B. D. Moor. "Graphical description of the action of local Clifford transformations on graph states". 69.2 (Feb. 2004), p. 022316 (cit. on pp. 52, 104, 119).

[79] M. S. Tame et al. "Compact Toffoli gate using weighted graph states". *Physical Review A* 79.2 (2009) (cit. on p. 56).

[80] U. Skosana and M. Tame. "Demonstration of Shor's factoring algorithm for N=21 on IBM quantum processors". *Scientific Reports* 11.1 (Aug. 2021) (cit. on pp. 58, 108, 109).

[81] L. M. K. Vandersypen et al. "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance". *Nature* 414.6866 (Dec. 2001), pp. 883–887 (cit. on pp. 58, 67, 82).

[82] X. Peng et al. "Quantum Adiabatic Algorithm for Factorization and Its Experimental Implementation". 101.22 (Nov. 2008), p. 220405 (cit. on p. 58).

[83] G. Vidal. "Efficient Classical Simulation of Slightly Entangled Quantum Computations". 91.14 (Oct. 2003), p. 147902 (cit. on pp. 58, 75).

[84] C.-Y. Lu et al. "Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits". *Phys. Rev. Lett.* 99 (25 Dec. 2007), p. 250504 (cit. on pp. 58, 67, 82, 103).

[85] A. Politi, J. C. F. Matthews, and J. L. O'Brien. "Shor's Quantum Factoring Algorithm on a Photonic Chip". *Science* 325.5945 (Sept. 2009), pp. 1221–1221 (cit. on pp. 58, 67).

[86] B. P. Lanyon et al. "Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement". *Phys. Rev. Lett.* 99 (25 Dec. 2007), p. 250505 (cit. on pp. 58, 67, 82).

[87] E. Lucero et al. "Computing prime factors with a Josephson phase qubit quantum processor". 8.10 (Aug. 2012), pp. 719–723 (cit. on pp. 58, 67).

[88] E. Martín-López et al. "Experimental realization of Shor's quantum factoring algorithm using qubit recycling". *Nature Photonics* 6.11 (Oct. 2012), pp. 773–776 (cit. on pp. 59, 67, 69, 74, 79, 82, 108, 109).

[89] R. B. Griffiths and C.-S. Niu. "Semiclassical Fourier Transform for Quantum Computation". 76.17 (Apr. 1996), pp. 3228–3231 (cit. on pp. 59, 67).

[90] M. Amico, Z. H. Saleem, and M. Kumph. "Experimental study of Shor's factoring algorithm using the IBM Q Experience". *Phys. Rev. A* 100 (1 July 2019), p. 012305 (cit. on pp. 59, 109).

[91] S. Pal et al. "Hybrid scheme for factorisation: Factoring 551 using a 3-qubit NMR quantum adiabatic processor". 92.2 (Jan. 2019) (cit. on p. 59).

[92] N. Xu et al. "Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System". 108.13 (Mar. 2012), p. 130501 (cit. on p. 59).

[93] A. Saxena, A. Shukla, and A. Pathak. "A hybrid scheme for prime factorization and its experimental implementation using IBM quantum processor". 20.3 (Mar. 2021) (cit. on p. 59).

[94] S. Parker and M. B. Plenio. "Efficient Factorization with a Single Pure Qubit andlogNMixed Qubits". 85.14 (Oct. 2000), pp. 3049–3052 (cit. on pp. 59, 67).

[95] S. Beauregard. "Circuit for Shor's Algorithm Using 2n+3 Qubits". *Quantum Info. Comput.* 3.2 (Mar. 2003), pp. 175–185 (cit. on pp. 59, 66).

[96] A. Y. Kitaev. "Quantum measurements and the Abelian Stabilizer Problem" (Nov. 1995). arXiv: quant-ph/9511026 [quant-ph] (cit. on p. 61).

[97] R. Cleve et al. "Quantum algorithms revisited". 454.1969 (Jan. 1998), pp. 339–354 (cit. on pp. 61, 63, 64).

[98] V. Vedral, A. Barenco, and A. Ekert. "Quantum networks for elementary arithmetic operations". 54.1 (July 1996), pp. 147–153 (cit. on p. 66).

[99] D. Beckman et al. "Efficient networks for quantum factoring". 54.2 (Aug. 1996), pp. 1034–1063 (cit. on pp. 66, 68).

[100] C. Zalka. "Fast versions of Shor's quantum factoring algorithm" (June 1998). arXiv: quant-ph/9806084 [quant-ph] (cit. on p. 66).

[101] T. Lawson. "Odd orders in Shor's factoring algorithm". *Quantum Information Processing* 14.3 (Jan. 2015), pp. 831–838 (cit. on p. 67).

[102] G. Song and A. Klappenecker. 2003. arXiv: quant-ph/0312225 [quant-ph] (cit. on p. 70).

[103] D. Maslov. "Advantages of using relative-phase Toffoli gates with an application to multiple control Toffoli optimization". *Phys. Rev. A* 93 (2 Feb. 2016), p. 022311 (cit. on pp. 70, 80).

[104] R. Jozsa and N. Linden. "On the role of entanglement in quantum-computational speed-up". 459.2036 (Aug. 2003), pp. 2011–2032 (cit. on p. 75).

[105] S. L. Braunstein et al. "Separability of Very Noisy Mixed States and Implications for NMR Quantum Computing". 83.5 (Aug. 1999), pp. 1054–1057 (cit. on p. 75).

[106] M. Bourennane et al. "Experimental Detection of Multipartite Entanglement using Witness Operators". 92.8 (Feb. 2004), p. 087902 (cit. on p. 75).

[107] G. Tóth. "QUBIT4MATLAB V3.0: A program package for quantum information science and quantum optics for MATLAB". *Comput. Phys. Commun.* 179.6 (2008), pp. 430–437 (cit. on pp. 75, 76, 125).

[108] D. Gross et al. "Quantum State Tomography via Compressed Sensing". 105.15 (Oct. 2010), p. 150401 (cit. on p. 79).

[109] H.-Y. Huang, R. Kueng, and J. Preskill. "Predicting many properties of a quantum system from very few measurements". 16.10 (June 2020), pp. 1050–1057 (cit. on p. 79).

[110] S. T. Flammia and Y.-K. Liu. "Direct Fidelity Estimation from Few Pauli Measurements". 106.23 (June 2011), p. 230501 (cit. on p. 79).

[111] F. Baccari et al. "Efficient Device-Independent Entanglement Detection for Multipartite Systems". 7.2 (June 2017), p. 021042 (cit. on p. 79).

[112] L. Knips et al. "Multipartite Entanglement Detection with Minimal Effort". 117.21 (Nov. 2016), p. 210504 (cit. on p. 79).

[113] K. Banaszek, M. Cramer, and D. Gross. "Focus on quantum tomography". *New Journal of Physics* 15.12 (Dec. 2013), p. 125020 (cit. on p. 79).

[114] A. Barenco et al. "Approximate Quantum Fourier Transform and Decoherence". *Phys. Rev. A* 54.1 (July 1996), pp. 139–146 (cit. on p. 80).

[115] D. Coppersmith. "An approximate Fourier transform useful in quantum factoring" (Jan. 2002). arXiv: quant-ph/0201067 [quant-ph] (cit. on p. 80).

[116] H. S. Park et al. "Two-photon four-qubit cluster state generation based on a polarization-entangled photon pair". *Opt. Express* 15.26 (Dec. 2007), pp. 17960–17966 (cit. on pp. 82, 97, 103, 106, 109).

[117] Y. Tokunaga et al. "Generation of High-Fidelity Four-Photon Cluster State and Quantum-Domain Demonstration of One-Way Quantum Computing". *Physical Review Letters* 100.21 (May 2008) (cit. on p. 82).

[118] N. Kiesel et al. "Experimental Analysis of a Four-Qubit Photon Cluster State". *Physical Review Letters* 95.21 (Nov. 2005) (cit. on p. 82).

[119] C.-Y. Lu et al. "Experimental entanglement of six photons in graph states". *Nature Physics* 3.2 (Jan. 2007), pp. 91–95 (cit. on pp. 82, 83, 94).

[120] G. Vallone et al. "One-way quantum computation via manipulation of polarization and momentum qubits in two-photon cluster states". *Laser Physics Letters* 5.5 (May 2008), pp. 398–403 (cit. on p. 82).

[121] B. A. Bell et al. "Experimental demonstration of graph-state quantum secret sharing". *Nature Communications* 5.1 (Nov. 2014) (cit. on p. 82).

[122] S. Gaertner et al. "Experimental Demonstration of a Quantum Protocol for Byzantine Agreement and Liar Detection". *Phys. Rev. Lett.* 100 (7 Feb. 2008), p. 070504 (cit. on p. 82).

[123] N. Kiesel et al. "Experimental Observation of Four-Photon Entangled Dicke State with High Fidelity". *Phys. Rev. Lett.* 98 (6 Feb. 2007), p. 063604 (cit. on p. 82).

[124] C. Schmid et al. "Experimental implementation of a four-player quantum game". 12.6 (June 2010), p. 063031 (cit. on pp. 82, 106).

[125] P. G. Kwiat et al. "New High-Intensity Source of Polarization-Entangled Photon Pairs". *Phys. Rev. Lett.* 75 (24 Dec. 1995), pp. 4337–4341 (cit. on p. 82).

[126] P. G. Kwiat et al. "Ultrabright source of polarization-entangled photons". *Physical Review A* 60.2 (Aug. 1999), R773–R776 (cit. on pp. 82, 84, 87, 94).

[127] D. M. Greenberger, M. A. Horne, and A. Zeilinger. *Going Beyond Bell's Theorem*. 2007. arXiv: 0712.0921 [quant-ph] (cit. on p. 82).

[128] J. S. Bell. "On the Einstein Podolsky Rosen paradox". *Physics Physique Fizika* 1 (3 Nov. 1964), pp. 195–200 (cit. on p. 82).

[129] D. F. V. James et al. "Measurement of qubits". *Phys. Rev. A* 64 (5 Oct. 2001), p. 052312 (cit. on pp. 83, 84, 86).

[130] Z. Hradil. "Quantum-state estimation". *Phys. Rev. A* 55 (3 Mar. 1997), R1561–R1564 (cit. on p. 83).

[131] R. Raussendorf, D. E. Browne, and H. J. Briegel. "Measurement-based quantum computation on cluster states". *Physical Review A* 68.2 (Aug. 2003) (cit. on p. 83).

[132] K. J. Resch, P. Walther, and A. Zeilinger. "Full Characterization of a Three-Photon Greenberger-Horne-Zeilinger State Using Quantum State Tomography". *Physical Review Letters* 94.7 (Feb. 2005) (cit. on p. 83).

[133] J. Fulconis et al. "Quantum interference with photon pairs using two micro-structured fibres". 9.8 (Aug. 2007), pp. 276–276 (cit. on p. 84).

[134] H. Weinfurter and M. Żukowski. "Four-photon entanglement from down-conversion". *Phys. Rev. A* 64 (1 June 2001), p. 010102 (cit. on p. 84).

[135] D. Branning, S. Bhandari, and M. Beck. "Low-cost coincidence-counting electronics for undergraduate quantum optics". *American Journal of Physics* 77.7 (2009), pp. 667–670. eprint: https://doi.org/10.1119/1.3116803 (cit. on p. 85).

[136] G. M. Akselrod et al. "Phase-compensated ultra-bright source of entangled photons: erratum". 15.8 (2007), p. 5260 (cit. on pp. 90, 93, 94).

[137] G. M. Akselrod et al. "Phase-compensated ultra-bright source of entangled photons: erratum". 15.8 (2007), p. 5260 (cit. on pp. 90, 93).

[138] R. Rangarajan, M. Goggin, and P. Kwiat. "Optimizing type-I polarization-entangled photons". 17.21 (Sept. 2009), p. 18920 (cit. on pp. 90, 92, 93, 94).

[139] S.-Y. Baek and Y.-H. Kim. "Spectral properties of entangled photon pairs generated via frequency-degenerate type-I spontaneous parametric down-conversion". *Phys. Rev. A* 77 (4 Apr. 2008), p. 043807 (cit. on pp. 90, 91).

[140] Y.-F. Huang et al. "Experimental generation of an eight-photon Greenberger–Horne–Zeilinger state". 2.1 (Sept. 2011) (cit. on p. 94).

[141] X.-L. Wang et al. "Experimental Ten-Photon Entanglement". 117.21 (Nov. 2016), p. 210502 (cit. on p. 94).

[142] J. G. Rarity and P. R. Tapster. "Experimental violation of Bell's inequality based on phase and momentum". *Phys. Rev. Lett.* 64 (21 May 1990), pp. 2495–2498 (cit. on p. 94).

[143] P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao. "High-visibility interference in a Bell-inequality experiment for energy and time". *Phys. Rev. A* 47 (4 Apr. 1993), R2472–R2475 (cit. on p. 94).

[144] A. Vaziri, G. Weihs, and A. Zeilinger. "Experimental Two-Photon, Three-Dimensional Entanglement for Quantum Communication". 89.24 (Nov. 2002), p. 240401 (cit. on p. 95).

[145] A. Mair et al. "Entanglement of the orbital angular momentum states of photons". 412.6844 (July 2001), pp. 313–316 (cit. on p. 95).

[146] S. Franke-Arnold et al. "Two-photon entanglement of orbital angular momentum states". *Phys. Rev. A* 65 (3 Feb. 2002), p. 033823 (cit. on p. 95).

[147] L. Allen et al. "Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes". *Phys. Rev. A* 45 (11 June 1992), pp. 8185–8189 (cit. on p. 95).

[148] P. G. Kwiat. "Hyper-entangled states". *Journal of Modern Optics* 44.11-12 (1997), pp. 2173–2184. eprint: https://www.tandfonline.com/doi/pdf/10.1080/09500349708231877 (cit. on p. 95).

[149] N. K. Langford. "Encoding, manipulating and measuring quantumnm information in optics". PhD thesis. School of Physicsal Sciences, 2007 (cit. on p. 96).

[150] T. Yang et al. "All-Versus-Nothing Violation of Local Realism by Two-Photon, Four-Dimensional Entanglement". 95.24 (Dec. 2005), p. 240406 (cit. on pp. 96, 97).

[151] S. Carrasco et al. "Spectral engineering of entangled two-photon states". 73.6 (June 2006), p. 063802 (cit. on p. 97).

[152] H. Abraham et al. *Qiskit: An Open-source Framework for Quantum Computing*. 2019 (cit. on p. 112).

[153] J. A. Smolin, J. M. Gambetta, and G. Smith. "Efficient Method for Computing the Maximum-Likelihood Quantum State from Measurements with Additive Gaussian Noise". 108.7 (Feb. 2012), p. 070502 (cit. on p. 113).

[154] Qiskit. *Learn quantum computing using Qiskit*. Available at https://qiskit.org/textbook/ch-quantum-hardware/measurement-error-mitigation.html (2019) (cit. on p. 113).

[155] B. Efron. "Bootstrap Methods: Another Look at the Jackknife". *Ann. Statist.* 7.1 (Jan. 1979), pp. 1–26 (cit. on p. 114).

[156] B. Efron. *The Jackknife, the bootstrap and other resampling plans*. CBMS-NSF Reg. Conf. Ser. Appl. Math. Lectures given at Bowling Green State Univ., June 1980. Philadelphia, PA: SIAM, 1982 (cit. on p. 114).

[157] A. Bouchet. "Recognizing locally equivalent graphs". *Discrete Mathematics* 114.1-3 (Apr. 1993), pp. 75–86 (cit. on p. 120).

[158] M. Soeken, D. M. Miller, and R. Drechsler. "On quantum circuits employing roots of the Pauli matrices". *Phys. Rev. A 88, 042322 (2013)* (Aug. 2013). arXiv: 1308.2493 [quant-ph] (cit. on p. 121).

[159] Sammorley-Short. *sammorley-short/gsc: v2.0*. 2019 (cit. on p. 122).

[160] J. C. Adcock et al. "Mapping graph state orbits under local complementation". *Quantum* 4 (Aug. 2020), p. 305 (cit. on p. 122).

[161] Thorlabs. *Thorlabs APT Controllers Host-Controller Communications Protocol*. https://www.thorlabs.com/software/apt/APT_Communications_Protocol_Rev_15.pdf. Accessed: 08-11-2021 (cit. on p. 128).

[162] Yet Another AcQuisition. *thorlabs-apt-protocol*. Version 25.2.0. Aug. 11, 2021 (cit. on p. 128).

[163] Pallets Projects. *Flask*. Version 2.0.2. Aug. 11, 2021 (cit. on p. 129).

[164] A. Shreve. *Ngrok*. Version 43. Aug. 11, 2021 (cit. on p. 129).

[165] The Expo Team. *Expo SDK*. Version 43. Aug. 11, 2021 (cit. on p. 129).

[166] S. Slussarenko and G. J. Pryde. "Photonic quantum information processing: A concise review". *Applied Physics Reviews* 6.4 (2019), p. 041303. eprint: https://doi.org/10.1063/1.5115814.

[167] M. A. Nielsen. "A simple formula for the average gate fidelity of a quantum dynamical operation". *Physics Letters A* 303.4 (Oct. 2002), pp. 249–252.

[168] E. Magesan, R. Blume-Kohout, and J. Emerson. "Gate fidelity fluctuations and quantum process invariants". *Physical Review A* 84.1 (July 2011).

[169] M. Barbieri et al. "Enhancing the Violation of the Einstein-Podolsky-Rosen Local Realism by Quantum Hyperentanglement". *Physical Review Letters* 97.14 (Oct. 2006).

[170] A. G. White et al. "Nonmaximally Entangled States: Production, Characterization, and Utilization". *Physical Review Letters* 83.16 (Oct. 1999), pp. 3103–3107.

[171] C. H. Bennett et al. "Mixed-state entanglement and quantum error correction". *Phys. Rev. A* 54 (5 Nov. 1996), pp. 3824–3851.

[172] Y. Shi. "Both Toffoli and Controlled-NOT need little help to do universal quantum computation" (May 2002). arXiv: quant-ph/0205115 [quant-ph].