Efficient Qudit Based Scheme for Photonic Quantum Computing

Master's Thesis

Supervisor
László Oroszlány
Dept. of Physics of Complex Systems,
Eötvös Loránd University

Co-Supervisor
Zoltán Zimborás
Wigner Research Centre for Physics

Author
Márton Karácsony
Physics MSc,
Eötvös Loránd University

ELTE
EÖTVÖS LORÁND
UNIVERSITY

Budapest, 2023

STATEMENT

Name: Márton Karácsony
Neptun ID: W9AVVJ

ELTE Faculty of Science: Physics MSc

specialization: Research Physicist Specialization

Title of diploma work: Efficient Qudit Based Scheme for Photonic Quantum Computing

As the author of the diploma work, I declare, with disciplinary responsibility that my thesis is my own intellectual product and the result of my own work. Furthermore, I declare that I have consistently applied the standard rules of references and citations.

I acknowledge that the following cases are considered plagiarism:
– using a literal quotation without quotation mark and adding citation;
– referencing content without citing the source;
– representing another person's published thoughts as my own thoughts.

Furthermore, I declare that the printed and electronical versions of the submitted diploma work are textually and contextually identical.

Budapest, 2023

Signature of Student

Abstract

Quantum information processing technologies aim to revolutionize the way we communicate, encrypt information and simulate physics. Optical processing of quantum information is one of the most established and promising technologies for the realization of quantum computation due to advancements in integrated photonics in the last decade. In this context, usually qubit based single-photon encodings are considered, however, photonic systems also naturally allow for qudit based information processing. This thesis investigates multi-rail qudits defined by the possible photon number states of a single photon in $d > 2$ optical modes, provides a numerical method for constructing many-qudit gates using linear optics and photon number resolving detectors and explores the use of qudit cluster states for solving d-ary combinatorial optimization problems. The resource advantage of the multi-rail qudit encoding over the dual-rail qubit encoding is demonstrated on the k-coloring problem.

Acknowledgements

I would like to thank my supervisors László Oroszlány and Zoltán Zimborás for their invaluable help and advice. And I am deeply grateful to my parents for their support during my studies.

Disclaimer This thesis is based on a previously submitted manuscript written by the author of this thesis titled: Márton Karácsony, László Oroszlány, and Zoltán Zimborás. "Efficient qudit based scheme for photonic quantum computing". arXiv:2302.07357, 2023.

Funding The author thanks the National Research, Development, and Innovation Office of Hungary for support via the Quantum Information National Laboratory grants 2022-2.1.1-NL-00004.

Contents

Chapter 1

Introduction

Classical computers are an integral part of modern scientific research and currently they are the best tools to study large and complex physical systems. However, even the exact simulation of few-body quantum mechanics is out of reach using classical computing, only quantum mechanical systems with a small number of degrees of freedom can be simulated exactly.

The fundamental limitations of classical information processing regarding the simulation of quantum systems were already evident in the early days of scientific computing, and for this reason, Richard Feynman proposed a new type of computer, the quantum computer [1]. The computer he proposed was a universal quantum simulator, a quantum system over which its user has great control and thus could imitate any other quantum system by evolving the simulator in the same manner as the system of interest would evolve.

Feynman proposed the quantum computer to simulate physics, but soon other computational problems were discovered, which could be solved more efficiently on quantum computers than on classical ones. The most famous example of such a problem is the factorization of integers. Currently no classical algorithm is known which could factorize integers in polynomial time. It is believed that no polynomial algorithm exists to solve this problem, so much so, that we rely on this property of integers to keep our sensitive information secret.

Although there is no known classical polynomial time algorithm for integer factorization, there is a quantum polynomial time algorithm discovered by Peter Shor [2]. Shor's algorithm is exponentially faster than the best classical algorithm we have for integer factorization. This means, that with a sufficiently large quantum computer it would be possible to break the RSA 2048-bit encryption within days [3].

While there are many problems where it is possible to achieve superpolynomial or polynomial speed up over classical algorithms using quantum computers, they are not a

replacement for classical computers, but tools to solve specific computational problems.

Due to the premise of quantum computing, the development of quantum computers and quantum algorithms has been an active research area for the last few decades, and huge investments have been made into this area of research by industry leading companies and governments. Because of this effort, many quantum computer architectures have been invented and experimentally realized, e.g., superconducting and photonic quantum computers. Furthermore, several milestones have been reached towards quantum supremacy [4–7] and fault-tolerance [8–10], however, despite the successes and breakthroughs, a scalable and fault-tolerant architecture is yet to be built.

Currently every architecture has its benefits and disadvantages, and there is no clear winner amongst the proposed designs, i.e., it is difficult to say which design idea, if any of them, will eventually develop into a useful quantum computer. The design goals that every architecture should aim for were summarized by David DiVincenzo [11] in five points:

1. A scalable physical system with well characterized qubits or qudits.
2. The ability to initialize the state of the qubits into a simple state.
3. Long relevant decoherence times.
4. A universal set of quantum gates.
5. A qubit-specific measurement capability.

All the points above were addressed by physical implementations, but currently there is no realization of a quantum computer which satisfies them simultaneously. For example, most superconducting devices satisfy the second, fourth and fifth points, but scalability and decoherence is an issue for them, while integrated photonic devices [12] are more scalable and lack the same kind of decoherence phenomena, but realizing a universal gate set is difficult with photonics due to the absence of interaction between photons.

Photonic quantum computation is one of the most established and promising ways to do quantum information processing. In recent years, many advancements have been made in integrated photonic quantum technologies. Integrated quantum photonic processors with on-chip linear optics [13, 14], single photon sources [15–17] and photon number resolving detectors (PNRD) [18–21] have been demonstrated. These integrated components and waveguides are usually printed onto silica, which makes it possible to miniaturize the chips and increase the number of on-chip components. Since photons couple very weakly to their environment, integrated quantum photonic processors typically do not require millikelvin temperatures to operate as opposed to other quantum information processing architectures like superconducting devices [22].

There has been considerable experimental progress towards photonic quantum supremacy via boson sampling (see, for example, Refs. [5–7]), however, the realization of universal photonic quantum computation still seems far from reality. This is because linear optics alone cannot be used to produce certain multi-photon states which are required in some form by all universal photonic schemes.

The most well-known universal photonic scheme is the KLM scheme [23] which solves the problem of creating entanglement between photonic qubits by applying post-selection based on ancilla measurements. This makes it possible to prepare entangled two qubit states non-deterministically using only linear optics and PNRDs. This measurement-based method combined with the quantum teleportation of qubits was shown to be able to create near-deterministic two qubit gates. However, the complete implementation of the KLM scheme proved to be out of reach with current technology, and only some of its techniques have been demonstrated experimentally.

Another approach for realizing universal quantum computation is to use measurement-based quantum computation (MBQC) [24]. In MBQC the quantum algorithms are performed by making single-qubit measurements on a large, entangled state, usually a cluster state [25, 26]. For photonics MBQC provides a resource efficient and deterministic way to implement universal quantum computation.

Encoding information in single-photon states has the advantage, that beyond photon loss due to light-matter interactions, there is no decoherence. The generation [27, 28] and detection [29] of single-photon states is possible with high fidelity and efficiency, thus single-photon information protocols are close to becoming viable.

Usually single-photon states are used to encode two-level systems, however, they can also encode $d > 2$ level systems called qudits [30]. Qudits have been considered in many areas of quantum computation, for example in topological quantum computation the braiding of $\mathbb{Z}_d$ parafermions [31] provides a natural way to implement qudits [32]. There also have been attempts to realize superconducting qudits [33, 34], but because of the flexibility in how photon states can be interpreted, qudits are most prominent in photonics [35–40]. The use of qudits increases the number of dimensions per computation unit. This property of qudits in theory can provide some benefits over qubit systems by reducing circuit complexity of quantum algorithms or by increasing the channel capacity and noise tolerance of communication protocols [41, 42].

This thesis aims to discuss and answer questions related to single-photon encoded multi-rail qudits and explore the possible resource benefits of using them. The two main topics of this thesis are the construction of entangling many-qudit gates and solving d-ary combinatorial optimization problems using qudit clusters states.

The construction of entangling gates is necessary for universal quantum computa-

tion, however, entangling qubits or qudits encoded by photons is difficult because of the absence of photon-photon interaction. In experiments either matter mediated interactions, e.g., the cross Kerr effect [43], or a measurement induced nonlinearity is used to create entanglement between photonic qubits. The latter method only requires linear optics and PNRDs to implement and can also be used to entangle photonic qudits. In Sec. 4.2 a method is presented for calculating interferometer configurations for locally optimal non-deterministic many-qudit gates.

As for the other topic of this thesis, d-ary combinatorial optimization problems come up in many areas of study, e.g., in biology [44] and in graph theory. It is conjectured that the Quantum Approximate Optimization Algorithm (QAOA) [45] can perform better than classical algorithms solving combinatorial optimization problems. One of the most famous examples of combinatorial optimization problems is the k-coloring problem. The k-coloring problem has important applications in scheduling [46] and compiler theory [47]. In Sec. 4.3 a qudit cluster state implementation of the QAOA is presented to solve the k-coloring problem, and in that context, the resource benefit of the multi-rail qudit encoding is demonstrated.

Chapter 2

Review of Quantum Optics

In this chapter the basic physical concepts of quantum optics are reviewed which are fundamental to photonic quantum information processing. Sometimes the term quantum optics is used, when the electromagnetic field itself is not quantized, but treated as an external classical field which perturbs some other quantum system. This approximation is often enough to explain the observed phenomena, however, to explain photon number states and other highly non-classical effects needed for quantum information protocols, one needs to quantize the radiation field.

2.1 Quantization of the Electromagnetic Field

Maxwell's equations in vacuum in the absence of sources are

$$\nabla \cdot \mathbf{E} = 0, \qquad \nabla \cdot \mathbf{B} = 0, \tag{2.1}$$

$$\nabla \times \mathbf{E} = -\partial_t \mathbf{B}, \qquad \nabla \times \mathbf{B} = \frac{1}{c^2}\partial_t \mathbf{E}, \tag{2.2}$$

which can be rewritten in terms of the vector and scalar potentials $\mathbf{A}$ and ϕ,

$$-\triangle\phi - \partial_t \nabla \cdot \mathbf{A} = 0 \tag{2.3}$$

$$\nabla(\nabla \cdot \mathbf{A}) - \triangle\mathbf{A} = \frac{1}{c^2}\left(\partial_t \nabla\phi - \partial_t^2 \mathbf{A}\right), \tag{2.4}$$

by using the identities

$$\mathbf{E} = -\nabla\phi - \partial_t \mathbf{A}, \qquad \mathbf{B} = \nabla \times \mathbf{A}. \tag{2.5}$$

The equations above do not completely define the potentials, there is an extra gauge freedom present. Choosing the Coulomb gauge $\nabla \cdot \mathbf{A} = 0$, simplifies the equations

considerably:

$$\triangle\phi = 0, \qquad -\triangle\mathbf{A} = \frac{1}{c^2}\left(\partial_t \nabla\phi - \partial_t^2\mathbf{A}\right). \tag{2.6}$$

Additionally, in the Coulomb gauge one can set ϕ equal to zero everywhere, then the equations of motion are simply

$$\left[\frac{1}{c^2}\partial_t^2 - \triangle\right]\mathbf{A} = 0. \tag{2.7}$$

Equation (2.7) can be solved with many different boundary conditions. The boundary conditions are usually dictated by the exact physical system, but in many cases the region of interest is far away from the boundary, thus, the choice of boundary conditions does not affect the results of the calculations. For this reason, the rest of the calculations are done in a periodic box with side lengths L and volume $V = L^3$.

Given periodic boundary conditions, the general real solution of Eq. (2.7) is

$$\tilde{\mathbf{A}}(\mathbf{x}, t) = \frac{1}{\sqrt{V}}\sum_{\mathbf{k}}\sum_{\lambda=1}^{3}\boldsymbol{\epsilon}_\lambda(\mathbf{k})A_\lambda(\mathbf{k})e^{i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)} + \boldsymbol{\epsilon}_\lambda^*(\mathbf{k})A_\lambda^*(\mathbf{k})e^{-i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)}, \tag{2.8}$$

where $\mathbf{k} \in \left\{\frac{2\pi}{L}\mathbf{n} \mid \mathbf{n} \in \mathbb{Z}^3\right\}$, $A_\lambda(\mathbf{k})$ are complex amplitudes, $\omega_k = c|\mathbf{k}|$, $\boldsymbol{\epsilon}_\lambda(\mathbf{k})$ for $\lambda \in \{1, 2\}$ are the transversal polarizations and $\boldsymbol{\epsilon}_3(\mathbf{k})$ is the longitudinal polarization vector. However, the vector potential must also satisfy the gauge condition $\nabla \cdot \mathbf{A} = 0$. The gauge condition implies that $\boldsymbol{\epsilon}_\lambda(\mathbf{k}) \cdot \mathbf{k} = 0$, i.e., only transversal polarizations are allowed. Thus, the vector potential takes the following form:

$$\mathbf{A}(\mathbf{x}, t) = \frac{1}{\sqrt{V}}\sum_{\mathbf{k}}\sum_{\lambda=1,2}\boldsymbol{\epsilon}_\lambda(\mathbf{k})A_\lambda(\mathbf{k})e^{i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)} + \boldsymbol{\epsilon}_\lambda^*(\mathbf{k})A_\lambda^*(\mathbf{k})e^{-i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)}, \tag{2.9}$$

where $\boldsymbol{\epsilon}_\lambda(\mathbf{k})$ are polarization vectors perpendicular to the wave vector $\mathbf{k}$ and they are orthogonal to each other $\boldsymbol{\epsilon}_\lambda^*(\mathbf{k}) \cdot \boldsymbol{\epsilon}_{\lambda'}(\mathbf{k}) = \delta_{\lambda\lambda'}$.

The Lagrangian density of the electromagnetic field in the Coulomb gauge is

$$\mathscr{L} = \frac{1}{2}\epsilon_0|\mathbf{E}|^2 - \frac{1}{2\mu_0}|\mathbf{B}|^2 = \frac{1}{2}\epsilon_0|\partial_t\mathbf{A}|^2 - \frac{1}{2\mu_0}|\nabla\times\mathbf{A}|^2 = \frac{1}{2}\epsilon_0|\partial_t\mathbf{A}|^2 - \frac{1}{2\mu_0}\triangle|\mathbf{A}|^2, \tag{2.10}$$

where we used the identity $|\nabla\times\mathbf{A}|^2 = \triangle|\mathbf{A}|^2 - (\nabla\cdot\mathbf{A})^2 = \triangle|\mathbf{A}|^2$ when $\nabla\cdot\mathbf{A} = 0$ to derive

the last equality. Therefore, the canonical momentum is

$$\mathbf{\Pi}(\mathbf{x},t)=\epsilon_0\partial_t\mathbf{A}(\mathbf{x},t)=\frac{-i\epsilon_0}{\sqrt{V}}\sum_{\mathbf{k}}\sum_{\lambda=1,2}\omega_k\left[\boldsymbol{\epsilon}_\lambda(\mathbf{k})A_\lambda(\mathbf{k})e^{i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)}-\boldsymbol{\epsilon}^*_\lambda(\mathbf{k})A^*_\lambda(\mathbf{k})e^{-i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)}\right] \tag{2.11}$$

where ϵ_0 and μ_0 are the vacuum permittivity and permeability.

To quantize the classical theory, one can evaluate the Poisson brackets

$$\left\{A_\lambda(\mathbf{k}),A_{\lambda'}(\mathbf{k}')\right\},\qquad\left\{A_\lambda(\mathbf{k}),A^*_{\lambda'}(\mathbf{k}')\right\},\qquad\left\{A^*_\lambda(\mathbf{k}),A^*_{\lambda'}(\mathbf{k}')\right\},$$

and promote the complex amplitudes $A_\lambda(\mathbf{k})$ to operators via the quantization rule $\{U,V\}\to\frac{1}{i\hbar}\left[\hat{U},\hat{V}\right]$, where the Poisson bracket of U and V is defined as

$$\{U,V\}=\int_V d^3x\sum_{i=1}^{3}\left(\frac{\delta U}{\delta\tilde{A}_i}\frac{\delta V}{\delta\tilde{\Pi}_i}-\frac{\delta V}{\delta\tilde{\Pi}_i}\frac{\delta U}{\delta\tilde{A}_i}\right). \tag{2.12}$$

The complex amplitudes $A_\lambda(\mathbf{k})$ can be expressed either using the fields $\mathbf{A}$ and $\mathbf{\Pi}$ or using the unconstrained fields $\tilde{\mathbf{A}}$ and $\tilde{\mathbf{\Pi}}$ the following way:

$$A_\lambda(\mathbf{k})=\frac{1}{2\sqrt{V}}\int_V\boldsymbol{\epsilon}^*_\lambda(\mathbf{k})\cdot\left(\tilde{\mathbf{A}}(\mathbf{x},t)+\frac{i}{\omega_k\epsilon_0}\tilde{\mathbf{\Pi}}(\mathbf{x},t)\right)e^{-i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)}d^3x. \tag{2.13}$$

In the equation above the constrained and unconstrained fields are interchangeable. From Eq. (2.13) the Poisson brackets of the complex amplitudes are:

$$\left\{A_\lambda(\mathbf{k}),A_{\lambda'}(\mathbf{k}')\right\}=0,\quad\left\{A_\lambda(\mathbf{k}),A^*_{\lambda'}(\mathbf{k}')\right\}=\frac{-i}{2\omega_k\epsilon_0}\delta_{\mathbf{k},\mathbf{k}'}\delta_{\lambda,\lambda'},\quad\left\{A^*_\lambda(\mathbf{k}),A^*_{\lambda'}(\mathbf{k}')\right\}=0. \tag{2.14}$$

It should be noted that when deriving the Poisson brackets displayed in Eq. (2.14) using Eq. (2.12) the functional derivatives are taken with respect to the unconstrained fields $\tilde{\mathbf{A}}$ and $\tilde{\mathbf{\Pi}}$ which do not obey the Coulomb gauge condition, as opposed to $\mathbf{A}$ and $\mathbf{\Pi}$, for which $\nabla\cdot\mathbf{A}=\nabla\cdot\mathbf{\Pi}=0$ holds. This yields surprising results for the Poisson brackets of $\mathbf{A}(\mathbf{x},t)$ and $\mathbf{\Pi}(\mathbf{y},t)$

$$\left\{A_i(\mathbf{x},t),\Pi_j(\mathbf{y},t)\right\}=\delta_{ij}\delta^{(3)}(\mathbf{x}-\mathbf{y})-\partial_i\partial_j G(\mathbf{x}-\mathbf{y}), \tag{2.15}$$

where $G(\mathbf{x})$ is the green function of the Laplace operator. The quantization of constrained systems is described in more detail in Ref. [48].

With the Poisson brackets evaluated, we can replace the complex amplitudes $A_\lambda(\mathbf{k})$ with ladder operators in the Heisenberg picture via the mapping $A_\lambda(\mathbf{k})\to\sqrt{\frac{\hbar}{2\omega_k\epsilon_0}}\hat{a}_\lambda(\mathbf{k})$,

and define their bosonic commutation relations based on Eq. (2.14)

$$\left[\hat{a}_\lambda(\mathbf{k}), \hat{a}_{\lambda'}(\mathbf{k}')\right] = 0, \quad \left[\hat{a}_\lambda(\mathbf{k}), \hat{a}^\dagger_{\lambda'}(\mathbf{k}')\right] = \delta_{\mathbf{k},\mathbf{k}'}\delta_{\lambda,\lambda'}, \quad \left[\hat{a}^\dagger_\lambda(\mathbf{k}), \hat{a}^\dagger_{\lambda'}(\mathbf{k}')\right] = 0. \tag{2.16}$$

And finally, the field and momentum operators take the form

$$\hat{\mathbf{A}} = \sum_{\mathbf{k}} \sum_{\lambda=1,2} \sqrt{\frac{\hbar}{2\omega_k \epsilon_0 V}} \left[\boldsymbol{\epsilon}_\lambda(\mathbf{k}) \hat{a}_\lambda(\mathbf{k}) e^{i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)} + \boldsymbol{\epsilon}^*_\lambda(\mathbf{k}) \hat{a}^\dagger_\lambda(\mathbf{k}) e^{-i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)}\right], \tag{2.17}$$

$$\hat{\mathbf{\Pi}} = -i \sum_{\mathbf{k}} \sum_{\lambda=1,2} \sqrt{\frac{\hbar\omega_k \epsilon_0}{2V}} \left[\boldsymbol{\epsilon}_\lambda(\mathbf{k}) \hat{a}_\lambda(\mathbf{k}) e^{i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)} - \boldsymbol{\epsilon}^*_\lambda(\mathbf{k}) \hat{a}^\dagger_\lambda(\mathbf{k}) e^{-i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)}\right]. \tag{2.18}$$

In this section the small hat notation was used to differentiate quantum mechanical operators from classical quantities. In the following sections the hat of the operators is omitted to simplify the notation.

2.2 Photon Number States

First let us write down the Hamiltonian of the quantized electromagnetic field. The Hamiltonian is defined in terms of the Lagrangian density given in Eq. (2.10) the following way:

$$H = \int_V d^3x \left(\mathbf{\Pi} \cdot \partial_t \mathbf{A} - \mathscr{L}\right) = \int_V d^3x \left(\frac{|\mathbf{\Pi}|^2}{2\epsilon_0} + \frac{\triangle |\mathbf{A}|^2}{2\mu_0}\right) = \sum_{\mathbf{k}} \sum_{\lambda=1,2} \hbar\omega_{\mathbf{k}} \left(a^\dagger_\lambda(\mathbf{k}) a_\lambda(\mathbf{k}) + \frac{1}{2}\right). \tag{2.19}$$

The above equation for the Hamiltonian shows that the electromagnetic field in the Coulomb gauge is made up of many harmonic oscillators, more precisely, there is a harmonic oscillator associated with every degree of freedom labeled by $\mathbf{k}$ and λ.

At this point, the operators obtained through the quantization procedure are only algebraic objects; their algebra is defined by the canonical commutation relations (CCR) given by Eq. (2.16). In order to make more elaborate calculations we should find their representation on some compatible Hilbert space. The CCRs imply that the operators $a^\dagger_\lambda(\mathbf{k})a_\lambda(\mathbf{k})$ are semi-positive definite and have non-negative integer eigenvalues, therefore, they are called number operators. The lowest eigenvalue state is the vacuum with zero eigenvalue, in other words, the vacuum of the harmonic oscillator labeled by $\mathbf{k}$ and λ is destroyed by the operator $a_\lambda(\mathbf{k})$, and the excited states are created from the vacuum by repeatedly applying $a^\dagger_\lambda(\mathbf{k})$. For this reason, $a_\lambda(\mathbf{k})$ and $a^\dagger_\lambda(\mathbf{k})$ are called the annihilation and creation operators.

One can construct the complete vacuum state of the electromagnetic field by taking

the tensor product of the ground states of all harmonic oscillators with the condition that the vacuum is normalized to one, i.e., $\langle 0|0\rangle = 1$. The vacuum constructed this way is destroyed by all the annihilation operators

$$a_\lambda(\mathbf{k})\,|0\rangle = 0, \qquad \forall \mathbf{k}, \quad \lambda = 1,2. \tag{2.20}$$

The interpretation of the states $a_\lambda^\dagger(\mathbf{k})\,|0\rangle = |\mathbf{k},\lambda\rangle$ is that they represent single-photon states, i.e., the operator $a_\lambda^\dagger(\mathbf{k})$ excites the vacuum and creates a photon with wave vector $\mathbf{k}$ and polarization λ. If we label the degrees of freedom using the positive integers, we can write down a general multi-photon state as

$$\prod_{i=1,2,\ldots} \frac{a_i^{\dagger n_i}}{\sqrt{n_i!}}\,|0\rangle = |n_1, n_2, \ldots\rangle\,, \qquad n_i = 0,1,2,\ldots, \tag{2.21}$$

where each index i corresponds to a unique tuple of $\mathbf{k}$ and λ. We interpret the states $|n_1, n_2, \ldots\rangle$ as that n_i is the number of photons present in the i-th optical mode with wave vector $\mathbf{k}_i$ and polarization λ_i. These multi-photon states are simultaneous eigenvectors of all number operators $a_i^\dagger a_i$ with corresponding eigenvalues n_i and of the Hamiltonian given in Eq. (2.19).

When calculating the vacuum energy from Eq. (2.19) one finds that it is not finite because every oscillator contributes a $\hbar\omega_k/2$ to the vacuum energy. However, the absolute energy of the vacuum is physically irrelevant, and only the energy differences between the vacuum state and excited states are physically important. Therefore, the vacuum energy can be subtracted from the Hamiltonian, and after the subtraction, all the occupation number states $|n_1, n_2, \ldots\rangle$ have a finite well-defined eigenvalue equal to $\hbar\sum_i \omega_{k_i} n_i$.

The vector space spanned by the occupation number states equipped with the inner product (implied by the CCRs)

$$\langle n_1, n_2, \ldots | m_1, m_2, \ldots\rangle = \prod_{i=1,2,\ldots} \delta_{n_i,m_i} \tag{2.22}$$

forms a Fock space, a Hilbert space which contains all the possible states of the electromagnetic field, including states with different photon numbers. On the occupation number states of the Fock space the annihilation and creation operators act as follows:

$$a_i\,|n_1, n_2, \ldots, n_i, \ldots\rangle = \sqrt{n_i}\,|n_1, n_2, \ldots, n_i - 1, \ldots\rangle\,, \tag{2.23}$$

$$a_i^\dagger\,|n_1, n_2, \ldots, n_i, \ldots\rangle = \sqrt{n_i + 1}\,|n_1, n_2, \ldots, n_i + 1, \ldots\rangle\,. \tag{2.24}$$

The photon number states introduced in this section are observable states of the electromagnetic field, however, their behavior is extremely non-classical. For example, a strange property of photon number states is that the photons that make up the state are indistinguishable; one can tell how many photons there are in a specific optical mode but cannot say which photon is in which mode. In the next section we will see other examples related to the interference of photon number states which also show their non-classical nature.

2.3 Coherent states

The classical wave description of light is one of the most successful theories in physics, however, it cannot explain some physical phenomena, e.g., the photoelectric effect. Today we know that the correct theory of light is quantum mechanical, and so far, we looked at the fundamentals of the quantum theory of light. But how does the quantum theory of light explain classical waves and interference?

The answer lies in coherent states. Although there are no states of the electromagnetic field which would behave exactly like a classical wave because of the uncertainty principle, there are states which experience a minimal amount of quantum fluctuations. These states are called coherent states. The coherent states in an optical mode with annihilation and creation operators a and $a^\dagger$ take the form

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle = e^{-\frac{|\alpha|^2}{2}} \left(\sum_{n=0}^{\infty} \frac{\alpha^n a^{\dagger n}}{n!} \right) |0\rangle = D(\alpha)\,|0\rangle\,, \tag{2.25}$$

where α is an arbitrary complex number and $D(\alpha) = e^{\alpha a^\dagger - \alpha^* a}$ is called a displacement operator. Displacement operators are the unitary representation of the transformation group $a \to a + \beta$ and satisfy the identity $D(\beta)\,|\alpha\rangle = |\alpha + \beta\rangle$ as their name suggests.

If we introduce the Hermitian quadrature operators of the optical mode

$$x = \frac{a + a^\dagger}{2}, \qquad\qquad p = \frac{a - a^\dagger}{2i}, \tag{2.26}$$

we get the uncertainty relation $\Delta x \Delta p \geq \frac{1}{4}$, where the equality holds for coherent states. Coherent states are also eigenvectors of the annihilation operator

$$a\,|\alpha\rangle = \alpha\,|\alpha\rangle\,, \tag{2.27}$$

thus, the expectation values of the quadrature with coherent states evaluate to

$$\langle\alpha|x|\alpha\rangle = \mathrm{Re}(\alpha), \qquad \langle\alpha|p|\alpha\rangle = \mathrm{Im}(\alpha). \tag{2.28}$$

To see the analogy between classical waves and coherent states, let us consider a monochromatic coherent state $|\mathbf{k},\lambda,\alpha\rangle$ with wave vector $\mathbf{k}$ and polarization λ. The state can be written as

$$|\mathbf{k},\lambda,\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n a_\lambda^\dagger(\mathbf{k})^n}{n!} |0\rangle \tag{2.29}$$

and the electric field operator has the form

$$\mathbf{E}(\mathbf{x},t) = \sum_{\mathbf{k}} \sum_{\lambda=1,2} \sqrt{\frac{\hbar\omega_k}{2\epsilon_0 V}} \boldsymbol{\epsilon}_\lambda(\mathbf{k}) a_\lambda(\mathbf{k}) e^{i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)} + \text{h.c.} = \mathbf{E}^{(+)}(\mathbf{x},t) + \mathbf{E}^{(-)}(\mathbf{x},t), \tag{2.30}$$

where $\mathbf{E}^{(+)} \sim e^{-i\omega t}$ and $\mathbf{E}^{(-)} \sim e^{i\omega t}$ are the positive and negative frequency parts of the electric field operator. The expectation values of the positive and negative frequency parts are

$$\langle\mathbf{k},\lambda,\alpha|\mathbf{E}^{(+)}|\mathbf{k},\lambda,\alpha\rangle = \sqrt{\frac{\hbar\omega_k}{2\epsilon_0 V}} \boldsymbol{\epsilon}_\lambda(\mathbf{k}) \alpha e^{i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)}, \tag{2.31}$$

$$\langle\mathbf{k},\lambda,\alpha|\mathbf{E}^{(-)}|\mathbf{k},\lambda,\alpha\rangle = \sqrt{\frac{\hbar\omega_k}{2\epsilon_0 V}} \boldsymbol{\epsilon}_\lambda^*(\mathbf{k}) \alpha^* e^{-i(\mathbf{k}\cdot\mathbf{x}-\omega_k t)}. \tag{2.32}$$

Equations (2.31) and (2.32) show that the expectation values of the positive and negative frequency parts evolve exactly like classical plane waves with amplitudes proportional to $|\alpha|$ and with relative phase $\phi = \arg(\alpha)$, where $\alpha = |\alpha|e^{i\phi}$. This indicates that monochromatic coherent states correspond to classical plane waves. Although they evolve classically, quantum mechanics predicts that even coherent states exhibit quantum fluctuations, this can be experimentally observed in the form of shot noise when the intensity of a coherent source is measured. This is because the average photon number $\bar{n}$ and its variance are both proportional to $|\alpha|^2$. Therefore, the fluctuations in the intensity of coherent light are proportional to $1/\sqrt{\bar{n}}$.

2.4 Linear optics

Now that we have established the correspondence between classical waves and coherent states, we can try to describe classical wave interference using quantum mechanics. To do so, let us consider the case of the lossless beamsplitter. The lossless beamsplitter can be classically described as a thin, linear dielectric media, which reflects some por-

tion of the incoming light waves and transmits the rest (see Fig. 2.1 for illustration). One can solve this problem for incoming plane waves using Maxwell's equations. The solution is that the outgoing waves are also plane waves and their complex amplitudes, α_{out} and β_{out}, can be written as the linear combination of the incoming waves complex amplitudes, α_{in} and β_{in},

$$\begin{pmatrix} \alpha_{\text{out}} \\ \beta_{\text{out}} \end{pmatrix} = S \begin{pmatrix} \alpha_{\text{in}} \\ \beta_{\text{in}} \end{pmatrix}, \tag{2.33}$$

where S is a 2×2 unitary indicating that the beamsplitter is lossless.

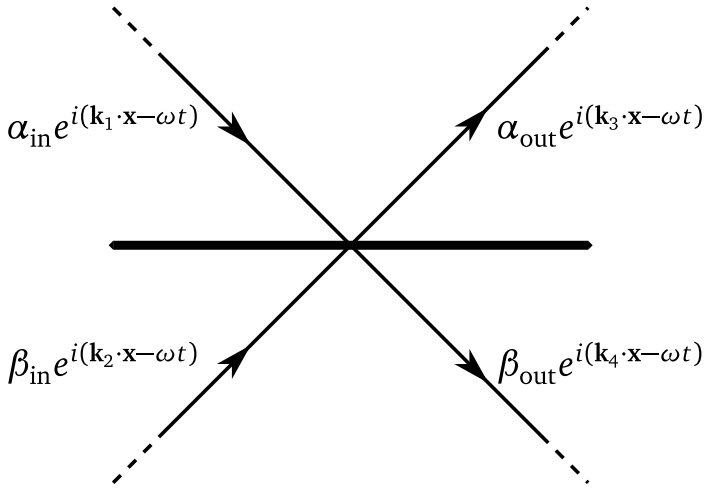


Figure 2.1: Plane waves interacting with a beamsplitter. $\alpha_{\text{in/out}}$ and $\beta_{\text{in/out}}$ are complex amplitudes representing the amplitudes and relative phases of the incoming and outgoing plane waves.

In the quantum picture the lossless beamsplitter must be represented as a unitary transformation $U(S)$ on the Fock space. And if we consider coherent states by the correspondence principal we can write

$$|\mathbf{k}_3, \lambda, \alpha_{\text{out}}\rangle \otimes |\mathbf{k}_4, \lambda, \beta_{\text{out}}\rangle = U(S) |\mathbf{k}_1, \lambda, \alpha_{\text{in}}\rangle \otimes |\mathbf{k}_2, \lambda, \beta_{\text{in}}\rangle , \tag{2.34}$$

assuming the beamsplitter does not mix polarizations. To simplify the notation let us relabel the relevant creation and annihilation operators $a_{\text{in}} = a_\lambda(\mathbf{k}_1)$, $b_{\text{in}} = a_\lambda(\mathbf{k}_2)$, $a_{\text{out}} = a_\lambda \mathbf{k}_3$ and $b_{\text{out}} = a_\lambda(\mathbf{k}_4)$. On the one hand we have

$$|\mathbf{k}_3, \lambda, \alpha_{\text{out}}\rangle \otimes |\mathbf{k}_4, \lambda, \beta_{\text{out}}\rangle = \exp(\alpha_{\text{out}} a_{\text{out}}^\dagger - \alpha_{\text{out}}^* a_{\text{out}}) \exp(\beta_{\text{out}} b_{\text{out}}^\dagger - \beta_{\text{out}}^* b_{\text{out}}) |0\rangle , \tag{2.35}$$

and on the other hand

$$|\mathbf{k}_3,\lambda,\alpha_{\text{out}}\rangle\otimes|\mathbf{k}_4,\lambda,\beta_{\text{out}}\rangle = \exp\left(\alpha_{\text{in}}U(S)a_{\text{in}}^\dagger U^\dagger(S)-\alpha_{\text{in}}^* U^\dagger(S)a_{\text{in}}U(S)\right) \times\exp\left(\beta_{\text{in}}U(S)b_{\text{in}}^\dagger U^\dagger(S)-\beta_{\text{in}}^* U^\dagger(S)b_{\text{in}}U(S)\right)|0\rangle\,, \tag{2.36}$$

this implies that

$$\begin{pmatrix}a_{\text{out}}^\dagger, & b_{\text{out}}^\dagger\end{pmatrix}\begin{pmatrix}\alpha_{\text{out}}\\ \beta_{\text{out}}\end{pmatrix}=\begin{pmatrix}a_{\text{out}}^\dagger, & b_{\text{out}}^\dagger\end{pmatrix}S\begin{pmatrix}\alpha_{\text{in}}\\ \beta_{\text{in}}\end{pmatrix}=\begin{pmatrix}U(S)a_{\text{in}}^\dagger U^\dagger(S), & U(S)b_{\text{in}}^\dagger U^\dagger(S)\end{pmatrix}\begin{pmatrix}\alpha_{\text{in}}\\ \beta_{\text{in}}\end{pmatrix}, \tag{2.37}$$

which further implies the following

$$S^\dagger\begin{pmatrix}a_{\text{out}}\\ b_{\text{out}}\end{pmatrix}=\begin{pmatrix}U(S)a_{\text{in}}U^\dagger(S)\\ U(S)b_{\text{in}}U^\dagger(S)\end{pmatrix}. \tag{2.38}$$

Equation (2.38) gives us a transformation rule to handle the lossless beamsplitter quantum mechanically. The rule is simply to replace the operators a_{in}, b_{in} the following way

$$\begin{pmatrix}a_{\text{in}}\\ b_{\text{in}}\end{pmatrix}\to S^\dagger\begin{pmatrix}a_{\text{out}}\\ b_{\text{out}}\end{pmatrix}. \tag{2.39}$$

This rule not only applies for coherent states, but for all states, including photon number states. An interesting effect related to the interference of photon number states is the Hong-Ou-Mandel (HOM) effect [49], which is observed when a photon is injected into both input modes of a symmetric beamsplitter. To state formally

$$\begin{aligned}|1_a,1_b\rangle_{\text{in}}=a_{\text{in}}^\dagger b_{\text{in}}^\dagger|0\rangle\xrightarrow{50:50}\frac{\left(a_{\text{out}}^\dagger+b_{\text{out}}^\dagger\right)}{\sqrt{2}}\frac{\left(a_{\text{out}}^\dagger-b_{\text{out}}^\dagger\right)}{\sqrt{2}}|0\rangle&=\frac{\left(a_{\text{out}}^\dagger\right)^2}{2}|0\rangle-\frac{\left(b_{\text{out}}^\dagger\right)^2}{2}|0\rangle\\ &=\frac{1}{\sqrt{2}}\left(|2_a,0_b\rangle_{\text{out}}-|0_a,2_b\rangle_{\text{out}}\right),\end{aligned} \tag{2.40}$$

if the S matrix of a symmetric beamsplitter has the form $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$.

The result above for the output state cannot be interpreted classically. Despite the fact that a single photon entering the symmetric beamsplitter would be found with equal probability in both output modes, when two indistinguishable photon enters, they are always exiting together and never apart. The HOM effect is a good example for the non-classical behavior of photon number states.

The lossless beamsplitter is a linear-optical element. The term linear refers to the fact that the light interacts with a linear media, which means that the relation between

the incoming and outgoing plane waves is linear and in the quantum case the creation and annihilation operators transform linearly. In general, for a linear-optical network with N different optical modes one can write

$$S^\dagger \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_N \end{pmatrix} = \begin{pmatrix} U(S)a_1U^\dagger(S) \\ U(S)a_2U^\dagger(S) \\ \vdots \\ U(S)a_NU^\dagger(S) \end{pmatrix}, \tag{2.41}$$

where S is an $N \times N$ unitary. Equation (2.41) is the generalization of Eq. (2.38) and gives the connection between the unitary S and its Fock space representation $U(S)$. One may use the representation theory of Lie algebras to find the representation $U(S) = \exp\left(i \sum_{k,l} H_{kl} a_k^\dagger a_l\right)$, where H is an $N \times N$ Hermitian matrix which generates S, i.e., $S = \exp(iH)$.

An important problem related to linear-optical interferometers is to calculate the matrix elements of $U(S)$ from the matrix elements of S. Matrix elements such as $\langle m_1, m_2, \ldots, m_N | U(S) | n_1, n_2, \ldots, n_N \rangle$ give the probability amplitude for finding a photon number sequence $m_1, m_2, \ldots, m_N$ when measuring the photon count in the output modes given an input photon number sequence $n_1, n_2, \ldots, n_N$, thus, the probability may be written as

$$P(m_1, m_2, \ldots, m_N | n_1, n_2, \ldots, n_N) = |\langle m_1, m_2, \ldots, m_N | U(S) | n_1, n_2, \ldots, n_N \rangle|^2 . \tag{2.42}$$

To calculate the probability, one can expand the state $U(S)|n_1, n_2, \ldots, n_N\rangle$ the following way

$$U(S)|n_1, n_2, \ldots, n_N\rangle = \prod_{j=1}^{N} \frac{1}{\sqrt{n_j!}} \left(\sum_{i=1}^{N} a_i^\dagger S_{ij} \right)^{n_j} |0\rangle . \tag{2.43}$$

One can further expand Eq. (2.43) and write $U(S)|n_1, n_2, \ldots, n_N\rangle$ as a linear combination of photon number states

$$U(S)|n_1, n_2, \ldots, n_N\rangle = \sum_{\substack{\{m_1, m_2, \ldots, m_N\} \\ \sum_i m_i = \sum_i n_i}} \frac{\mathrm{perm}\left(S\left[1^{m_1}, 2^{m_2}, \ldots, N^{m_N} | 1^{n_1}, 2^{n_2}, \ldots, N^{n_N}\right]\right)}{\sqrt{\prod_i n_i! m_i!}} |m_1, m_2, \ldots, m_N\rangle , \tag{2.44}$$

where $S\left[1^{m_1}, 2^{m_2}, \ldots, N^{m_N} | 1^{n_1}, 2^{n_2}, \ldots, N^{n_N}\right]$ is an inflated (or deflated) matrix created from S by repeating each of its i-th row m_i times than repeating the each of its j-th column n_j times, and $\mathrm{perm}(M)$ denotes the permanent of the matrix M. The inflated

matrix can be written in the form of a block matrix the following way

$$S[1^{m_1},2^{m_2},\ldots,N^{m_N}|1^{n_1},2^{n_2},\ldots,N^{n_N}] = \begin{pmatrix} [S_{11}]_{m_1\times n_1} & [S_{12}]_{m_1\times n_2} & \cdots & [S_{1N}]_{m_1\times n_N} \\ [S_{21}]_{m_2\times n_1} & [S_{22}]_{m_2\times n_2} & \cdots & [S_{2N}]_{m_2\times n_N} \\ \vdots & \vdots & \ddots & \vdots \\ [S_{N1}]_{m_N\times n_1} & [S_{N2}]_{m_N\times n_2} & \cdots & [S_{NN}]_{m_N\times n_N} \end{pmatrix}, \tag{2.45}$$

where $\left[S_{ij}\right]_{m_i\times n_j}$ is a $m_i \times n_j$ block filled with the matrix element S_{ij}. Finally, we can write down an expression for the matrix elements

$$\langle m_1,m_2,\ldots,m_N|U(S)|n_1,n_2,\ldots,n_N\rangle = \frac{\mathrm{perm}\left(S[1^{m_1},2^{m_2},\ldots,N^{m_N}|1^{n_1},2^{n_2},\ldots,N^{n_N}]\right)}{\sqrt{\prod_i n_i!m_i!}}. \tag{2.46}$$

For the derivation of Eq. (2.44) see Ref. [50].

The definition of the permanent is similar to the definition of the determinant but the ± signs of the permutations are left out

$$\mathrm{perm}(M) = \sum_{\sigma\in S_n}\prod_{i=1}^{n} M_{i,\sigma(i)}, \tag{2.47}$$

where S_n denotes the permutations of the set $\{1,2,\ldots,n\}$. Despite the similarity, calculating the permanent is computationally difficult [51]; the fastest algorithm for calculating the permanent of an $n\times n$ matrix has a time complexity $O(n2^n)$ [52]. This means that calculating the probabilities $P(m_1,m_2,\ldots,m_N|n_1,n_2,\ldots,n_N)$ or sampling their distribution is also computationally demanding.

Generating samples from the distribution $P(m_1,m_2,\ldots,m_N|n_1,n_2,\ldots,n_N)$ is called the boson sampling problem and classical computers cannot do it efficiently. Even sampling an approximation of this distribution is difficult using classical computers [53]. However, one might construct a linear-optical network which approximates the underlying transformation S and use actual photons and detectors to sample an approximation of $P(m_1,m_2,\ldots,m_N|n_1,n_2,\ldots,n_N)$. Such a boson sampling device would be fundamentally more powerful than any classical computer.

Indeed, boson sampling devices have been built and evidence for their supremacy was demonstrated (see Refs. [5–7]). However, boson sampling devices are not universal as other types of quantum computers, so their application is severely limited. Nevertheless, boson sampling displays the strength of linear optics.

Chapter 3

Universal Photonic Quantum Computing

Single-photon states allow the definition of qubits and qudits, and linear optics, e.g., a network of beamsplitters and phase shifters, offer great control over single-photon states. However, a network of linear-optical elements cannot create entanglement between qubits or qudits encoded by single-photons. For this reason, it was unclear for a long time whether linear optics can be used to implement universal quantum computation. In the early 2000's Knill, Laflamme and Milburn showed that linear optics and photon number resolving detectors (PNRD) together can be used to implement universal quantum computation [23]. This chapter reviews the standard model of quantum computation, the quantum circuit model, and describes two ways to efficiently simulate the quantum circuit model using linear optics and PNRDs.

3.1 Quantum Circuit Model

The quantum circuit model provides a mathematical framework to define precisely what we mean by quantum computation and quantum algorithms, similarly to how the Turing machine defines computability and notion of a classical algorithm. The quantum circuit model is arbitrary in many ways, and it is possible to define other, seemingly different models for quantum computation. However, all other models for quantum computation currently known are either equivalent to, or weaker than the quantum circuit model. In this context, the equivalence of two models means that they can simulate each other with a polynomial resource overhead.

The qubit is a two-level quantum system, and it is the basic constituent of the quantum computer in the quantum circuit model. The Hilbert space of a single qubit is isomorphic to $\mathbb{C}^2$, thus, we may represent the state of qubit with a two-component complex

vector

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} \in \mathbb{C}^2, \tag{3.1}$$

where $\{|0\rangle, |1\rangle\}$ is an orthogonal basis of the qubit's Hilbert space. A finite collection of qubits forms a quantum register and the combined Hilbert space of the qubits contains all the possible states of the register.

In the quantum circuit model, the quantum computer is a machine with a quantum register which can perform a set of reversible, unitary transformations on its quantum register along with qubit specific measurements and a special reset operation. The reset operation resets the state of the quantum register into a simple state which can serve as a well-defined starting point for quantum computation, e.g., the state $|0\rangle^{\otimes N}$.

The most basic form of quantum information processing usually involves the following three steps:

1. Encoding classical or quantum information into a quantum state.
2. Controlled evolution of the quantum state.
3. Measuring the quantum state to retrieve some classical information.

In this context, classical information means a sequence of zeros and ones, and quantum information refers to the information needed to describe a quantum state.

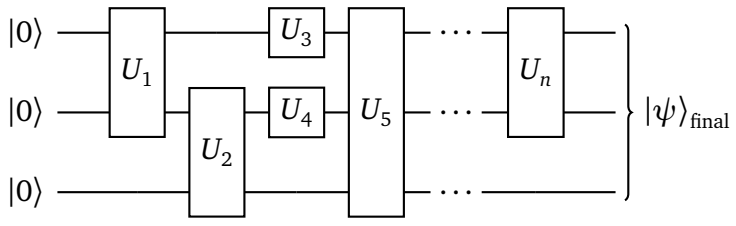
One may use the quantum computer described above to achieve these three steps. After resetting the quantum register into the starting state the user of the quantum computer may instruct it to perform a sequence of quantum gates $U_1, U_2, \ldots, U_n$ to carry out steps one and two, and arrive at a final state

$$|\psi\rangle_{\text{final}} = U_n U_{n-1} U_{n-2} \ldots U_1\,|0\rangle^{\otimes N}. \tag{3.2}$$

The above gate sequence can be thought of as an algorithm for preparing the state $|\psi\rangle_{\text{final}}$.

A quantum algorithm in the quantum circuit model is defined as a sequence of quantum gates, and the output of the computation is either taken to be the final quantum state $|\psi\rangle_{\text{final}}$, or the result of a measurement made in the state $|\psi\rangle_{\text{final}}$.

A sequence of quantum gates can be depicted using simple drawings



(3.3)

where each qubit is represented by a horizontal *wire* and gates are drawn as boxes placed on top of the appropriate wires indicating which qubits they affect. These drawings resemble logical circuits, but instead of logic gates (AND, OR, XOR etc.), the boxes here indicate quantum gates. Hence the name quantum circuit model.

Using the concept of the quantum computer defined by the quantum circuit model, it is now possible to define universality. A gate set $\mathfrak{B}$ is universal, if any unitary can be approximated using a finite sequence of quantum gates from the set $\mathfrak{B}$, such that the error of the approximation can be made vanishingly small.

Quantum computers which implement a universal gate set are extremely powerful, but one might fear that such a gate set would be too large to physically realize with hardware. Fortunately, this is not the case; a universal gate set can be as small as to only contain a few single-qubit and one two-qubit gate.

Notable single-qubit gates which frequently appear in the description of quantum algorithms are the Pauli X, Y, Z gates

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{3.4}$$

and the phase and Hadamard gates

$$P(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}, \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3.5}$$

Using the gates defined above it is possible synthesize any other single-qubit gate, however, they cannot create entanglement between qubits. It turns out that it is enough to introduce a single two-qubit gate the controlled-X gate

$$CX = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X \tag{3.6}$$

to create a universal gate set. For example, the gate sets

$$\{CX, \text{all single-qubit gates}\}, \qquad \left\{CX, H, P\left(\frac{\pi}{4}\right)\right\} \tag{3.7}$$

are both universal [54, 55].

A universal quantum computer can simulate a classical computer and a classical computer can simulate a quantum computer with exponential resource overhead, thus, the notion of computability is the same in both the quantum and classical case [56, 57]; quantum computers offer only a potential speed up over classical computation.

3.2 The KLM Scheme

The core idea of the KLM scheme [23] is to encode qubits using single-photon states and use linear optics and PNRDs to implement a universal gate set. A single qubit is encoded by two optical modes, labeled l_1 and l_2, as follows: $\|0\rangle\!\rangle = |1,0\rangle_{l_1,l_2}$ and $\|1\rangle\!\rangle = |0,1\rangle_{l_1,l_2}$, where the double-ket symbol $\|\rangle\!\rangle$ is used to denote the logical states of the qubit and the single-kets $|\rangle$ denote photon number states. This encoding is called the dual-rail encoding.

The dual-rail encoding is a great choice for encoding qubits in a linear-optical scheme, because linear-optical transformations of the qubit's modes can reproduce all single-qubit gates. Let us denote the creation operators of the two modes as $a_0^\dagger$ and $a_1^\dagger$, then the state of the qubit $\alpha\|0\rangle\!\rangle + \beta\|1\rangle\!\rangle$ is encoded by the photon number state $(\alpha a_0^\dagger + \beta a_1^\dagger)|0\rangle$, thus, applying the optical transformation $S \in \mathrm{U}(2)$

$$\begin{pmatrix} a_0^\dagger, & a_1^\dagger \end{pmatrix} \to \begin{pmatrix} a_0^\dagger, & a_1^\dagger \end{pmatrix} S \tag{3.8}$$

yields the state

$$\begin{pmatrix} a_0^\dagger, & a_1^\dagger \end{pmatrix} S \begin{pmatrix} \alpha \\ \beta \end{pmatrix} |0\rangle = \alpha' \|0\rangle\!\rangle + \beta' \|1\rangle\!\rangle, \quad \text{where} \quad \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = S \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{3.9}$$

In other words, the linear-optical transformation S acts on the qubit's Hilbert space as a single-qubit gate.

It is possible to create any transformation $S \in \mathrm{U}(2)$ using only beamsplitters and phase shifters, e.g., a general beamsplitter parameterized by two angles θ and φ

$$\mathrm{BS}(\theta,\varphi) = \begin{pmatrix} \cos\theta & -e^{i\varphi}\sin\theta \\ e^{-i\varphi}\sin\theta & \cos\theta \end{pmatrix} \tag{3.10}$$

and two phase shifters can realize any 2×2 unitary linear-optical transformation, and therefore any single-qubit gate on the qubit's Hilbert space.

Universal quantum computation requires a universal gate set, which must include an entangling gate (e.g., CX). Unfortunately, it is not possible to use linear optics to create entangled dual-rail qubits. One may use elementary matrix algebra to prove this. For the proof see Appendix A.

The lack of entanglement can be related to the absence of nonlinearity, in other words, the absence of interaction between photons. To make photons interact we may use a nonlinear crystal, e.g., a Kerr crystal, but in practice the nonlinearities of such crystals are too small to entangle single-photon states. We may avoid nonlinear crystals

by using ancilla photons and measurements instead to create nonlinear effects, however, this comes at the cost of determinism.

The nonlinear phase shift operation is defined on a single optical mode as follows

$$\mathrm{NS}_\phi : \alpha_0 |0\rangle + \alpha_1 |1\rangle + \alpha_2 |2\rangle \to \alpha_0 |0\rangle + \alpha_1 |1\rangle + e^{i\phi} \alpha_2 |2\rangle . \tag{3.11}$$

The application of the NS_ϕ operation on a state which is a linear combination of zero, one and two-photons states results in the two-photon state acquiring an extra $e^{i\phi}$ phase. It is possible to use beamsplitters, phase shifters and PNRDs to realize it. The configuration of ancilla modes and detectors is depicted by Fig. 3.1. However, the NS_ϕ operation only succeeds if the ancilla measurement yields one photon in the first ancilla and zero photons in the second ancilla as indicated on Fig. 3.1. The linear-optical implementation of NS_ϕ is thus nondeterministic.

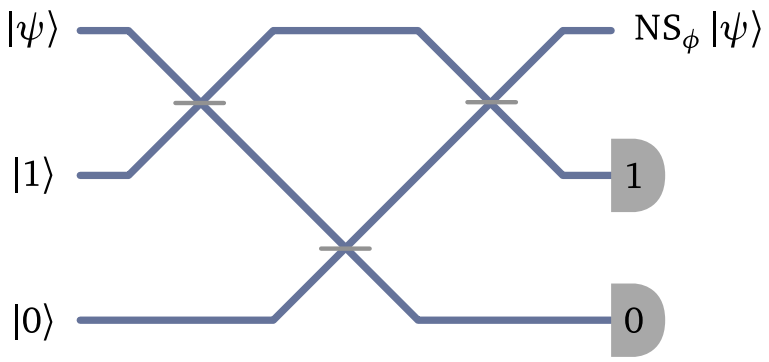


Figure 3.1: Nonlinear phase shift implemented using linear optics and photon number resolving detectors.

One can use the nonlinear phase shift to implement the controlled Z gate on dual rail qubits. On the logical qubits the CZ gate acts as follows

$$CZ \, \|k\rangle\rangle \, \|l\rangle\rangle = (-1)^{kl} \, \|k\rangle\rangle \, \|l\rangle\rangle . \tag{3.12}$$

It is easy to check, that the combination of beamsplitters and nonlinear phase shifts depicted on Fig. 3.2 acts as a CZ gate on two dual-rail qubits. If the nonlinear phase shifts are implemented using linear optics, then the CZ gate is non-deterministic with a success probability of $1/16$, since both NS_π have to succeed at once and each of them has a success probability of $1/4$. For the calculation of these probabilities see Appendix B.

To use this non-deterministic CZ gate one may apply postselection. Postselection is to discard measurements based on the results of the ancilla measurements, and only build statistics from measurements to which prior the gate had succeeded. After posts-

election the measurement results yield the same statistic as if they were made after the application of a deterministic CZ gate.

The gate set $\mathfrak{B} = \{CZ, \text{all single-qubit gates}\}$ is also a universal gate set, since the CX and CZ gates are connected by a single-qubit similarity transformation

$$(\mathbb{1} \otimes H)CZ(\mathbb{1} \otimes H^\dagger) = CX. \tag{3.13}$$

Therefore, via postselection one could in theory simulate any quantum gate using linear optics and PNRDs. However, postselection by itself is highly inefficient, because a measurement is only kept if all the ancilla measurements turned out correct. In the case of a quantum circuit containing $O(n)$ number of CZ gates, the CZ gates would need to succeed independently to keep a measurement when postselecting, thus, the probability of retaining a measurement would be $1/16^{O(n)}$. For this reason, many polynomial time quantum circuits would require an exponential overhead to be simulated by linear optics and postselection.

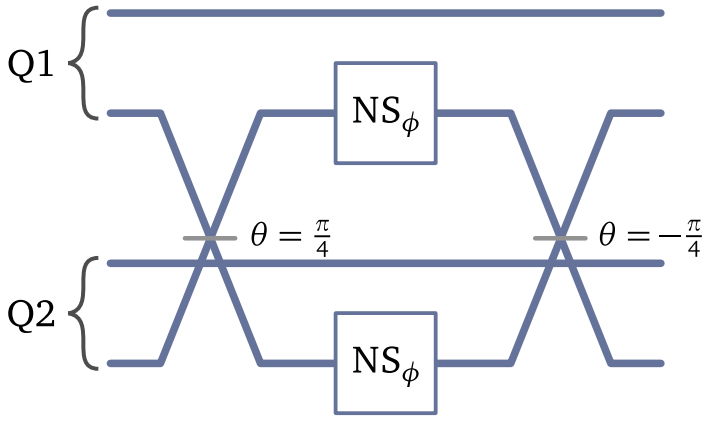


Figure 3.2: Controlled phase gate on dual-rail qubits implemented using symmetric beamsplitters BS$(\pm\pi/4, 0)$ and nonlinear phase shifts. For $\phi = \pi$, this is the controlled Pauli Z gate.

The problem with the non-deterministic CZ gate is that when it fails it spoils the whole computation, because the dual-rail qubits are destroyed. However, one can utilize quantum teleportation to significantly lessen this destructive effect.

Quantum teleportation can be used to move the quantum information of a *source* mode to another *destination* mode without the source and destination modes ever directly interfering. Let us label the source mode with 1 and introduce two ancilla modes labeled by 2 and 3. If we prepare the state

$$|\phi\rangle_{2,3} = \frac{1}{\sqrt{2}}(|1,0\rangle_{2,3} + |0,1\rangle_{2,3}) \tag{3.14}$$

on the two ancilla modes, then a set of measurements can be used to teleport the state of the source mode $|\psi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1$ to mode 3. As per usual for quantum teleportation protocols, these measurements should be made on the Bell basis $|0,0\rangle \pm |1,1\rangle$ and $|0,1\rangle \pm |1,0\rangle$.

We may do a partial Bell measurement using linear optics by implementing the transformation $F \in \mathrm{U}(2)$

$$\left(a_1^\dagger, \quad a_2^\dagger\right) \to \left(a_1^\dagger, \quad a_2^\dagger\right) \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \left(a_1^\dagger, \quad a_2^\dagger\right) F. \tag{3.15}$$

Applying F to the state $|\psi\rangle_1 \otimes |\phi\rangle_{2,3}$ gives us

$$\begin{aligned} U(F)|\psi\rangle_1 \otimes |\phi\rangle_{2,3} =& \frac{1}{2}|1,0\rangle_{1,2} \otimes (\alpha|0\rangle_3 + \beta|1\rangle_3) + \frac{1}{2}|0,1\rangle_{1,2} \otimes (\alpha|0\rangle_3 - \beta|1\rangle_3) \\ &+ \frac{1}{2}\left(\frac{1}{\sqrt{2}}|0,0\rangle_{1,2} + \frac{1}{2}|2,0\rangle_{1,2} - \frac{1}{2}|0,2\rangle_{1,2}\right) \otimes (\alpha|1\rangle_3 + \beta|0\rangle_3) \\ &+ \frac{1}{2}\left(\frac{1}{\sqrt{2}}|0,0\rangle_{1,2} - \frac{1}{2}|2,0\rangle_{1,2} + \frac{1}{2}|0,2\rangle_{1,2}\right) \otimes (\alpha|1\rangle_3 - \beta|0\rangle_3), \end{aligned} \tag{3.16}$$

thus, if now we measure modes 1 and 2 and the outcome of the measurement is $|1,0\rangle_{1,2}$, then the state $|\psi\rangle$ successfully teleported from mode 1 to mode 3. If the measurement outcome is $|0,1\rangle_{1,2}$, then applying the phase shift $a_3^\dagger \to -a_3^\dagger$ recovers the state $|\psi\rangle$ on mode 3. In case of the other outcomes, the state $|\psi\rangle$ cannot be recovered, therefore, this teleportation protocol fails with probability $1/2$.

Using the teleportation protocol described above it is possible to implement the CZ gate with probability $1/4$. Given two dual-rail qubits, where the first qubit is defined by modes 1, 2 and the second qubit is defined by modes 3, 4, and ancilla modes labeled 5, 6, 7, 8 in the state

$$|cs\rangle_{5,6,7,8} = \frac{1}{2}|1,0,1,0\rangle_{5,6,7,8} + \frac{1}{2}|1,0,0,1\rangle_{5,6,7,8} + \frac{1}{2}|0,1,1,0\rangle_{5,6,7,8} - \frac{1}{2}|0,1,0,1\rangle_{5,6,7,8}. \tag{3.17}$$

Teleporting mode 2 onto mode 6 and mode 4 onto mode 8 realizes the CZ gate if both teleportation succeeds. This is done by making one Bell measurement on modes 2 and 5, and another Bell measurement on modes 4 and 7 along with the phase corrections on modes 6 and 8 as prescribed by the teleportation protocol. Since the teleportation protocol succeeds with probability $1/2$ the CZ gate implemented this way has a success rate of $1/4$. The preparation of the state $|cs\rangle$ and the linear-optical network for the teleportation of modes is shown by Fig. 3.3.

Using quantum teleportation to implement the CZ gate has the advantage that fail-

ing to prepare the ancillas is non-destructive. The preparation can be tried repeatedly, until the state preparation succeeds. Furthermore, the teleportation protocol can be improved by generalizing the Bell measurement protocol to succeed with probability $n/(n+1)$ by using $2n$ number of ancilla modes. This way the teleportation based CZ gate has a success rate $n^2/(n+1)^2$, thus, it can be made near-deterministic by increasing n.

The KLM scheme can efficiently simulate the quantum circuit model using linear optics and PNRDs, but in practice it also requires quantum memories to store ancilla states, and optical switching to perform the teleportation protocol. Also, everything must be done with perfect timing, making the KLM scheme unrealistic to implement with physical hardware. Despite the difficulties of the KLM scheme, Knill et al. showed that in theory it is possible to use linear optics for universal quantum computation which was at the time believed by many to be not the case. This discovery paved the way for other improved schemes for linear-optical quantum computation (LOQC), most famously cluster state computation, which we will discuss in the next section.

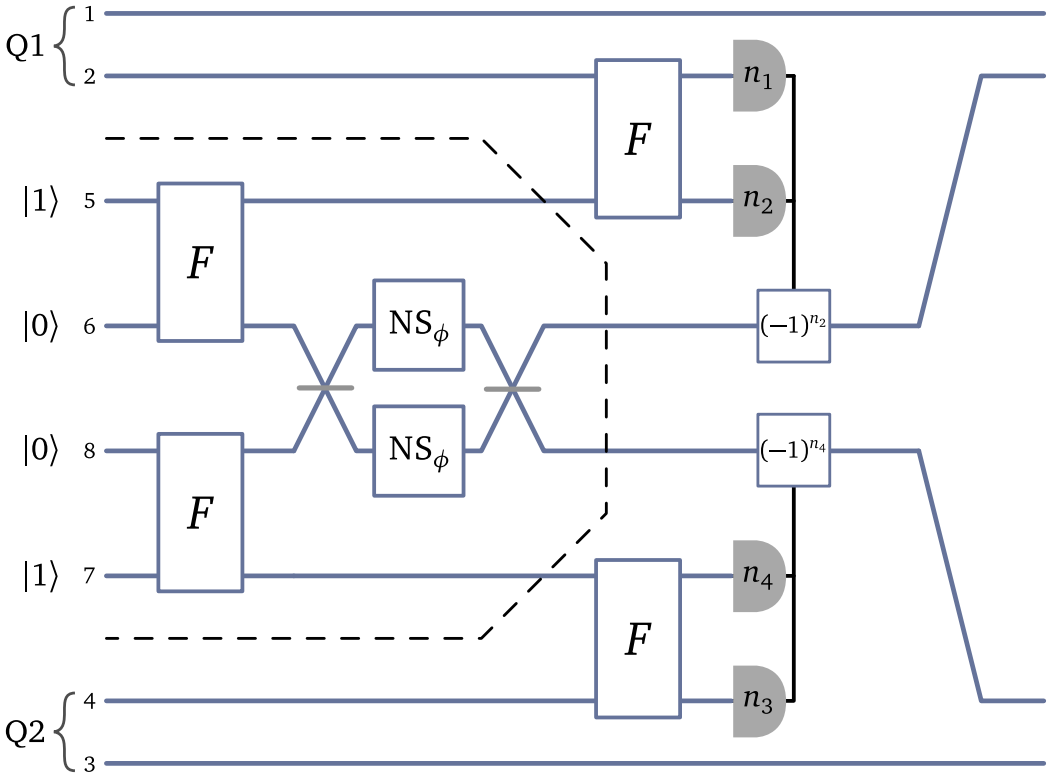


Figure 3.3: Non-deterministic CZ gate with success rate $1/4$ ($\phi = \pi$ case). The linear-optical network inside the dashed line repeatedly attempts to prepare the state $|cs\rangle_{5,6,7,8}$ using nonlinear phase shifts until it succeeds. Once $|cs\rangle_{5,6,7,8}$ is prepared successfully, the teleportation protocol performs the CZ gate on qubits Q1 and Q2. The measurement outcomes of the Bell measurements are indicated by the photon numbers n_1, n_2, n_3 and n_4.

3.3 Cluster State Quantum Computation

Cluster state quantum computation is a form of measurement-based quantum computation (MBQC), where the idea is to use a highly entangled resource states to simulate a universal quantum gate set by making only local measurements. MBQC is particularly fitting for quantum computer architectures in which non-local operations on qubits are non-deterministic or unreliable, for example, in the case of photonic quantum computers.

In the KLM scheme to implement a near-deterministic gate, entangled ancilla resources need to be prepared on demand with incredible timing constraints. While in MBQC it is enough to prepare a single resource state ahead of computation, and after the preparation of the resource state linear optics can simulate a universal gate set deterministically by performing local operations. For this reason, MBQC is believed to be one of the best computational models for LOQC.

Cluster state quantum computation uses resources states called cluster states sometimes referred to as graph states. Each mathematical graph G, a set of vertices V and edges E, defines a cluster state

$$|G\rangle = \left(\prod_{\{i,j\}\in E} CZ_{ij} \right) |+\rangle^{\otimes |V|}, \tag{3.18}$$

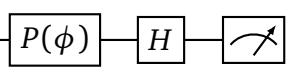
where each qubit corresponds to a vertex of G. The single-qubit state $|+\rangle$ is defined as $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $CZ_{ij} = |0\rangle\langle 0|_i \otimes \mathbb{1}_j + |1\rangle\langle 1|_i \otimes Z_j$ is the unitary action of the controlled Z gate performed on qubits i and j.

Similarly to how the quantum circuit model defines a model of quantum computation, MBQC defines an alternative model of quantum computation, sometimes called the one-way quantum computer. The one-way computer can make the following actions:

1. Prepare a cluster state $|G\rangle$.
2. Qubit-specific adaptive measurements in the X–Y plane of the Bloch sphere. See Appendix C for the definition of the Bloch sphere.

Above, the adaptivity of measurements means that the basis of each measurement can be determined on the fly based on the results of the previous measurements.

A measurement in the X–Y plane is equivalent to a unitary transformation parameterized by an angle and a measurement on the computational basis of the qubit

$M(\phi) =$  , (3.19)

where $M(\phi)$ denotes a general measurement in the X–Y plane. This equivalence can be used to translate the measurements of the one-way computer into a quantum circuit.

The one-way computer can only make measurements on the cluster state $|G\rangle$, therefore, in this computation model it is natural to define an algorithm as measurement pattern on $|G\rangle$:

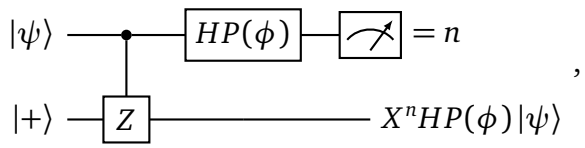
$$M_{i_1}(\phi_1),\ M_{i_2}(\phi_2),\ \ldots,\ M_{i_m}(\phi_m), \tag{3.20}$$

where the measurements are performed in the order indicated by the numbers $1, 2, \ldots, m$ and $M_{i_k}(\phi_k)$ denotes the measurement of the i_k-th qubit. Since we may make adaptive measurements, the angles describing the basis of the measurement can depend on the results of the previous measurements. In general, we may write

$$\phi_k = f_k(n_1, n_2, \ldots, n_{k-1}), \tag{3.21}$$

where $n_1, n_2, \ldots, n_{k-1}$ denote the previous $k-1$ measurement results and f_k is an arbitrary computable function evaluated by a classical computer.

This definition of quantum computation seems to be completely different from the definition given using the quantum circuit model. However, despite the differences, the measurement-based model of quantum computation is equivalent to the quantum circuit model, i.e., they can simulate each other efficiently. We can show this using the following circuit identity



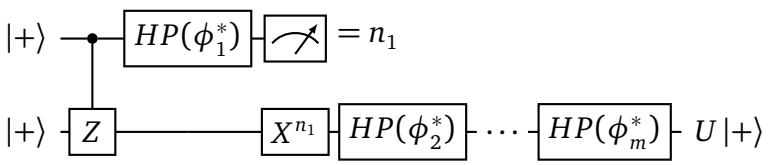
, (3.22)

where n is the outcome of the measurement made on the top qubit.

First, let us try to convert a single-qubit gate into an equivalent measurement pattern on some cluster state. To do this, we can use the lemma, that any single-qubit gate $U \in \mathrm{U}(2)$ can be decomposed into a product of the form [26]

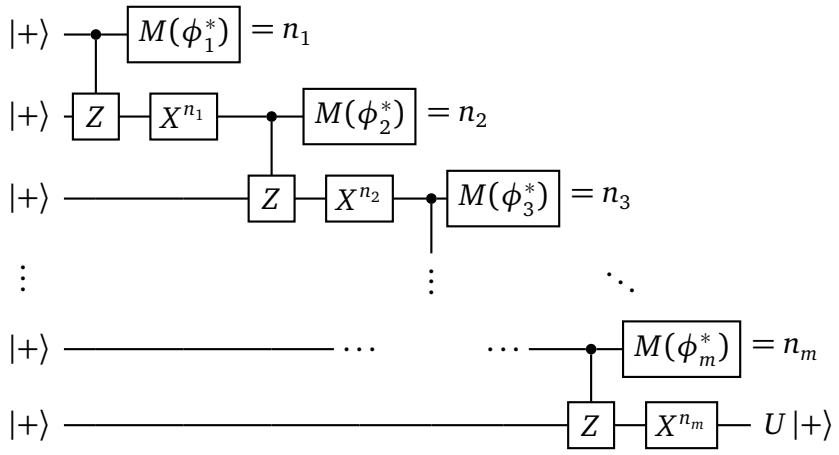
$$U = HP(\phi_m^*)HP(\phi_{m-1}^*)\cdots HP(\phi_1^*). \tag{3.23}$$

Therefore, using Eqs. (3.22) and (3.19) we can start to transform the circuit of U into a sequence of measurements



(3.24)

Iterating the step above we arrive at the following sequence of measurements



(3.25)

This sequence of gates and measurements can also be represented as a string of operations

$$X_{m+1}^{n_m} M_m(\phi_m^*) CZ_{m,m+1} \cdots M_3(\phi_3^*) X_3^{n_2} M_2(\phi_2^*) CZ_{23} X_2^{n_1} M_1(\phi_1^*) CZ_{1,2} |+\rangle^{\otimes N}, \tag{3.26}$$

where $N = m+1$. This sequence is like a measurement pattern, but the X and CZ gates are still in between the measurement operations. Thus, the above sequence is not a measurement pattern yet. To move all the CZ gates to the right we can make use of the identity

$$CZ_{i,j} X_i = X_i Z_j CZ_{i,j}. \tag{3.27}$$

Moving all the CZ gates to the right leaves us a sequence of local operations on a cluster state

$$X_{m+1}^{n_m} Z_{m+1}^{n_{m-1}} M_m(\phi_m^*) X_m^{n_{m-1}} Z_m^{n_{m-2}} \cdots X_4^{n_3} Z_4^{n_2} M_3(\phi_3^*) X_3^{n_2} Z_3^{n_1} M_2(\phi_2^*) X_2^{n_1} M_1(\phi_1^*) |G\rangle, \tag{3.28}$$

where $|G\rangle = \left(\prod_{i=1}^{m} CZ_{i,i+1}\right) |+\rangle^{\otimes N}$. Now, we can use the measurement identity

$$M(\phi^*) X^n Z^m = M(\phi), \quad \text{where} \quad \phi = (-1)^n \phi^* + m\pi, \tag{3.29}$$

to rewrite Eq. (3.28) as an adaptive measurement pattern on the cluster state $|G\rangle$

$$X_{m+1}^{n_m} Z_{m+1}^{n_{m-1}} M_m(\phi_m) \cdots M_3(\phi_3) M_2(\phi_2) M_1(\phi_1) |G\rangle, \tag{3.30}$$

where

$$\phi_k = f_k(n_{k-1}, n_{k-2}) = (-1)^{n_{k-1}} \phi_k^* + n_{k-2}\pi. \tag{3.31}$$

This sequence of adaptive measurements can be executed using a one-way computer

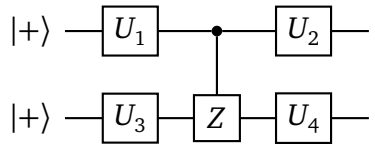
on the linear cluster state $|G\rangle$ prepared on $m+1$ qubits. The last qubit remaining after the measurements will be in the state $Z^{n_{m-1}}X^{n_m}U|+\rangle$, thus, the above measurement pattern is equivalent to the single-qubit quantum circuit we started from up to the Pauli errors $Z^{n_{m-1}}X^{n_m}$ which can be corrected for at the end of the calculation.

We shown that by making measurement patterns on a linear cluster state we can simulate any single-qubit gate. Furthermore, since the gate set

$$\{CZ, \text{all single-qubit gates}\} \tag{3.32}$$

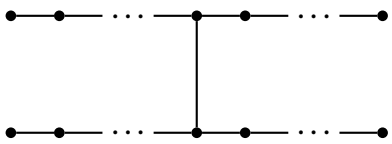
is a universal, any quantum circuit can be decomposed into a product of single-qubit and CZ gates. The existence of such a decomposition makes it possible to construct a cluster state and a measurement pattern for any quantum circuit, such that the execution of the measurement pattern on the cluster state simulates the quantum circuit up to known single-qubit Pauli errors [26, 58].

For example, let us consider the two-qubit circuit



; (3.33)

the single-qubit gates U_1, U_2, U_3 and U_4 can be replaced with a linear cluster state and the CZ gate simply becomes an edge between the appropriate qubits, this yields a cluster state with the following topology



, (3.34)

where the black dots denote vertices or qubits and the lines between the vertices are the edges of the graph G. The cluster state $|G\rangle$ can simulate the two-qubit circuit defined above.

In general, a quantum wire in the quantum circuit model can be translated into a linear cluster state, and a CZ gate between two qubits can be translated into an edge interconnecting the linear cluster states corresponding to the qubits on which the CZ gate acts. On such a cluster state we can always find a measurement pattern which simulates the desired quantum circuit by measuring the vertices of the cluster state from left to right. After, the measurements the remaining qubits of the cluster will encode the final state.

We can thus conclude that cluster state quantum computation is just as powerful as the gate-based quantum computation described by the quantum circuit model, since for every quantum circuit we may construct a cluster state which can simulate the desired quantum circuit without an excessive resource overhead. But these cluster states are specific to the quantum circuits they simulate. Thus, the following question arises naturally: Is there a cluster state which can simulate any quantum circuit? The answer to this question is: Yes.

Resource states which can simulate any quantum circuit with some arbitrary bound on the number of qubits is called a universal resource state. For example, a cluster state defined by a two-dimensional lattice can simulate any quantum circuit with less than n qubits—given the lattice is large enough—where $n \in \mathbb{N}^+$ is arbitrary integer. Cluster states based on three-dimensional lattices also allow the implementation of quantum error correction [24].

While universal resource states would be extremely useful, their generation is notoriously difficult. Since the invention of MBQC several theoretical approaches have been developed to generate them, but to date the generation of large universal cluster states is still an unsolved problem in the practical sense. Methods for creating photonic cluster states include linear-optical protocols based on the percolation of lattices [59], and the use of optically addressable quantum emitters [60].

3.4 Qudits and High-Dimensional Cluster States

In the definition of the quantum circuit model, we made the rather arbitrary decision to build our quantum computer out of two-level systems—named qubits. Equivalently, one may define a quantum computer build out of high-dimensional units, $d > 2$ level quantum systems called qudits.

The quantum circuit model generalizes easily to qudits. When using qudits to describe quantum computation, the main difference is that the Hilbert space of an individual qudits is larger (d-dimensional), and thus local operations on the qudit register are represented by unitaries in $\mathrm{U}(d)$.

There are several different conventions in use for the generalization of the well-known Pauli X and Z gates for qudit systems. We will use the following definitions

$$X = \sum_{n=0}^{d-1} |n \oplus 1\rangle \langle n| , \qquad Z = \sum_{n=0}^{d-1} \omega^n |n\rangle \langle n| , \tag{3.35}$$

where $\oplus$ means addition modulo d and $\omega = \exp(i2\pi/d)$. One can immediately see that X and Z are unitary and $X^d = Z^d = \mathbb{1}$. However, it is important to note that they are

not Hermitian for $d > 2$.

Since the qudit gates X and Z defined above have the same eigenvalues, they satisfy the similarity relation,

$$HXH^\dagger = Z, \tag{3.36}$$

where the corresponding basis change operator defines the qudit Hadamard gate

$$H = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} \sum_{m=0}^{d-1} \omega^{nm} |n\rangle \langle m| . \tag{3.37}$$

The Hadamard gate is often used to prepare the qudit state

$$|+\rangle = H|0\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} |n\rangle , \tag{3.38}$$

which plays a key role in many quantum algorithms.

The controlled X and Z gates are defined as

$$CX = \sum_{n=0}^{d-1} |n\rangle \langle n| \otimes X^n, \qquad CZ = \sum_{n=0}^{d-1} |n\rangle \langle n| \otimes Z^n. \tag{3.39}$$

From Eq. (3.36) it follows that

$$CX = \left(\mathbb{1} \otimes H^\dagger\right) CZ \left(\mathbb{1} \otimes H\right). \tag{3.40}$$

From Eq. (3.39) it follows that $CX\,|n\rangle \otimes |m\rangle = |n\rangle \otimes |n \oplus m\rangle$, thus, one can write

$$\begin{aligned} CX^\dagger(\mathbb{1} \otimes Z)CX\,|n\rangle \otimes |m\rangle &= CX^\dagger(\mathbb{1} \otimes Z)\,|n\rangle \otimes |n \oplus m\rangle \\ &= CX^\dagger \omega^{n+m}\,|n\rangle \otimes |n \oplus m\rangle \\ &= \omega^{n+m}\,|n\rangle \otimes |m\rangle = Z \otimes Z\,|n\rangle \otimes |m\rangle , \end{aligned} \tag{3.41}$$

where $n, m \in \{0, 1, 2, \ldots d-1\}$, therefore

$$CX^\dagger(\mathbb{1} \otimes Z^m)CX = Z^m \otimes Z^m, \tag{3.42}$$

and by a similar derivation we can obtain

$$CX(\mathbb{1} \otimes Z^{-m})CX^\dagger = Z^m \otimes Z^{-m}. \tag{3.43}$$

Equations (3.42) and (3.43) will prove to be useful later when one needs to decompose unitaries of the form $\exp(i\alpha Z \otimes Z)$.

Another useful qudit gate is the *one-level controlled-Z* gate $\overline{\mathrm{CZ}}$, which is defined by its action on the basis states $|k\rangle \otimes |l\rangle$ as

$$\overline{\mathrm{CZ}}\,|k\rangle \otimes |l\rangle = \exp\left(i2\pi l \delta_{k,d-1}/d\right)|k\rangle \otimes |l\rangle\,, \tag{3.44}$$

where $\delta_{k,l}$ denotes the Kronecker delta.

Similarly to the qubit case the gate one can look for universal gate sets. Important examples of universal gate sets include the following two [30]:

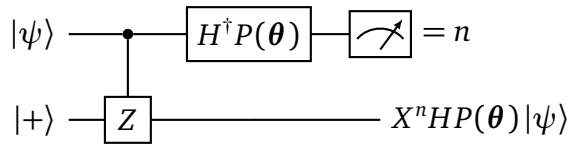
$$\{\overline{CZ}, \text{all single-qudit gates}\}, \qquad \{CZ, \text{all single-qudit gates}\}, \tag{3.45}$$

the latter we can simulate by high-dimensional MBQC.

The definitions of the above gates generalize the properties of the qubit gates—their Clifford algebra—that we used in the previous section to define a universal one-way computer operating on cluster states. Now it is possible to extend those definitions and define high-dimensional cluster state computation without much further explanation.

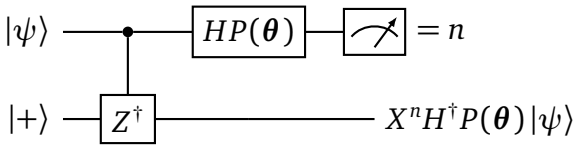
A high-dimensional cluster state is also associated with a graph G. Each vertex of the graph corresponds to a qudit and every edge of the graph describes an entangled pair of qudits. In the high-dimensional case there are actually at least two possible ways to entangle a qudit pair and still have the nice properties of cluster states. We may use either CZ or $CZ^\dagger$ to entangle two qudits—noting that $CZ \neq CZ^\dagger$ for $d > 2$. Allowing the $CZ^\dagger$ edges is not necessary to simulate the quantum circuit model, but it helps translating quantum circuits into cluster states and measurement patterns.

As in the qubit case we have the teleportation identities [61]



(3.46)

and



(3.47)

which we can use to translate any qudit quantum circuit into a qudit cluster state with CZ and $CZ^\dagger$ edges and a measurement pattern. In the above equations $P(\boldsymbol{\theta})$, $\boldsymbol{\theta} \in \mathbb{R}^d$ is the phase gate defined by the action: $P(\boldsymbol{\theta})\,|k\rangle = \exp(i\theta_k)\,|k\rangle$ for qudit levels $|k\rangle$.

The translation of quantum circuits into cluster states and measurement patterns works the same way as in the qubit case. Qudit wires are translated into linear cluster

states and CZ or $CZ^\dagger$ gates become edges interconnecting the corresponding pairs of linear clusters. An example of this is shown by Fig. 3.4. The figure shows the qudit cluster state which can implement the two-qudit unitary $U = CXP(\boldsymbol{\theta})CX^\dagger$.

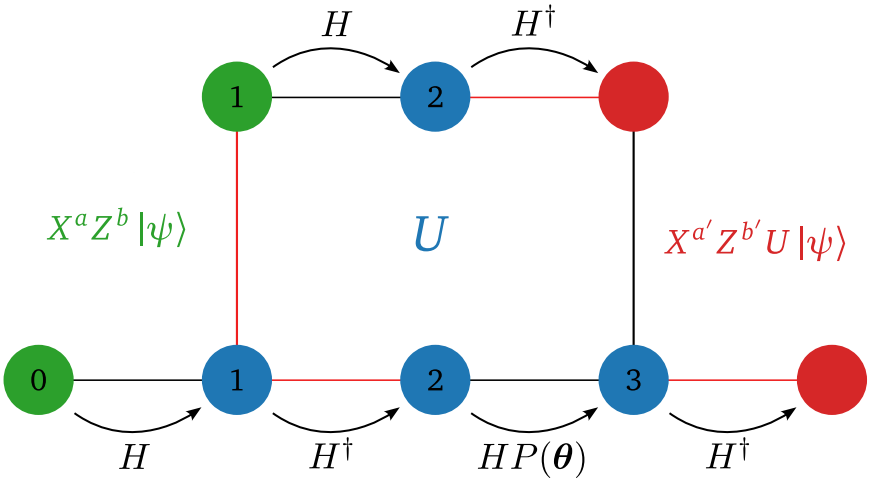


Figure 3.4: Qudit cluster state with the measurement instructions to implement the two qudit unitary $U = CXP(\boldsymbol{\theta})CX^\dagger$. The black and red edges denote the CZ and $CZ^\dagger$ connections between the physical qudits. The initial state with its Pauli errors is encoded in the green qudits. The measurement order is indicated by the numbers. After the execution of all the measurements, the final state is encoded in the red qubits. The arrows show how the qudit states are teleported from one qudit to the next, and the unitary of each arrow indicates what transformation should the teleportation perform.

Chapter 4

Results

This chapter describes the two main results of this work. The first result is on the the linear-optical synthesis of locally optimal many-qudit gates acting on multi-rail encoded qudits. The second result is about the resource efficient solution of d-ary optimization problems using high-dimensional cluster states encoded by multi-rail photonic qudits. The second result is illustrated on the k-coloring problem. This chapter is based on the author's manuscript titled: "Efficient qudit based scheme for photonic quantum computing". arXiv:2302.07357, 2023.

4.1 Multi-Rail Encoding

The multi-rail encoding is the generalization of the dual-rail encoding introduced in Sec. 3.2. A single qudit is encoded into d number of optical modes by a single photon. If the d modes are labeled with indices $i_0, i_1, \dots i_{d-1}$

$$\|k\rangle\!\rangle_I = |0\rangle_{i_0} |0\rangle_{i_1} \cdots |1\rangle_{i_k} \cdots |0\rangle_{i_{d-1}}, \tag{4.1}$$

where I is the ordered d-tuple $(i_0, i_1, \dots, i_{d-1})$ and $k \in \{0, 1, \dots, d-1\}$ denotes the possible qudit levels. The $\|\rangle\!\rangle$ notation is used to denote the logical qudit states and the simple kets $|\rangle$ denote photon number states. The tensor product notations $|i\rangle_a \otimes |j\rangle_b$, $|i\rangle_a |j\rangle_b$ and $|i, j\rangle_{a,b}$ are used interchangeably.

We may consider the effect of a linear-optical transformation $S \in \mathrm{U}(d)$ on modes in the tuple I encoding a single qudit

$$\left(a_{i_0}^\dagger, \;\; a_{i_1}^\dagger, \;\; \cdots, \;\; a_{i_{d-1}}^\dagger\right) \to \left(a_{i_0}^\dagger, \;\; a_{i_1}^\dagger, \;\; \cdots, \;\; a_{i_{d-1}}^\dagger\right) S \tag{4.2}$$

on the arbitrary state $\|\psi\rangle\!\rangle_I = \sum_{k=0}^{d-1} \alpha_k \|k\rangle\!\rangle_I$ representing an element of the single-qudit

Hilbert space $\mathscr{H}$. The state $\|\psi\rangle\!\rangle_I$ transforms as follows

$$\|\psi\rangle\!\rangle_I \to \left(a_{i_0}^\dagger,\ a_{i_1}^\dagger,\ \cdots,\ a_{i_{d-1}}^\dagger\right) S \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} |0\rangle = \sum_{k=0}^{d-1} \alpha'_k \|k\rangle\!\rangle_I \in \mathscr{H}, \tag{4.3}$$

where $\alpha'_k = \sum_{l=0}^{d-1} S_{kl}\alpha_l$. Thus, the linear-optical transformation S acts as single-qudit gate on $\mathscr{H}$. The corollary of this is that we may implement any single-qudit gate using a network of beamsplitters and phase shifters. The required configuration of beamsplitters and phase shifters can be calculated using the Clements decomposition [62].

On the other hand, entangling two-qudit gates cannot be realized using only linear-optical networks. The proof of this statement is essentially the same as the proof presented in Appendix A. However, we can synthesize two-qudit gates using the nonlinear phase shift operation as shown by Fig. 4.1. The construction shown by the figure is the generalization of the KLM non-deterministic CZ gate (see Sec. 3.2).

Figure 4.1 shows a linear-optical implementation of the non-deterministic $\overline{CZ}$ gate. It is important to note that the nonlinear phase shifts require ancilla modes and PNRDs to implement. This decomposition requires $2(d-1)$ symmetric beamsplitters and the same number of nonlinear phase shifts. Since the success probability of a nonlinear phase shift is at most $1/4$ (see Appendix B), the success probability of the non-deterministic $\overline{CZ}$ constructed from nonlinear phase shifts is bounded from above by $1/16^{d-1}$. This means that the success rate gets exponentially small with increasing d.

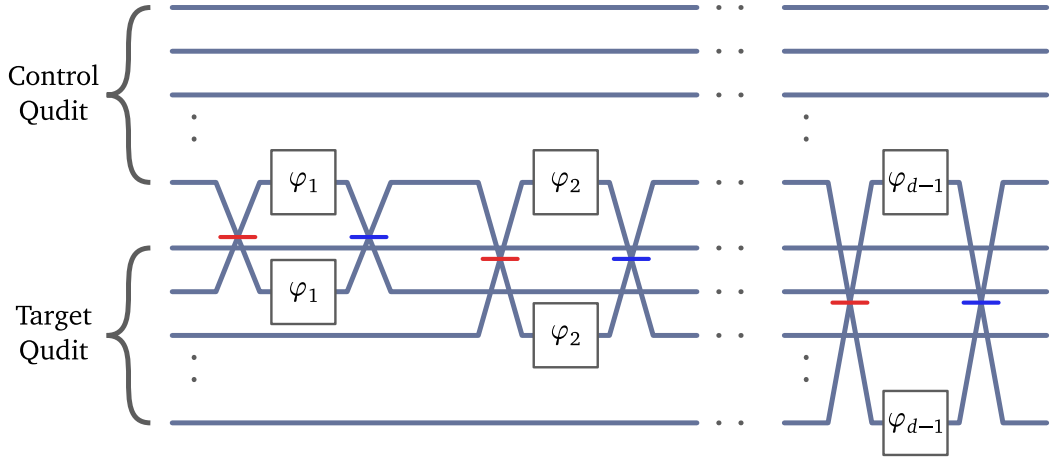


Figure 4.1: Realization of the $\overline{\text{CZ}}$ gate entangling two qudits defined by the multi-rail encoding. The red and blue segments indicate symmetric beamsplitters with angles $\theta = \pm\pi/4$ and $\phi = 0$ (red is plus and blue is minus), and the white boxes denote nonlinear phase shifts with angles $\varphi_k = 2\pi k/d$.

4.2 Locally Optimal Many-Qudit gates

The immediate question regarding the construction presented by Fig 4.1 is that, can we achieve a better success rate? Or more generally, what is the optimal way—optimal in success probability—to implement a non-deterministic entangling gate using linear optics and PNRDs?

It turns out answering these questions are fundamentally difficult—unless an unlikely breakthrough is made in the complexity theory of permanents [53]. For the qubit case, these questions were addressed in Ref. [63], where they gave locally optimal solutions for many-qubit gates using numerical optimization techniques. In this section the methods of Ref. [63] are developed further to find locally optimal solutions for entangling many-qudit gates acting on multi-rail encoded qudits.

A qudit register of N-qudits can be encoded into $d \cdot N$ different optical modes. The qudit register's Hilbert space is just the following subset of the Fock space

$$\mathscr{H} = \left\{ \sum_{k_0,k_1,\ldots,k_{N-1}=0}^{d-1} \alpha_{k_0,k_1,\ldots,k_{N-1}} \left\|k_0\right\rangle\!\right\rangle_{I_0} \left\|k_1\right\rangle\!\right\rangle_{I_1} \cdots \left\|k_{N-1}\right\rangle\!\right\rangle_{I_{N-1}} \;\middle|\; \alpha_{k_0,k_1,\ldots,k_{N-1}} \in \mathbb{C} \right\}, \tag{4.4}$$

where $I_0, I_1, \ldots, I_{N-1}$ are disjoint d-tuples containing the labels of $d \cdot N$ different optical modes which encode $\mathscr{H}$.

In order to linear-optically synthesize entangling qudit gates we can use the general interferometer configuration shown by Fig. 4.2. The input computational state $|\psi_{\text{in}}\rangle_c \in \mathscr{H}$ is first transformed by the linear-optical transformation S along with the ancilla state $|1\rangle^{\otimes N_a} |0\rangle^{\otimes N_v}$, then the ancilla modes are measured using PNRDs. If S is chosen correctly $|\psi_{\text{out}}\rangle_c \in \mathscr{H}$ is prepared after the ancilla measurement with some probability P, where $|\psi_{\text{out}}\rangle_c$ is related to $|\psi_{\text{in}}\rangle_c$ by a unitary transformation of the qudit register $T : \mathscr{H} \to \mathscr{H}$.

We may represent the state of the qudit register as a complex vector with d^N components, hence T can be represented as a $d^N \times d^N$ unitary matrix corresponding to a entangling N-qudit gate. If $|\psi_{\text{in}}\rangle = \sum_{k=0}^{d^N-1} \alpha_k \left\|k\right\rangle\!\right\rangle$ and $|\psi_{\text{out}}\rangle = \sum_{k=0}^{d^N-1} \beta_k \left\|k\right\rangle\!\right\rangle$ then

$$\begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{d^N-1} \end{pmatrix} = \begin{pmatrix} T_{0,0} & T_{0,1} & \cdots & T_{0,d^N-1} \\ T_{1,1} & T_{1,2} & \cdots & T_{1,d^N-1} \\ \vdots & \vdots & \ddots & \vdots \\ T_{d^N-1,0} & T_{d^N-1,1} & \cdots & T_{d^N-1,d^N-1} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d^N-1} \end{pmatrix}, \tag{4.5}$$

where $\left\|k\right\rangle\!\right\rangle \in \{\left\|k_0\right\rangle\!\right\rangle_{I_0} \left\|k_1\right\rangle\!\right\rangle_{I_1} \cdots \left\|k_{N-1}\right\rangle\!\right\rangle_{I_{N-1}} \mid k_0, k_1, \ldots, k_{N-1} \in \{0, 1, \ldots, d-1\}\}$.

Unfortunately, an entangling many-qudit gate cannot be implemented using a linear-

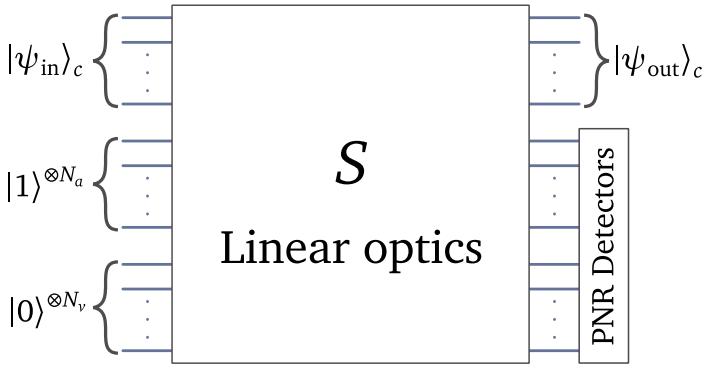


Figure 4.2: Configuration of an interferometer for a general nonlinear operation. The input many-qudit state is encoded in the top computational modes and the ancilla modes are shown below them. The ancilla modes are measured using PNRDs and the measurement result is used to determine whether the operation was successful or not. In the event of success, the computational output is encoded in the many-qudit state $|\psi_{\text{out}}\rangle_c$.

optical transformation S, such that $|\psi_{\text{out}}\rangle_c = U(S)|\psi_{\text{in}}\rangle_c$ for any $|\psi_{\text{in}}\rangle_c \in \mathscr{H}$. However, we may write down a weaker equality which holds for any $|\psi_{\text{in}}\rangle_c \in \mathscr{H}$ for some linear-optical transformation S

$$U(S)|\psi_{\text{in}}\rangle_c |1\rangle^{\otimes N_a} |0\rangle^{\otimes N_v} = \xi\sqrt{P}\,|\psi_{\text{out}}\rangle_c |1\rangle^{\otimes N_a} |0\rangle^{\otimes N_v} + \text{other ancilla projections}, \quad (4.6)$$

given the numbers N_a and N_v are large enough. Above $P > 0$ is the probability of measuring the ancilla state $|1\rangle^{\otimes N_a} |0\rangle^{\otimes N_v}$ and ξ is an arbitrary global phase ($|\xi| = 1$). By preparing the output state on an ancilla projection the gate T can be implemented non-deterministically via postselection with success probability P.

From Eq. (4.6) the relation between the matrix T and matrix S can be given as follows

$$\begin{cases} \langle\tilde{\mathbf{n}}|\, U(S)\, \|m\rangle\!\rangle\, |1\rangle^{\otimes N_a} |0\rangle^{\otimes N_v} = \xi\sqrt{P}\, T_{n,m}, & \text{if } \exists n : |\tilde{\mathbf{n}}\rangle = \|n\rangle\!\rangle\, |1\rangle^{\otimes N_a} |0\rangle^{\otimes N_v} \\ \langle\tilde{\mathbf{n}}|\, U(S)\, \|m\rangle\!\rangle\, |1\rangle^{\otimes N_a} |0\rangle^{\otimes N_v} = 0 & \text{otherwise,} \end{cases} \quad (4.7)$$

where $|\tilde{\mathbf{n}}\rangle = |\mathbf{n}\rangle\, |1\rangle^{\otimes N_a} |0\rangle^{\otimes N_v}$ and $|\mathbf{n}\rangle = |n_1, n_2, \ldots\rangle$ is an N-photon occupation number state $\left(\sum_k n_k = N\right)$ defined on the modes encoding the computational space. The notation can be simplified if we introduce the non-square matrices $\tilde{T}$ and $\tilde{U}$

$$\tilde{T}_{\mathbf{n},m} = \begin{cases} T_{n,m} & \text{if } \exists n : |\mathbf{n}\rangle = \|n\rangle\!\rangle \\ 0 & \text{otherwise} \end{cases} \quad (4.8)$$

and

$$\tilde{U}_{\mathbf{n},m} = \langle \tilde{\mathbf{n}} | \, U(S) \, \| m \rangle\!\rangle \, |1\rangle^{\otimes N_a} |0\rangle^{\otimes N_v}, \tag{4.9}$$

where $\mathbf{n} \in \left\{ \mathbf{n} \mid \sum_k n_k = N \right\}$ and $m \in \{0, 1, \ldots, d^N - 1\}$. With this new notation Eq. (4.7) can be rewritten as

$$\tilde{U}_{\mathbf{n},m} = \xi \sqrt{P} \tilde{T}_{\mathbf{n},m}. \tag{4.10}$$

If the matrix elements $\tilde{U}_{\mathbf{n},m}$ are expanded using the permanent formula given in Eq. (2.46), then Eq. (4.10) becomes a system of multivariate polynomial equations whose unknown variables are the matrix elements of S. This system of polynomial equations cannot be solved analytically even for the simplest entangling gates; therefore, a numerical approach is necessary.

The problem of for solving the matrix S can be encoded into the optimization problem defined by the cost function

$$L = F + \lambda P + \sigma C, \tag{4.11}$$

where

$$F = \frac{|\mathrm{Tr}\left(\tilde{U}^\dagger \tilde{T}\right)|^2}{\mathrm{Tr}\left(\tilde{U}^\dagger \tilde{U}\right) \mathrm{Tr}\left(\tilde{T}^\dagger \tilde{T}\right)}, \qquad P = \frac{\mathrm{Tr}\left(\tilde{U}^\dagger \tilde{U}\right)}{\mathrm{Tr}\left(\tilde{T}^\dagger \tilde{T}\right)}, \qquad C = -\mathrm{Tr}\left\{ \left(S^\dagger S - \mathbb{1}\right)^2 \right\} \tag{4.12}$$

and λ, σ are non-negative real constants. The value of F gives the fidelity of the gate implementation; the Cauchy-Schwarz inequality implies that F is equal to 1 if and only if Eq. (4.10) holds for some probability P. The C term in L simply ensures that S is unitary. Therefore, local maxima of L correspond to locally optimal implementations of the many-qudit gate T—optimal in the success probability P.

The optimization problem defined by L was solved using a trust-region method [64]. The optimization process went as follows. First the problem was solved using $\lambda = 0$. Once a solution with $F = 1$ and $C = 0$ was found λ was gradually increased to the largest possible value for which the solution still converged to $F = 1$.

At the beginning N_a and N_v were chosen such that the system of equations for the matrix elements of S would be under-defined. After finding a solution N_a and N_v would be decreased until no solution with $F = 1$ and $C = 0$ could be found. This process was carried out for the qutrit $\overline{CZ}$ and CZ gates (see Table 4.1).

There is a significant improvement in the success rate when the gates are optimized. These optimized gates could be used to non-deterministically prepare entangled photon states which are necessary for many measurement-based architectures like optical cluster state computing. In the following sections we will look at how high-dimensional

cluster states might be used in photonic qudit schemes in general and in particular for the k-coloring problem.

T	P_{naive}	P	N_a	N_v
CZ (qubit) [65]	0.0625	0.0740	2	0
$\overline{\text{CZ}}$ (qutrit)	≈ 0.0016	0.011	3	3
CZ (qutrit)	≈ 0.00000256	0.000507	5	4

Table 4.1: Optimized two-qutrit gates. The probability P_{naive} is the gate success rate when the gates are decomposed into many nonlinear phase shifts. The probability P is the best success rate found after performing the optimization process for many different randomly selected initial conditions.

4.3 Graph Coloring With Qudit Cluster States

Graph coloring is one of the most studied topics of graph theory because of its applications in solving scheduling problems and compiler theory [46, 47]. Coloring refers to the assignment of labels (colors) from a label set to the vertices of a graph G. This assignment defines a map $C : V \to L$, where V is the set containing the vertices of G and L is the label set.

Arbitrarily ordering the vertices of G allows us to represent a coloring as string of labels: If we call the i-th vertex $v_i \in V$ and its assigned color $C(v_i) = l_i \in L$, then the string $\mathbf{l} = l_1 l_2 l_3 \ldots l_{|V|}$ completely characterizes the coloring C. The k-coloring problem of a graph is to decide whether the vertices of the graph can be colored using k colors, such that no adjacent vertices have the same color. The smallest k for which the k-coloring is possible for a given graph is called the chromatic number of the graph. The k-coloring problem of an arbitrary graph is known to be NP-complete [66–68].

It was shown that there are exponential time quantum algorithms which can solve the k-coloring problem faster than the best classical algorithms known for the problem [69], and even certain heuristic variational quantum algorithms for a similar problem have been hinted to outperform classical methods [70]. Therefore, one might conjecture that a heuristic graph coloring algorithm based on the quantum approximate optimization algorithm (QAOA) [45] might have an edge over classical computers. In the text below a qubit and a high-dimensional version of the QAOA algorithm for solving the k-coloring problem are presented.

Qubit algorithm

The k-coloring problem can be reformulated as a combinatorial optimization problem where the goal is to minimize the number of edges connecting vertices with identical colors by searching through the possible $|V|$ length strings of the label set $L = \{0, 1, 2, \ldots, k-1\}$. On qubit-based architectures, binary optimization problems can be solved using QAOA. Encoding the strings of L as bit-strings means that we can use QAOA to solve the k-coloring problem as well; such a QAOA type of approach for the k-coloring (and the related k-SAT problem) has been studied in Refs. [71–75].

The encoding of colorings into bit-strings is most easily done via the one-hot encoding, this means that the strings of L are encoded into $N = |V| \cdot k$ bits, where each set of k consecutive bits encodes the color of a vertex. The color of the i-th vertex l_i is indicated by the i-th set of k bits of the form $00\ldots010\ldots00$, where the l_i-th bit is flipped and the rest of the k bits is zero. We will denote the j-th bit of the i-th set of k bits by $x_{i,j}$.

Minimizing the cost function $f : \{0,1\}^N \to \mathbb{R}$

$$f(\mathbf{x}) = C \sum_{n=1}^{|V|} \left(1 - \sum_{i=0}^{k-1} x_{n,i} \right)^2 + D \sum_{n=1}^{|V|} \sum_{m=1}^{|V|} \sum_{i=0}^{k-1} A_{nm} x_{n,i} x_{m,i}, \tag{4.13}$$

is equivalent to finding a solution to the k-coloring problem, where $\mathbf{x}$ is a bit-string of length N, A_{nm} are the matrix elements of the adjacency matrix of G and C and D are arbitrary positive real constants. The first term in Eq. (4.13) weighted by C is a penalty term, since not every bit-string of length N corresponds to a coloring. For every $n \in \{1, 2, \ldots, |V|\}$ exactly one of the k bits $x_{n,j}$, where $j \in \{0, 1, \ldots, k-1\}$, has to equal one in order for $\mathbf{x}$ to encode a coloring. The remaining term simply counts the number of edges that connect vertices with the same color.

To construct the QAOA cost Hamiltonian we can use the recipe

$$H_C = \sum_{\mathbf{x} \in \{0,1\}^N} f(\mathbf{x}) \left| \mathbf{x} \right\rangle \left\langle \mathbf{x} \right|, \tag{4.14}$$

where $|\mathbf{x}\rangle$ is the computational state

$$\bigotimes_{n=1}^{|V|} \left(\bigotimes_{i=0}^{k-1} |x_{n,i}\rangle \right).$$

Substituting Eq. (4.13) into Eq. (4.14), the cost Hamiltonian becomes

$$H_C = \frac{C}{4} \sum_{n=1}^{|V|} \left(2\mathbb{1} - \sum_{i=0}^{k-1} \left(\mathbb{1} - Z_{n,i} \right) \right)^2 + \frac{D}{4} \sum_{n=1}^{|V|} \sum_{m=1}^{|V|} \sum_{i=0}^{k-1} A_{nm} \left(\mathbb{1} - Z_{n,i} \right) \left(\mathbb{1} - Z_{m,i} \right), \tag{4.15}$$

where $Z_{n,i}$ is the Pauli Z matrix acting on the $(k \cdot (n-1)+i)$-th qubit labeled by the tuple (n,i). Obtaining the ground state of H_C is the same as finding a bit-string that minimizes the cost function f [72].

QAOA minimizes the expectation value $\langle \psi(\boldsymbol{\alpha},\boldsymbol{\beta})| H_C |\psi(\boldsymbol{\alpha},\boldsymbol{\beta})\rangle$, where

$$|\psi(\boldsymbol{\alpha},\boldsymbol{\beta})\rangle = \left(\prod_{n=1}^{p} e^{i\alpha_n H_M} e^{i\beta_n H_C}\right) |+\rangle^{\otimes N}, \tag{4.16}$$

$\boldsymbol{\alpha},\boldsymbol{\beta} \in \mathbb{R}^p$ and

$$H_M = \sum_{n=1}^{|V|}\sum_{i=0}^{k-1} X_{n,i}$$

is the mixing Hamiltonian, where p denotes the number of QAOA layers.

Preparation of $|\psi(\boldsymbol{\alpha},\boldsymbol{\beta})\rangle$ requires the implementation of two parameterized unitary $U_M(\alpha) = e^{i\alpha H_M}$ and $U_C(\beta) = e^{i\beta H_C}$. U_M can be realized using single qubit rotations and only U_C requires entangling gates. U_C can be further separated into the product of two unitaries, where one of the unitary requires only single qubit phase gates and the other unitary requires only controlled rotations.

This can be achieved by separating the cost Hamiltonian into a non-interacting and an interacting part, $H_C = H_0 + H_1$, where

$$H_1 = \frac{C}{2}\sum_{n=1}^{|V|}\sum_{i<j=0}^{k-1} Z_{n,i}Z_{n,j} + \frac{D}{2}\sum_{\{n,m\}\in E}\sum_{i=0}^{k-1} Z_{n,i}Z_{m,i}. \tag{4.17}$$

In Eq. (4.17) E denotes the set containing the edges of the graph. The Hamiltonians H_0 and H_1 commute since they only contain Pauli Z matrices, thus

$$U_C(\alpha) = e^{i\alpha H_0} e^{i\alpha H_1}. \tag{4.18}$$

The unitary $e^{i\alpha H_1}$ can be decomposed into the product of $|V|\binom{k}{2} + k|E|$ number of controlled rotations

$$\begin{aligned} e^{i\alpha H_1} = &\prod_{n=1}^{|V|}\left(\prod_{i<j=1}^{k} CX_{n,i;n,j} P_{n,j}(\alpha C/2) CX_{n,i;n,j}\right) \\ &\times \prod_{\{n,m\}\in E}\left(\prod_{i=0}^{k-1} CX_{n,i;m,i} P_{m,i}(\alpha D/2) CX_{n,i;m,i}\right), \end{aligned} \tag{4.19}$$

where $P_{n,j}(\alpha) = e^{i\alpha Z_{n,j}}$ is the phase gate acting on the qubit labeled by the pair of indices (n,j) and $CX_{n,i;n,j}$ is a controlled NOT gate between the control qubit (n,i) and the target qubit (n,j). Eq. (4.19) can be derived using the identity $e^{i\alpha Z\otimes Z} = CX\,(\mathbb{1}\otimes P(\alpha))\,CX$.

The physical realization of the unitary $e^{i\alpha H_1}$ requires by far the most-amount of physical resources compared to the other parts of the algorithm, since only this part needs entangling gates. Therefore, focusing only on the implementation details of $e^{i\alpha H_1}$ can give us a good lower bound on the resources necessary to carry out the QAOA.

Graph coloring using qudits

When using qudits with dimension $d = k$, there is a one-to-one correspondence between the computational basis and the possible graph colorings with k colors via the mapping

$$l_1 l_2 l_3 \dots l_{|V|} \to |l_1\rangle \otimes |l_2\rangle \otimes |l_3\rangle \otimes \cdots \otimes |l_{|V|}\rangle\,, \tag{4.20}$$

where $l_i \in \{0, 1, 2, \dots, k-1\}$. This means that the coloring problem can be formulated as an unconstrained d-ary optimization problem which can be solved by the QAOA generalized to qudits [76–78]. Because the optimization problem is unconstrained, the decomposition of the QAOA layers will turn out to be simpler due to lack of penalty terms.

The QAOA for qudits is very similar to the qubit version only the form of the mixing and cost Hamiltonian is different. The mixing Hamiltonian is still a simple sum of single-qudit terms, e.g., the r-nearby-values single-qudit mixer $H_M = \sum_{n=1}^{|V|} \sum_{i=1}^{r} \left(X_n^i + X_n^{\dagger i}\right)$ as in Ref. [77], and the cost Hamiltonian is

$$H_C = \sum_{n=1}^{|V|} \sum_{m=1}^{|V|} \sum_{i=0}^{k-1} A_{nm} Z_n^i Z_m^{k-i} = \sum_{\{n,m\}\in E} \sum_{i=0}^{k-1} Z_n^i Z_m^{k-i}, \tag{4.21}$$

where Z_n is the qudit Pauli Z gate acting on the n-th qudit and A_{nm} are the matrix elements of the adjacency matrix of the graph G.

The ground states of the Hamiltonian H_C correspond to optimal k-colorings of G. Similarly to the qubit case, we can decompose the unitary $U_C(\alpha) = e^{i\alpha H_C}$ into $|E|$ number of controlled qudit rotations

$$e^{i\alpha H_C} = \prod_{\{n,m\}\in E} CX_{n;m} P_m(\alpha) CX_{n;m}^{\dagger}, \tag{4.22}$$

where $P_m(\alpha)$ is a single-qudit phase gate which acts on the m-th qudit the following way

$$P_m(\alpha)\,|\mathbf{x}\rangle = e^{i\alpha \sum_{n=0}^{k-1} Z_m^n}\,|\mathbf{x}\rangle = \begin{cases} e^{i\alpha k}\,|\mathbf{x}\rangle & \text{if } x_m = 0, \\ |\mathbf{x}\rangle & \text{otherwise.} \end{cases} \tag{4.23}$$

Cluster states for the qubit and qudit implementations

Having established all the necessary techniques to implement the QAOA solution of the k-coloring problem both using qubits and qudits, we can now compare the physical resources used by the two methods. A single layer of the qudit QAOA algorithm without the mixing part can be executed on the qudit cluster state C_d constructed from many copies of R_d, where R_d is a cluster with the topology depicted by Fig. 3.4 made up by d-dimensional qudits. When the number of colors is k, one has to use $d{=}k$-dimensional qudits for the algorithm. The construction of C_d is shown by Fig. 4.3. The construction of C_2, the qubit equivalent of C_d, works differently. In the qubit case, one must add k copies of R_2 for each edge of G and $k(k-1)/2$ copies for each node of G. These construction rules follow from the decompositions in Eqs. (4.19) and (4.22).

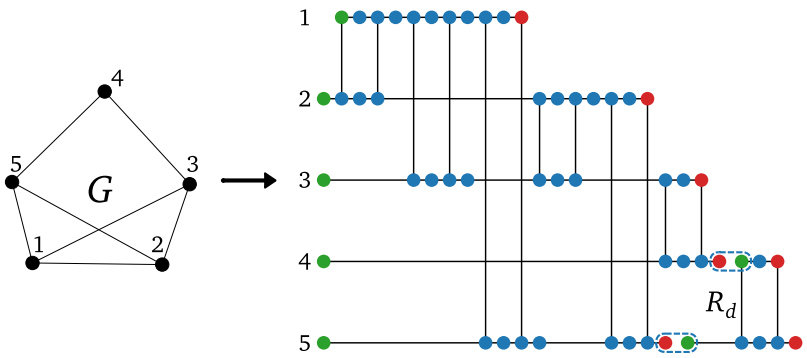


Figure 4.3: Qudit cluster state for a single layer of the qudit QAOA. Each edge of G corresponds to a controlled qudit rotation in the decomposition of $\exp(i\alpha H_C)$ described by Eq. (4.22). Thus one can chain many copies of R_d to form the complete qudit cluster. The two input nodes of R_d are merged with two output nodes of the unfinished cluster state based on the topology of G. Each row of physical qudits represents a logical qudit labeled by the numbers. Each logical qudit encodes the color of a node in G.

The number of qudits in C_d is approximately

$$|C_d| \approx |R_d| \cdot |E| = 8|E|, \tag{4.24}$$

where $|E|$ is the number of edges in G, which is equal to the number of copies of R_d used to build C_d, and $|R_d|$ is the number of qudits in R_d. The approximation can be made exact by carefully considering the precise sequence of node additions and removals in the cluster growing process, however, for large enough graphs Eq. (4.24) provides a highly accurate estimate. Similarly, the number of qubits in C_2 is

$$|C_2| \approx |R_2| \cdot \left(\binom{k}{2}|V| + k|E|\right) = 8\binom{k}{2}|V| + 8k|E|. \tag{4.25}$$

In general, the ratio $|C_2|/|C_d|$ is strictly larger than k, and in the large dense graph limit, when $|E| \gg |V|$, this ratio approaches k. This is illustrated by Fig. 4.4 for Erdős-Rényi random graphs. If one uses the multi-rail encoding described in Sec. 4.2, the photon numbers of the cluster states is equal to their size. The number of optical modes required to encode the cluster state C_d is $d|C_d|$ including the qubit case $d = 2$. Thus, the number of photons decreases by a k-fold and the number of optical modes halves, when using multi-rail qudits instead of KLM qubits to encode the k-coloring problem.

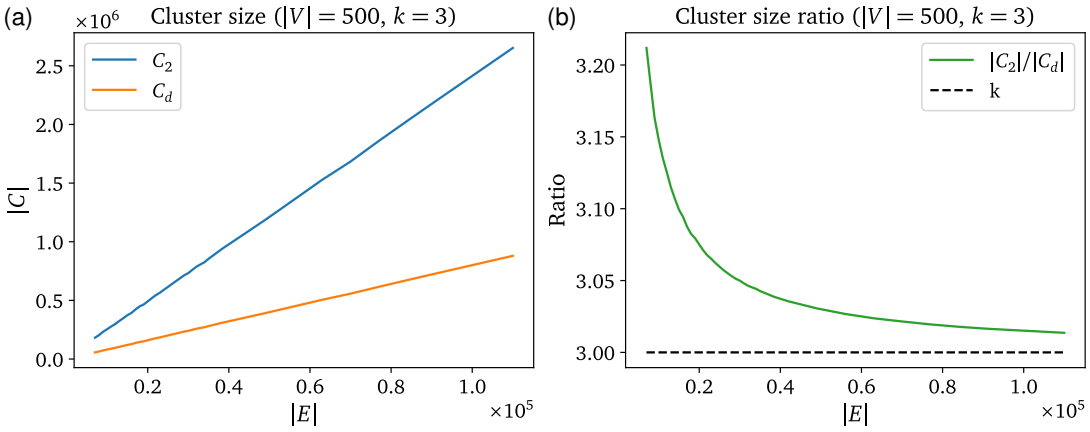


Figure 4.4: (a) Number of physical qubits and qudits versus the number of edges in G, the graph to be colored. $|C_2|$ is the number of physical qubits in the qubit cluster state implementation of $\exp(i\alpha H_1)$, where H_1 is defined by Eq. (4.17). $|C_d|$ is the number of physical qudits in the cluster state implementation of $\exp(i\alpha H_C)$, where H_C is defined in Eq. (4.21). (b) Ratio of the qubit and qudit cluster sizes when $|V| = 500$ and $k = 3$, where $|V|$ is the number of vertices in G and k is the number of colors used for the coloring.

Chapter 5

Conclusion

Nanofabrication techniques can integrate configurable linear-optical elements, PNRDs and single-photon sources onto a single chip in a scalable manner, for this reason, LOQC is one of the most promising directions towards scalable quantum information processing. In Chap. 4 two results were presented related to high-dimensional LOQC. First, the linear-optical synthesis of non-deterministic many-qudit gates was discussed, then the high-dimensional cluster state implementation of the k-coloring QAOA ansatz was introduced.

Single-qudit gates and measurements in LOQC can be done with relative ease, however, entangling gates require ancilla resources and postselection. Section 4.2 presented a numerical approach which can find linear-optical implementations of many-qudit gates with locally optimal probabilities. Using this technique locally optimal solutions were found for the $\overline{CZ}$ and CZ qutrit gates. Although, the synthesized two-qutrit gates are locally optimal, their success probability is low.

There seems to be a relation between the number of ancilla photons and the success probability of an optimal gate. The observation is that the more ancilla photons are needed to find a solution, the optimal probability gets excessively smaller. For this reason, for $d > 3$, linear-optical implementations of entangling many-qudit gates are unlikely to be practical. But for $d = 3$, the linear-optical implementation of CZ or $\overline{CZ}$ might be used for the linear-optical preparation of qutrit cluster states.

The method presented for the optimization of qudit gates works surprisingly well, despite the complexity of the equations (4.10). However, there are several questions to be answered about the mathematics of solving these equations. One of the most important questions is about the global maximum of the success rate. The global maximum seems to depend on the gate itself, e.g., the CZ and $\overline{CZ}$ gates have differences of several magnitudes in their local maxima, thus, it is unlikely they have the same global maxima. Another factor seems to be the configuration of the ancilla resources. In Sec. 4.2 only

the ancilla configuration $|1\rangle^{\otimes N_a}|0\rangle^{\otimes N_v}$ was considered, however, it is not clear whether starting or finishing with this ancilla configuration is the optimal way to implement a qudit gate.

The other topic of this thesis was the application of high-dimensional cluster state quantum computing to solve d-ary optimization problems with photonics. In Sec. 4.3 this application of qudit cluster states was illustrated on the k-coloring problem. To color any graph with k colors, either a qudit—with dimension $d{=}k$—or a qubit cluster state can be constructed, such that the former can implement the high-dimensional version of the k-coloring QAOA ansatz, and latter can implement the binary version of the k-coloring QAOA ansatz.

When these qudit and qubit cluster states are compared for large, dense graphs, the qudit cluster states encoded by the multi-rail encoding require k-times fewer number of photons and half as many optical modes than what it is needed to encode the corresponding qubit cluster states with dual-rail qubits. This result illustrates how high-dimensional cluster state computation could be used to reduce the resource requirements of certain algorithms.

The real difficulty of cluster state computation is in the generation of the cluster states, thus, results involving cluster states rely on the assumption that they can be generated efficiently. In a recent work it was shown that one can produce this type of high-dimensional cluster states deterministically using quantum emitters [79]. The methods shown in Ref. [79] combined with the result of this work give a convincing argument for the usefulness of multi-rail encoded high-dimensional cluster states.

References

[1] Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, Jun 1982.

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

[3] Craig Gidney and Martin Ekerå. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5:433, April 2021.

[4] Frank Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, Oct 2019.

[5] Han-Sen Zhong et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, 2020.

[6] Han-Sen Zhong et al. Phase-programmable gaussian boson sampling using stimulated squeezed light. *Phys. Rev. Lett.*, 127:180502, Oct 2021.

[7] Lars S. Madsen et al. Quantum computational advantage with a programmable photonic processor. *Nature*, 606(7912):75–81, Jun 2022.

[8] William P. Livingston et al. Experimental demonstration of continuous quantum error correction. *Nature Communications*, 13(1):2307, Apr 2022.

[9] Rajeev Acharya et al. Suppressing quantum errors by scaling a surface code logical qubit. *Nature*, 614(7949):676–681, Feb 2023.

[10] Zhongchu Ni et al. Beating the break-even point with a discrete-variable-encoded logical qubit. *Nature*, 616(7955):56–60, Apr 2023.

[11] David P. DiVincenzo. The physical implementation of quantum computation. *Fortschritte der Physik*, 48(9-11):771–783, 2000.

[12] Taira Giordani et al. Integrated photonics in quantum technologies. *La Rivista del Nuovo Cimento*, 46(2):71–103, Feb 2023.

[13] Caterina Taballione et al. A universal fully reconfigurable 12-mode quantum photonic processor. *Materials for Quantum Technology*, 1(3):035002, aug 2021.

[14] Wim Bogaerts et al. Programmable photonic circuits. *Nature*, 586(7828):207–216, Oct 2020.

[15] Justin B. Spring et al. Chip-based array of near-identical, pure, heralded single-photon sources. *Optica*, 4(1):90–96, Jan 2017.

[16] Erman Engin et al. Photon pair generation in a silicon micro-ring resonator with reverse bias enhancement. *Opt. Express*, 21(23):27826–27834, Nov 2013.

[17] Ashish Chanana et al. Ultra-low loss quantum photonic circuits integrated with single quantum emitters. *Nature Communications*, 13(1):7693, Dec 2022.

[18] J. P. Sprengers et al. Waveguide superconducting single-photon detectors for integrated quantum photonic circuits. *Applied Physics Letters*, 99(18), 11 2011. 181110.

[19] W. H. P. Pernice et al. High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits. *Nature Communications*, 3(1):1325, Dec 2012.

[20] Simone Ferrari, Carsten Schuck, and Wolfram Pernice. Waveguide-integrated superconducting nanowire single-photon detectors. *Nanophotonics*, 7(11):1725–1758, 2018.

[21] Samuel Gyger et al. Reconfigurable photonics with on-chip single-photon detectors. *Nature Communications*, 12(1):1408, Mar 2021.

[22] Jianwei Wang et al. Integrated photonic quantum technologies. *Nature Photonics*, 14(5):273–284, May 2020.

[23] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, Jan 2001.

[24] H. J. Briegel et al. Measurement-based quantum computation. *Nature Physics*, 5(1):19–26, Jan 2009.

[25] Hans J. Briegel and Robert Raussendorf. Persistent entanglement in arrays of interacting particles. *Phys. Rev. Lett.*, 86:910–913, Jan 2001.

[26] Michael A. Nielsen. Cluster-state quantum computation. *Reports on Mathematical Physics*, 57(1):147–161, 2006.

[27] Olivier Morin, Virginia D'Auria, Claude Fabre, and Julien Laurat. High-fidelity single-photon source based on a Type II optical parametric oscillator. *Opt. Lett.*, 37(17):3738–3740, Sep 2012.

[28] Xin Zhang, Chang Xu, and Zhongzhou Ren. High fidelity heralded single-photon source using cavity quantum electrodynamics. *Scientific Reports*, 8(1):3140, Feb 2018.

[29] Esmaeil Zadeh et la. Superconducting nanowire single-photon detectors: A perspective on evolution, state-of-the-art, future developments, and applications. *Applied Physics Letters*, 118(19), 05 2021. 190502.

[30] Yuchen Wang, Zixuan Hu, Barry C. Sanders, and Sabre Kais. Qudits and high-dimensional quantum computing. *Frontiers in Physics*, 8, 2020.

[31] Jason Alicea and Paul Fendley. Topological phases with parafermions: Theory and blueprints. *Annual Review of Condensed Matter Physics*, 7(1):119–139, 2016.

[32] Arpit Dua, Boris Malomed, Meng Cheng, and Liang Jiang. Universal quantum computing with parafermions assisted by a half-fluxon. *Phys. Rev. B*, 100:144508, Oct 2019.

[33] W. Y. Liu, H. K. Xu, F. F. Su, Z. Y. Li, Ye Tian, Siyuan Han, and S. P. Zhao. Coupled superconducting qudit-resonator system: Energy spectrum, state population, and state transition under microwave drive. *Phys. Rev. B*, 97:094513, Mar 2018.

[34] M. A. Yurtalan, J. Shi, M. Kononenko, A. Lupascu, and S. Ashhab. Implementation of a walsh-hadamard gate in a superconducting qutrit. *Phys. Rev. Lett.*, 125:180504, Oct 2020.

[35] Christian Reimer et al. High-dimensional one-way quantum processing implemented on d-level cluster states. *Nature Physics*, 15(2):148–153, Feb 2019.

[36] G. Lima et al. Experimental quantum tomography of photonic qudits via mutually unbiased basis. *Opt. Express*, 19(4):3542–3552, Feb 2011.

[37] B. Marques et al. Experimental simulation of decoherence in photonics qudits. *Scientific Reports*, 5(1):16049, Nov 2015.

[38] N. Bent et al. Experimental realization of quantum tomography of photonic qudits via symmetric informationally complete positive operator-valued measures. *Phys. Rev. X*, 5:041006, Oct 2015.

[39] Yunzhe Zheng, Hemant Sharma, and Johannes Borregaard. Entanglement distribution with minimal memory requirements using time-bin photonic qudits. *PRX Quantum*, 3:040319, Nov 2022.

[40] Hsuan-Hao Lu, Andrew M. Weiner, Pavel Lougovski, and Joseph M. Lukens. Quantum information processing with frequency-comb qudits. *IEEE Photonics Technology Letters*, 31(23):1858–1861, 2019.

[41] Hasnaa Hajji and Morad El Baz. Qutrit-based semi-quantum key distribution protocol. *Quantum Information Processing*, 20(1):4, Jan 2021.

[42] Ming-Xing Luo, Song-Ya Ma, Xiu-Bo Chen, and Yi-Xian Yang. The power of qutrit logic for quantum computation. *International Journal of Theoretical Physics*, 52(8):2959–2965, Aug 2013.

[43] Meiyu Wang, Fengli Yan, and Ting Gao. Generation of four-photon polarization entangled decoherence-free states with cross-kerr nonlinearity. *Scientific Reports*, 6(1):38233, Nov 2016.

[44] Gita Naseri and Mattheos A. G. Koffas. Application of combinatorial optimization strategies in synthetic biology. *Nature Communications*, 11(1):2446, May 2020.

[45] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum approximate optimization algorithm, 2014.

[46] Satish Thadani, Seema Bagora, and Anand Sharma. Applications of graph coloring in various fields. *Materials Today: Proceedings*, 66:3498–3501, 2022. 3rd International Conference on "Advancement in Nanoelectronics and Communication Technologies" (ICANCT-2022).

[47] G. J. Chaitin. Register allocation & spilling via graph coloring. In *Proceedings of the 1982 SIGPLAN Symposium on Compiler Construction*, SIGPLAN '82, page 98–105, New York, NY, USA, 1982. Association for Computing Machinery.

[48] Paul Adrien Maurice Dirac. *Lectures on quantum mechanics*. Dover Publications, 2001.

[49] Z.Y. Ou, C.K. Hong, and L. Mandel. Relation between input and output states for a beam splitter. *Optics Communications*, 63(2):118–122, 1987.

[50] Stefan Scheel. Permanents in linear optical networks. arXiv:quant-ph/0406127, 2004.

[51] Scott Aaronson. A linear-optical proof that the permanent is #P-hard. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 467(2136):3393–3405, 2011.

[52] Albert Nijenhuis and Herbert S Wilf. *Combinatorial algorithms: for computers and calculators*. Elsevier, 2014.

[53] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. arXiv:1011.3245 [quant-ph], 2010.

[54] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457–3467, Nov 1995.

[55] P.Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. A new universal and fault-tolerant quantum basis. *Information Processing Letters*, 75(3):101–107, 2000.

[56] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*. American Association of Physics Teachers, 2002.

[57] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[58] Vincent Danos, Elham Kashefi, and Prakash Panangaden. The measurement calculus. *J. ACM*, 54(2):8–es, apr 2007.

[59] K. Kieling, T. Rudolph, and J. Eisert. Percolation, renormalization, and quantum computing with nondeterministic gates. *Phys. Rev. Lett.*, 99:130501, Sep 2007.

[60] I. Schwartz et al. Deterministic generation of a cluster state of entangled photons. *Science*, 354(6311):434–437, 2016.

[61] William Hall. Cluster state quantum computation for many-level systems. arXiv:quant-ph/0512130, 2006.

[62] William R. Clements, Peter C. Humphreys, Benjamin J. Metcalf, W. Steven Kolthammer, and Ian A. Walmsley. Optimal design for universal multiport interferometers. *Optica*, 3(12):1460–1465, Dec 2016.

[63] Dmitry B. Uskov, A. Matthew Smith, and Lev Kaplan. Generic two-qubit photonic gates implemented by number-resolving photodetection. *Phys. Rev. A*, 81:012303, Jan 2010.

[64] Andrew R. Conn, Nicholas I. M. Gould, and Philippe L. Toint. *Trust Region Methods*. Society for Industrial and Applied Mathematics, 2000.

[65] E. Knill. Quantum gates using linear optics and postselection. *Phys. Rev. A*, 66:052306, Nov 2002.

[66] Abdón Sánchez-Arroyo. Determining the total colouring number is np-hard. *Discrete Mathematics*, 78(3):315–319, 1989.

[67] Fedor V. Fomin, Serge Gaspers, and Saket Saurabh. Improved exact algorithms for counting 3- and 4-colorings. In Guohui Lin, editor, *Computing and Combinatorics*, pages 65–74, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[68] Michael R. Garey and David S. Johnson. *Computers and Intractability; A Guide to the Theory of NP-Completeness*. W. H. Freeman & Co., USA, 1990.

[69] Kazuya Shimizu and Ryuhei Mori. Exponential-time quantum algorithms for graph coloring problems. *Algorithmica*, 84(12):3603–3621, Dec 2022.

[70] Sami Boulebnane and Ashley Montanaro. Solving boolean satisfiability problems with the quantum approximate optimization algorithm. arXiv:2208.06909 [quant-ph], 2022.

[71] Tobias Stollenwerk, Stuart Hadfield, and Zhihui Wang. Toward quantum gate-model heuristics for real-world planning problems. *IEEE Transactions on Quantum Engineering*, 1:1–16, 2020.

[72] Zsolt Tabi et al. Quantum optimization for the graph coloring problem with space-efficient embedding. In *2020 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pages 56–62, 2020.

[73] Ramin Fakhimi, Hamidreza Validi, I. Hicks, Tamás Terlaky, and Luis Zuluaga. Quantum-inspired formulations for the max k-cut problem. Technical report, ISE Technical Report 21T-007 Lehigh University, 12 2021.

[74] Franz G Fuchs, Herman Øie Kolden, Niels Henrik Aase, and Giorgio Sartor. Efficient encoding of the weighted max k-cut on a quantum computer using qaoa. *SN Computer Science*, 2(2):89, 2021.

[75] Bence Bakó, Adam Glos, Özlem Salehi, and Zoltán Zimborás. Near-optimal circuit design for variational quantum optimization. *arXiv preprint arXiv:2209.03386*, 2022.

[76] Sergey Bravyi, Alexander Kliesch, Robert Koenig, and Eugene Tang. Hybrid quantum-classical algorithms for approximate graph coloring. *Quantum*, 6:678, mar 2022.

[77] Stuart Hadfield et al. From the quantum approximate optimization algorithm to a quantum alternating operator ansatz. *Algorithms*, 12(2):34, 2019.

[78] Yannick Deller et al. Quantum approximate optimization algorithm for qudit systems with long-range interactions, 2022.

[79] Zahra Raissi et al., Edwin Barnes, and Sophia E. Economou. Deterministic generation of qudit photonic graph states from quantum emitters, 2022.

Appendix A

Proof: Linear Optics Cannot Entangle Dual-Rail Qubits

Let us consider two dual-rail qubits and denote the creation operators of the first qubit as $a_0^\dagger$ and $a_1^\dagger$, and the creation operators of the second qubit as $b_0^\dagger$ and $b_1^\dagger$. Then an arbitrary two-qubit state is the form

$$\alpha_0 \|0\rangle\!\rangle_a \otimes \|0\rangle\!\rangle_b + \alpha_1 \|0\rangle\!\rangle_a \otimes \|1\rangle\!\rangle_b + \alpha_2 \|1\rangle\!\rangle_a \otimes \|0\rangle\!\rangle_b + \alpha_3 \|1\rangle\!\rangle_a \otimes \|1\rangle\!\rangle_b = \\ \left(\alpha_0 a_0^\dagger b_0^\dagger + \alpha_1 a_0^\dagger b_1^\dagger + \alpha_2 a_1^\dagger b_0^\dagger + \alpha_3 a_1^\dagger b_1^\dagger\right)|0\rangle = \left(\mathbf{a}^\dagger \otimes \mathbf{b}^\dagger\right) \cdot \boldsymbol{\alpha}\,|0\rangle\,, \quad \text{(A.1)}$$

where we introduced the vectors $\mathbf{a}^\dagger = \begin{pmatrix} a_0^\dagger, & a_1^\dagger \end{pmatrix}$, $\mathbf{b}^\dagger = \begin{pmatrix} b_0^\dagger, & b_1^\dagger \end{pmatrix}$ and $\otimes$ denotes the Kronecker product of vectors. Using block matrices, a general linear-optical transformation of the four optical modes is written as follows

$$\begin{pmatrix} \mathbf{c}^\dagger, & \mathbf{d}^\dagger \end{pmatrix} = \begin{pmatrix} \mathbf{a}^\dagger, & \mathbf{b}^\dagger \end{pmatrix} S, \quad \text{where} \quad S = \begin{pmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{pmatrix} \in \mathrm{U}(4), \quad \text{(A.2)}$$

and $S_{ij} \in \mathbb{C}^{2\times 2}$. Since S is unitary, we must have also

$$S_{11}S_{11}^\dagger + S_{12}S_{12}^\dagger = \mathbb{1}, \quad \text{(A.3)}$$

$$S_{21}S_{21}^\dagger + S_{22}S_{22}^\dagger = \mathbb{1}, \quad \text{(A.4)}$$

$$S_{11}S_{21}^\dagger + S_{12}S_{22}^\dagger = 0. \quad \text{(A.5)}$$

The two-qubit state after the transformation is

$$\begin{aligned}&\left(\mathbf{c}^\dagger \otimes \mathbf{d}^\dagger\right)\cdot\boldsymbol{\alpha} = \\ &\left\{\left(\mathbf{a}^\dagger S_{11}\right)\otimes\left(\mathbf{a}^\dagger S_{12}\right)+\left(\mathbf{a}^\dagger S_{11}\right)\otimes\left(\mathbf{b}^\dagger S_{22}\right)+\left(\mathbf{b}^\dagger S_{21}\right)\otimes\left(\mathbf{a}^\dagger S_{12}\right)+\left(\mathbf{b}^\dagger S_{21}\right)\otimes\left(\mathbf{b}^\dagger S_{22}\right)\right\}\cdot\boldsymbol{\alpha}.\end{aligned} \tag{A.6}$$

However, Eq. (A.6) must have the form $\left(\mathbf{a}^\dagger \otimes \mathbf{b}^\dagger\right)\cdot\boldsymbol{\alpha}'$ to stay inside the two-qubit Hilbert space. This implies, that the terms $\left(\mathbf{a}^\dagger S_{11}\right)\otimes\left(\mathbf{a}^\dagger S_{12}\right)$ and $\left(\mathbf{b}^\dagger S_{21}\right)\otimes\left(\mathbf{b}^\dagger S_{22}\right)$ must vanish

$$\left(\mathbf{a}^\dagger S_{11}\right)\otimes\left(\mathbf{a}^\dagger S_{12}\right) = 0, \tag{A.7}$$

$$\left(\mathbf{b}^\dagger S_{21}\right)\otimes\left(\mathbf{b}^\dagger S_{22}\right) = 0. \tag{A.8}$$

Taking the expectation value of Eq. (A.7) with a coherent state $|\boldsymbol{\gamma},\boldsymbol{\delta}\rangle$ we get

$$\left(\boldsymbol{\gamma}^\dagger S_{11}\right)\otimes\left(\boldsymbol{\delta}^\dagger S_{12}\right) = 0, \quad \text{for all} \quad \boldsymbol{\gamma},\boldsymbol{\delta}\in\mathbb{C}^2, \tag{A.9}$$

where $|\boldsymbol{\gamma},\boldsymbol{\delta}\rangle$ is the coherent state which satisfies the following equations

$$a_i\,|\boldsymbol{\gamma},\boldsymbol{\delta}\rangle = \gamma_i\,|\boldsymbol{\gamma},\boldsymbol{\delta}\rangle\,, \tag{A.10}$$

$$b_i\,|\boldsymbol{\gamma},\boldsymbol{\delta}\rangle = \delta_i\,|\boldsymbol{\gamma},\boldsymbol{\delta}\rangle\,. \tag{A.11}$$

Equation (A.9) implies that either the vector $\boldsymbol{\gamma}^\dagger S_{11}$, or $\boldsymbol{\delta}^\dagger S_{12}$ must be equal to the zero vector for all $\boldsymbol{\gamma},\boldsymbol{\delta}\in\mathbb{C}^2$. This further implies that either the matrix S_{11} or S_{12} must be the zero matrix. If $S_{11}=0$, then Eqs. (A.3), (A.4) and (A.5) imply that S_{12} is unitary, and thus S_{22} vanishes as well. Similarly, if S_{12} is zero, then S_{11} is unitary and S_{21} vanishes.

Finally, we conclude that S must be either

$$\begin{pmatrix} S_{11} & 0 \\ 0 & S_{22}\end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & S_{12} \\ S_{21} & 0\end{pmatrix}. \tag{A.12}$$

The first case corresponds to the two-qubit gate $S_{11}\otimes S_{22}$, and the second case corresponds to the two-qubit gate SWAP$(S_{12}\otimes S_{21})$. It is easy to see, that none of these gates are entangling, since if they act on a tensor product state the result will be also a tensor product state. Thus, it is impossible to entangle dual-rail qubits using only beamsplitters and phase shifters.

Appendix B

Linear-Optical Synthesis of Nonlinear Phase Shift

We may use two ancilla modes and an additional photon to synthesize the nonlinear phase shift $\mathrm{NS}_\phi : \alpha_0 |0\rangle_1 + \alpha_1 |1\rangle_1 + \alpha_2 |2\rangle_1 \to \alpha_0 |0\rangle_1 + \alpha_1 |1\rangle_1 + e^{i\phi}\alpha_2 |2\rangle_1$ for any angle ϕ. Since the $\phi = 0$ case is trivial, it is the identity operation, we need only consider the $\phi \neq 0$ case.

Let us introduce three modes: the target mode $a_1^\dagger$ on which we want to perform NS_ϕ, and two ancilla modes $a_2^\dagger$ and $a_3^\dagger$. At the beginning of the synthesis a single photon is injected into one of the ancilla modes so that the state

$$|\psi\rangle_{\mathrm{in}} = (\alpha_0 |0\rangle_1 + \alpha_1 |1\rangle_1 + \alpha_2 |2\rangle_1) \otimes |10\rangle_{23} = \left(\alpha_0 a_2^\dagger + \alpha_1 a_1^\dagger a_2^\dagger + \frac{\alpha_2}{\sqrt{2}} a_1^{\dagger 2} a_2^\dagger\right)|0\rangle \quad \text{(B.1)}$$

enters the linear-optical elements, where $\alpha_0, \alpha_1, \alpha_2$ are arbitrary complex coefficients.

The linear optics should be configured such that the output state is

$$|\psi\rangle_{\mathrm{out}} = \xi\sqrt{P}(\alpha_0 |0\rangle_1 + \alpha_1 |1\rangle_1 + e^{i\phi}\alpha_2 |2\rangle_1) \otimes |10\rangle_{23} + \text{other ancilla projections}, \quad \text{(B.2)}$$

where ξ is a global phase ($|\xi| = 1$) and $P > 0$ is the probability of measuring the ancilla state $|10\rangle_{23}$. This way, if we were to measure the ancilla state $|10\rangle_{23}$, then we would successfully perform NS_ϕ on the target mode.

We can rewrite Eq. (B.2) in terms of the matrix $S \in \mathrm{U}(3)$ which transforms the creation operators of the modes as $\left(a_1^\dagger,\ a_2^\dagger,\ a_3^\dagger\right) \to \left(a_1^\dagger,\ a_2^\dagger,\ a_3^\dagger\right)S$. After the substitution of the transformed operators and collecting the relevant terms the output state

are of the form

$$|\psi\rangle_{\text{out}} = \left\{\alpha_0 S_{22}|0\rangle_1 + \alpha_1(S_{11}S_{22}+S_{12}S_{21})|1\rangle_1 + \alpha_2(S_{11}^2 S_{22}+2S_{11}S_{12}S_{21})|2\rangle_1\right\}\otimes|10\rangle_{23} + \text{other ancilla projections.} \quad \text{(B.3)}$$

Comparing Equations (B.2) and (B.3) we find that the following equations should hold for the matrix elements of S

$$S_{22} = \xi\sqrt{P}, \quad \text{(B.4)}$$

$$S_{11}S_{22}+S_{12}S_{21} = \xi\sqrt{P}, \quad \text{(B.5)}$$

$$S_{11}^2 S_{22}+2S_{11}S_{12}S_{21} = \xi\sqrt{P}e^{i\phi} \quad \text{(B.6)}$$

along with the unitary conditions $S^\dagger S = SS^\dagger = \mathbb{1}$.

Substituting Eqs. (B.4), (B.5) and (B.6) into each other one finds that

$$S_{11}^2 - 2S_{11} + e^{i\phi} = 0, \quad \text{(B.7)}$$

and since $|S_{11}| \leq 1$ because S is unitary, we must have $S_{11} = 1-\sqrt{1-e^{i\phi}}$. From the unitary conditions one can deduce that S must have the form

$$S_{11} = 1-\sqrt{1-e^{i\phi}}, \quad |S_{12}| \in \left(0, \sqrt{1-|S_{11}|^2}\right), \quad |S_{13}| = \sqrt{1-|S_{11}|^2-|S_{12}|^2},$$
$$S_{21} = \frac{\xi\sqrt{P}(1-S_{11})}{S_{12}}, \quad S_{22} = \xi\sqrt{P}, \quad S_{23} = \frac{\xi\sqrt{P}\left(|S_{11}|^2-|S_{12}|^2-S_{11}^*\right)}{S_{12}S_{13}^*},$$
$$S_{3i} = \sum_{k,l}\epsilon_{ikl}S_{1k}^*S_{2l}^*,$$

where

$$P = \left[\frac{\left||S_{11}|^2-|S_{12}|^2-S_{11}^*\right|^2}{|S_{12}|^2(1-|S_{11}|^2-|S_{12}|^2)} + \frac{|1-S_{11}|^2}{|S_{12}|^2}+1\right]^{-1}. \quad \text{(B.8)}$$

The success probability of the nonlinear phase shift is given by P defined in Eq. (B.8), where P is entirely determined by the angle ϕ and by the magnitude $|S_{12}|$, thus one may find the best success rate for a fix angle ϕ by finding the maximum

$$P_{\text{best}} = \max_{\{|S_{12}|\}} P. \quad \text{(B.9)}$$

Figure B.1 shows the best probabilities for every angle. The global maximum, $P = 1/4$ is achieved when $\phi = \pi$. This case corresponds to the nonlinear sign flip which can be used to implement the CZ gate non-deterministically with a success rate of $1/16$.

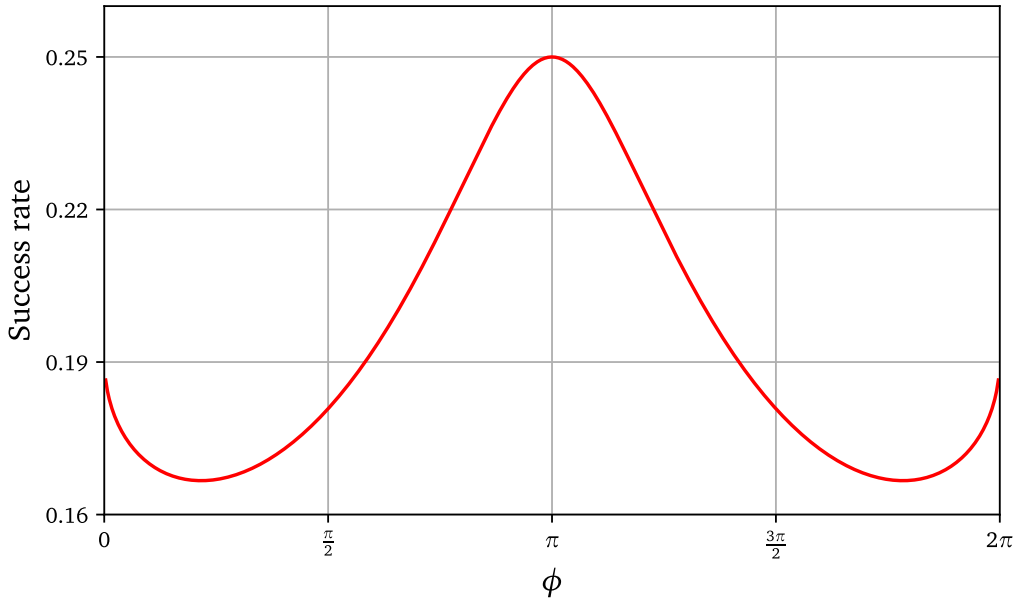


Figure B.1: Success rate of the nonlinear phase shift NS_ϕ when synthesized using linear optics and PNRDs.

Appendix C

The Bloch Sphere Representation of Qubit States

The state of the qubit $|\psi\rangle$ most easily represented as a linear combination

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \alpha,\beta \in \mathbb{C} \tag{C.1}$$

where $\{|0\rangle\,,|1\rangle\}$ is an orthogonal basis of the qubit's Hilbert space. However, this representation is actually redundant if $|\psi\rangle$ represents a physical state.

First of all, a physical state should be normalized such that $|\alpha|^2 + |\beta|^2 = 1$, thus we can parameterize α and β using three angles $\phi_1, \phi_2 \in [0, 2\pi)$ and $\theta \in [0, \pi]$.

$$|\psi\rangle = e^{i\phi_1}\cos\frac{\theta}{2}\,|0\rangle + e^{i\phi_2}\sin\frac{\theta}{2}\,|1\rangle\,. \tag{C.2}$$

Also, $|\psi\rangle$ is physically indistinguishable from the state $\cos\frac{\theta}{2}\,|0\rangle + e^{i(\phi_2-\phi_1)}\sin\frac{\theta}{2}\,|1\rangle$, thus, we may eliminate an other angle and represent $|\psi\rangle$ using only two angles $\phi \in [0, 2\pi)$ and $\theta \in [0, \pi]$

$$|\psi\rangle \equiv \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\,. \tag{C.3}$$

Using the two angles θ and ϕ one can plot the state on the surface of a sphere the following way

$$\mathbf{p} = \begin{pmatrix} \langle\psi|X|\psi\rangle \\ \langle\psi|Y|\psi\rangle \\ \langle\psi|Z|\psi\rangle \end{pmatrix} = \begin{pmatrix} \sin\theta\cos\phi \\ \sin\theta\sin\phi \\ \cos\theta \end{pmatrix} \in S^2 \subset \mathbb{R}^3, \tag{C.4}$$

where X, Y and Z are the Pauli matrices. This sphere is called the Bloch sphere and its surface contains all possible physical qubit states. For illustration see Fig. C.1.

In the Bloch sphere representation single-qubit gates gain a new meaning. Each

single-qubit gate is a rotation on the Bloch sphere. For example, the Pauli X, Y, Z gates are the generators of the rotations around the X, Y, Z axis

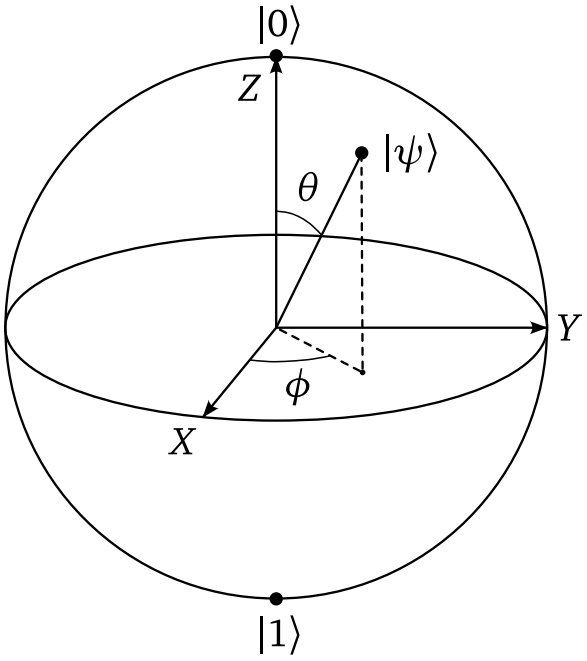


Figure C.1: The state $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$ represented on the Bloch sphere.