Devising accreditation protocols for near-term quantum computing devices

by

Samuele Ferracin

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Department of Physics

March 2020

There is a time for everything, and a season for every activity under the heavens:

A time to be born and a time to die,
A time to plant and a time to uproot,
A time to kill and a time to heal,
A time to tear down and a time to build,
A time to weep and a time to laugh,
A time to mourn and a time to dance,
A time to scatter stones and a time to gather them,
A time to embrace and a time to refrain from embracing,
A time to search and a time to give up,
A time to keep and a time to throw away,
A time to tear and a time to mend,
A time to be silent and a time to speak,
A time to love and a time to hate,
A time for war and a time for peace.

What do workers gain from their toil?

Ecclesiastes 3, 1-9

Contents

List of Figures

List of Tables

List of Boxes

Abbreviations

BwS Brickwork State.

CPTP Completely Positive Trace-Preserving.

GST Gate Set Tomography.

MBQC Measurement-Based Quantum Computing.

NISQ Noisy Intermediate-Scale Quantum.

RB Randomized Benchmarking.

QPT Quantum Process Tomography.

QOTP Quantum One-Time Pad.

Declarations

This thesis is submitted to the University of Warwick in support of my application for the degree of Doctor of Philosophy. It has been composed by myself and has not been submitted in any previous application for any degree.

Parts of this thesis have been published by the author:

- Chapter 4 has been published as Ferracin, Kapourniotis, Datta, *Reducing resources for verification of quantum computations*, Phys. Rev. A 98, 022323 (2018).

- Chapters 5 has been published as Ferracin, Kapourniotis, Datta, *Accrediting outputs of noisy intermediate-scale quantum computing devices*, New J. Phys. 21 113038 (2019).

- Chapter 7 has been published as an Appendix of Ferracin, Kapourniotis, Datta, *Accrediting outputs of noisy intermediate-scale quantum computing devices*, New J. Phys. 21 113038 (2019).

The accreditation protocol presented in Chapter 5 is available on IBM's Qiskit-ignis Github repository at the URL:
https://github.com/Qiskit/qiskit-ignis/tree/master/qiskit/ignis/verification/accreditation.

Abstract

In theory, perfect quantum computers can solve certain problems that are considered intractable with classical computers. In practice, quantum computers are imperfect, since their internal components are afflicted by noise. The aim of this thesis is to devise protocols to verify the correctness of the outputs of quantum computations implemented on the Noisy Intermediate-Scale Quantum (NISQ) computing devices currently being built.

We begin by optimizing some of the existing protocols based on interactive proof systems. Moving beyond these protocols (which are impractical for NISQ devices due to their overhead in qubits and gates), we then present a protocol (that we name "accreditation protocol") that encompasses all the main limitations of NISQ devices, including the limited availability of qubits and noisy gates. The accreditation protocol returns an upper-bound on the variation distance between ideal and noisy probability distributions of the outputs of an arbitrary quantum computation. Relying on the accuracy of single-qubit gates (which are the least noisy components in all currently available NISQ devices), the accreditation protocol can detect all types of noise in state-preparation, measurements and two-qubit gates. To conclude our work, we present a modified version of the accreditation protocol that relies on more assumptions on the noise (motivated by empirical evidence) and provides tighter bounds on the variation distance.

Our accreditation protocols are scalable, unlike the protocols based on classical simulations of quantum circuits. They are practical for implementation on NISQ devices, unlike the protocols based on interactive proof systems. Moreover, they can detect noise that may be missed by protocols based on quantum process tomography and randomized benchmarking. Thus, they represent the state-of-the-art of circuit characterization, and we expect them to be widely used in future quantum computations.

Chapter 1

Introduction

The advent of quantum computers is expected to boost our computing capabilities well beyond their current limits. After Richard Feynman's seminal intuition in 1982 [4], pivotal theoretical results showed that quantum computers may provide exponential scaling advantages over the best known classical algorithm for integer factorization [5]. Similar speedups were subsequently shown for other problems of great interest, such as simulating the physics of many-body systems [6–9] and sampling problems [10–12]. These speedups well motivate the significant investments in quantum computing made by governments of leading powers, including the United States of America (USD \$1.1 billion [13]), Canada (CAD \$1 billion [14]) and the United Kindgdom (GBP£1 billion [15]).

The last few years have seen unprecedented technological advances in the field, eventually culminating in the creation of the first prototypes of quantum computers [16–20]. These prototypes employ a variety of technologies, such as superconducting circuits [16–18], trapped ions [21] and linear optics [22] . Presently, these prototypes—commonly referred to as Noisy Intermediate-Scale Quantum (NISQ) computing devices [23]—contain between 5 and 53 qubits (Table 1.1) and lack the resources to implement fault-tolerant protocols. Consequently, they suffer non-negligible levels of noise and can only reliably implement circuits of limited size. Nonetheless, NISQ devices have been used to perform computational tasks that are currently intractable for modern supercomputers [16]. Moreover, they have provided fertile ground for testing the predictions of quantum mechanics [24–26] and demonstrating the building blocks of future quantum computers [27, 28].

Due to the error-prone nature of NISQ devices, any worthwhile use of current quantum computers relies upon the capability of checking the correctness of their outputs. To date, this is done by classically simulating the circuit of interest and

	Number of qubits	One-qubit errors	Two-qubit errors	SPAM errors
Google Sycamore [16]	53	$\approx 0.15\%$	$\approx 0.62\%$	$\approx 3.8\%$
Rigetti Aspen-7 [17]	32	$\approx 1.3\%$	$\approx 4.8\%$	$\approx 3.6\%$
IBMQ Melbourne [18]	15	$\approx 0.2\%$	$\approx 7\%$	$\approx 4\%$
IBMQ Ourense [18]	5	$\approx 0.04\%$	$\approx 0.8\%$	$\approx 2.5\%$
IonQ [21]	11	$\approx 0.5\%$	$\approx 2.5\%$	$\approx 0.7\%$

Table 1.1. Specifics of some of the main existing NISQ devices. “SPAM errors” stands for “State Preparation and Measurement errors”. Google, Rigetti and IBMQ devices are made up of superconducting transmon qubits, IonQ utilizes trapped ions.

comparing the results of these classical simulations with those obtained experimentally [3, 16, 29]. This approach is viable for small circuits, as well as for circuits containing special classes of gates (e.g. Clifford gates and few non-Clifford gates [1–3]). However, worthwhile quantum circuits (such as those for simulating the physics of many-body systems [6–9]) are not efficiently simulable on classical computers, since time and memory required by the classical simulation grow exponentially with the size of the circuit. Hence, it is crucial to seek alternative methods.

Another approach employed in experiments consists of individually testing classes of gates present in the target circuit. This can be undertaken with protocols based on process tomography [30–32] and gate-set tomography [33–35], which provide full characterization of the noise afflicting quantum gates. Alternatively, a family of protocols centered around randomized benchmarking and its extensions [36–45] provide partial characterization of gate sets, allowing the efficient extraction of the fidelity of gates or cycles of gates. While practical for present experiments, all the protocols for gate characterization rely on assumptions that be may invalid in experiments, for example time independence of the noise [46, 47]. Quantum circuits are more than the sum of their gates, and the noise in the target circuit exhibits characteristics that cannot be captured by benchmarking its individual gates independently [48].

A third approach consists of employing a class of protocols [49–62] based on interactive proof systems [63]. In these protocols (commonly referred to as “verification protocols”), the correctness of the outputs of a quantum computation is verified through an interaction between a trusted verifier and an untrusted prover, who represents *all that can go wrong* in a computation. The verifier is typically allowed to possess a noiseless quantum device able to prepare [49–54] or measure [55–59] single qubits. However, recently a protocol for a fully classical verifier was devised that only relies on post-quantum cryptography (i.e., on cryptographic schemes that are widely believed to be secure against attacks by quantum computers) and requires no quantum device on the verifier's side [64].

Verification protocols are scalable, possessing linear overhead in the number of qubits and gates. However, they are impractical for present experiments, since they require implementing computations that are larger (both in number of qubits and gates) than the computation being verified (the "target" computation). For instance, suppose that the target computation requires initialising a hundred qubits and applying a hundred gates. With the existing verification protocols the prover must be capable of initializing a large cluster state containing thousands of qubits [49–52, 55]; appending several teleportation gadgets to the circuit implementing the target computation (one for each T-gate in the circuit and six for each Hadamard gate) [54]; or building Feynman-Kitaev clock states, which require entangling the system with an auxiliary qubit per gate in the target computation [56, 64, 65]. Alternatively, the verifier can seek help of two provers, provided that they can share thousands of copies of maximally entangled states such as Bell states [60, 61]. Thus, the requirements on the prover's side clearly exceed the potential of NISQ devices.

Overall, the protocols proposed so far can check the correctness of the outputs of circuits that can be classically simulated (such as those implemented in present experiments), or else of circuits implemented on large-scale quantum computers (which will not be available in the near term [23]). Crucially, none of the existing protocols has the potential to check the correctness the outputs of classically non-simulable circuits implemented on NISQ devices [66].

1.1 Summary of the results

This thesis is concerned with developing protocols to check the correctness of the outputs of classically non-simulable computations implemented on NISQ devices. After presenting the mathematical background (Chapter 2) and an overview of related works (Chapter 3), we begin our investigation by optimizing some of the existing verification protocols (Chapter 4). Specifically, we present a verification protocol where the target computation is executed as a Measurement-Based Quantum Computation (MBQC, Section 2.5). In our protocol the verifier (Alice) only prepares certain types of single-qubit states, while the MBQC is carried out by an untrusted prover (Bob).

Our protocol reduces the requirements for Alice, who only needs to prepare eight different types of states as opposed to ten in previous protocols [49–52]. However, we show that the requirements on Bob's side remain impractical for verification of worthwhile quantum computations on NISQ devices (Section 4.6). Essentially, this is due to the *quantum overhead* of the protocol, i.e., to the number of extra qubits and gates needed to map the target computation into a MBQC.

Moving beyond the optimization of existing protocols, in Chapter 5 we define a different type of protocol that we call "accreditation protocol". An accreditation protocol must be able to *accredit* the outputs of a quantum computation, i.e., to guarantee with high confidence that these outputs are close to the correct ones. We then present an accreditation protocol that provides (i) an upper-bound on the variation distance between the probability distributions of the ideal and experimentally observed outputs of a target circuit and (ii) a confidence on the upper-bound.

Our accreditation protocol is designed to encompass all the limitations of NISQ devices, including limited availability of qubits and non-negligible levels of noise. Importantly, it requires implementing circuits containing no more qubits and gates than the target circuit, unlike the existing verification protocols [49–62]. Moreover, relying only on the quality of single-qubit gates (which are the least noisy components in all currently available NISQ devices, Table 1.1), this accreditation protocol tests entire circuits rather than individual gates. It can therefore detect all types of noise in state preparation, measurements and two-qubit gates, including noise that may be missed by the protocols based on tomography or randomized benchmarking (such as noise that creates correlations in space, missed by the protocols in Ref. [30–32, 36–44], or time-dependent noise, missed by the protocols in Ref. [30–32, 36–45]).

While the accreditation protocol can detect quantum noise in its full generality, recent works indicate that simplified noise models seem to describe well the experimental noise [16, 45]. Motivated by this empirical evidence, in Chapter 6 we present a modified version of the accreditation protocol (which we name "single-run accreditation protocol") that relies on more assumptions on the noise—assumptions that are also required by protocols based on tomography [30–32] and randomized benchmarking [36–45]. We then show that the bound on the variation distance provided by the single-run accreditation protocol is significantly tighter than that provided by the original accreditation protocol.

We demonstrate the single-run accreditation protocol by implementing it on IBMQ Ourense, an IBM quantum computer available online [18]. We show that it can correctly upper-bound the variation distance of circuits containing 2,3 and 4 qubits and up to 7 rounds of gates. Being scalable, readily implementable on NISQ devices and robust against *standard* noise models, the single-run accreditation

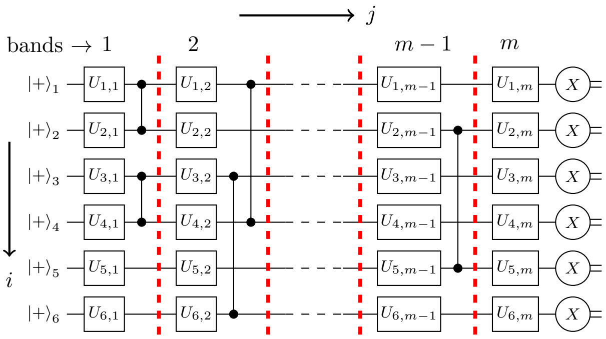


Figure 1.1: An example of the type of circuit considered in this thesis. Each band contains a round of single-qubit gates and a round of two-qubit gates (apart from the last band, which contains no two-qubit gates).

protocol represents the state-of-the-art of circuit characterization. We thus expect it to play a central role in the accreditation of classically non-simulable computations implemented on future NISQ devices.

In Chapter 7 we explain how the accreditation protocol in Chapter 5 can be turned into a verification protocol. Specifically, we provide a verification protocol where Alice and Bob implement the various steps of the accreditation protocol. This verification protocol is different from the other verification protocols in two crucial aspects. First, Alice's actions take place *in the middle* of the protocol: Alice must be able to receive n qubits from Bob (where n is the number of qubits in the target computation), implement a single-qubit gate on each of them and return them all to Bob. Second, she must repeat these operations many times during the protocol run. This is different from the previous protocols, where Alice's actions take place at the beginning of the protocol (Alice prepares the input states [49–54, 67]) or at the end (Alice performs measurements [55–59]). We thus name our protocol "mesothetic" (from the Greek "being in a middle position").

1.2 Numerical studies as a tool to assess the utility of our protocols

All the protocols for verification or accreditation have overheads, for example in qubits and gates, that unavoidably increase the noise levels in the target computation. As a result, they may sometimes be the reason why the target computation returns incorrect outputs. This clearly defeats the purpose of these protocols and makes them useless.

Protocol	Improvements required
Verification protocol in Chapter 4	Reducing error rates by a factor ≈ 1500 as compared to Google Sycamore.
Accreditation protocol in Chapter 5	Reducing error rates by a factor ≈20–30 as compared to Google Sycamore.
Single-run accreditation protocol in Chapter 6	Reducing error rates by a factor ≈ 8 as compared to Google Sycamore.

Table 1.2. Summary of the results of the numerical studies.

To assess the *utility* of each protocol presented in this thesis—i.e., the capability of proving that a quantum computer is returning correct outputs when this is indeed the case—we simulate a protocol run assuming (i) that the target circuit contains 60 qubits and 22 "bands" of gates (each band containing 60 single-qubit gates and 20 two-qubit gates; cfr. Figure 1.1) and (ii) that the target circuit suffers Pauli noise (see Section 2.4 for a definition of Pauli noise).

We regard this as an insightful testbed for three reasons. First, it is reasonable to expect that circuits containing 60 qubits and 22 bands will be implemented by the next generation of NISQ devices, since the largest circuit implemented so far contains 53 qubits and 20 bands [16]. Second, circuits containing 60 qubits and 22 bands can implement computations that cannot be simulated by classical computers in reasonable time (such as sampling from the outputs of random quantum circuits [16]), therefore their outputs cannot be accredited with the protocols currently in use. Third, noise (including non-Pauli noise) can be turned into Pauli noise by compiling random gates into the circuit being implemented, as we show in the proofs of Lemmas 1 and 4 (see also Ref. [68]).

This analysis allows us to quantify the improvements on the hardware that must be made before our protocols become useful for NISQ devices. Targeting computations containing 60 qubits and 22 bands, it indicates that (Table 1.2):

- To become useful, the verification protocol in Chapter 4 requires that the error rates of each component (single and two-qubit qubit gates, state preparation and measurements) are reduced by a factor of ≈ 1500 as compared to Google Sycamore (Table 1.1);

- the accreditation protocol in Chapter 5 requires that the error rates are reduced by a factor of ≈20–30 as compared to Google Sycamore;

- the single-run accreditation protocol in Chapter 6 requires that the error rates are reduced by a factor of ≈ 8 as compared to Google Sycamore.

It is worth pointing out that if the error rates are decreased by a factor of ≈ 8 as compared to Google Sycamore, the probability that an error occurs in a circuit containing 60 qubits and 22 bands amounts to $\approx 50\%$ (Figure 6.4). By rejecting these outputs, our protocols in Chapters 5 and 6 indicate that they cannot be trusted.

Chapter 2

Mathematical background

In this Section we introduce the basics of the gate model of quantum computing. We then present a statement of the Pauli Twirl theorems and the notion of Quantum One-Time Pad (QOTP), our definition of Pauli noise and the main concepts of MBQC.

2.1 Basics of quantum computing

In the circuit model for quantum computing, running a quantum computation consists in implementing one or more quantum circuits [69]. A quantum circuit takes as input a set of qubits, modifies their quantum state using gates and finally measures their state. Presently, several physical systems are used to realize quantum circuits in experiments, such as trapped ions [21], superconducting circuits [16–18] and photonic systems [22].

The quantum state of an n-qubit system is represented by an operator called "density matrix" of the form

$$\rho = \sum_{i=1}^{K} p_i \left|\psi^{(i)}\right\rangle \left\langle\psi^{(i)}\right| \in \mathcal{L}(\mathcal{H}) \ , \tag{2.1}$$

where $|\psi^{(i)}\rangle = (\psi_1^{(i)}, \psi_2^{(i)}, \dots, \psi_{2^n}^{(i)})^T$ are column vectors in a 2^n-dimensional Hilbert space $\mathcal{H}$, $\langle\psi^{(i)}| = (\psi_1^{*\,(i)}, \psi_2^{*\,(i)}, \dots, \psi_{2^n}^{*\,(i)})$ is the conjugate transpose of $|\psi^{(i)}\rangle$, $\mathcal{L}(\mathcal{H})$ is the space of linear operators acting on the vectors in $\mathcal{H}$ and the numbers p_i are probabilities (i.e., all $p_i \in [0,1]$ and $\sum_{i=1}^{K} p_i = 1$). Each $|\psi^{(i)}\rangle$ is normalized such that $\langle\psi^{(i)}|\psi^{(i)}\rangle = 1$, therefore $\mathrm{Tr}(\rho) = 1$ for all the states ρ.

If $K = 1$ and $\rho = |\psi^{(1)}\rangle \langle\psi^{(1)}|$, we say that the state is "pure" and represent it with a vector $|\psi^{(1)}\rangle$. Examples of single-qubit pure states are

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \ , \ |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \ , \ |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ and } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \ . \tag{2.2}$$

In general, single-qubit pure states can be written as a linear combination of the states $|0\rangle$ and $|1\rangle$, namely

$$|\psi\rangle = \alpha\,|0\rangle + e^{i\phi}\beta\,|1\rangle \ , \tag{2.3}$$

where α and β are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$ and $\phi \in [0, 2\pi]$. In other terms, single-qubit pure states are represented by vectors in a 2-dimensional complex vector space and $|0\rangle$ and $|1\rangle$ form a basis for this space. For this reason they are called *computational basis states.*

The physical implementation of the computational basis states depends on the system used to build the quantum computer. For example, in trapped-ion quantum computers the states $|0\rangle$ and $|1\rangle$ can be realized using the electronic states of an ion, while in photonic quantum computers they can be realized using the polarization of light [22, 69].

In analogy with the single-qubit case, n-qubit pure states are vectors in a 2^n-dimensional complex vector space, hence they can be written as a linear combination of 2^n basis states. For example, two-qubit pure states can be written as a linear combination of the four states

$$|00\rangle = |0\rangle \otimes |0\rangle = \big(1, 0, 0, 0\big)^T \tag{2.4}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \big(0, 1, 0, 0\big)^T \tag{2.5}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \big(0, 0, 1, 0\big)^T \tag{2.6}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \big(0, 0, 0, 1\big)^T \tag{2.7}$$

where the symbol $\otimes$ represents the Kronecker product.

Gates acting on n qubits are represented by $2^n \times 2^n$ unitary matrices. A gate U acting on a state ρ returns

$$\rho' = U\rho U^\dagger \tag{2.8}$$

Examples of single-qubit gates are

$$I = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \ , X = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} \ , Z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix} \text{ and } Y = \begin{pmatrix}0 & -i\\i & 0\end{pmatrix} = iXZ \ , \tag{2.9}$$

where I is the identity matrix and X, Z and Y are the Pauli matrices. Other examples are

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \ , \ S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \ , \ R_Z(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \text{ and } R_X(\phi) = HR_Z(\phi)H \ , \tag{2.10}$$

where H is the "Hadamard gate", S is the "phase gate" and $R_Z(\phi)$ (respectively $R_X(\phi)$) is a "R_Z-rotation" (respectively "R_X-rotation") by angle ϕ. Single-qubit gates are represented graphically as in Figure 2.1a.

Examples of two-qubit (or "entangling") gates are the "controlled-Z" gate

$$cZ = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{2.11}$$

and the "controlled-X" gate

$$cX = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.12}$$

Two-qubit gates are represented graphically as in Figure 2.1b.

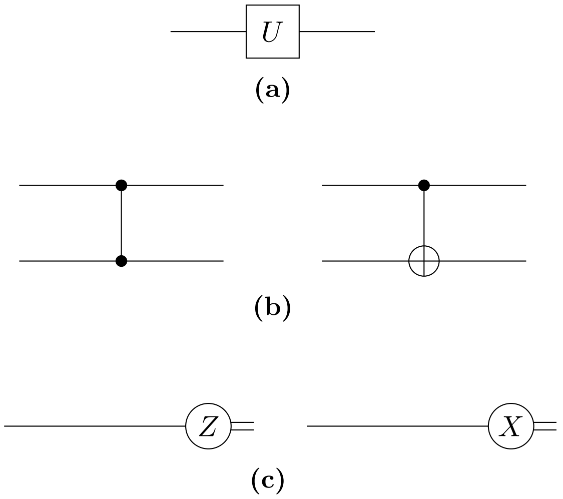
As for qubits, also the physical implementation of quantum gates depends on the system used to build the quantum computer. For example, in trapped-ion quantum computers single-qubit gates are applied by exposing an ion to an external magnetic field, while in photonic quantum computers they are realized by using mirrors, phase shifters and beam splitters [69].

Measurements are represented by a collection $\{M_m\}$ of *measurement operators*. Here, the index m refers to the output of the measurement. If the state ρ is measured with measurement operators $\{M_m\}$, the probability of obtaining output m is

$$\text{prob}(m) = \text{Tr}(M_m \rho M_m^\dagger) \ , \tag{2.13}$$

and the state of the system after the measurement is

$$\rho'_m = \frac{M_m \rho M_m^\dagger}{\text{Tr}(M_m \rho M_m^\dagger)} \ . \tag{2.14}$$



(a)

(b)

(c)

Figure 2.1: Graphical representation of **(a)** single-qubit gate U, **(b)** two-qubit gates (cZ on the left side and cX on the right) and **(c)** Pauli-Z measurements (left) and Pauli-X measurements (right).

The measurement operators must satisfy *completeness equation* $\sum_m M_m^\dagger M_m = I$. This guarantees that $\sum_m \text{prob}(m) = 1$.

Examples of single-qubit measurement operators are those for "Pauli-Z measurements" $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ or for "Pauli-X measurements" $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ (represented graphically as in Figure 2.1c.).

While being processed by a quantum circuit, the qubits may experience noise. This may be caused by several factors, such as imperfect gates, cross-talks between qubits and interactions between qubits and environment. The effect of noise may be coherent (the noise appends an extra unitary to the circuit) or incoherent (the noise is a random process). To model quantum noise we use the formalism of Completely Positive Trace-Preserving (CPTP) maps. Specifically, we model the noise afflicting n qubits in the state ρ as a positive map $\mathcal{E} = \{E_j\}_{j=1}^J$ such that

$$\mathcal{E}(\rho) = \sum_{j=1}^{J} E_j \rho E_j^\dagger \ , \tag{2.15}$$

where E_j are $2^n \times 2^n$ matrices satisfying $\sum_{j=1}^J E_j^\dagger E_j = I$ (which ensure trace preservation, i.e. $\text{Tr}\big[\mathcal{E}(\rho)\big] = 1$). We refer to the matrices E_j as "Kraus operators of the map $\mathcal{E}$". This allows to model coherent noise processes (CPTP maps with a single Kraus operator) as well as incoherent ones (CPTP maps with more than one Kraus operator).

Since the quantum gates are special cases of CPTP maps (indeed, CPTP maps with a single Kraus operator), we denote $\mathcal{I} = \{I\}$, $\mathcal{X} = \{X\}$, $\mathcal{Y} = \{Y\}$, $\mathcal{Z} = \{Z\}$, $\mathcal{H} = \{H\}$ and $\mathcal{S} = \{S\}$, $c\mathcal{Z} = \{cZ\}$, $c\mathcal{X} = \{cX\}$. Moreover, we use the symbol $\circ$ to denote the composition of CPTP maps: $\circ_{p=1}^{q}\mathcal{E}_p(\rho) = \mathcal{E}_q \ldots \mathcal{E}_1(\rho)$.

We define the trace distance between two states ρ_1 and ρ_2 as

$$D(\rho_1, \rho_2) := \mathrm{Tr}\frac{|\rho_1 - \rho_2|}{2} \tag{2.16}$$

and the variation distance between two probability distributions $\{p_i\}_{i=1}^{K}$ and $\{q_i\}_{i=1}^{K}$ as

$$V(\{p_i\}_{i=1}^{K}, \{q_i\}_{i=1}^{K}) := \frac{1}{2}\sum_{i=1}^{K}\left|p_i - q_i\right| \ , \tag{2.17}$$

where $K \geq 1$ is the number of elements in the sets $\{p_i\}$ and $\{q_i\}$. Notice that $D(\rho_1, \rho_2) \in [0, 1]$ for all the states ρ_1 and ρ_2 and $V(\{p_i\}, \{q_i\}) \in [0, 1]$ for all the distributions $\{p_i\}$ and $\{q_i\}$.

2.2 The Pauli twirl

We hereby provide statement and proof of the "Pauli Twirl" Theorem [70]:

Theorem 1. [Pauli Twirl]. *Let ρ be a $2^n \times 2^n$ density matrix and let P, P' be two n-fold tensor products of the set of Pauli operators $\{I, X, Y, Z\}$. Denoting by $\{Q_r\}$ the set of all n-fold tensor products of the set of Pauli operators $\{I, X, Y, Z\}$,*

$$\sum_{r=1}^{4^n} Q_r P Q_r \rho Q_r P' Q_r = 0 \ \forall \ P \neq P'. \tag{2.18}$$

Proof. (As proven in Ref. [70]). We begin by rewriting P as $Z_{\mathbf{a}}X_{\mathbf{a}'} = Z^{a_1} \otimes \ldots \otimes Z^{a_n} \otimes X^{a'_1} \otimes \ldots \otimes X^{a'_n}$, with $\mathbf{a} = (a_1, \ldots, a_n)$, $\mathbf{a}' = (a'_1, \ldots, a'_n)$ and $a_i, a'_i \in \{0, 1\}$ for all $i \in \{1, \ldots, n\}$. Similarly we rewrite P' as $Z_{\mathbf{b}}X_{\mathbf{b}'}$ and Q_r as $Z_{\mathbf{c}}X_{\mathbf{c}'}$. This gives

$$\begin{aligned}\sum_{r=1}^{4^n} Q_r P Q_r \rho Q_r P' Q_r &= \sum_{\mathbf{c},\mathbf{c'}} Z_{\mathbf{c}}X_{\mathbf{c}'}Z_{\mathbf{a}}X_{\mathbf{a}'}Z_{\mathbf{c}}X_{\mathbf{c}'}\rho Z_{\mathbf{c}}X_{\mathbf{c}'}Z_{\mathbf{b}}X_{\mathbf{b}'}Z_{\mathbf{c}}X_{\mathbf{c}'} \\ &= \sum_{\mathbf{c}}(-1)^{\mathbf{c}\cdot(\mathbf{a}'\oplus\mathbf{b}')}\sum_{\mathbf{c}'}(-1)^{\mathbf{c}'\cdot(\mathbf{a}\oplus\mathbf{b})}Z_{\mathbf{a}}X_{\mathbf{a}'}\rho Z_{\mathbf{b}}X_{\mathbf{b}'} \ , \end{aligned} \tag{2.19}$$

where we used that $Z_{\mathbf{k}}X_{\mathbf{k}'} = (-1)^{\mathbf{k}\oplus\mathbf{k}'}X_{\mathbf{k}'}Z_{\mathbf{k}}$ for all $\mathbf{k}, \mathbf{k}'$. We then note that if $\mathbf{a}' \neq \mathbf{b}'$, then $\sum_{\mathbf{c}}(-1)^{\mathbf{c}\cdot(\mathbf{a}'\oplus\mathbf{b}')} = 0$, because half of the elements in the summation are equal to 1 and half to -1. The same holds for $\sum_{\mathbf{c}'}(-1)^{\mathbf{c}'\cdot(\mathbf{a}\oplus\mathbf{b})}$, therefore Equation 2.19 equals zero. □

We also state a restricted version of the Pauli Twirl [51]:

Theorem 2. [Restricted Pauli Twirl]. *Let ρ be a $2^n \times 2^n$ density matrix and let P, P' be two n-fold tensor products of the set of Pauli operators $\{I, Z\}$. Denoting by $\{Q_r\}$ the set of all n-fold tensor products of the set of Pauli operators $\{I, X\}$,*

$$\sum_{r=1}^{2^n} Q_r P Q_r \rho Q_r P' Q_r = 0 \;\forall\; P \neq P'. \tag{2.20}$$

The same holds if P and P' are two n-fold tensor products of the set of Pauli operators $\{I, X\}$ and $\{Q_r\}$ is the set of all n-fold tensor products of the set of Pauli operators $\{I, Z\}$.

Proof. (As proven in Ref. [51]). We present the proof for $P, P' \in \{I, Z\}^{\otimes n}$ and $Q_r \in \{I, X\}^{\otimes n}$ (the proof for $P, P' \in \{I, X\}^{\otimes n}$ and $Q_r \in \{I, Z\}^{\otimes n}$ follows trivially). We begin by rewriting P as $Z_{\mathbf{a}} = Z^{a_1} \otimes \ldots \otimes Z^{a_n}$, with $\mathbf{a} = (a_1, \ldots, a_n)$ and $a_i \in \{0, 1\}$ for all $i \in \{1, \ldots, n\}$, and similarly P' as $Z_{\mathbf{b}}$ and Q_r as $X_{\mathbf{c}}$. This gives

$$\begin{aligned} \sum_{r=1}^{4^n} Q_r P Q_r \rho Q_r P' Q_r &= \sum_{\mathbf{c}} X_{\mathbf{c}} Z_{\mathbf{a}} X_{\mathbf{c}} \rho X_{\mathbf{c}} Z_{\mathbf{b}} X_{\mathbf{c}} \\ &= \sum_{\mathbf{c}} (-1)^{\mathbf{c}\cdot(\mathbf{a}\oplus\mathbf{b})} Z_{\mathbf{a}} \rho Z_{\mathbf{b}} \ , \end{aligned} \tag{2.21}$$

where we used that $Z_{\mathbf{k}} X_{\mathbf{k}'} = (-1)^{\mathbf{k}\oplus\mathbf{k}'} X_{\mathbf{k}'} Z_{\mathbf{k}}$ for all $\mathbf{k}, \mathbf{k}'$. We then note that if $\mathbf{a} \neq \mathbf{b}$, then $\sum_{\mathbf{c}}(-1)^{\mathbf{c}\cdot(\mathbf{a}\oplus\mathbf{b})} = 0$, because half of the elements in the summation are equal to 1 and half to -1. Hence, Equation 2.21 equals zero. □

2.3 Quantum One-Time Pad

Let us denote by $\{P_k\}_{k=1}^{4^n}$ the set of all n-fold tensor products of the set of Pauli operators $\{I, X, Y, Z\}$. Given an n-qubit state ρ, we define a Quantum One-Time Pad (QOTP) as the CPTP map

$$\mathcal{O}(\rho) = \frac{1}{4^n} \sum_{k=1}^{4^n} P_k \rho P_k \ . \tag{2.22}$$

It can be shown that for all the states ρ, $\mathcal{O}(\rho) = I^{\otimes n}/2^n$, where $I^{\otimes n}$ is the $2^n \times 2^n$ identity matrix and $I^{\otimes n}/2^n$ is the "n-qubit maximally mixed state" [71].

The QOTP can be used to encrypt quantum information [72]. To do so, let us imagine that a sender Alice prepares an n-qubit quantum state ρ, applies a Pauli operator P_k chosen uniformly at random from the full set $\{P_k\}_{k=1}^{4^n}$ and sends the state $P_k \rho P_k$ to a recipient Bob. Let us assume that Alice and Bob share a secure classical communication channel, so that Alice can securely reveal to Bob what operator P_k was applied. Then, Bob can apply P_k and retrieve the state ρ. In this scenario, if an eavesdropper Eve intercepts the quantum state, then she holds the maximally mixed state $\mathcal{O}(\rho) = I^{\otimes n}/2^n$ (since P_k was chosen uniformly at random by Alice and was not revealed to Eve), hence she cannot retrieve any information about the state ρ that Alice wants to send to Bob.

2.4 Pauli noise model

Consider a unitary $\mathcal{U} = \{U\}$ acting on an n-qubit state ρ as $\mathcal{U}(\rho) = U \rho U^\dagger$. We say that $\mathcal{U}$ suffers Pauli noise if its noisy implementation $\widetilde{\mathcal{U}}$ acts on ρ as

$$\widetilde{\mathcal{U}}(\rho) = (1-r)\mathcal{U}(\rho) + r\mathcal{P}\mathcal{U}(\rho) \tag{2.23}$$

where $\mathcal{P} = \{P_k\}$ is an arbitrary n-qubit CPTP-map whose Kraus operators are proportional to n-qubit Pauli operators P_k and $r \in [0,1]$ is the "error rate". More generally, a composition of q unitaries $\mathcal{U}_1, \ldots, \mathcal{U}_q$ suffering Pauli noise returns

$$\circ_{p=1}^{q} \widetilde{\mathcal{U}}_p(\rho) = \left(\prod_{p=1}^{q}(1-r_p)\right)\mathcal{U}_q \cdots \mathcal{U}_1(\rho) + \left(1 - \prod_{p=1}^{q}(1-r_p)\right)\sigma \ , \tag{2.24}$$

where σ is a quantum state encompassing the effects of the noise.

2.5 Measurement-based quantum computation

Measurement-Based Quantum Computation (MBQC) is a model for quantum computation [73] where two resources are used: the first is a multi-qubit state, the second is a classical scheme to decide in what order and basis the various qubits must be measured [74]. We now describe a family of states, the "Brickwork States" (BwS), and measurement bases that render MBQC universal for quantum computing. All the results illustrated in this Section are proven and discussed in more detail in Ref. [75].

BwS are two-dimensional graph states of the type of Figure 2.2. In a BwS the qubits are arranged in a 2-dimensional lattice obtained by concatenating "bricks"

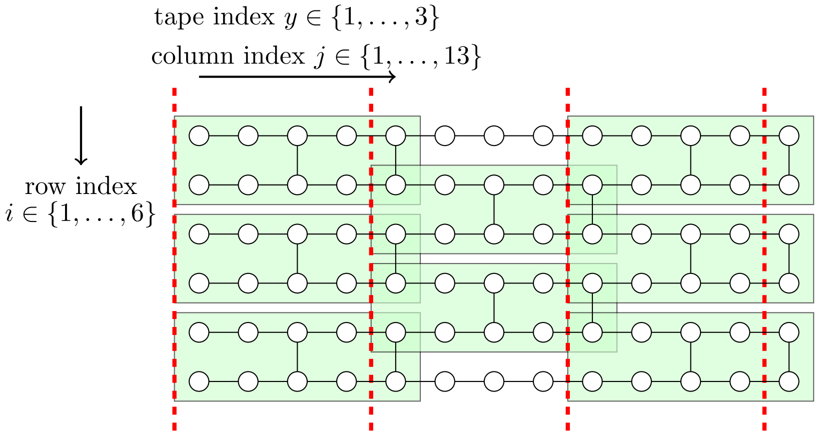

tape index $y \in \{1, \ldots, 3\}$
column index $j \in \{1, \ldots, 13\}$
row index
$i \in \{1, \ldots, 6\}$

Figure 2.2: Example of BwS. The circles represent qubits, the edges represent cZ gates and the green boxes represent the 10-qubit bricks. We label the qubits in a BwS with indices i and j, where $i \in \{1, \ldots, n\}$ is the row index and $j \in \{1, \ldots, d\}$ the column index. We divide the BwS into "tapes" (four-column bands between dashed red lines) and label them with index $y = 1, .., w$. Any $n \times d$ BwS contains $w = (d-1)/4$ tapes.

of 10 qubits (the sub-lattice contained in the green boxes in Figure 2.2). All the qubits are initialized in the state $|+\rangle$ and entangled with their neighbors using cZ gates.

To perform a MBQC, all the qubits in a BwS are measured in a basis $\{|\pm\rangle_\phi\langle\pm|\} = \{R_Z(\phi)|\pm\rangle\langle\pm|R_Z^\dagger(\phi)\}$, where $\phi \in [0, 2\pi)$ is an angle. The measurements are performed column-by-column from left to right: first, one measures all the qubits in the first column, then all those in the second *etc.* Thus, in the circuit model a computation on a $(n \times d)$-dimensional BwS (i.e., a BwS with n rows and d columns) corresponds to the circuit in Figure 2.3.

We will often describe the computations on a BwS using quantum circuits. Using the circuit identity in Figure 2.4, one can show that the overall effect of measuring a qubit in position (i, j) in a BwS corresponds to teleporting its state into the qubit in position $(i, j+1)$ and applying a gate $X^{s_{i,j}} H R_Z(\phi_{i,j})$. Here, $s_{i,j}$ is the output of the measurement of qubit (i, j), which is 0 with probability 1/2 and 1 with probability 1/2. As shown in Ref. [73], the random gate $X^{s_{i,j}}$ can be removed by recomputing the measurements outcomes of unmeasured qubits (specifically, by recomputing $\phi_{i,j+1}$ as $(-1)^{s_{i,j}}\phi_{i,j+1}$ and $\phi_{i,j+2}$ as $\phi_{i,j+2} + s_{i,j}\pi$). Therefore, discarding measured qubits and using $R_X(\phi) = HR_Z(\phi)H$, we can redraw the circuit in Figure 2.3 as in Figure 2.5.

The two circuits in Figures 2.3 and 2.5 describe the same computation in two different models. We refer to circuit in Figure 2.3 (i.e., to the MBQC computation) as "physical circuit" and to the circuit in Figure 2.5 (i.e., to the associated circuit)

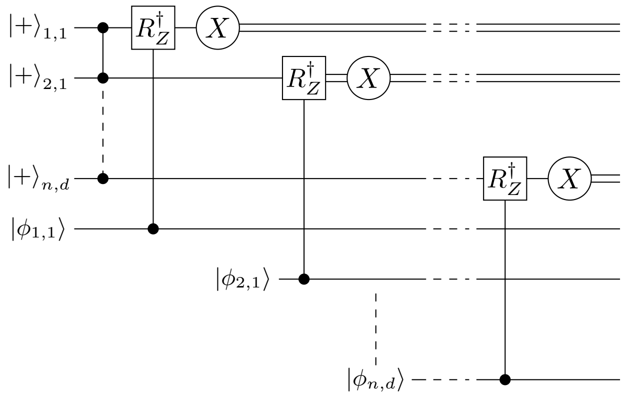


Figure 2.3: Representation of a computation on an $n \times d$ BwS in the circuit model. The BwS is generated by applying a global entangling operation to nm qubits in the state $|+\rangle$. Since $\{|\pm\rangle_\phi\langle\pm|\} = \{R_Z(\phi)|\pm\rangle\langle\pm|R_Z^\dagger(\phi)\}$, the measurements are expressed as controlled rotations followed by Pauli-X measurements. Note that a computation on a $n \times d$ BwS requires executing nd single-qubit gates, nd Pauli-X measurements and $\approx nd$ cZ gates (Figure 2.2).

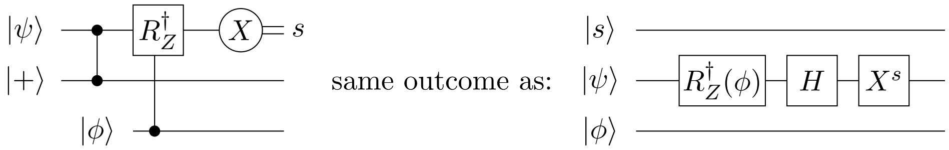


Figure 2.4: Equivalence between circuits. The measurement in the l.h.s. circuit teleports the state of the first qubit into the second qubit and applies the gate $X^s HR_Z(\phi)$.

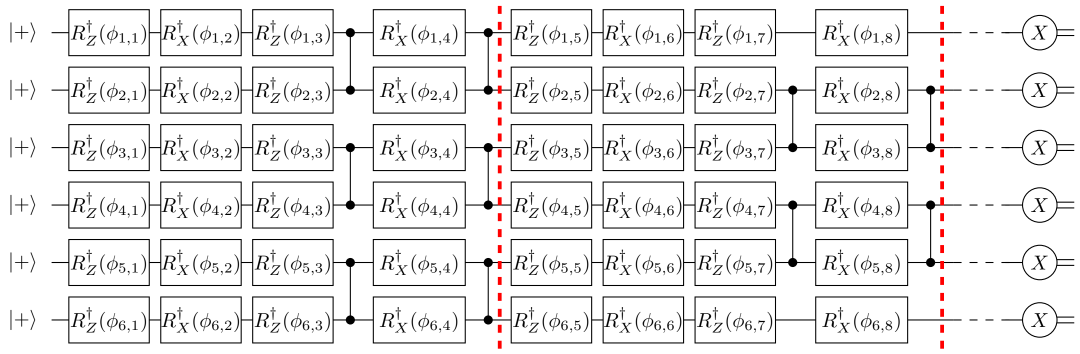

$|+\rangle$
$R_Z^\dagger(\phi_{1,1})$ $R_X^\dagger(\phi_{1,2})$ $R_Z^\dagger(\phi_{1,3})$ $R_X^\dagger(\phi_{1,4})$ $R_Z^\dagger(\phi_{1,5})$ $R_X^\dagger(\phi_{1,6})$ $R_Z^\dagger(\phi_{1,7})$ $R_X^\dagger(\phi_{1,8})$
$R_Z^\dagger(\phi_{2,1})$ $R_X^\dagger(\phi_{2,2})$ $R_Z^\dagger(\phi_{2,3})$ $R_X^\dagger(\phi_{2,4})$ $R_Z^\dagger(\phi_{2,5})$ $R_X^\dagger(\phi_{2,6})$ $R_Z^\dagger(\phi_{2,7})$ $R_X^\dagger(\phi_{2,8})$
$R_Z^\dagger(\phi_{3,1})$ $R_X^\dagger(\phi_{3,2})$ $R_Z^\dagger(\phi_{3,3})$ $R_X^\dagger(\phi_{3,4})$ $R_Z^\dagger(\phi_{3,5})$ $R_X^\dagger(\phi_{3,6})$ $R_Z^\dagger(\phi_{3,7})$ $R_X^\dagger(\phi_{3,8})$
$R_Z^\dagger(\phi_{4,1})$ $R_X^\dagger(\phi_{4,2})$ $R_Z^\dagger(\phi_{4,3})$ $R_X^\dagger(\phi_{4,4})$ $R_Z^\dagger(\phi_{4,5})$ $R_X^\dagger(\phi_{4,6})$ $R_Z^\dagger(\phi_{4,7})$ $R_X^\dagger(\phi_{4,8})$
$R_Z^\dagger(\phi_{5,1})$ $R_X^\dagger(\phi_{5,2})$ $R_Z^\dagger(\phi_{5,3})$ $R_X^\dagger(\phi_{5,4})$ $R_Z^\dagger(\phi_{5,5})$ $R_X^\dagger(\phi_{5,6})$ $R_Z^\dagger(\phi_{5,7})$ $R_X^\dagger(\phi_{5,8})$
$R_Z^\dagger(\phi_{6,1})$ $R_X^\dagger(\phi_{6,2})$ $R_Z^\dagger(\phi_{6,3})$ $R_X^\dagger(\phi_{6,4})$ $R_Z^\dagger(\phi_{6,5})$ $R_X^\dagger(\phi_{6,6})$ $R_Z^\dagger(\phi_{6,7})$ $R_X^\dagger(\phi_{6,8})$
X

Figure 2.5: Circuit associated with the BwS in Figure 2.2. Red dashed lines separate operations implemented within different tapes of the BwS.

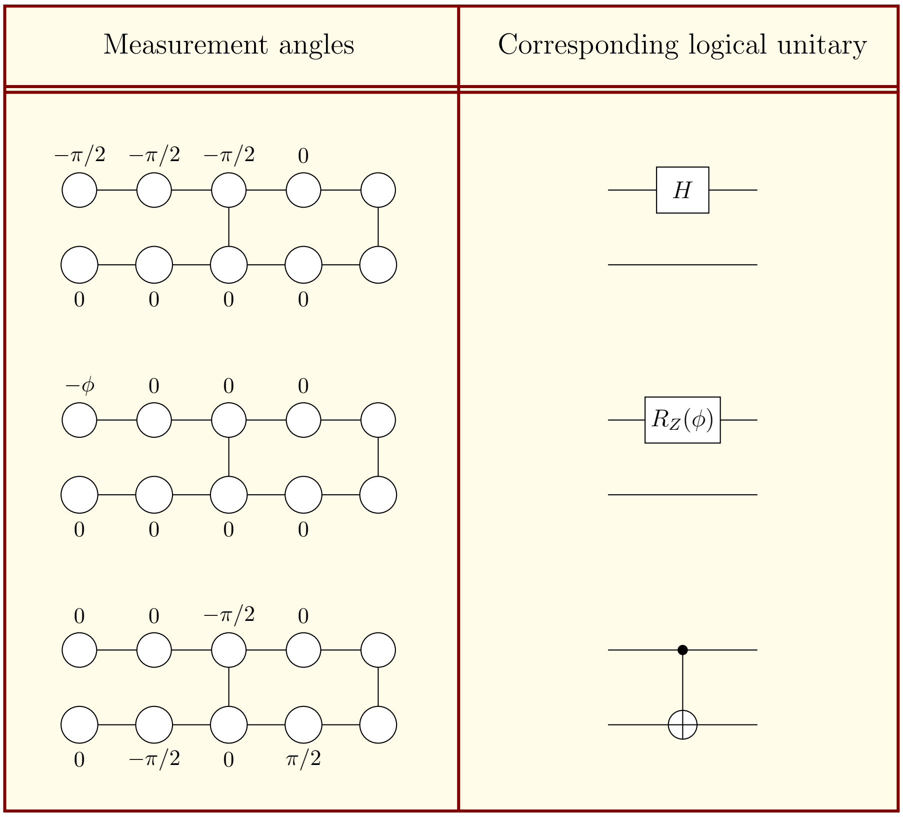


Figure 2.6: Measurement angles for bricks implementing (from top to bottom) Hadamard gate, R_Z-rotation and controlled-X gate. Since H, $R_Z(\phi)$ and cX form a universal set of gates, the bricks can be used as a resource for universal quantum computation. This proves the equivalence between measurement-based and circuit models.

as “logical circuit”. The equivalence between physical and logical circuits allows to prove the equivalence between measurement-based and circuit models. In more detail, it allows proving that by measuring with angles from the set $\phi \in \{0, \pi/4, .., 7\pi/4\}$, one can implement the set of gates $\{H, R_Z(\phi), cX\}$ in the logical circuit (Figure 2.6). This set of gates is universal for quantum computing, hence all the computations in the circuit model can be reproduced by implementing a MBQC on a BwS.

Chapter 3

Overview of existing protocols

Quantum computers can solve problems, such as factoring [5] and searching from a database [76], that belong to the complexity class NP (nondeterministic polynomial time), namely the class of problems whose solution can be efficiently verified on a classical computer. Moreover, they can solve problems outside NP, such as problems that require simulating the physics of many-body systems [6–9] or that involve sampling [10–12]. Can they also efficiently convince the user that the solution is correct?

This question was first posed by Daniel Gottesman in a 2004 conference [77]. It was then formalized by Scott Aaronson in a 2007 blog-post as follows [77]: "Does every language in the class of quantumly tractable problems (BQP) admit an interactive proof where the prover is in BQP and the verifier is in the class of classically tractable problems (BPP)?" As quantum computers begin to outperform classical computers in certain tasks [16], it has become of utmost importance to answer this question.

In this Chapter we provide an overview of the main existing protocols to check if the outputs of a quantum computation are correct or "close" to correct. We begin with a brief description of non-scalable protocols based on quantum tomography and classical simulations of quantum circuits. We then present an introduction to the protocols based on randomized benchmarking and to the verification protocols.

3.1 Protocols based on quantum tomography

This set of protocols includes Quantum Process Tomography (QPT) [30, 32] and Gate Set Tomography (GST) [33–35]. QPT was firstly introduced as a tool to characterize the dynamics of a *quantum black box* [30]. This characterization is done by preparing an input state, sending it through the black box, measuring the value of an observable and repeating for different input states and observables, until it is possible to reconstruct *a posteriori* the CPTP map $\mathcal{E}$ implemented by the black box.

In principle, QPT allows understanding if a quantum circuit implements a unitary that is close to the the desired one, hence if the outputs of the circuit are close to the correct ones. In practice, implementing QPT is problematic for two reasons. Firstly, it requires noiseless state preparation and measurements. Secondly, it is not scalable, since $\mathcal{E}$ is a tensor specified by $2^{4n} - 2^{2n}$ independent and unknown parameters (where n is the number of qubits in the circuit). To date, the largest process that has been characterized through QPT is a 3-qubit process [31].

GST is a modification of QPT that is robust to errors in state preparation and measurements. GST is more demanding than QPT in terms of experiments required and post-processing of the data [34]. To date, GST has only been used to characterize sets of single-qubit gates [35].

3.2 Protocols based on classical simulations

The protocols commonly employed in experiments are based on classical simulations of quantum circuits. These protocols are practical for the present, where the circuits contain few qubits and gates. They can be used to demonstrate progresses in experiments and to identify speedups over classical algorithms [16]. However, they require time and memory that grow exponentially with the number of qubits (unless the circuit being simulated belongs to special classes such as Clifford circuits [1–3]).

An example of a protocol based on classical simulation is the Cross-Entropy Benchmarking (XEB) protocol used in the recent demonstration of quantum computational supremacy [11, 16]. XEB requires assuming that the circuit returns the correct state with probability $\alpha \in [0, 1]$ or the maximally mixed state with probability $1 - \alpha$. That is, XEB requires assuming that the state of the system at the end of the circuit is of the form

$$\widetilde{\rho} = \alpha\rho + (1 - \alpha)\frac{I^{\otimes n}}{2^n} \ , \tag{3.1}$$

where ρ is the state at the end of a noiseless implementation of the circuit and n is the number of qubits [11]. By computing the states ρ (through classical simulations) and $\widetilde{\rho}$ (through experiments), XEB allows estimation of the probability α. To date, XEB has been implemented for circuits containing up to 53 qubits [16].

3.3 Protocols based on randomized benchmarking

The protocols based on Randomized Benchmarking (RB) allow partial characterization of the noise afflicting the gates in quantum circuits. Specifically, they provide a range of noise parameters such as average gate fidelities [36–38], loss rates [39, 41] and leakage rates [42]. These noise parameters can witness improvements in experiments and progress towards fault-tolerant quantum computing [78].

In its original formulation [37], RB takes as input a set of n-qubit gates $\mathbb{G} = \{\mathcal{G}_i\}$ forming a unitary 2-design [70], and for which the inverse of each gate can be found efficiently (e.g., the Clifford group). RB then proceeds as follows:

1. Choose a sequence-length m and a number K_m of runs for sequence-length m.

2. For $i \in \{1, \dots, K_m\}$:

   - Choose m gates $\mathcal{G}_{i_1}, \dots, \mathcal{G}_{i_m} \in \mathbb{G}$ independently at random and calculate $\mathcal{G}_{i_{m+1}} = (\mathcal{G}_{i_m} \dots \mathcal{G}_{i_1})^{-1}$.
   - Prepare the state $\rho_{\text{out}} = \widetilde{\mathcal{G}}_{i_{m+1}} \dots \widetilde{\mathcal{G}}_{i_1} \mathcal{R}\big(|\psi\rangle\langle\psi|\big)$, where $|\psi\rangle$ is a fixed n-qubit state, $\mathcal{R}$ is the noise in the initialization of $|\psi\rangle$ and $\widetilde{\mathcal{G}}_{i_j}$ is a noisy implementation of $\mathcal{G}_{i_j}$.
   - Estimate the "survival probability" $\Phi_i = \text{Tr}\big[E_\psi \mathcal{M} \widetilde{\mathcal{G}}_{i_{m+1}} \dots \widetilde{\mathcal{G}}_{i_1} \mathcal{R}\big(|\psi\rangle\langle\psi|\big)\big]$, where $E_\psi = |\psi\rangle\langle\psi|$ and $\mathcal{M}$ is the noise in the measurement.

   Estimate the average survival probability at sequence length m as $\widehat{\Phi}(m) = \sum_i^{K_m} \Phi_i$.

3. Repeat steps 1 and 2 for different values of m.

4. Fit the average survival probabilities $\widehat{\Phi}(m)$ with the curve $Ap^m - B$ and find the number $p \in [0, 1]$. Calculate $F_{\text{ave}} = p + (1 - p)/2^n$.

The number F_{ave} found in step 4 coincides with the average fidelity of the gates in $\mathbb{G}$, provided that the following assumptions can be made:

RB1. Markovianity, meaning that a noisy implementation of a gate $\mathcal{G} \in \mathbb{G}$ is of the form $\widetilde{\mathcal{G}} = \mathcal{E}\mathcal{G}$, where $\mathcal{E}$ is a CPTP map.

RB2. Time-independence, meaning that distinct implementations of the same gate $\mathcal{G} \in \mathbb{G}$ are characterized by the same noise, that is $\circ_{j=1}^m \widetilde{\mathcal{G}} = \circ_{j=1}^m (\mathcal{E}\mathcal{G})$.

RB3. Gate-independence, meaning that all the gates $\mathcal{G} \in \mathbb{G}$ are afflicted by the same noise, that is $\widetilde{\mathcal{G}}_k = \mathcal{E}\mathcal{G}_k$ for all $\mathcal{G}_k \in \mathbb{G}$.

RB4. Noise in state preparation and measurement (the maps $\mathcal{R}$ and $\mathcal{M}$) does not change throughout the whole protocol run.

Over the years the original RB protocol [37] has been modified in many ways, for instance to benchmark gate-sets not forming a unitary-2 design [40, 44], cycles of gates [45] or logical gates [43]. Assumptions RB1, RB2, RB3 and RB4 remain crucial for the majority of RB protocols [39, 41–45, 78]. A recent analysis in Ref. [46] has shown that assumption RB3 is not necessary for the original RB protocol [37], however it remains unclear whether it may also be dropped for other RB protocols [43, 45].

3.4 Verification protocols

In verification protocols [49–62] a verifier (Alice) delegates a "target" quantum computation to a prover (Bob). Alice regards Bob as an untrusted party: he may be honest and follow Alice's instructions, or else he may be dishonest and deviate.

Verification protocols are characterized by two properties:

- Completeness: if Bob is honest, the protocol accepts the outputs of the target computation with probability larger than 2/3.
- Soundness: if Bob is dishonest, the protocol accepts the outputs of the target computation with probability lower than 1/3.

These properties of verification enable Alice to check Bob's behavior while he is implementing the target computation.

Verification protocols are scalable (since they have a linear overhead in the number of qubits and gates), moreover they rely on no assumptions on Bob's side. All assumptions are made on Alice's side, to provide her with resources to check Bob's behavior. Based on these assumptions it is possible to classify verification protocols as follows:

- Prepare-and-send protocols: Alice owns a device able to generate different types of single-qubit states and send them to Bob [49–53, 53, 54].
- Receive-and-measure protocols: Alice owes a device able to receive qubits from Bob and measure in different bases [55–59].
- Multi-prover protocols: Alice owns no quantum device. She can interact with two entangled and spatially separated (i.e., non-communicating) provers [60–62].

- Protocols based on post-quantum cryptography: Alice owns no quantum device. She encrypts the instructions to Bob using post-quantum cryptography, i.e., encryption schemes that are believed to be hard to break by a BQP prover [64, 79].

With a few exceptions [56, 57], the main property of verification protocols [49–52, 55, 58–62] is "blindness", which enables Alice to delegate a given quantum computation (named "target") to Bob in a way that he cannot distinguish this computation from any other computation of the same size. Employing blindness, verification is then achieved by hiding the target computation among several "trap" computations, which return a fixed known output if Bob is honest or a different output (with high probability) if Bob is dishonest.

In this thesis we will mainly be concerned with verification protocols for MBQC (Section 2.5). This includes both prepare-and-send [49–52] and receive-and-measure protocols [55, 58, 59]. In prepare-and-send protocols for MBQC Alice generates qubits in the states $|+\rangle_\theta = \big(|0\rangle + e^{-i\theta}|1\rangle\big)/\sqrt{2}$, with $\theta \in \{0, \pi/4, .., 7\pi/4\}$, and in the states $|0\rangle, |1\rangle$. She send qubits to Bob, who uses them to generate a BwS (Section 2.5) and to carry out a measurement-based computation. The first eight types of states generated by Alice ensure blindness [75], while $|0\rangle$ and $|1\rangle$ ensure verifiability. In receive-and-measure protocols for MBQC Bob generates a BwS and sends each qubit to Alice, one by one. Alice can perform measurements in the bases $\{|\pm\rangle_\theta\langle\pm|\} = \{R_Z(\theta)|\pm\rangle\langle\pm|R_Z^\dagger(\theta)\}$, with $\theta \in \{0, \pi/4, 2\pi/4, 3\pi/4\}$, as well as in the bases $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. The first four bases ensure universality and blindness, while $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ ensures verifiability.

Chapter 4

Reducing requirements of verification protocols

4.1 Summary of the results

Our efforts begin with the optimization of existing verification protocols. In this Chapter we focus on the verification protocols for MBQC (Section 3.4) and show that it is possible to reduce the set of operations performed by Alice. In more detail:

1. We present a prepare-and-send verification protocol for MBQC where Alice only prepares single qubits in the states $\{|+\rangle_\theta = (|0\rangle + e^{i\theta}|1\rangle)/\sqrt{2}\}$, where $\theta \in \{0, \pi/4, .., 7\pi/4\}$ (Protocol 1, Section 4.3).

2. We show how this protocol can be adapted to scenario where Alice can measure qubits in the set of bases $\{|\pm\rangle_\theta\langle\pm|\} = \{R_Z(\theta)|\pm\rangle\langle\pm|R_Z^\dagger(\theta)\}$, where $\theta \in \{0, \pi/4, .., 7\pi/4\}$ and reuse the qubits after the measurements (Protocol 2, Section 4.4).

Protocol 1 requires Alice to prepare eight types of single-qubit states, as opposed to ten in previous protocols [49, 51, 52]. Protocol 2 requires Alice to measure in four bases, as opposed to five in [55]. Thus, our protocols reduce the experimental requirements for prepare-and-send and receive-and-measure protocols. Moreover, our results prove that blindness is sufficient for verifiability, since our protocols enable Alice to verify MBQC by performing no more operations than those required

[1] This Chapter presents the results of Ferracin, Kapourniotis, Datta, *Reducing resources for verification of quantum computations*, Phys. Rev. A 98, 022323 (2018).

for blindness (cfr. Section 3.4). Elaborating on this unique feature of our protocols, subsequent work has shown that Protocol 1 can be turned into a protocol based on post-quantum cryptography [79].

This Chapter is structured as follows. In Section 4.2 we provide the necessary definitions, in Section 4.3 we present Protocol 1, in Section 4.4 we present Protocol 2, in Section 4.5 we provide a detailed comparison between our protocols and the existing ones, in Section 4.6 we analyze the utility of Protocol 1. All the proofs are contained in Section 4.7.

4.2 Definitions

We denote with $\mathcal{H}_A$ the Hilbert space associated with Alice's register and with with $\mathcal{H}_B$ that associated to Bob's register. We define a common register C used to move qubits from Alice to Bob and vice-versa and denote with $\mathcal{H}_C$ the Hilbert space associated with C. We denote with $\mathcal{L}(\mathcal{H}_{ABC}) = \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ the space of linear operators on $\mathcal{H}_{ABC} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$.

We can now define the notion of protocol used in this Chapter:

Definition 1. [Interactive Protocol]. *We define a q-step interactive protocol on input $\rho_{\text{in}} \in \mathcal{L}(\mathcal{H}_{ABC})$ as a series of maps $\{\mathcal{E}^{(p)}_{ABC}\}^q_{p=1} = \{\mathcal{E}^{(p)}_{AC} \otimes \mathcal{E}^{(p)}_{BC}\}^q_{p=1}$ acting on both Alice's and Bob's registers and on the common register, and such that the output is of the form $\rho_{\text{out}} = \circ^q_{p=1}\mathcal{E}^{(p)}_{ABC}(\rho_{\text{in}})$.*

An interactive protocol is thus a sequence of instructions defining the actions that Alice and Bob must undertake.

A typical requirement for verification protocols is blindness [49–52, 55, 58–62]. In simple terms, blindness ensures that if Bob is dishonest and *deviates* (i.e., if he applies a set of maps $\{\widetilde{\mathcal{E}}^{(p)}_{BC}\}^q_{p=1}$ that is different from the instructions $\{\mathcal{E}^{(p)}_{BC}\}^q_{p=1}$), he cannot increase his knowledge. More formally:

Definition 2. [Blindness]. *Suppose that Alice and Bob jointly run a q-step interactive protocol $\{\mathcal{E}^{(p)}_{ABC}\}^q_{p=1} = \{\mathcal{E}^{(p)}_{AC} \otimes \mathcal{E}^{(p)}_{BC}\}^q_{p=1}$ on input $\rho_{\text{in}} \in \mathcal{L}(\mathcal{H}_{ABC})$. The protocol is blind if, for any set of maps $\{\widetilde{\mathcal{E}}^{(p)}_{BC}\}^q_{p=1}$ implemented by Bob instead of $\{\mathcal{E}^{(p)}_{BC}\}^q_{p=1}$, the state $\widetilde{\rho}_B = \text{Tr}_{\text{AC}}[\circ^q_{p=1}\{\mathcal{E}^{(p)}_{AC} \otimes \widetilde{\mathcal{E}}^{(p)}_{BC}\}(\rho_{\text{in}})]$ in Bob's register at the end of the protocol leaks at most the size of the target computation (the number of qubits and gates used).*

In verification protocols for MBQC Alice verifies the outputs of a given computation (the "target" computation) by hiding it among several "trap" computations. If Bob is honest, with high probability all these trap computations return a fixed output (here denoted by $|\text{acc}\rangle$). If Bob is dishonest, with high probability they return a different output. Denoting the input state ρ_{in} as a tensor product between the input state $\rho_{\text{in}}^{\text{target}}$ of the target computation and the input state $|\text{trap}\rangle\langle\text{trap}|$ of the traps, we formally define verifiability as follows [80, 81]:

Definition 3. [Verifiability]. *Suppose that Alice and Bob jointly run a q-step interactive protocol $\{\mathcal{E}_{ABC}^{(p)}\}_{p=1}^{q} = \{\mathcal{E}_{AC}^{(p)} \otimes \mathcal{E}_{BC}^{(p)}\}_{p=1}^{q}$ on input $\rho_{\text{in}} = \rho_{\text{in}}^{\text{target}} \otimes |\text{trap}\rangle\langle\text{trap}| \in \mathcal{L}(\mathcal{H}_{ABC})$. The protocol is "$\delta$-complete" if the output $\rho_{\text{out}} = \circ_{p=1}^{q} \mathcal{E}_{ABC}^{(p)}(\rho_{\text{in}})$ is such that the trace distance*

$$D\Big(\text{Tr}_{BC}\big[\rho_{\text{out}}\big],\, \text{Tr}_{BC}\big[\ \rho_{\text{out}}^{\text{target}} \otimes |\text{acc}\rangle\langle\text{acc}|\ \big]\Big) \leq 1 - \delta\ , \tag{4.1}$$

where $0 \leq \delta \leq 1$, $\rho_{\text{out}}^{\text{target}}$ is the correct output of the target computation and $|\text{acc}\rangle\langle\text{acc}|$ is a fixed state. If $\delta = 1$, then we say that the protocol is "complete".

The protocol is "ε-sound" if, for any set of maps $\{\widetilde{\mathcal{E}}_{BC}^{(p)}\}_{p=1}^{q}$ acting on Bob's register B and on the common register C, the output $\widetilde{\rho}_{\text{out}} = \circ_p \big(\mathcal{E}_{AC}^{(p)} \otimes \widetilde{\mathcal{E}}_{BC}^{(p)}\big)\big(\rho_{\text{in}}\big)$ is such that the trace distance

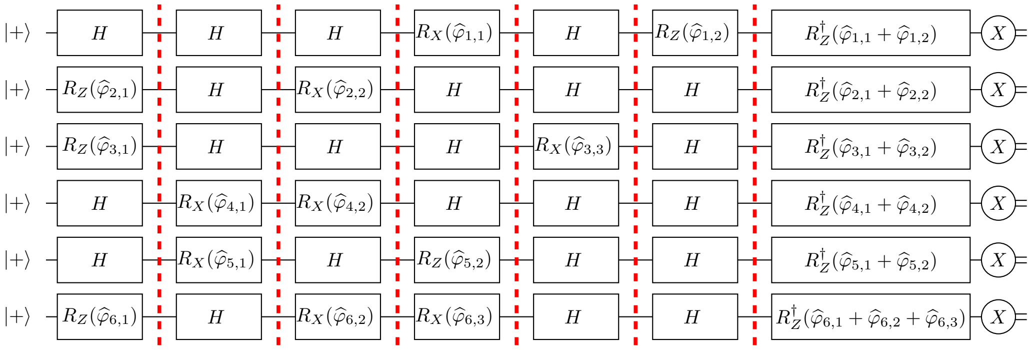
$$D\Big(\text{Tr}_{BC}\big[\widetilde{\rho}_{\text{out}}\big],\, \text{Tr}_{BC}\big[l\ \rho_{\text{out}}^{\text{target}} \otimes |\text{acc}\rangle\langle\text{acc}| + (1-l)\ \widetilde{\rho}_{\text{out}}^{\text{target}} \otimes |\text{rej}\rangle\langle\text{rej}|\big]\Big) \leq \varepsilon\ , \tag{4.2}$$

where $0 \leq \varepsilon \leq 1$ is called "soundness", $0 \leq l \leq 1$, $\widetilde{\rho}_{\text{out}}^{\text{target}}$ is an arbitrary state and $|\text{rej}\rangle$ is orthogonal to $|\text{acc}\rangle$. If the protocol is both ε-sound and δ-complete, then we say that it is "(ε, δ)-verifiable".

In simple terms, completeness $\delta \approx 1$ means that if Bob is honest, then with high probability the protocol returns the correct outputs and Alice accepts these outputs. Instead, soundness $\varepsilon \approx 0$ means that if Bob is dishonest, then with high probability Alice rejects incorrect outputs.

4.3 Our prepare-and-send protocol

In this Section we present our prepare-and-send protocol and show that it is blind and verifiable. We assume that the target computation is compiled as a MBQC computation (Section 2.5) and is specified by an $n \times d$ BwS and by a set of measurement angles $\phi_{i,j} \in \{0, \pi/4, \ldots, 7\pi/4\}$ for each qubit (i, j) in the BwS.



$|+\rangle$ H H H $R_X(\widehat{\varphi}_{1,1})$ H $R_Z(\widehat{\varphi}_{1,2})$ $R_Z^\dagger(\widehat{\varphi}_{1,1}+\widehat{\varphi}_{1,2})$ X
$|+\rangle$ $R_Z(\widehat{\varphi}_{2,1})$ H $R_X(\widehat{\varphi}_{2,2})$ H H H $R_Z^\dagger(\widehat{\varphi}_{2,1}+\widehat{\varphi}_{2,2})$ X
$|+\rangle$ $R_Z(\widehat{\varphi}_{3,1})$ H H H $R_X(\widehat{\varphi}_{3,3})$ H $R_Z^\dagger(\widehat{\varphi}_{3,1}+\widehat{\varphi}_{3,2})$ X
$|+\rangle$ H $R_X(\widehat{\varphi}_{4,1})$ $R_X(\widehat{\varphi}_{4,2})$ H H H $R_Z^\dagger(\widehat{\varphi}_{4,1}+\widehat{\varphi}_{4,2})$ X
$|+\rangle$ H $R_X(\widehat{\varphi}_{5,1})$ H $R_Z(\widehat{\varphi}_{5,2})$ H H $R_Z^\dagger(\widehat{\varphi}_{5,1}+\widehat{\varphi}_{5,2})$ X
$|+\rangle$ $R_Z(\widehat{\varphi}_{6,1})$ H $R_X(\widehat{\varphi}_{6,2})$ $R_X(\widehat{\varphi}_{6,3})$ H H $R_Z^\dagger(\widehat{\varphi}_{6,1}+\widehat{\varphi}_{6,2}+\widehat{\varphi}_{6,3})$ X

Figure 4.1: Logical circuit associated with an R-trap. In all the tapes each qubit undergoes a Hadamard gate with probability 1/2 or a rotation (R_Z or R_X) with probability 1/2 (cfr. Figure 4.3). Using $HR_X(\phi)H = R_Z(\phi)$, it can be seen that R-traps implement the identity on each qubit, therefore R-traps are expected to output $\overline{s} = \overline{0}$.

4.3.1 Description of the protocol

Our protocol is formally presented in Box 4.1, page 28. Our protocol takes as input the angles $\phi_{i,j} \in \{0, \pi/4, \ldots, 7\pi/4\}$ and the number $v \geq 1$ of trap computations. Before starting the interaction with Bob, Alice chooses what computation $v_0 \in \{1, \ldots, v+1\}$ will be used to implement the target (Step 1 of the protocol, cfr. Box 4.1), next she decides the angles for the trap computations (Step 2).

To decide the angles for the trap computations Alice uses either Routine 1 or Routine 2 at random (Box 4.2 and 4.3, pages 29 and 30). When she uses Routine 1 we say that the trap computation is an “R-trap” (for “rotation trap”). This is because in the logical circuit associated with an R-trap, each qubit $i \in \{1, \ldots, n\}$ is rotated around the Pauli-Z axis of the Bloch sphere by a random angle $\widehat{\varphi}_i \in \{0, \pi/4, \ldots, 7\pi/4\}$ and then measured in the basis $\{|\pm\rangle_{\widehat{\varphi}_i}\langle\pm|\}$ (Figure 4.1). Therefore, if an R-trap is implemented correctly, the associated logical circuit returns $\overline{s} = \overline{0}$.

When Alice uses Routine 2 we say that the trap is a “C-trap” (for “CNOT trap”). This is because the logical circuit associated with a C-trap contains a series of CNOT gates with randomly chosen target (Figure 4.2). C-traps end with measurements in the basis $\{|\pm\rangle\langle\pm|\}$. Since $cX\,|{+}{+}\rangle = |{+}{+}\rangle$, if implemented correctly also the logical circuit associated with a C-trap returns $\overline{s} = \overline{0}$.

The interaction between Alice and Bob happens in Step 3, where the various computations are implemented. Every computation $k \in \{1, \ldots, v+1\}$ starts with Alice choosing nd random numbers $\theta_{i,j}^{(k)} \in \{0, \pi/4, .., 7\pi/4\}$ and $2nd$ random bits

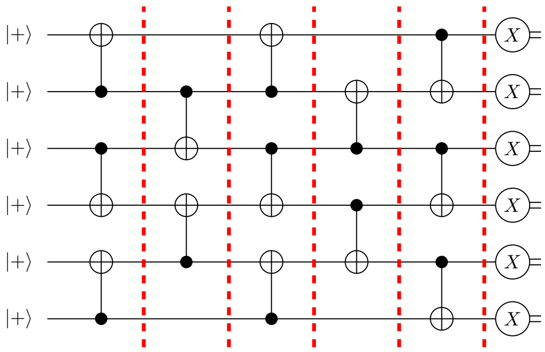


Figure 4.2: Logical circuit associated with a C-trap. In all the tapes a cX gate is implemented (with random target and control qubits, cfr. Figure 4.4). Since $cX\,|{+}{+}\rangle = |{+}{+}\rangle$, all the C-traps are expected to output $\overline{s} = \overline{0}$.

$r_{i,j}^{(k)}, r_{i,j}^{\prime\,(k)} \in \{0,1\}$. Next, Alice sends Bob nd qubits in the state

$$R_Z\left(\theta_{i,j}^{(k)} + \pi \sum_{(i',j')\sim(i,j)} r_{i',j'}^{\prime\,(k)}\right)|+\rangle \ , \tag{4.3}$$

where the summation runs over all the qubits (i', j') that are nearest neighbors of qubit (i, j). After receiving all the qubits, Bob entangles them and creates the BwS. Next, Alice instructs Bob to measure the various qubits column-by-column with angles $\delta_{i,j}^{(k)} = (-1)^{r_{i,j}^{\prime\,(k)}} \phi_{i,j}^{(k)} + \theta_{i,j}^{(k)} + r_{i,j}^{(k)}\pi$ and to reveal to her the measurement outputs $s_{i,j}^{(k)} \in \{0,1\}$. After every measurement, Alice updates the measurement output as $s_{i,j}^{(k)} \oplus r_{i,j}^{(k)}$, next she recomputes the angles of the unmeasured qubits (the measurements are performed adaptively).

In Step 4, Alice ends the protocol by checking if the logical circuits associated with the trap computations returned the correct outputs $\overline{s} = \overline{0}$. If they did she keeps the output of the target computation, otherwise she rejects it.

We conclude this Section by analyzing the complexity of Protocol 1, i.e., the number of qubits and bits sent by Alice to Bob and vice-versa. The number of classical bits and qubits sent by Alice to Bob is $3(v+1)nd$ and $(v+1)nd$ respectively. Bob sends to Alice $(v+1)nd$ bits and no qubits. The complexity of our Protocol 1 is thus linear in the size of the target circuit.

4.3.2 Correctness

In Section 4.7.1 (Theorem 4) we show that our protocol is *correct*, that is, the random numbers $\theta_{i,j}^{(k)}$, $r_{i,j}^{(k)}$ and $r_{i,j}^{\prime\,(k)}$ do not change the outputs of the target and trap computations. Specifically, we prove that the measurements by angles $\{\delta_{i,j}^{(k)}\}$

Box 4.1. Protocol 1 (prepare-and-send protocol for MBQC).

Assumption:

Alice can prepare qubits in the state $|+\rangle_\theta = (|0\rangle + e^{i\theta}|1\rangle)/\sqrt{2}$, where $\theta \in \{0, \pi/4, .., 7\pi/4\}$ and send them to Bob.

Input:

- The set of measurement angles $\{\phi_{i,j}\}$ for the target computation.
- The number of trap computations v.

Routine:

1. Alice randomly chooses $v_0 \in \{1, \ldots, v+1\}$ and sets $\{\phi_{i,j}^{(v_0)}\} = \{\phi_{i,j}\}$.

2. For $k \in \{1, \ldots, v+1\}$:
   If $k \neq v_0$, Alice randomly runs Routine 1 or Routine 2 on input (n, d) and obtains the set of angles $\{\phi_{i,j}^{(k)}\}$.

3. For $k \in \{1, \ldots, v+1\}$:

   3.1 For $i \in \{1, \ldots, n\}$ and for $j \in \{1, \ldots, d\}$:
   Alice randomly chooses $\theta_{i,j}^{(k)} \in \{0, \pi/4, .., 7\pi/4\}$ and $r_{i,j}^{(k)}, r_{i,j}'^{(k)} \in \{0, 1\}$. Next, she sends Bob a qubit in the state $R_Z(\theta_{i,j}^{(k)} + \pi \sum_{(i',j')\sim(i,j)}^{(k)} r_{i',j'}'^{(k)})\,|+\rangle$, where the summation runs over all qubits (i', j') that are nearest neighbors of qubit (i, j) in the kth computation.

   3.2 Bob entangles the qubits in his register and creates the BwS.

   3.3 For $j \in \{1, .., d\}$ and for $i \in \{1, .., n\}$:
   Alice instructs Bob to measure qubit (i, j) with angle $\delta_{i,j}^{(k)} = (-1)^{r_{i,j}'^{(k)}} \phi_{i,j}^{(k)} + \theta_{i,j}^{(k)} + r_{i,j}^{(k)}\pi$. Bob reveals the measurement output $s_{i,j}^{(k)}$ to Alice. If $r_{i,j}^{(k)} = 1$ Alice bit-flips $s_{i,j}^{(k)}$. Next, she recomputes measurement angles of the unmeasured qubits as $\{(-1)^{s_X}\phi_{i,j}^{(k)} + s_Z\pi\}$.

4. Alice initializes a flag bit to the state $|\text{acc}\rangle = |0\rangle$. Next, for all $k \in \{1, \ldots, v+1\}$: if $k \neq v_0$ (trap circuit) and $\{s_{i,d}^{(k)}\}_{i=1}^n \neq (0, 0, .., 0)$, Alice sets the flag bit to $|\text{rej}\rangle = |\text{acc} \oplus 1\rangle$.

Output: The measurement outputs $\{s_{i,j}^{(v_0)}\}$ of the target circuit and the flag bit.

Box 4.2 Routine 1 (angles for R-trap).

```
Input:
• The size of the target computation: $(n, d)$.
Routine:
1. Initialize $n \times d$ numbers $\phi_{i,j} = 0$.
2. For all $i \in \{1, \dots, n\}$ initialize $c = 0$. Next:
   2.1 For all $y \in \{1, \dots, (d-1)/4 - 1\}$:
       Initialize a random bit $h_y \in \{0, 1\}$, next:
       • If $h_y = 0$: set $c = c \oplus 1$ and replace $\phi_{i,4y-3}$, $\phi_{i,4y-2}$ and $\phi_{i,4y-1}$ with $\pi/2$.
       • Else, if $h_y = 1$ and $c = 0$: replace $\phi_{i,4y-3}$ and $\phi_{i,4y-1}$ with random angles from the set $\{0, \pi/4, .., 7\pi/4\}$ and replace $\phi_{i,d}$ with $\mathrm{mod}(\phi_{i,d} + \phi_{i,4y-3} + \phi_{i,4y-1}, 2\pi)$.
       • Else, if $h_y = 1$ and $c = 1$: replace $\phi_{i,4y-2}$ with a random angle from the set $\{0, \pi/4, .., 7\pi/4\}$ and replace $\phi_{i,d}$ with $\mathrm{mod}(\phi_{i,d} + \phi_{i,4y-2}, 2\pi)$.
   2.2 For $y = (d-1)/4$:
       • If $c = 0$ replace $\phi_{i,4y-3}$ and $\phi_{i,4y-1}$ with random angles from the set $\{0, \pi/4, .., 7\pi/4\}$ and replace $\phi_{i,d}$ with $\mathrm{mod}(\phi_{i,d} + \phi_{i,4y-3} + \phi_{i,4y-1}, 2\pi)$.
       • If $c = 1$ replace $\phi_{i,4y-3}$, $\phi_{i,4y-2}$ and $\phi_{i,4y-1}$ with $\pi/2$.
Output: The set of measurement angles $\{\phi_{i,j}\}$.
```

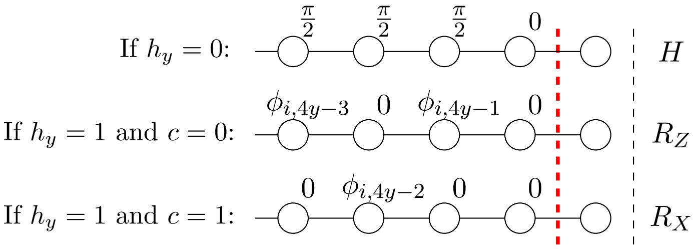


Figure 4.3: In Step 2 of Routine 1 all the angles are assigned such that the bricks implement Hadamard gates, $R_X(\phi_{i,4y-2})$ or $R_Z(\phi_{i,4y-3})R_Z(\phi_{i,4y-1})$, with $\phi_{i,4y-2}, \phi_{i,4y-3}, \phi_{i,4y-1} \in \{0, \pi/4, .., 7\pi/4\}$ chosen at random (see also Figure 2.6). Using $HR_X(\varphi)H = R_Z(\varphi)$, Hadamard gates and rotations are concatenated so that the qubits in the logical circuit undergo an overall R_Z-rotation by a random angle.

Box 4.3 Routine 2 (angles for C-trap).

```
Input:
• The size of the target computation: $(n, d)$.
Routine:
1. Initialize $n \times d$ numbers $\phi_{i,j} = 0$.
2. For all $i \in \{1, \dots, n\}$:
    2.1 For all $y \in \{1, \dots, (d-1)/4\}$:
        If $\mathrm{mod}(i + y, 2) = 0$, with probability $1/2$ replace
            $\phi_{i,4y-1}$ with $\pi/2$
            $\phi_{i+1,4y-2}$ with $\pi/2$
            $\phi_{i+1,4y}$ with $-\pi/2$ ,
        otherwise replace
            $\phi_{i+1,4y-1}$ with $\pi/2$
            $\phi_{i,4y-2}$ with $\pi/2$
            $\phi_{i,4y}$ with $-\pi/2$
Output: The set of measurement angles $\{\phi_{i,j}\}$.
```

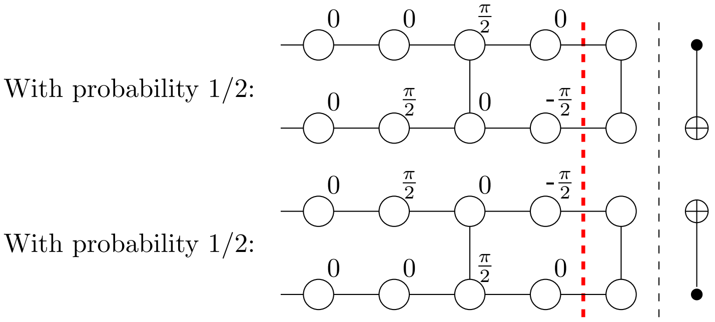


Figure 4.4: In Step 2.1 of Routine 2 the angles are assigned so that the bricks implement a CNOT with random target and control qubits (Figure 2.6).

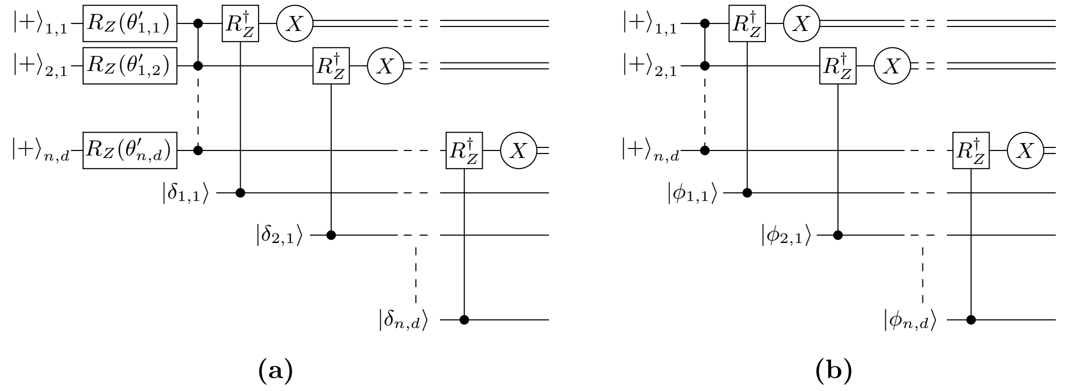


Figure 4.5: **(a)** Computations implemented by Alice and honest Bob, where for convenience we denote by $\theta'_{i,j} = \theta^{(k)}_{i,j} + \pi \sum^{(k)}_{(i',j')\sim(i,j)} r'^{(k)}_{i',j'}$ the rotations in the input qubits. Measuring by angles $\delta_{i,j}$ and bit-flipping the outputs as in Step 3.3 of the protocol is equivalent to undoing the initial rotations and measuring by angles $\phi_{i,j}$, i.e., to implement the computation in **(b)**.

and the subsequent bit-flip operated by Alice (Step 3.3) undo the Pauli-Z rotations in the qubits prepared by Alice (Figure 4.5). Therefore, if Bob is honest, the protocol always returns the correct outputs (i.e., the same outputs as those that would be obtained by setting $\theta^{(k)}_{i,j} = 0$, $r^{(k)}_{i,j} = 0$ and ${r'}^{(k)}_{i,j} = 0$ for all i, j and k).

4.3.3 Blindness

In Section 4.7.2 (Theorem 5) we prove that our prepare-and-send protocol is blind. The proof relies on showing that the random numbers $\theta^{(k)}_{i,j}$, $r^{(k)}_{i,j}$ and ${r'}^{(k)}_{i,j}$ operate a one-time-pad on the measurement angles $\{\phi^{(k)}_{i,j}\}$ and on the measurement outputs $s^{(k)}_{i,j}$. In simple terms, due to the random numbers all the angles and outputs look like random to Bob, hence he cannot distinguish the computation implementing the target from those implementing traps.

4.3.4 Completeness and soundness

In Section 4.7.3 we calculate completeness and soundness for our protocol. We prove the following result:

Theorem 3. **[Completeness and Soundness].** *Suppose that Alice and Bob implement Protocol 1 with v trap computations. Then, Protocol 1 is (δ, ε)-verifiable*

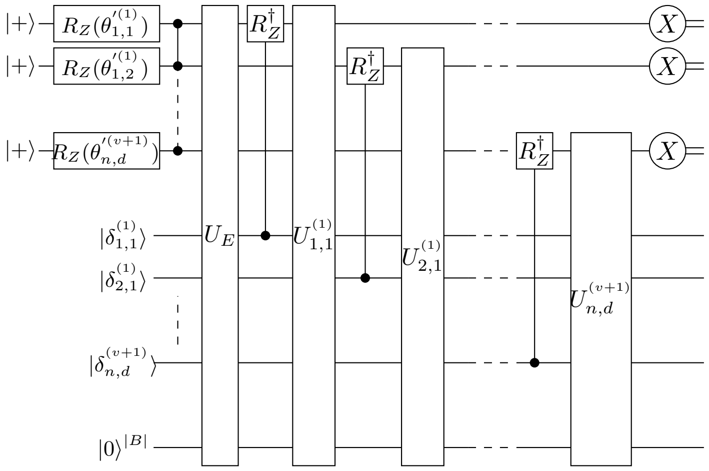

$|+\rangle$
$R_Z(\theta'^{(1)}_{1,1})$
$|+\rangle$
$R_Z(\theta'^{(1)}_{1,2})$
$|+\rangle$
$R_Z(\theta'^{(v+1)}_{n,d})$
$|\delta^{(1)}_{1,1}\rangle$
$|\delta^{(1)}_{2,1}\rangle$
$|\delta^{(v+1)}_{n,d}\rangle$
$|0\rangle^{|B|}$
U_E
$R_Z^\dagger$
$U^{(1)}_{1,1}$
$R_Z^\dagger$
$U^{(1)}_{2,1}$
$R_Z^\dagger$
$U^{(v+1)}_{n,d}$
X
X
X

Figure 4.6: Protocol run with dishonest Bob, where for convenience we denote by $\theta'_{i,j}$ the rotations in the input qubits. Without loss of generality we represent Bob's deviations as unitaries *after* the corresponding operation.

with

$$\delta = 1 \quad \text{and} \quad \varepsilon = \frac{7}{v+1}\left(\frac{7}{8}\right)^6 \approx \frac{3.14}{v+1} \tag{4.4}$$

Proof. (Sketch. See Section 4.7.3 for full details.) Completeness $\delta = 1$ follows trivially from Theorem 4 (correctness) and from the fact that if correctly implemented, the logical circuits associated with the traps always output $\overline{s} = \overline{0}$ by construction.

To calculate soundness, let us describe Bob's deviations as a series of unitary gates acting on the unmeasured qubits, on the angles and on a private register (Figure 4.6). Using the Pauli Twirl (Theorem 1) we show that on average (i.e., summing over the random numbers $\theta^{(k)}_{i,j}$, $r^{(k)}_{i,j}$ and $r'^{(k)}_{i,j}$), Bob's deviations reduce to stochastic Pauli-Z errors happening before the measurements. Formally:

Lemma 1. [Twirl for Bob's deviations]. *Summed over the random numbers $\theta^{(k)}_{i,j}$, $r^{(k)}_{i,j}$ and $r'^{(k)}_{i,j}$, the state in Alice's register at the end of Step 3 of our Protocol 1 is*

$$\rho_{\text{out}} = \sum_{\overline{s}^{(1)},\ldots,\overline{s}^{(v+1)}} \sum_{\mathcal{P}} \frac{\text{prob}\big(\overline{s}^{(1)},\ldots,\overline{s}^{(v+1)}|\mathcal{P}\big)}{2^{nd(v+1)}} \left(\bigotimes_{i,j,k} Z^{s^{(k)}_{i,j}}|+\rangle\langle+|Z^{s^{(k)}_{i,j}}\right), \tag{4.5}$$

where

$$\begin{aligned}&\mathrm{prob}(\overline{s}^{(1)},\dots,\overline{s}^{(v+1)}|\mathcal{P}) \\ &= \mathrm{prob}\big(\mathcal{P}\big)\Big[\otimes_{i,j,k}\langle +|Z^{s^{(k)}_{i,j}}\Big]\Big[\mathcal{P}\Big(\otimes_{i,j,k}\mathcal{R}^{\dagger}_{Z}(\phi^{(k)}_{i,j})\Big)c\mathcal{Z}\big(\rho_{\mathrm{in}}\big)\Big]\Big[\otimes_{i,j,k}Z^{s^{(k)}_{i,j}}|+\rangle\Big]\end{aligned} \tag{4.6}$$

is the probability of obtaining measurement outputs $\overline{s}^{(1)},\dots,\overline{s}^{(v+1)}$ *when a Pauli error* $\mathcal{P}\in\{I,Z\}^{\otimes nd(v+1)}$ *occurs and prob*$(\mathcal{P})$ *is the probability of error* $\mathcal{P}$ *occurring.*

Lemma 1 greatly simplifies Alice's task, as it renders verification no harder than Pauli error detection. These Pauli errors may involve multiple computations at the same time, creating cross-circuit correlations. However, the probability that an error $\mathcal{P}$ occurrs is independent of the angles $\phi^{(k)}_{i,j}$ (Equation 4.6). This means that Bob cannot decide how to deviate based on the traps that are being implemented in the protocol run (which is a consequence of blindness).

The next step in the proof is to show that our trap computations can detect all the Pauli errors that may possibly arise from Bob's deviations. We prove the following Lemmas:

Lemma 2. [R-traps lemma]. *Consider a BwS implementing an R-trap and suppose that Pauli-Z errors afflict some of the qubits in the BwS. For any combination of Pauli-Z errors, apart from two sets of errors denoted as "Type-I" and "Type-II" (which we define in the proof of Lemma 2, cfr. Section 4.7.3), the probability that the R-trap returns the correct output* $\overline{s}=\overline{0}$ *is at most 3/4 (i.e., the errors are detected with probability at least 1/4).*

Lemma 3. [C-traps lemma]. *Consider a BwS implementing a C-trap and suppose that Pauli-Z errors afflict some of the qubits in the BwS. Then, for any combination of Pauli-Z errors belonging to the Type-I or Type-II sets or to their union, the probability that the C-trap returns the correct output* $\overline{s}=\overline{0}$ *is at most 1/2 (i.e., the errors are detected with probability at least 1/2).*

We can now calculate soundness. To do so, suppose that Bob deviates on $\widetilde{v}$ computations, with $1\leq\widetilde{v}\leq v+1$. In this case, the probability $p(E_1\wedge E_2|\widetilde{v})$ of the events E_1 *Bob corrupts the target computation* and E_2 *Bob is not detected* when Bob deviates on $\widetilde{v}$ computations equals

$$p(E_1\wedge E_2|\widetilde{v}) = p(E_1|\widetilde{v})\;p(E_2|E_1\wedge\widetilde{v})\;. \tag{4.7}$$

Since the protocol is blind, Bob cannot distinguish between target and trap computations, therefore $p(E_1|\widetilde{v})=\widetilde{v}/(v+1)$. Moreover, due to Lemmas 2 and 3 we have

$$p(E_2|E_1 \wedge \widetilde{v}) \leq \left(\frac{1}{2} \times \frac{3}{4} + \frac{1}{2} \times 1\right)^{\widetilde{v}-1} = \left(\frac{7}{8}\right)^{\widetilde{v}-1} , \tag{4.8}$$

since Bob's optimal strategy is to introduce Pauli errors that are not detected by the C-traps and are detected by the R-traps with probability 1/4. Maximizing $p(E_1 \wedge E_2|\widetilde{v})$ over $\widetilde{v}$ yields:

$$\varepsilon = \max_{\widetilde{v}} \; p(E_1 \wedge E_2|\widetilde{v}) \approx \frac{3.14}{v+1}, \text{ for } \widetilde{v} = 7 \; . \tag{4.9}$$

□

4.4 Protocol for Alice performing measurements

Our Protocol 2 relies on the fact that any state ρ measured in the basis $\{|\psi\rangle\langle\psi|, |\psi_\perp\rangle\langle\psi_\perp|\}$ (where $\langle\psi|\psi_\perp\rangle = 0$) collapses into $|\psi\rangle$ or $|\psi_\perp\rangle$. Building on this we show that Alice, who can now only perform single-qubit measurements in the basis $\{0, \pi/4, \ldots, 7\pi/4\}$, can blindly generate the same input state as in Protocol 1 and thus verify Bob's behavior by running Protocol 1.

Protocol 2 is formally presented in Box 4.4. State preparation in Protocol 2 works as follows. For all qubits (i, j) in all computations $k \in \{1, \ldots, v+1\}$ (traps and target) Bob prepares eight qubits, each in one of the states $|+\rangle_\tau$, $\tau \in \{0, \pi/4, .., 7\pi/4\}$ and sends them to Alice. Alice measures each qubit $|+\rangle_\tau$ in the corresponding basis $\{|+\rangle_\tau\langle+|\}$. If all the measurements output 0, she sends a qubit at random to Bob and discards the other seven qubits, otherwise she restarts preparation of qubit (i, j).

The correctness of Protocol 2 can be shown with the same calculations as in the proof of Theorem 4. To show the blindness of Protocol 2 we begin by using the no-communication theorem [69], which states that Alice cannot send information to Bob by measuring qubits in her register, even if these qubits are entangled with qubits in Bob's register. Consequently, Bob cannot retrieve information about the state of the qubits that he receives from Alice. Blindness can then be proven using the same arguments as in the proof of Theorem 5. Finally, with the same calculations as in the proof of Theorem 3 it can be shown that Protocol 2 has the same completeness and soundness as Protocol 1.

We now analyze the complexity of Protocol 2, i.e., the number of qubits and bits sent by Alice to Bob and vice-versa. The number of classical bits and qubits

Box 4.4. Protocol 2.

Assumption:

Alice can receive qubits from Bob, measure them in the bases $\{|\pm\rangle_{\tau}\langle\pm|\}$, with $\tau \in \{0, \pi/4, .., 7\pi/4\}$, and send them to Bob.

Input:

- The set of measurement angles $\{\phi_{i,j}\}$ for the target computation.
- The number of trap computations v.

Routine:

1. Alice randomly chooses $v_0 \in \{1, \ldots, v+1\}$ and sets $\{\phi_{i,j}^{(v_0)}\} = \{\phi_{i,j}\}$. Moreover, she generates the random bits $r_{i,j}^{(k)}, r_{i,j}^{\prime(k)} \in \{0,1\}$ for $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, d\}$ and $k \in \{1, \ldots, v+1\}$.

2. For $k \in \{1, \ldots, v+1\}$:
   If $k \neq v_0$, Alice randomly runs Routine 1 or Routine 2 on input $n \times d$ and obtains the set of angles $\{\phi_{i,j}^{(k)}\}$.

3. For $k \in \{1, \ldots, v+1\}$:

   3.1 For $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, d\}$:
   Bob creates eight qubits in the states $|+\rangle_{\tau_{i,j}^{(k)}}$, with $\tau_{i,j}^{(k)} \in \{0, \pi/4, .., 7\pi/4\}$, and sends them to Alice. Alice measures each qubit $|+\rangle_{\tau_{i,j}^{(k)}}$ it in the basis $\{|\pm\rangle_{\tau_{i,j}^{(k)}}\langle\pm|\}$. If all the measurements output 0, she sends to Bob a random qubit in the state $|+\rangle_{\widehat{\tau}_{i,j}^{(k)}}$ and discards the others, moreover she defines $\theta_{i,j}^{(k)} = \widehat{\tau}_{i,j}^{(k)} + \pi \sum_{(i',j') \sim (i,j)}^{(k)} r_{i',j'}^{\prime(k)}$. Otherwise, she restarts preparation of qubit (i,j).

   3.2 Bob entangles the qubits in his register and creates the BwS.

   3.3 For $j \in \{1, \ldots, d\}$ and for $i \in \{1, \ldots, n\}$:
   Alice instructs Bob to measure qubit (i,j) with angle $\delta_{i,j}^{(k)} = (-1)^{r_{i,j}^{\prime(k)}} \phi_{i,j}^{(k)} + \theta_{i,j}^{(k)} + r_{i,j}^{(k)} \pi$. Bob reveals the measurement output $s_{i,j}^{(k)}$ to Alice. Alice replaces $s_{i,j}^{(k)}$ with $s_{i,j}^{(k)} \oplus r_{i,j}^{(k)}$, next she recomputes measurement angles of the unmeasured qubits as $\{(-1)^{s_X} \phi_{i,j}^{(k)} + s_Z \pi\}$.

4. Alice initializes a flag bit to the state $|\mathrm{acc}\rangle = |0\rangle$. Next, for all $k \in \{1, \ldots, v+1\}$: if $k \neq v_0$ (trap circuit) and $\{s_{i,d}^{(k)}\}_{i=1}^{n} \neq (0,0,..,0)$, Alice sets the flag bit to $|\mathrm{rej}\rangle = |\mathrm{acc} \oplus 1\rangle$.

Output: The measurement outputs of the target circuit and the flag bit.

sent by Alice to Bob is $3(v+1)nd$ and $(v+1)nd$ respectively. Bob sends $9(v+1)nd$ qubits and $(v+1)nd$ bits to Alice.

4.5 Comparison with related works

In this Section we compare our protocols with the existing protocols. We refer the reader to Ref. [81] for a recent detailed review of verification protocols.

Our Protocol 1 (Section 4.3) belongs to the class of prepare-and-send protocols, such as [49, 51, 52, 54]. Compared to our protocol, these protocols require more resources on Alice's side while achieving (in the best case) the same overhead. In more detail, in Fitzsimons and Kashefi's protocol [49] Alice needs to prepare qubits in the state $|+\rangle_\theta$, $\theta \in \{0, \pi/4, .., 7\pi/4\}$, as well as in the states $|0\rangle$ and $|1\rangle$. The overhead of Fitzsimons and Kashefi's protocol is quadratic in the size of the computation, although it was subsequently made linear [51, 52]. Similarly, in Broadbent's protocol [54], Alice needs to generate qubits in the states $|0\rangle$ and $|+\rangle$ and to apply the gates X, Z, S and T. Overall, Broadbent's protocol requires the same resources as the Fitzsimons and Kashefi's one and has the same overhead. Other prepare-and-send protocols include those by Aharonov et al. [67]. These protocols are more demanding for Alice, who must hold a multi-qubit register and implements quantum error correction [82].

Protocol 2 (Section 4.4) belongs to the class of receive-and-measure protocols, such as the "measurement-only" scheme [55] and the "post-hoc" verification techniques [56, 57]. In Ref. [55] Alice measures in five bases, hence it requires more resources than our protocol. Also, in Ref. [55] soundness decreases as $\varepsilon \approx 1/\sqrt{v+1}$ (where v is the number of traps), as opposed to $\varepsilon \approx 1/(v+1)$ in our protocol. Nevertheless, it must be mentioned that in Ref. [55] Alice discards all the qubits after the measurements. We leave as an open question the possibility of adapting Protocol 2 to the more realistic scenario where the qubits can not be reused after being measured.

The post-hoc protocols in [56, 57] are non-trap-based protocols with a single round of communication between the verifier and the prover. Verification is performed after the computation has been carried out. In these protocols, Alice makes measurements in the Pauli-Z and Pauli-X bases. Unlike our protocols, post-hoc protocols are not blind [81], moreover their overhead is quadratic in the input.

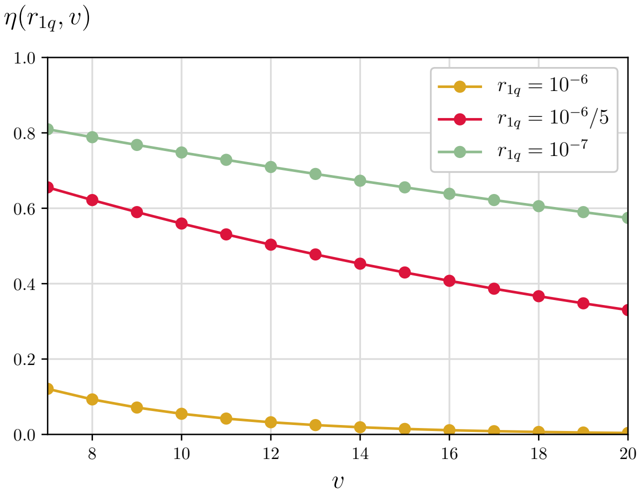


Figure 4.7: The probability $\eta(r_{1q}, v)$ that Bob returns the correct outputs and Alice accepts them (larger is better), plotted as a function of the number v of traps and for different error rates r_{1q}. As it can be observed, $\eta(r_{1q}, v)$ decreases as v increases. Moreover, smaller error rates correspond to higher $\eta(r_{1q}, v)$. Therefore, to maximise the probability of success, Alice and Bob must implement few traps and at the same time improve their devices.

4.6 Utility of the prepare-and-send protocol

In this Section we analyze the utility of Protocol 1. Specifically, we suppose that Alice wants to verify the outputs of a quantum circuit containing $n = 60$ qubits and $m = 22$ bands (Figure 1.1). We assume that Bob is honest, however all the operations performed by his quantum computer (gates and measurements) suffer Pauli noise (Section 2.4, page 14). Specifically, we assume that all single-qubit gates have error rate r_{1q}, all two-qubit gates have error rate r_{2q}, state-preparation and measurement (SPAM) errors happen with probability r_s. As in Google Sycamore (Table 1.1, page 2), we set $r_{2q} = 4r_{1q}$ and $r_s = 20r_{1q}$. We then calculate the probability $\eta(r_{1q}, v) := \text{prob}(\text{correct} \wedge \text{accept} \mid r_{1q}, v)$ that the protocol returns the correct outputs of the target and that these outputs are accepted, given that the error rate of the single-qubit gates is r_{1q}.

We begin by calculating the size of the BwS prepared by Bob. This contains $n = 60$ rows of qubits. As for the number d of columns, based on the circuit identities in Figure 2.6 we have $d \geq 8m = 176$, and for simplicity we assume $d = 176$. To carry a computation on a BwS with 60 rows and 176 columns Bob implements 10560 single-qubit gates, 10560 Pauli-X measurements and ≈ 10560 cZ gates (see caption of Figure 2.3). Therefore, using Equation 2.24 on page 14, the probability that Bob returns the correct outputs and Alice accepts them is

$$\eta(r_{1q}, v) \approx \Big[(1 - r_{1q})(1 - 4r_{1q})(1 - 20r_{1q})\Big]^{10560(v+1)} \tag{4.10}$$

In Figure 4.7 we plot the r.h.s. of the above Equation for various error rates r_{1q} and numbers v of trap computations. As it can be observed, to return the correct output and convince Alice to accept it with *high* probability (e.g., above 10%), Bob must possess a quantum computer with error rates below 10^{-6}. This is ≈ 1500 times smaller than in Google Sycamore (where single-qubit gates have error rate $r_{1q} \approx 1.5 \times 10^{-3}$, see Table 1.1 on page 2). Therefore, the error rates must be improved by three orders of magnitude as compared to current technology before Protocol 1 can be useful.

4.7 Proofs

In this Section we provide a formal proof of the main statements and theorems contained in this Chapter.

4.7.1 Correctness of prepare-and-send protocol

We begin by proving the correctness of the prepare-and-send protocol.

Theorem 4. [Correctness]. *If Bob is honest, the outputs in Alice's register at the end of Step 3 of Protocol 1 are the same as those that she obtains by setting* $\theta_{i,j}^{(k)}, r_{i,j}^{(k)}, r_{i,j}^{\prime\,(k)} = 0$ *for all* $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, d\}$, $k \in \{1, \ldots, v+1\}$.

The proof follows the same arguments as in Ref. [75].

Proof. We begin by considering the case $v = 1$ (Alice and Bob implement a single computation). If Bob is honest, for a fixed choice of random numbers $\theta_{i,j}$, $r_{i,j}$ and $r'_{i,j}$ (where for simplicity we omit the index (1)) the state of the system at the end of the computation is of the form (Figure 4.5a)

$$\rho_{\text{out}} = \mathcal{M}_X c\mathcal{R}^\dagger_{n,d} \ldots c\mathcal{R}^\dagger_{1,1} c\mathcal{Z}\big(\rho_{\text{in}}^{\bar{\theta},\bar{r}'} \otimes |\delta_{i,j}\rangle\langle\delta_{i,j}|\big) \ , \tag{4.11}$$

where $c\mathcal{Z}$ represents the entangling operation, $c\mathcal{R}^\dagger_{i,j}$ represents the controlled rotation on qubit (i,j), $\mathcal{M}_X$ is the final round of Pauli-X measurements and

$$\rho_{\text{in}}^{\overline{\theta},\overline{r}'} = \bigotimes_{i,j} \left[R_Z\left(\theta_{i,j} + \pi \sum_{(i',j')\sim(i,j)} r'_{i',j'}\right)|+\rangle_{i,j}\langle+|R_Z^{\dagger}\left(\theta_{i,j} + \pi \sum_{(i',j')\sim(i,j)} r'_{i',j'}\right)\right] . \tag{4.12}$$

We now rewrite the controlled rotations as uncontrolled ones and trace out the classical register. We obtain

$$\rho'_{\text{out}} = \mathcal{M}_X \mathcal{R}^{\dagger}_{n,d}(\delta_{n,d}) \ldots \mathcal{R}^{\dagger}_{1,1}(\delta_{1,1}) c\mathcal{Z}\big(\rho_{\text{in}}^{\overline{\theta},\overline{r}'}\big) , \tag{4.13}$$

where $\mathcal{R}^{\dagger}_{i,j}(\delta_{i,j})$ is a R_Z-rotation on qubit (i,j) by angle $-\delta_{i,j}$.

Since $\delta_{i,j} = (-1)^{r'_{i,j}}\phi_{i,j} + \theta_{i,j} + r_{i,j}\pi$ we rewrite all the rotations as

$$\mathcal{R}^{\dagger}\big((-1)^{r'_{i,j}}\phi_{i,j} + \theta_{i,j} + r_{i,j}\pi\big) = \mathcal{Z}^{r_{i,j}}\mathcal{X}^{r'_{i,j}}\mathcal{R}^{\dagger}_{i,j}\big(\phi_{i,j}\big)\mathcal{X}^{r'_{i,j}}\mathcal{R}^{\dagger}_{i,j}\big(\theta_{i,j}\big) . \tag{4.14}$$

Commuting the various $\mathcal{X}^{r'_{i,j}}\mathcal{R}^{\dagger}_{i,j}\big(\theta_{i,j}\big)$ with $c\mathcal{Z}$ then gives

$$\rho'_{\text{out}} = \mathcal{M}_X \mathcal{X}^{r'_{n,d}}\mathcal{Z}^{r_{n,d}}\mathcal{R}^{\dagger}_{n,d}\big(\phi_{n,d}\big) \ldots \mathcal{X}^{r'_{1,1}}\mathcal{Z}^{r_{1,1}}\mathcal{R}^{\dagger}_{1,1}\big(\phi_{1,1}\big) c\mathcal{Z}\big(\rho_{\text{in}}^{\overline{0},\overline{0}}\big) , \tag{4.15}$$

where $\rho_{\text{in}}^{\overline{0},\overline{0}} = \otimes_{i,j}|+\rangle_{i,j}\langle+|$. Using $\mathcal{M}_X\mathcal{X}^{r'_{n,d}} \ldots \mathcal{X}^{r'_{1,1}} = \mathcal{M}_X$ (X gates before Pauli-X measurements have no effect), we can omit all the $\mathcal{X}^{r'_{i,j}}$. Moreover, we can also omit all the $\mathcal{Z}^{r_{i,j}}$ (if $r_{i,j} = 1$, $\mathcal{Z}^{r_{i,j}}$ bit-flips the output of qubit (i,j), but Alice undoes this bit flip in Step 3.3). This yields

$$\rho'_{\text{out}} = \mathcal{M}_X \mathcal{R}^{\dagger}_{n,d}\big(\phi_{n,d}\big) \ldots \mathcal{R}^{\dagger}_{1,1}\big(\phi_{1,1}\big) c\mathcal{Z}\big(\rho_{\text{in}}^{\overline{0},\overline{0}}\big) . \tag{4.16}$$

Finally, expressing rotations as controlled rotations we obtain

$$\rho''_{\text{out}} = \mathcal{M}_X c\mathcal{R}^{\dagger}_{n,d} \ldots c\mathcal{R}^{\dagger}_{1,1} c\mathcal{Z}\big(\rho_{\text{in}}^{\overline{0},\overline{0}} \otimes |\phi_{i,j}\rangle\langle\phi_{i,j}|\big) . \tag{4.17}$$

This proves the theorem for $v = 1$. Generalization to $v > 1$ follows trivially by repeating the same calculations for all the computations. □

4.7.2 Blindness of prepare-and-send protocol

In this Section we prove the following Theorem:

Theorem 5. [Blindness]. *Protocol 1 is blind.*

The proof relies on the same arguments as in Ref. [83]. For brevity in the proof we define $\widehat{r}_{i,j}^{(k)} = \sum_{(i',j')\sim(i,j)} r'^{(k)}_{i',j'}$ and $\theta'^{(k)}_{i,j} = \theta^{(k)}_{i,j} + \pi\widehat{r}^{(k)}_{i,j}$.

Proof. For a fixed choice of random numbers $\theta_{i,j}^{(k)}$, $r_{i,j}^{(k)}$ and $r'^{\,(k)}_{i,j}$, after Bob receives all the qubits and measurement angles he holds the state (Figure 4.5a)

$$\rho_B = \bigotimes_{i,j,k} \left(R_Z\big(\theta'^{(k)}_{i,j}\big)|+\rangle_{i,j}^{(k)}\langle +|R_Z^\dagger\big(\theta'^{(k)}_{i,j}\big) \otimes |\delta_{i,j}^{(k)}\rangle\langle\delta_{i,j}^{(k)}| \right) . \tag{4.18}$$

To prove blindness, let us define a classically controlled unitary U_{cc} whose action on a state ρ and on an angle δ is defined as

$$U_{\mathrm{cc}}\big(\rho \otimes |\delta\rangle\langle\delta|\big)U_{\mathrm{cc}}^\dagger = R_Z(-\delta)\rho R_Z^\dagger(-\delta) \otimes |\delta\rangle\langle\delta| \, . \tag{4.19}$$

Applying U_{cc} to ρ_B and using

$$R_Z\big(\theta'^{(k)}_{i,j} - \delta_{i,j}^{(k)}\big) = Z^{r_{i,j}^{(k)} \oplus \widehat{r}_{i,j}^{(k)}} X^{r'^{(k)}_{i,j}} R_Z\big(-\phi_{i,j}^{(k)}\big) X^{r'^{(k)}_{i,j}} \tag{4.20}$$

gives

$$\begin{aligned} \rho'_B =& CUU(\rho_B)CUU^\dagger \\ =& \bigotimes_{i,j,k} \Big[Z^{r_{i,j}^{(k)} \oplus \widehat{r}_{i,j}^{(k)}} X^{r'^{(k)}_{i,j}} R_Z\big(-\phi_{i,j}^{(k)}\big)|+\rangle_{i,j}^{(k)}\langle +|R_Z^\dagger\big(-\phi_{i,j}^{(k)}\big) X^{r'^{(k)}_{i,j}} Z^{r_{i,j}^{(k)} \oplus \widehat{r}_{i,j}^{(k)}} \\ & \otimes |\delta_{i,j}^{(k)}\rangle\langle\delta_{i,j}^{(k)}| \Big] \, . \end{aligned} \tag{4.21}$$

Summing over all $\theta_{i,j}^{(k)}$ (which are randomly chosen, and which are now only contained in $\delta_{i,j}^{(k)}$), we obtain

$$\begin{aligned} &\sum_{\{\theta_{i,j}^{(k)}\}} \frac{\rho'_B}{8^{nd(v+1)}} \qquad (4.22) \\ =& \bigotimes_{i,j,k} \left[Z^{r_{i,j}^{(k)} \oplus \widehat{r}_{i,j}^{(k)}} X^{r'^{(k)}_{i,j}} R_Z\big(-\phi_{i,j}^{(k)}\big)|+\rangle_{i,j}^{(k)}\langle +|R_Z^\dagger\big(-\phi_{i,j}^{(k)}\big) X^{r'^{(k)}_{i,j}} Z^{r_{i,j}^{(k)} \oplus \widehat{r}_{i,j}^{(k)}} \otimes \frac{I^{\otimes 3}}{2^3} \right] , \end{aligned}$$

where $I^{\otimes q}/2^q$ is the q-qubit maximally mixed state. We can now sum over the random numbers parameter $r_{i,j}^{(k)}$ and $r'^{\,(k)}_{i,j}$, obtaining

$$\rho''_B = \sum_{\{r_{i,j}^{(k)}\},\{r'^{\,(k)}_{i,j}\},\{\theta_{i,j}^{(k)}\}} \frac{\rho'_B}{2^{2nd(v+1)}8^{nd(v+1)}} = \bigotimes_{i,j,k} \left[\frac{I^{\otimes 1}}{2} \otimes \frac{I^{\otimes 3}}{2^3} \right] \tag{4.23}$$

as a consequence of the QOTP (Section 2.3).

The state ρ''_B is equivalent the state ρ_B in Bob's register, up to the unitary

U_{cc}. Since ρ''_B is the maximally mixed state, also ρ_B is maximally mixed. Therefore, the state in Bob's register carries no information about the angles $\phi_{i,j}^{(k)}$, and this proves blindness. □

4.7.3 Verifiability of prepare-and-send protocol

In this Section we conclude the proof of Theorem 3 (Completeness and Soundness) by proving Lemmas 1 (Twirl for Bob's deviations), 2 (R-traps lemma) and 3 (C-traps lemma) in pages 31-33. We begin by proving Lemma 1.

Proof of Lemma 1 (Twirl for Bob's deviations)

Proof. (Lemma 1 is stated on page 32). We describe Bob's deviations through a collection of unitaries acting on the unmeasured qubits, on the angles and on Bob's private system (Figure 4.6). The state of the system at the end of the protocol is thus

$$\tau = \mathcal{M}_X\, \mathcal{U}_{n,d}^{(v+1)} c\mathcal{R}_{n,d}^{\dagger\,(v+1)} \ldots \mathcal{U}_{1,1}^{(1)} c\mathcal{R}_{1,1}^{\dagger\,(1)} \mathcal{U}_E\; c\mathcal{Z}\big(\rho_{\mathrm{in}}^{\overline{\theta},\overline{r}'} \otimes |\delta_{i,j}^{(k)}\rangle\langle\delta_{i,j}^{(k)}| \otimes |0\rangle_B\langle 0|\big)\ , \tag{4.24}$$

where

$$\rho_{\mathrm{in}}^{\overline{\theta},\overline{r}'} = \bigotimes_{i,j,k} \left[R_Z\left(\theta_{i,j}^{(k)} + \pi \sum_{(i',j')\sim(i,j)} r'^{\,(k)}_{i',j'}\right) |+\rangle_{i,j}^{(k)}\langle +| R_Z^\dagger\left(\theta_{i,j}^{(k)} + \pi \sum_{(i',j')\sim(i,j)} r'^{\,(k)}_{i',j'}\right)\right]\ , \tag{4.25}$$

$c\mathcal{Z}$ is the entangling operation, $\mathcal{U}_E = \{U_E\}$ is the deviation following entanglement, $c\mathcal{R}_{i,j}^{\dagger\,(k)}$ is the controlled rotation on qubit (i,j) in computation k, $\mathcal{U}_{i,j}^{(k)} = \{U_{i,j}^{(k)}\}$ is the deviation before measurement of qubit (i,j) in computation k and $\mathcal{M}_X$ is the final round of Pauli-X measurements.

We now move all the deviations towards the end of the circuit and merge them into a single unitary $\mathcal{U}_B = \{U_B\}$. We also rewrite the controlled R_Z-gates as uncontrolled rotations, obtaining (Figure 4.8)

$$\tau = \mathcal{M}_X\, \mathcal{U}_B \mathcal{R}_Z^\dagger(\delta_{n,d}^{(v+1)}) \ldots \mathcal{R}_Z^\dagger(\delta_{1,1}^{(1)})\; c\mathcal{Z}\big(\rho_{\mathrm{in}}^{\overline{\theta},\overline{r}'} \otimes |\delta_{i,j}^{(k)}\rangle\langle\delta_{i,j}^{(k)}| \otimes |0\rangle_B\langle 0|\big)\ . \tag{4.26}$$

Since $\delta_{i,j}^{(k)} = (-1)^{r'^{(k)}_{i,j}} \phi_{i,j}^{(k)} + \theta_{i,j}^{(k)} + r_{i,j}^{(k)}\pi$ we have

$$\mathcal{R}_Z^\dagger(\delta_{i,j}^{(k)}) = \mathcal{X}^{r'^{\,(k)}_{i,j}} \mathcal{Z}^{r^{(k)}_{i,j}} \mathcal{R}_Z^\dagger(\phi_{i,j}^{(k)}) \mathcal{X}^{r'^{\,(k)}_{i,j}} \mathcal{R}_Z^\dagger(\theta_{i,j}^{(k)})\ , \tag{4.27}$$

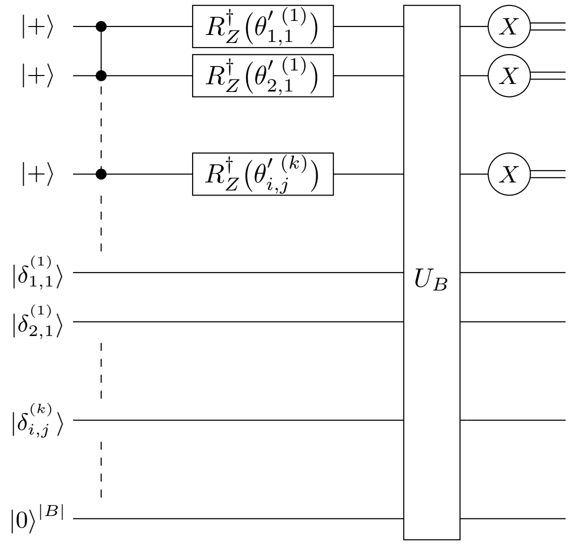

$|+\rangle$
$|+\rangle$
$|+\rangle$
$R_Z^\dagger(\theta'^{(1)}_{1,1})$
$R_Z^\dagger(\theta'^{(1)}_{2,1})$
$R_Z^\dagger(\theta'^{(k)}_{i,j})$
$|\delta^{(1)}_{1,1}\rangle$
$|\delta^{(1)}_{2,1}\rangle$
$|\delta^{(k)}_{i,j}\rangle$
$|0\rangle^{|B|}$
U_B
X
X
X

Figure 4.8: Simplification of circuit in Figure 4.6 where the deviations are moved toward the end of the circuit and merged into U_B. For convenience we denote by $\theta'^{(k)}_{i,j}$ the rotations in the input qubits.

where we omit unimportant global phases. Therefore, we can rewrite τ as

$$
\begin{aligned}
\tau =& \\
&= \mathcal{M}_X\, \mathcal{U}_B \Big[\otimes_{i,j,k} \mathcal{X}^{r'^{(k)}_{i,j}} \mathcal{Z}^{r^{(k)}_{i,j}} \mathcal{R}_Z^\dagger(\phi^{(k)}_{i,j}) \mathcal{X}^{r'^{(k)}_{i,j}} \mathcal{R}_Z^\dagger(\theta^{(k)}_{i,j}) \Big] c\mathcal{Z}\big(\rho_{\text{in}}^{\overline{\theta},\overline{r}'} \otimes |\delta^{(k)}_{i,j}\rangle\langle\delta^{(k)}_{i,j}| \otimes |0\rangle_B\langle 0|\big) \\
&= \mathcal{M}_X\, \mathcal{U}_B \Big[\otimes_{i,j,k} \mathcal{X}^{r'^{(k)}_{i,j}} \mathcal{Z}^{r^{(k)}_{i,j}} \mathcal{R}_Z^\dagger(\phi^{(k)}_{i,j}) \Big] c\mathcal{Z}\big(\rho_{\text{in}}^{\overline{0},\overline{0}} \otimes |\delta^{(k)}_{i,j}\rangle\langle\delta^{(k)}_{i,j}| \otimes |0\rangle_B\langle 0|\big)\ , \qquad (4.28)
\end{aligned}
$$

where in the second equality we used the same arguments as in the proof of Theorem 4. Summing over all random the $\theta^{(k)}_{i,j}$ (which are now only contained in $|\delta^{(k)}_{i,j}\rangle\langle\delta^{(k)}_{i,j}|$) gives

$$
\frac{1}{2^{3nd(v+1)}} \sum_{\{\theta^{(k)}_{i,j}\}} |\delta^{(k)}_{i,j}\rangle\langle\delta^{(k)}_{i,j}| = \frac{I^{\otimes 2^{3nd(v+1)}}}{2^{3nd(v+1)}}\ . \qquad (4.29)
$$

Thus, tracing Bob's private register out yields

$$
\begin{aligned}
\tau' &= \mathrm{Tr}_B\Bigg[\sum_{\{\theta^{(k)}_{i,j}\}} \frac{\tau}{2^{3nd(v+1)}} \Bigg] \\
&= \mathcal{M}_X\ \mathcal{E}\ \Big[\otimes_{i,j,k} \mathcal{X}^{r'^{(k)}_{i,j}} \mathcal{Z}^{r^{(k)}_{i,j}} \mathcal{R}_Z^\dagger(\phi^{(k)}_{i,j}) \Big] c\mathcal{Z}\left(\rho_{\text{in}}^{\overline{0},\overline{0}} \otimes \frac{I^{\otimes 2^{3nd(v+1)}}}{2^{3nd(v+1)}} \right) \qquad (4.30)
\end{aligned}
$$

for some CPTP map $\mathcal{E} = \{E_u\}$ that does not depend on $\phi^{(k)}_{i,j}$, $r^{(k)}_{i,j}$ and $r'^{(k)}_{i,j}$.

For convenience we now express $\otimes_{i,j,k}\mathcal{R}_Z^{\dagger}(\phi_{i,j}^{(k)})c\mathcal{Z}\big(\rho_{\text{in}}^{\overline{0},\overline{0}}\big)$ as σ and omit the maximally mixed state. Decomposing the Kraus operators $E_u = \sum_{\mu} a_{u,\mu}P_\mu$ in the Pauli basis (with $a_{u,\mu}$ complex numbers) and expanding the various maps we have

$$\tau' = \sum_{\overline{s}^{(1)},\ldots,\overline{s}^{(v+1)}} \sum_{u,\mu,\nu} \frac{a_{u,\mu}a^*_{u,\nu}}{2^{nd(v+1)}} \left(\otimes_{i,j,k} Z^{s_{i,j}^{(k)}}|+\rangle\langle+|Z^{s_{i,j}^{(k)}}\right)\times \tag{4.31}$$
$$\left[\otimes_{i,j,k}\langle+|Z^{s_{i,j}^{(k)}}\right]P_\mu \left[\otimes_{i,j,k} X^{r'^{(k)}_{i,j}} Z^{r^{(k)}_{i,j}}\right]\sigma\left[\otimes_{i,j,k} X^{r'^{(k)}_{i,j}} Z^{r^{(k)}_{i,j}}\right]P_\nu\left[\otimes_{i,j,k} Z^{s_{i,j}^{(k)}}|+\rangle\right]$$

Since the measurements are in the Pauli-X basis, the Pauli-X component of P_μ and P_ν has no effect on the computation and we can assume $P_\mu, P_\nu \in \{I, Z\}^{\otimes nd(v+1)}$. Moreover, we can include extra Pauli-X gates before the measurements, obtaining

$$\tau' = \sum_{\overline{s}^{(1)},\ldots,\overline{s}^{(v+1)}} \sum_{u,\mu,\nu} \frac{a_{u,\mu}a^*_{u,\nu}}{2^{nd(v+1)}} \left(\otimes_{i,j,k} Z^{s_{i,j}^{(k)}}|+\rangle\langle+|Z^{s_{i,j}^{(k)}}\right)\times \tag{4.32}$$
$$\left[\otimes_{i,j,k}\langle+|Z^{s_{i,j}^{(k)}}X^{r'^{(k)}_{i,j}}\right]P_\mu\left[\otimes_{i,j,k} X^{r'^{(k)}_{i,j}} Z^{r^{(k)}_{i,j}}\right]\sigma\left[\otimes_{i,j,k} X^{r'^{(k)}_{i,j}} Z^{r^{(k)}_{i,j}}\right]P_\nu\left[\otimes_{i,j,k} X^{r'^{(k)}_{i,j}} Z^{s_{i,j}^{(k)}}|+\rangle\right]$$

Summing over $r_{i,j}^{(k)}$ and using the Restricted Pauli Twirl (Theorem 2) we obtain

$$\tau'' = \mathrm{Tr}_B\left[\sum_{\{r_{i,j}^{(k)}\}} \frac{\tau'}{2^{nd(v+1)}}\right] = \sum_{\overline{s}^{(1)},\ldots,\overline{s}^{(v+1)}} \sum_{u,\mu,\nu} \frac{|a_{u,\mu}|^2}{2^{nd(v+1)}} \left(\otimes_{i,j,k} Z^{s_{i,j}^{(k)}}|+\rangle\langle+|Z^{s_{i,j}^{(k)}}\right)\times$$
$$\left[\otimes_{i,j,k}\langle+|Z^{s_{i,j}^{(k)}\oplus r_{i,j}^{(k)}}\right]P_\mu\sigma P_\mu\left[\otimes_{i,j,k} Z^{s_{i,j}^{(k)}\oplus r_{i,j}^{(k)}}|+\rangle\right]. \tag{4.33}$$

After Alice recomputes $s_{i,j}^{(k)}$ as $s_{i,j}^{(k)} \oplus r_{i,j}^{(k)}$ (Step 3.3 in the protocol) we finally have

$$\rho_{\text{out}} = \sum_{\overline{s}^{(1)},\ldots,\overline{s}^{(v+1)}} \sum_{u,\mu} \frac{|a_{u,\mu}|^2}{2^{nd(v+1)}} \left(\otimes_{i,j,k} Z^{s_{i,j}^{(k)}}|+\rangle\langle+|Z^{s_{i,j}^{(k)}}\right)\times \tag{4.34}$$
$$\left[\otimes_{i,j,k}\langle+|Z^{s_{i,j}^{(k)}}\right]P_\mu\left(\otimes_{i,j,k}\mathcal{R}_Z^{\dagger}(\phi_{i,j}^{(k)})c\mathcal{Z}\big(\rho_{\text{in}}^{\overline{0},\overline{0}}\big)\right)P_\mu\left[\otimes_{i,j,k} Z^{s_{i,j}^{(k)}}|+\rangle\right].$$

The quantities $b_\mu = \sum_u |a_{u,\mu}|^2$ are positive numbers such that $\sum_\mu b_\mu = 1$. We can thus regard b_μ as the probability associated with P_μ, and this concludes the proof. □

Due to Lemma 1 (Twirl for Bob's deviations), arbitrary deviations by Bob average to stochastic Pauli-Z errors occurring before the measurements. Since $Z =$

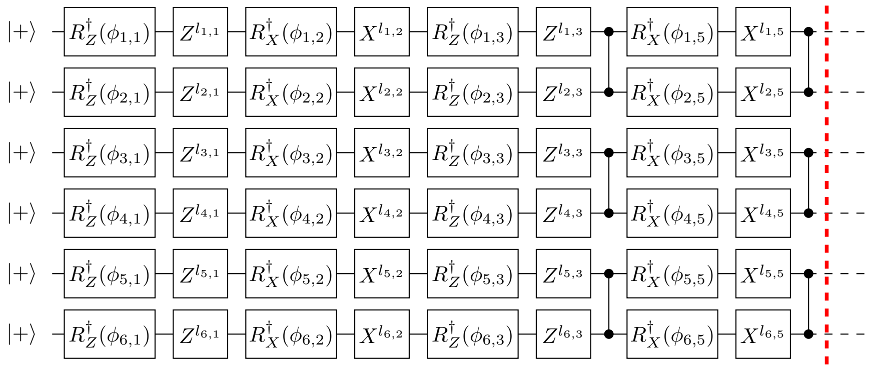

$|+\rangle$ $R^\dagger_Z(\phi_{1,1})$ $Z^{l_{1,1}}$ $R^\dagger_X(\phi_{1,2})$ $X^{l_{1,2}}$ $R^\dagger_Z(\phi_{1,3})$ $Z^{l_{1,3}}$ $R^\dagger_X(\phi_{1,5})$ $X^{l_{1,5}}$
$|+\rangle$ $R^\dagger_Z(\phi_{2,1})$ $Z^{l_{2,1}}$ $R^\dagger_X(\phi_{2,2})$ $X^{l_{2,2}}$ $R^\dagger_Z(\phi_{2,3})$ $Z^{l_{2,3}}$ $R^\dagger_X(\phi_{2,5})$ $X^{l_{2,5}}$
$|+\rangle$ $R^\dagger_Z(\phi_{3,1})$ $Z^{l_{3,1}}$ $R^\dagger_X(\phi_{3,2})$ $X^{l_{3,2}}$ $R^\dagger_Z(\phi_{3,3})$ $Z^{l_{3,3}}$ $R^\dagger_X(\phi_{3,5})$ $X^{l_{3,5}}$
$|+\rangle$ $R^\dagger_Z(\phi_{4,1})$ $Z^{l_{4,1}}$ $R^\dagger_X(\phi_{4,2})$ $X^{l_{4,2}}$ $R^\dagger_Z(\phi_{4,3})$ $Z^{l_{4,3}}$ $R^\dagger_X(\phi_{4,5})$ $X^{l_{4,5}}$
$|+\rangle$ $R^\dagger_Z(\phi_{5,1})$ $Z^{l_{5,1}}$ $R^\dagger_X(\phi_{5,2})$ $X^{l_{5,2}}$ $R^\dagger_Z(\phi_{5,3})$ $Z^{l_{5,3}}$ $R^\dagger_X(\phi_{5,5})$ $X^{l_{5,5}}$
$|+\rangle$ $R^\dagger_Z(\phi_{6,1})$ $Z^{l_{6,1}}$ $R^\dagger_X(\phi_{6,2})$ $X^{l_{6,2}}$ $R^\dagger_Z(\phi_{6,3})$ $Z^{l_{6,3}}$ $R^\dagger_X(\phi_{6,5})$ $X^{l_{6,5}}$

Figure 4.9: First tape in a logical circuit associated with a BwS afflicted by Pauli-Z errors. Each number $l_{i,j}$ equals 1 if a Pauli-Z afflicts qubit (i, j) in the BwS, 0 otherwise.

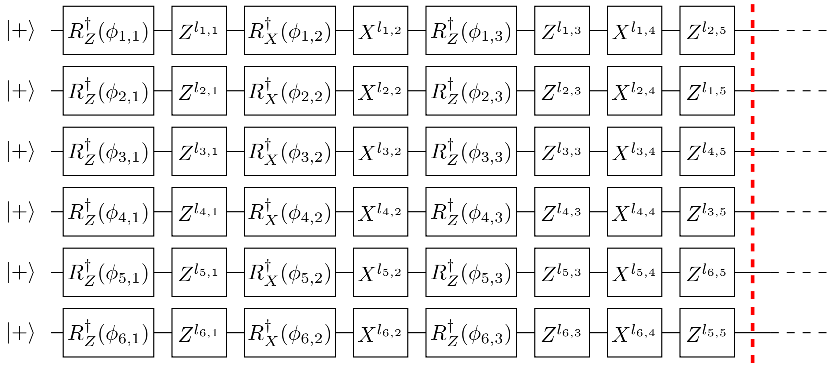

$|+\rangle$ $R^\dagger_Z(\phi_{1,1})$ $Z^{l_{1,1}}$ $R^\dagger_X(\phi_{1,2})$ $X^{l_{1,2}}$ $R^\dagger_Z(\phi_{1,3})$ $Z^{l_{1,3}}$ $X^{l_{1,4}}$ $Z^{l_{2,5}}$
$|+\rangle$ $R^\dagger_Z(\phi_{2,1})$ $Z^{l_{2,1}}$ $R^\dagger_X(\phi_{2,2})$ $X^{l_{2,2}}$ $R^\dagger_Z(\phi_{2,3})$ $Z^{l_{2,3}}$ $X^{l_{2,4}}$ $Z^{l_{1,5}}$
$|+\rangle$ $R^\dagger_Z(\phi_{3,1})$ $Z^{l_{3,1}}$ $R^\dagger_X(\phi_{3,2})$ $X^{l_{3,2}}$ $R^\dagger_Z(\phi_{3,3})$ $Z^{l_{3,3}}$ $X^{l_{3,4}}$ $Z^{l_{4,5}}$
$|+\rangle$ $R^\dagger_Z(\phi_{4,1})$ $Z^{l_{4,1}}$ $R^\dagger_X(\phi_{4,2})$ $X^{l_{4,2}}$ $R^\dagger_Z(\phi_{4,3})$ $Z^{l_{4,3}}$ $X^{l_{4,4}}$ $Z^{l_{3,5}}$
$|+\rangle$ $R^\dagger_Z(\phi_{5,1})$ $Z^{l_{5,1}}$ $R^\dagger_X(\phi_{5,2})$ $X^{l_{5,2}}$ $R^\dagger_Z(\phi_{5,3})$ $Z^{l_{5,3}}$ $X^{l_{5,4}}$ $Z^{l_{6,5}}$
$|+\rangle$ $R^\dagger_Z(\phi_{6,1})$ $Z^{l_{6,1}}$ $R^\dagger_X(\phi_{6,2})$ $X^{l_{6,2}}$ $R^\dagger_Z(\phi_{6,3})$ $Z^{l_{6,3}}$ $X^{l_{6,4}}$ $Z^{l_{5,5}}$

Figure 4.10: "Effective" circuit obtained by canceling the cZ gates from the circuit in Figure 4.9. Qubits remain disentangled all along the circuit.

$R_Z(\pi)$, a Pauli-Z error on qubit (i, j) is equivalent to measuring qubit (i, j) by angle $\phi_{i,j} + \pi$. This generates Pauli-Z and Pauli-X errors in the logical circuit associated with the BwS (Figure 4.9).

We can now prove Lemma 2 (R-traps lemma).

Proof of Lemma 2 (R-traps lemma)

Proof. (Lemma 2 is stated on page 33) To prove the lemma we proceed as follows:

Step 1: We consider a BwS implementing an R-trap. We explain how Pauli-Z errors in the BwS afflict the associated logical circuit.

Step 2: We consider a qubit $i \in \{1, \dots, n\}$ and a tape $y \in \{1, \dots (d-1)/4\}$ in the logical circuit. We show that if qubit i is afflicted by errors only in tape y (and in no other tapes), the final measurement of qubit i returns 1 with probability at least 1/4.

$(l_1, l_2, l_3, l_4, l_5)$	$R_Z(\phi_1+\phi_3)$	$R_X(\phi_2)$	H
(1,0,0,0,0)	$R_Z(\phi_1+\phi_3)Z$	$R_X(\phi_2)Z$	HZ
(0,1,0,0,0)	$R_Z(-\phi_1+\phi_3)X$	$R_X(\phi_2)X$	HXZ
(0,0,1,0,0)	$R_Z(\phi_1+\phi_3)Z$	$R_X(-\phi_2)Z$	HX
(0,0,0,1,0)	$R_Z(-\phi_1-\phi_3)X$	$R_X(\phi_2)X$	HZ
(0,0,0,0,1)	$R_Z(\phi_1+\phi_3)Z$	$R_X(-\phi_2)Z$	HX
(1,1,0,0,0)	$R_Z(-\phi_1+\phi_3)XZ$	$R_X(\phi_2)XZ$	HX
(1,0,1,0,0)		$R_X(-\phi_2)$	HXZ
(1,0,0,1,0)	$R_Z(-\phi_1-\phi_3)XZ$	$R_X(\phi_2)XZ$	
(1,0,0,0,1)		$R_X(-\phi_2)$	HXZ
(0,1,1,0,0)	$R_Z(-\phi_1+\phi_3)XZ$	$R_X(-\phi_2)XZ$	HZ
(0,1,0,1,0)	$R_Z(\phi_1-\phi_3)$		HX
(0,1,0,0,1)	$R_Z(-\phi_1+\phi_3)XZ$	$R_X(-\phi_2)XZ$	HZ
(0,0,1,1,0)	$R_Z(-\phi_1-\phi_3)XZ$	$R_X(-\phi_2)XZ$	HXZ
(0,0,1,0,1)			
(0,0,0,1,1)	$R_Z(-\phi_1-\phi_3)XZ$	$R_X(-\phi_2)XZ$	HXZ
(1,1,1,0,0)	$R_Z(-\phi_1+\phi_3)X$	$R_X(-\phi_2)X$	
(1,1,0,1,0)	$R_Z(\phi_1-\phi_3)Z$	$R_X(\phi_2)Z$	HX
(1,1,0,0,1)	$R_Z(-\phi_1+\phi_3)X$	$R_X(-\phi_2)X$	
(1,0,1,1,0)	$R_Z(-\phi_1-\phi_3)X$	$R_X(-\phi_2)X$	HX
(1,0,1,0,1)	$R_Z(\phi_1+\phi_3)Z$	$R_X(\phi_2)Z$	HZ
(1,0,0,1,1)	$R_Z(-\phi_1-\phi_3)X$	$R_X(-\phi_2)X$	HX
(0,1,1,1,0)	$R_Z(\phi_1-\phi_3)Z$	$R_X(-\phi_2)Z$	
(0,1,1,0,1)	$R_Z(-\phi_1+\phi_3)X$	$R_X(\phi_2)X$	HXZ
(0,1,0,1,1)	$R_Z(\phi_1-\phi_3)Z$	$R_X(-\phi_2)Z$	
(0,0,1,1,1)	$R_Z(-\phi_1-\phi_3)X$	$R_X(\phi_2)X$	HZ
(1,1,1,1,0)	$R_Z(\phi_1-\phi_3)$	$R_X(-\phi_2)$	HZ
(1,1,1,0,1)	$R_Z(-\phi_1+\phi_3)XZ$	$R_X(\phi_2)XZ$	HX
(1,1,0,1,1)	$R_Z(\phi_1-\phi_3)$	$R_X(-\phi_2)$	HZ
(1,1,0,1,1)	$R_Z(-\phi_1-\phi_3)XZ$	$R_X(\phi_2)XZ$	
(0,1,1,1,1)	$R_Z(\phi_1-\phi_3)$		HX
(1,1,1,1,1)	$R_Z(\phi_1-\phi_3)Z$	$R_X(\phi_2)Z$	HXZ

Table 4.1. The effects of errors on the unitary $U_i^{(y)}$ implemented on qubit i in tape y. We leave blank spaces when the errors have no effect, i.e., when $\widetilde{U}_i^{(y)} = U_i^{(y)}$.

Step 3: We show that the same holds if qubit i is afflicted by errors in more than one tape.

We now elaborate on each of the above steps.

Step 1: Consider the logical circuit associated with a BwS afflicted by Pauli errors (Figure 4.9). In R-traps $\phi_{i,4y} = 0$ for all qubits i and tapes y (see Routine 1), therefore the only gates in between the cZ gates are the Pauli-X errors. Using the identities

$$\begin{aligned} cZ(X_1 \otimes I_2)cZ &= (X_1 \otimes Z_2) && (4.35)\\ cZ(I_1 \otimes X_2)cZ &= (Z_1 \otimes X_2) && (4.36)\\ cZ(X_1 \otimes X_2)cZ &= (Z_1X_1 \otimes Z_2X_2) && (4.37) \end{aligned}$$

(where we omit irrelevant phases), we can cancel the cZ gates and obtain an "effective" circuit where the qubits remain disentangled all along the computation (Figure 4.10) and the errors cannot propagate across qubits.

Step 2: Suppose that qubit i is afflicted by errors in tape y of the effective circuit (Figure 4.10). Let $U_i^{(y)} = R_Z(\phi_3)R_X(\phi_2)R_Z(\phi_1)$ be the unitary implemented on qubit i in tape y in the absence of errors, with $\phi_1, \phi_2, \phi_3 \in \{0, \pi/4, \ldots, 7\pi/4\}$. Let

$$\begin{aligned} \widetilde{U}_i^{(y)} =& X^{l_4}Z^{l_5 \oplus l_3}R_Z(\phi_3)X^{l_2}R_X(\phi_2)Z^{l_1}R_Z(\phi_1)\\ =& R_Z\big((-1)^{l_4}\phi_3\big)R_X\big((-1)^{l_3\oplus l_5}\phi_2\big)R_Z\big((-1)^{l_4\oplus l_2}\phi_1\big)X^{l_4\oplus l_2}Z^{l_5\oplus l_3\oplus l_1} \quad (4.38) \end{aligned}$$

be an implementation of $U_i^{(y)}$ with Pauli errors, with $l_1, \ldots, l_5 \in \{0, 1\}$ (cfr. Figure 4.10). We now consider the events F *qubit i is afflicted by errors in tape y* and E *measurement of qubit i outputs 1* and show that $\text{prob}(E|F) \geq 1/4$.

Since $\text{prob}(F) = 1$ by assumption, we begin by rewriting $\text{prob}(E|F)$ as

$$\begin{aligned} \text{prob}(E|F) &= \text{prob}(E \wedge G|F) + \text{prob}(E \wedge G'|F)\\ &= \text{prob}(E \wedge G|F)\\ &= \text{prob}(E|F \wedge G)\text{prob}(F \wedge G)\\ &= \text{prob}(E|F \wedge G)\text{prob}(G|F)\ , \qquad (4.39) \end{aligned}$$

where G (G') is the event "$\widetilde{U}_i^{(y)} \neq U_i^{(y)}$" ("$\widetilde{U}_i^{(y)} = U_i^{(y)}$"). To calculate $\text{prob}(E|F \wedge G)$, in Table 4.1 we provide $\widetilde{U}_i^{(y)}$ for all possible values of $l_1, \ldots, l_5$ and for $U_i^{(y)}$ implementing a R_Z-rotation by angle $\phi_1 + \phi_3$, a R_X-rotation by angle ϕ_2 or a

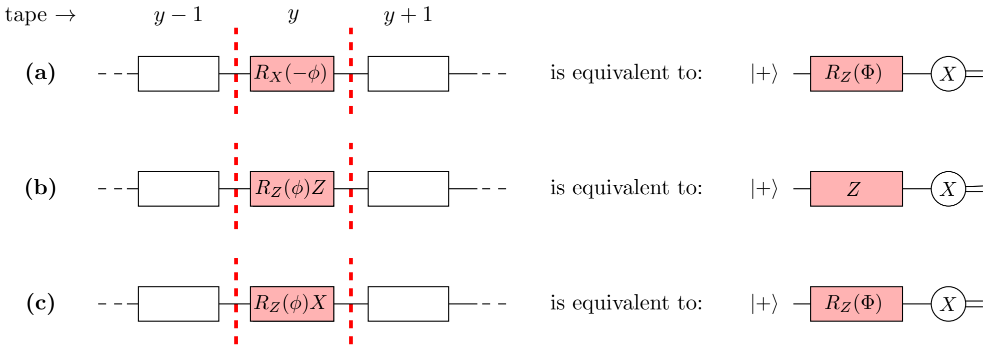


Figure 4.11: Examples of errors afflicting qubit i in tape y (red gate). **(a)** illustrates an error of the type C1, which produces an over-rotation by angle $\Phi = -2\phi \in \{0, \pi/2, \pi, 3\pi/2\}$ (circuit on the l.h.s.). **(b)** and **(c)** illustrate errors of the type C3.

Hadamard gate. As it can be seen in Table 4.1, errors have no effect on $U_i^{(y)}$, otherwise they modify it in one of the following ways:

C1. The errors flip the sign of a rotation angle. For instance, this is the case when $U_i^{(y)}$ implement a R_Z-rotation and $(l_1, l_2, l_3, l_4, l_5) = (0, 1, 0, 0, 0)$.
Since $-\phi = \phi - 2\phi$, these errors cause a R_Z-rotation of qubit i by a *random* angle $\Phi \in \{0, \pi/2, \pi, 3\pi/2\}$ (Figure 4.11**(a)**). From

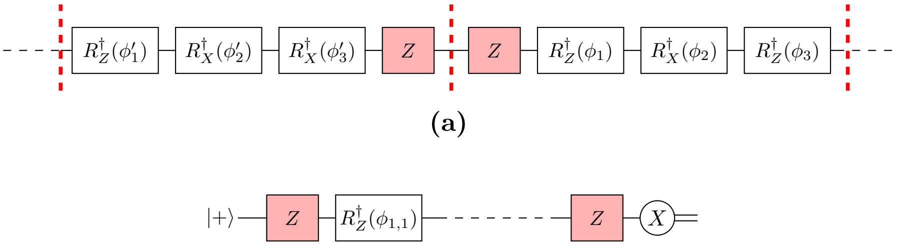
$$\sum_{\Phi \in \{0,\pi/2,\pi,3\pi/2\}} \frac{\left|\langle + | R_Z(\Phi) | + \rangle\right|^2}{4} = \frac{1}{2} \,, \tag{4.40}$$

it follows that measurement of qubit i returns 1 with probability 1/2.

C2. The errors flip the sign of a rotation angle and also produce a Pauli by-product. For instance, this is the case when $U_i^{(y)}$ implements a R_Z-rotation and $(l_1, l_2, l_3, l_4, l_5) = (1, 1, 0, 0, 0)$.
As in C1 above, the sign-flip causes a R_Z-rotation by a random angle, therefore measurement of qubit i returns 1 with probability 1/2 (by Equation 4.40).

C3. The errors produce a Pauli by-product. For instance, this is the case when $U_i^{(y)}$ implement a Hadamard gate and $(l_1, l_2, l_3, l_4, l_5) = (0, 0, 1, 0, 0)$.
These errors cause an R_Z-rotation of qubit i by angle π (Figure 4.11**(b)**) or by a random angle $\Phi \in \{0, \pi/2, \pi, 3\pi/2\}$ (Figure 4.11**(c)**). In the first case the final measurement returns 1 with probability 1, in the second it returns 1 with probability 1/2 (by Equation 4.40).

Therefore, $\text{prob}(E|F \wedge G) \geq 1/2$.



(b)

Figure 4.12: **(a)** Type-I errors (red gates) afflicting two neighboring bands and **(b)** Type-II errors (red gates).

To compute prob$(G|F)$ we notice (Table 4.1) that all errors[1] give $\widetilde{U}_i^{(y)} \neq U_i^{(y)}$ with probability larger than 1/2. This is because $U_i^{(y)}$ implements a Hadamard gate with probability 1/2 or a rotation (either R_Z or R_X) with probability 1/2 (cfr. Routine 1). This yields prob$(G|F) \geq 1/2$, therefore prob$(E|F) \geq 1/4$.

Step 3: Suppose that errors afflict qubit i in two neighboring tapes $y-1$ and y (we generalize to non-neighboring tapes later). From Table 4.1 we note that with few exceptions, the errors produce the same by-product for both rotations (R_Z and R_X) and a different one for the Hadamard gate[2]. For these errors the probability that the by-products produced in tape y cancel with those in tape $y-1$ is 1/2 or smaller, since tapes $y-1$ and y implement Hadamard with probability 1/2 or rotations with probability 1/2. Therefore, with the same arguments used in C3 (step 2 of the proof) it can be shown that these errors are detected with probability 1/4 or larger.

We now analyze the exceptions, i.e., the errors where the same by-products are produced for all three choices of $U_i^{(y)}$:

- $(l_1, l_2, l_3, l_4, l_5) = (1, 0, 0, 0, 0)$. This error yields $U_i^{(y)} Z$. If error $(l_1, l_2, l_3, l_4, l_5) = (0, 0, 1, 0, 0)$ occurs in tape $y-1$ the errors cancel and leave no trace, hence they are not detected. We name errors of this type as "Type-I" errors (Figure 4.12)

- $(l_1, l_2, l_3, l_4, l_5) = (0, 0, 1, 1, 0)$. This error flips the sign of rotation angles, therefore it is detected with probability 1/4 or larger (equation 4.40) regardless of the unitary implemented in tape $y-1$. The same happens for the following

[1] All errors except $(l_1, l_2, l_3, l_4, l_5) = (0, 0, 1, 0, 1)$. However $l_5 = 1$ implies a $(l_4 = 1)$-type error on qubit $i+1$ or $i-1$ (Figure 4.10), therefore also this error is detected.

[2] For instance, $(l_1, l_2, l_3, l_4, l_5) = (0, 1, 0, 0, 0)$ produces a Pauli-X by-product if $U_i^{(y)}$ is a R_Z-gate or R_X-gate and produces a Pauli-Y by-product if $U_i^{(y)} = H$.

cases: $(l_1, l_2, l_3, l_4, l_5) = (0, 0, 0, 1, 1), (1, 0, 0, 1, 1), (1, 0, 1, 1, 0)$.

- $(l_1, l_2, l_3, l_4, l_5) = (1, 0, 1, 0, 1)$. This error yields $U_i^{(y)} Z$. However, it also produces a $(l_4 = 1)$-type error on qubit $i-1$ or $i+1$ (cfr. Figure 4.10), therefore it is detected with probability 1/4 or larger.

Overall, we have shown that all the errors afflicting two neighboring tapes are detected with probability 1/4 or larger, with the only exception of Type-I errors (which are detected by C-traps, as we show in the proof of Lemma 3).

We must prove that errors are detected with probability 1/4 or larger even if they occur in two non-neighboring tapes y and y'. This can be shown with the same arguments used above: the unitaries implemented in tapes $y, \dots, y'$ are chosen at random, therefore error cancellation happens with probability 1/2 or smaller and errors are detected with probability larger than 1/4. The only exception is if error $(l_1, l_2, l_3, l_4, l_5) = (1, 0, 0, 0, 0)$ occurs in first tape $y = 1$ and $(l_1, l_2, l_3, l_4, l_5) = (0, 0, 1, 0, 0)$ occurs in the last tape $y = (d-1)/4$. This is because the global unitary implemented on qubit i, namely $U_i^{((d-1)/4)} \cdots U_i^{(2)} U_i^{(1)}$, is a R_Z-gate by angle $\widehat{\phi}$ and $Z R_Z(\widehat{\phi}) Z = R_Z(\widehat{\phi})$ for all $\widehat{\phi}$. Thus, this error is not detected by R-traps, and we name it Type-II error (Figure 4.12).

The arguments above can be easily generalized to errors occurring in more than two tapes. This concludes the proof. □

Proof of Lemma 3 (C-traps lemma)

Proof. (Lemma 3) is stated on page 33 To prove the lemma we proceed as follows.

Step 1: We explain how type-I errors affect C-traps. We show that type-I afflicting a single tape in a C-trap are detected with probability 1.
Step 2: We show that type-I affecting a more than one tape in a C-trap are detected with probability 1/2. The same applies to type-II errors.

We now elaborate on the steps above.

Step 1: In a C-trap all the tapes implement a cX-gate on two neighboring qubits i and $i+1$ with random target and control. Type-I errors cancel if they afflict the control qubit, otherwise if they afflict the control qubit they produce a Pauli-Z by-product on the target qubit and a Pauli-X by-product on the control

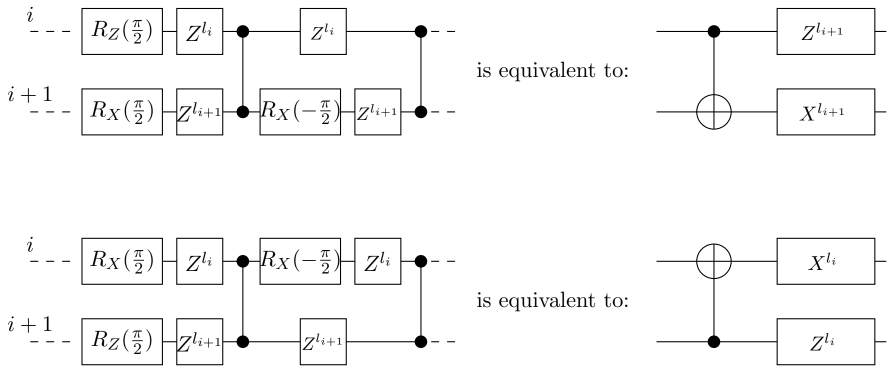


Figure 4.13: In a C-trap, Type-I errors produce Pauli-Z by-products.

qubit (Figure 4.13). Using the identities

$$cX(X_1 \otimes I_2)cX = (X_1 \otimes X_2) \tag{4.41}$$

$$cX(I_1 \otimes X_2)cX = (I_1 \otimes X_2) \tag{4.42}$$

$$cX(X_1 \otimes X_2)cX = (X_1 \otimes I_2) \tag{4.43}$$

Pauli-X by-products can be commuted all the way to the end of the circuit. Doing this, the by-products may spread to other qubits in the circuit, however since $X\left|\pm\right\rangle = \pm\left|\pm\right\rangle$ they do not affect the measurement outputs. Since

$$cX(Z_1 \otimes I_2)cX = (Z_1 \otimes I_2) \tag{4.44}$$

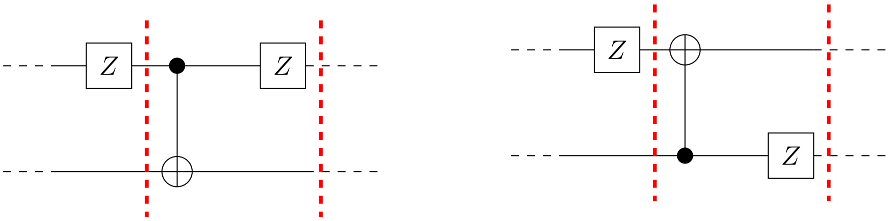
$$cX(I_1 \otimes Z_2)cX = (Z_1 \otimes Z_2) \tag{4.45}$$

$$cX(Z_1 \otimes Z_2)cX = (Z_1 \otimes Z_2) \tag{4.46}$$

also Pauli-Z by-products can be commuted all the way to the end of the circuit and spread to other qubits. Since $Z\left|\pm\right\rangle = \left|\mp\right\rangle$, Pauli-$Z$ by-products cause flips in the measurement outputs.

Step 2: Since in all the tapes of C-traps target and control qubits are chosen at random, Type-I errors which afflict a single tape in a C-trap produce Pauli-Z by-products with probability 1/2 (Figure 4.13). These errors always flip the measurement outputs, hence they are always detected. Overall, it follows that Type-I errors afflicting a single tape are detected with probability 1/2.

If Type-I errors occur in more than one tape, the by-products may happen to cancel. However, error cancellation happens with probability 1/2 or smaller. To see this, consider first Type-I errors occurring in two neighboring tapes $y-1$ and y.



(a) Pauli-Z by-products cancel.

(b) Pauli-Z by-products do not cancel.

Figure 4.14: Pauli-Z by-products in two neighboring bands $y-1$ and y cancel with probability $1/2$, depending on the random orientation of cX in band y.

In this case the Pauli-Z by-products have at most probability $1/2$ of canceling due to the random orientation of the cX gates in band y (Figure 4.14), and if they do not cancel then they are detected with probability 1. The same can be argued for errors occurring in two non-neighboring tapes y, y' due to the random orientation of the cX gates in bands $y+1, \ldots, y'$, as well as for errors occurring in more than two tapes and for Type-II errors (which also are Pauli-Z by-products).

□

Chapter 5

From verification to accreditation

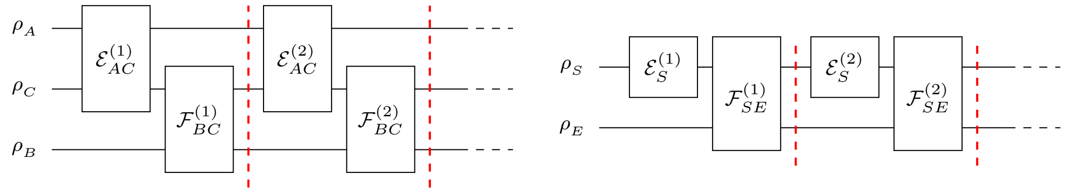
In the previous Chapter we presented an optimization of the existing verification protocols. This optimization reduces the experimental requirements on the verifier side, since Alice only needs to prepare qubits in eight different types of states (as opposed to ten in the previous protocols [49, 51, 52]) or measure in four different bases (as opposed to five [55]). Is it enough to make verification feasible on NISQ devices?

The answer is negative for a number of reasons. First, the operations on Bob's side remain too demanding for NISQ devices. This is due to the large overhead in qubits and gates required to map a quantum circuit into a BwS (Section 4.6). Second, in our protocols Alice must possess a noiseless device and exchange qubits with Bob (Figure 5.1a). However, in real-world experiments there are no noiseless devices (Figure 5.1b), moreover cross-platform exchange of qubits may increase the levels of noise.

We could now attempt optimization of other verification protocols, however in all the verification protocols the operations on Bob's side remain impractical for NISQ devices. Indeed, in these protocols Bob must either carry out the computation on a BwS [49, 51, 52, 55], append several teleportation gadgets to the target circuit (one for each T-gate in the circuit and six for each Hadamard gate) [54], or else

[1] This Chapter presents the results of Ferracin, Kapourniotis, Datta, *Accrediting outputs of noisy intermediate-scale quantum computing devices*, New J. Phys. 21 113038 (2019).

[2] The accreditation protocol presented in this Chapter is available is available on IBM's Qiskit-ignis Github repository at the URL https://github.com/Qiskit/qiskit-ignis/tree/master/qiskit/ignis/verification/accreditation.



(a) **(b)**

Figure 5.1: **(a)** In verification protocols Alice and Bob apply operations on their own registers A and B and on a shared register C. **(b)** In experiments all operations applied to the system S are noisy. Noise couples the system to an environment E.

prepare Feynman-Kitaev clock states[1] (which require appending an auxiliary qubit per gate in the target circuit) [56, 64, 65]. Alternatively, he must be able to share many copies of two-qubit maximally entangled states such as Bell states with another prover located at far distance (so far that they cannot possibly communicate during the execution of the protocol) [60, 61]. Moreover, most of the other protocols also require noiseless devices for Alice and exchange of qubits between Alice and Bob [49, 52, 54–56, 65, 84].

All in all, verification protocols will not be usable in the near term, no matter how much we try to optimize them. To devise protocols for NISQ devices we must think in a different way and develop a different type of approach.

5.1 Summary of the results

In this Chapter we define the notion of "accreditation protocol", namely a protocol that can upper-bound with confidence the variation distance between noisy and noiseless probability distributions of the outputs of a "target" quantum circuit (Definition 5). We then present an accreditation protocol that encompasses all the main limitations of NISQ devices.

Inspired by verification protocols [49–62, 64, 65, 67, 84, 85], our accreditation protocol is trap-based, meaning that the target circuit is implemented together with trap circuits (classically simulable circuits used to detect the noise). As we show in Theorems 6 and 7, the trap circuits are able to detect all types of noise subject to the following conditions:

N1: Noise in state preparation, entangling gates, and measurements is an arbitrary

[1] Let $\mathcal{C}$ be a circuit containing T gates in total. Let $|\psi(t)\rangle$ be the state of the system after the first $t \in \{0, \ldots, T\}$ gates have been applied. The *Feynman-Kitaev clock state* of the circuit $\mathcal{C}$ is defined as $|\Phi\rangle = 1/\sqrt{T+1}\sum_{t=0}^{T} |1\rangle^{\otimes t} |0\rangle^{\otimes T-t} |\psi(t)\rangle$ [65].

Completely Positive Trace Preserving (CPTP) map encompassing the whole system and the environment (Equation 5.2);

N2: Noise in single-qubit gates is a CPTP map $\mathcal{F}_{SE}$ of the form $\mathcal{F}_{SE} = (1-r)\mathcal{I} + r\mathcal{F}'_{SE}$ with $0 \leq r < 1$, where $\mathcal{I}_{SE}$ is the identity on system and environment and $\mathcal{F}'_{SE}$ is an arbitrary (potentially gate-dependent) CPTP map encompassing the whole system and the environment.

A single run of our protocol requires implementing the target circuit and $v \geq 1$ trap circuits. It provides a binary outcome in which the outputs of the target circuit are either accepted as *correct* (with confidence increasing linearly with v) or rejected as *potentially incorrect.* More usefully, consider running our protocol d times, each time with the same target and v unique trap circuits. Suppose that the output of the target is accepted as correct by $N_{\text{acc}} > 0$ runs. With confidence $1-2\text{exp}(-2d\theta^2)$, for each of these accepted outputs our protocol ensures that

$$\frac{1}{2}\sum_{\overline{s}} \left|p_{\text{noiseless}}(\overline{s}) - p_{\text{noisy}}(\overline{s})\right| \leq \frac{\varepsilon}{N_{\text{acc}}/d - \theta} \ , \tag{5.1}$$

where $p_{\text{noiseless}}(\overline{s})$ and $p_{\text{noisy}}(\overline{s})$ are the noiseless and noisy probability distributions of the outputs $\{\overline{s}\}$ of the target circuit (with overbar indicating that $\overline{s}$ is a bit-string), $\varepsilon \propto 1/v$ and $\theta \in (0, N_{\text{acc}}/d)$ is a tunable parameter that affects both the confidence and the upper-bound.

Crucially, all the circuits implemented in our protocol are no wider (in the number of qubits) nor deeper (in the number of gates) than the target circuit. Thus, our accreditation protocol has no quantum overhead, unlike verification protocols [49–62, 64, 65, 67, 84, 85]. Moreover, the accreditation protocol requires no noiseless device nor cross-platform exchange of qubits. This makes it ready for use on current NISQ devices and scalable for the long term applications.

In addition to its ready implementability on NISQ devices, our accreditation protocol can detect all types of noise typically considered by protocols centered around randomized benchmarking (Section 3.3). Moreover, it can detect noise that may be missed by those protocols, such as time-dependent noise. By testing circuits rather than gates, our protocol ensures that all possible noise (subject to conditions N1 and N2) in state preparation, measurement and gates is detected, even noise that arises only when these components are put together to form a circuit. On the contrary, benchmarking isolated gates can sometimes yield over-estimates of their fidelities [43], and consequently of the fidelity of the resulting circuit.

This Chapter is structured as follows: in Section 5.2 we provide the necessary definitions, in Section 5.3 we present our accreditation protocol, in Section 5.4 we show the results of numerical studies. All the proofs are contained in Section 5.5.

5.2 Definitions

We start by defining the notion of protocol used in this Chapter:

Definition 4. [Protocol]. *Consider a system S in the state ρ_S. A protocol on input ρ_S is a collection of CPTP maps $\{\mathcal{E}_S^{(p)}\}_{p=1}^q$ acting on S and yielding the state $\rho_{\text{out}} = \circ_{p=1}^q \mathcal{E}_S^{(p)}(\rho_S)$.*

When implemented on real devices protocols suffer the effects of noise. Modeling noise as a set $\{\mathcal{F}_{SE}^{(p)}\}$ of CPTP maps acting on system and environment (Figure 5.1b), the state of the system at the end of a noisy protocol run is

$$\rho_{\text{out}} = \text{Tr}_E \big[\circ_{p=1}^q \mathcal{F}_{SE}^{(p)} (\mathcal{E}_S^{(p)} \otimes \mathcal{I}_E)(\rho_S \otimes \rho_E) \big] \ , \tag{5.2}$$

where ρ_E is the state of the environment at the beginning of the protocol. We allow each map $\mathcal{F}_{SE}^{(p)}$ to depend arbitrarily on the corresponding operation $\mathcal{E}_S^{(p)}$.

We now define accreditation protocols as follows:

Definition 5. [Accreditation Protocol]. *Consider a protocol $\{\mathcal{E}_S^{(p)}\}_{p=1}^q$ with input ρ_S, where ρ_S contains a classical description of the target circuit and the number v of trap circuits. Consider also a set of CPTP maps $\{\mathcal{F}_{SE}^{(p)}\}_{p=1}^q$ (the noise) acting on system and environment. We say that the protocol $\{\mathcal{E}_S^{(p)}\}_{p=1}^q$ can accredit the outputs of the target circuit in the presence of noise $\{\mathcal{F}_{SE}^{(p)}\}_{p=1}^q$ if the following two properties hold:*

1) The state of the system at the end of a single protocol run (Equation 5.2) can be expressed as

$$\rho_{\text{out}} = b\ \tau'^{\text{tar}}_{\text{out}} \otimes |\text{acc}\rangle\langle\text{acc}| + (1-b)\Big(l\ \sigma^{\text{tar}}_{\text{out}} \otimes |\text{acc}\rangle\langle\text{acc}| + (1-l)\tau^{\text{tar}}_{\text{out}} \otimes |\text{rej}\rangle\langle\text{rej}|\Big) \tag{5.3}$$

where $\sigma^{\text{tar}}_{\text{out}}$ ($\tau'^{\text{tar}}_{\text{out}}$) is the state of the target circuit at the end of a noiseless (noisy) protocol run, $\tau^{\text{tar}}_{\text{out}}$ is an arbitrary state for the target circuit, $|\text{acc}\rangle$ is a "flag" state indicating acceptance, $|\text{rej}\rangle = |\text{acc} \oplus 1\rangle$, $0 \le l \le 1$, $0 \le b \le \varepsilon$ and $\varepsilon \in [0,1]$.

2) After d protocol runs with the same target circuit and v unique trap circuits, if all these runs are affected by independent and identically distributed (i.i.d.) noise, *then the variation distance between noisy and noiseless probability distribution of the outputs of each of the* $N_{\text{acc}} \in \{0, 1, \ldots, d\}$ *protocol runs ending with flag state* $|\text{acc}\rangle$ *is upper-bounded as in Equation 5.1.*

Property 1 ensures that the probability of accepting the outputs of a single protocol run when the target circuit is affected by noise (the number b in Equation 5.3) is smaller than a constant ε. This constant is a function of the number of trap circuits, of the protocol and of the noise model. The quantity $1-\varepsilon$ quantifies the *credibility* of the accreditation protocol.

Note that Property 1 in Definition 5 implies Property 2. To see this, assume Property 1 is valid for a given protocol. Suppose that this protocol is run d times with i.i.d. noise (a standard assumption in trap-based verification protocols [51, 57]) and suppose that $N_{\text{acc}} > 0$ protocol runs end with flag state $|\text{acc}\rangle$. For each of these N_{acc} runs, the state of the system at the end of the protocol run is of the form (cfr. Equation 5.3)

$$\rho_{\text{out, acc}} = \frac{(1-b)l\ \sigma_{\text{out}}^{\text{tar}} + b\ \tau_{\text{out}}^{\prime\ \text{tar}}}{(1-b)l + b} \otimes |\text{acc}\rangle\langle\text{acc}| \tag{5.4}$$

This yields a bound on the variation distance of the type [69]

$$\begin{aligned}\frac{1}{2}\sum_{\bar{s}} \left|p_{\text{noiseless}}(\bar{s}) - p_{\text{noisy}}(\bar{s})\right| \leq\ & D\left(\sigma_{\text{out}}^{\text{tar}}\ ,\ \frac{(1-b)l\ \sigma_{\text{out}}^{\text{tar}} + b\ \tau_{\text{out}}^{\prime\ \text{tar}}}{(1-b)l + b}\right) \\ \leq\ & \frac{b}{(1-b)l + b} \\ \leq\ & \frac{\varepsilon}{\text{prob(acc)}}\ , \end{aligned} \tag{5.5}$$

where in the last inequality we used that $b \leq \varepsilon$ (Property 1) and that the quantity $\text{prob(acc)} = (1-b)l + b$ is the probability of accepting (Equation 5.3). Hoeffding's Inequality [86] ensures that $|\text{prob(acc)} - N_{\text{acc}}/d| \leq \theta$ with confidence $1 - 2\exp(-2d\theta^2)$ and this yields Property 2.

5.3 The accreditation protocol

In this Section we describe the accreditation protocol and state the main claims of the Chapter.

5.3.1 Description of the protocol

Our accreditation protocol (Box 5.1) takes as input a classical description of the target circuit and the number v of trap circuits. The target circuit (Figure 1.1) must start with qubits in the state $|+\rangle$, contain only single-qubit gates and cZ gates and end with a round of measurements in the Pauli-X basis[2]. Moreover, it must be decomposed as a sequence of bands, each one containing one round of single-qubit gates and one round of cZ gates. We will indicate the number of qubits with n and the number of bands with m.

In our accreditation protocol $v+1$ circuits are implemented, one (chosen at random) being the target and the remaining v being the traps. The trap circuits are obtained by replacing the single-qubit gates in the target circuit with other single-qubit gates, but input state, measurements and cZ gates are the same as in the target (Figure 5.2a; all single-qubit gates acting on the same qubit in the same band must be recompiled into one gate). These single-qubit gates are chosen as follows (Routine 4 in Box 5.3): For each band $j \in \{1, \ldots, m-1\}$ and for each qubit $i \in \{1, \ldots, n\}$:

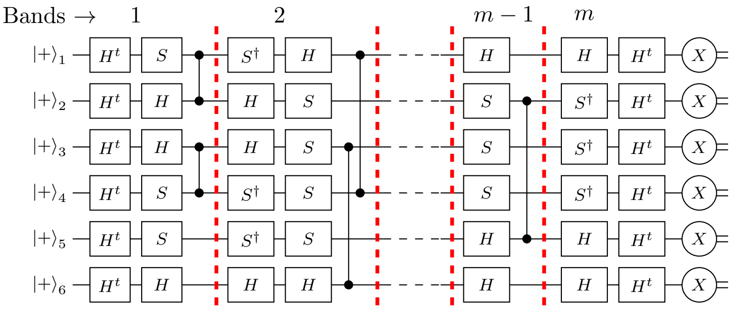
• If qubit i is connected to another qubit i' by a cZ gate, a gate is chosen at random from the set $\{H_i \otimes S_{i'}, S_i \otimes H_{i'}\}$ and is implemented on qubits i and i' in band j. This gate is then undone in band $j+1$.

• Otherwise, if qubit i is not connected to any other qubit by a cZ gate, a gate is chosen at random from the set $\{H_i, S_i\}$ and is implemented on qubit i in band j. This gate is then undone in band $j+1$.

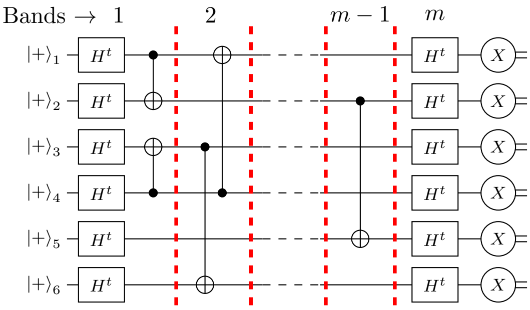
Moreover, depending on the random bit $t \in \{0,1\}$, the traps may begin and end with a round of Hadamard gates. Since $(S \otimes H)cZ(S^\dagger \otimes H) = cX$, the trap circuits are a sequence of (randomly oriented) cX gates acting on $|+\rangle^{\otimes n}$ (if $t=0$) or $|0\rangle^{\otimes n}$ (if $t=1$)—Figure 5.2b. Since $cX\,|00\rangle = |00\rangle$ and $cX\,|{+}{+}\rangle = |{+}{+}\rangle$, in the absence of noise the traps always output $\overline{s} = \overline{0}$.

Our protocol requires appending a QOTP (Section 2.3) to all the single-qubit gates in all circuits (target and traps). This is done by running Routine 3 (Box 5.2), which is as follows:

[2] This does not result in any loss of generality: every experimental architecture has its native input states, entangling gates and measurement basis, but these can always be mapped to $|+\rangle$ states, cZ gates and Pauli-X measurements.



(a)



(b)

Figure 5.2: **(a)** Example of trap circuit for the target circuit in Figure 1.1 and **(b)** overall computation implemented through this trap circuit. All the single-qubit gates acting on the same qubit in the same band must be recompiled into one gate (for example, in Figure 5.2a, the H^t-gate and subsequent S-gate acting on qubit 1 in band 1 must be implemented as one gate SH^t).

• For all the bands $j \in \{1, \ldots, m\}$ and qubits $i \in \{1, \ldots, n\}$, a random Pauli gate is appended *after* each gate $U_{i,j}$ (Figure 5.3a). This gives

$$U'_{i,j} = X_i^{\alpha'_{i,j}} Z_i^{\alpha_{i,j}} U_{i,j} \ , \tag{5.6}$$

with $\alpha_{i,j}, \alpha'_{i,j} \in \{0, 1\}$ random bits.

• A random Pauli-X gate is appended *before* each gate in the first band. This gives

$$U''_{i,1} = X_i^{\alpha'_{i,1}} Z_i^{\alpha_{i,1}} U_{i,1} X_i^{\gamma_i} \ , \tag{5.7}$$

where $\gamma_i \in \{0, 1\}$ are random bits.

• For all the bands $j \in \{2, \ldots, m\}$ and qubits $i \in \{1, \ldots, n\}$, another Pauli gate is appended *before* each single-qubit gate. This Pauli gate is chosen so that it undoes the QOTP coming from the previous band. Thus, if in band j qubit i is connected

Box 5.1. Accreditation protocol.

Input:

- A target circuit that takes as input n qubits in the state $|+\rangle$, contains only single-qubit gates and cZ gates arranged in m bands and ends with Pauli-X measurements (Figure 1.1).
- The number v of trap circuits.

Routine:

1. Choose a random number $v_0 \in \{1, \ldots, v+1\}$ and define $\{U_{i,j}^{(v_0)}\} = \{U_{i,j}\}$, where $\{U_{i,j}\}$ is the set of single-qubit gates in the target circuit.

2. For $k = 1, \ldots, v+1$: If $k \neq v_0$ (trap circuit), run Routine 4 and obtain the set of single-qubit gates $\{U_{i,j}^{(k)}\}$ for the k-th trap circuit.

3. For $k = 1, \ldots, v+1$: Run Routine 3 and obtain $\{U_{i,j}^{\prime\prime(k)}\}$, together with the bit-string $(\alpha_{1,m}^{(k)}, \ldots \alpha_{n,m}^{(k)})$.

4. For $k = 1, \ldots, v+1$:
   4.1 Create a state $\rho_{\text{in}} = |+\rangle^{\otimes n}$.
   4.2 Implement circuit k with single-qubit gates from the set $\{U_{i,j}^{\prime\prime(k)}\}$ and obtain output $\overline{s}^{(k)} = (s_1^{(k)}, \ldots, s_n^{(k)})$. Next, for all $i = 1, \ldots, n$, recompute $s_i^{(k)}$ as $s_i^{(k)} \oplus \alpha_{i,m}^{(k)}$.

5. Initialize a flag bit to $|\text{acc}\rangle = |0\rangle$. Then, for $k = 1, \ldots, v+1$: if $\overline{s}^{(k)} \neq \overline{0}$ and $k \neq v_0$ (trap circuit), set the flag bit to $|\text{rej}\rangle = |\text{acc} \oplus 1\rangle$.

Output: The output $\overline{s}^{(v_0)}$ of the target circuit and the flag bit.

Box 5.2. Routine 3 (Quantum One-Time Pad)

Input:

- A set $\{U_{i,j}\}$ of single-qubit gates, for $j = 1, \ldots, m$ and $i = 1, \ldots, n$.

Routine:

1. For $j = 1, \ldots, m$ and $i = 1, \ldots, n$:
   Choose two random bits $\alpha_{i,j}$ and $\alpha'_{i,j}$. Next, define $U'_{i,j} = X^{\alpha'_{i,j}} Z^{\alpha_{i,j}} U_{i,j}$.

2. For $i = 1, \ldots, n$:
   Choose a random bit γ_i and define $U''_{i,1} = U'_{i,1} X^{\gamma_i}$.

3. For $j = 2, \ldots, m-1$:
   If in band j qubit i is connected to qubit i', define

$$U''_{i,j} = X_i^{\alpha'_{i,j}} Z_i^{\alpha_{i,j}} U_{i,j} X_i^{\alpha'_{i,j-1}} Z_i^{\alpha_{i,j-1} \oplus \alpha_{i',j-1}} \; ; \tag{5.8}$$

   otherwise, if in band j qubit i is not connected to any other qubit define

$$U''_{i,j} = X_i^{\alpha'_{i,j}} Z_i^{\alpha_{i,j}} U_{i,j} X_i^{\alpha'_{i,j-1}} Z_i^{\alpha_{i,j-1}} \; . \tag{5.9}$$

Output: The set $\{U''_{i,j}\}$ and the n-bit string $(\alpha_{1,m}, \ldots, \alpha_{n,m})$.

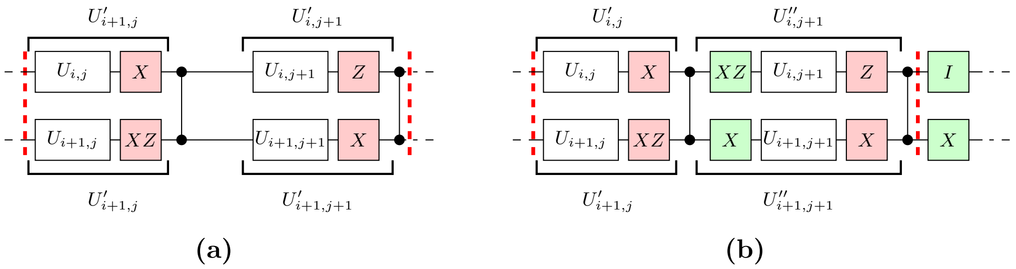


Figure 5.3: Example of QOTP. **(a)** The red Pauli gates apply the QOTP. **(b)** The green gates undo the QOTP coming from previous bands.

Box 5.3. Routine 4 (Single-qubit gates for trap circuits).

Input:

- A description of the target circuit.

Routine:

1. Initialize the set $\{U_{i,j} = I_i\}$, for $i = 1, \ldots, n$ and $j = 1, \ldots, m$.
2. For all $j = 1, \ldots, m - 1$:
   - 2.1 For all $i = 1, \ldots, n$: If in band j of the target circuit qubits i and i' are connected by a cZ gate, set
     - $U_{i,j} = S_i U_{i,j}$ and $U_{i',j} = H_{i'} U_{i',j}$ with probability 1/2.
     - $U_{i,j} = H_i U_{i,j}$ and $U_{i',j} = S_{i'} U_{i',j}$ with probability 1/2.

     Otherwise, set $U_{i,j} = S_i U_{i,j}$ or $U_{i,j} = H_i U_{i,j}$ with probability 1/2.
   - 2.2 For all $i = 1, \ldots, n$: Set $U_{i,j+1} = U^\dagger_{i,j}$.
3. For all $i = 1, \ldots, n$:
   Choose a random bit $t \in \{0, 1\}$. Next, set $U_{i,1} = U_{i,1} H^t$ and $U_{i,m} = H^t U_{i,m}$.

Output: The set $\{U_{i,j}\}$.

to qubit i', we define (Figure 5.3b)

$$U''_{i,j} = X_i^{\alpha'_{i,j}} Z_i^{\alpha_{i,j}} U_{i,j} X_i^{\alpha'_{i,j-1}} Z_i^{\alpha_{i,j-1} \oplus \alpha_{i',j-1}} \ , \tag{5.10}$$

where we use that $(X_1 \otimes I_2) cZ = cZ(X_1 \otimes Z_2)$ and $(Z_1 \otimes I_2) cZ = cZ(Z_1 \otimes I_2)$; otherwise, if in band j qubit i is not connected to any other qubit we define

$$U''_{i,j} = X_i^{\alpha'_{i,j}} Z_i^{\alpha_{i,j}} U_{i,j} X_i^{\alpha'_{i,j-1}} Z_i^{\alpha_{i,j-1}} \ . \tag{5.11}$$

Overall, replacing each gate $U_{i,j}$ with $U''_{i,j}$ yields a new circuit that is equivalent to the the original one, apart from the un-recovered QOTP $\otimes_{i=1}^n X^{\alpha'_{i,m}} Z^{\alpha_{i,m}}$ in the last band. Since all measurements are in the Pauli-X basis, the Pauli-X component of this un-recovered QOTP is irrelevant, while its Pauli-Z component bit-flips some of the outputs. These bit-flips are undone by replacing each output s_i with $s_i \oplus \alpha_{i,m}$

in Step 4.2 of the protocol (a procedure that we call "classical post-processing of the outputs"). This allows recovery of the correct outputs.

After all the circuits have been implemented and the outputs have been post-processed, a flag bit is initialized to $|\text{acc}\rangle = |0\rangle$, then it is checked whether all the traps gave the correct output $\overline{s} = \overline{0}$. If they do, the protocol returns the output of the target together with the bit $|\text{acc}\rangle$, otherwise it returns the output of the target together with the bit $|\text{rej}\rangle = |1\rangle$. The output of the target is only accepted in the first case, while it is discarded in the second case.

In the absence of noise, our protocol always returns the correct output of the target circuit and always accepts it. Correctness of the target is ensured by the fact that the QOTP has no effect on the computation, as all the extra Pauli gates cancel out with each other or are countered by the classical post-processing of the outputs. Acceptance is ensured by the fact that in the absence of noise all the trap circuits always yield the correct outcome $\overline{s} = \overline{0}$.

We conclude this Section by calculating the overhead of the accreditation protocol. The accreditation protocol has no quantum overhead, as all circuits have the same size as the one being accredited. The classical overhead consists in $O(nm)$ bits for each of the $v+1$ computations. Specifically, the target computation has an overhead of $2nm+n$ bits (the $2nm$ random bits $\alpha_{i,j}, \alpha'_{i,j}$ and the n random bits γ_i in Routine 3), while the traps have an overhead of at most $2nm+n+nm$ bits (the $2nm+n$ random bits in Routine 3 and at most nm random bits in Routine 4).

5.3.2 The credibility of the protocol

In this Section we calculate the credibility $1-\varepsilon$ of our accreditation protocol. As per Equation 5.2, we model noise as a set of CPTP maps acting on the whole system and on the environment (Figure 5.4). For simplicity we begin with the assumption that all the rounds of single-qubit gates in our protocol are noiseless, i.e. that for all circuits $k = 1, \ldots, v+1$ and bands $j = 1, \ldots, m$, a noisy implementation of the round of single-qubit gates is (cfr. Figure 5.4 for notation)

$$\widetilde{\mathcal{U}}_j^{\prime\prime(k)} = \mathcal{E}_j^{(k)}\big(\mathcal{U}_j^{\prime\prime(k)} \otimes \mathcal{I}_E\big) \quad \text{with} \quad \mathcal{E}_j^{(k)} = \mathcal{I}_{SE}\ , \tag{5.12}$$

where $\mathcal{I}_{SE}$ is the identity on system and environment. We prove the following Theorem:

Theorem 6. **[Credibility with noiseless single-qubit gates].** *Suppose that all single-qubit gates in our accreditation protocol are noiseless (Equation 5.12). For*

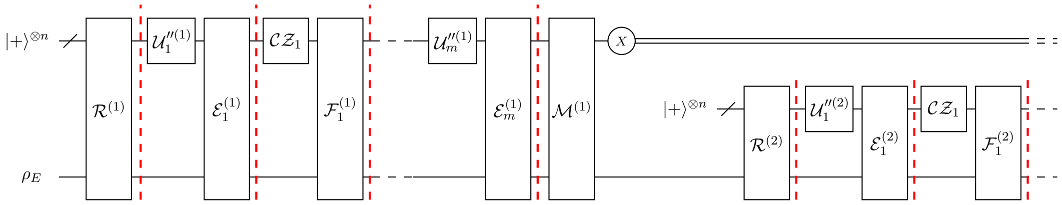


Figure 5.4: Schematic illustration of a noisy implementation of our protocol where all boxes represent CPTP maps. $\mathcal{U}_j''^{(k)}$ implements the round of single-qubit gates in band j of circuit k, $\mathcal{CZ}_j$ implements the round of cZ gates in band j. In each circuit $k = 1, \dots, v+1$: $\mathcal{R}^{(k)}$ is the noise in state preparation, $\mathcal{M}^{(k)}$ is the noise in measurements, $\mathcal{E}_j^{(k)}$ is the noise in the round of single-qubit gates in band j and $\mathcal{F}_j^{(k)}$ is the noise in the round of cZ gates in band j.

any number $v \geq 1$ of trap circuits, our accreditation protocol can accredit the outputs of a noisy quantum computer affected by noise of the form N1 with

$$\varepsilon = \frac{\kappa}{v+1} \,, \tag{5.13}$$

where $\kappa = 3(3/4)^2 \approx 1.7$.

Proof. (Sketch. See Section 5.5 for more details.) Using the Pauli Twirl (Theorem 1) we show that on average (i.e., summing over all random bits $\alpha_{i,j}^{(k)}$, $\alpha_{i,j}'^{(k)}$ and $\gamma_i^{(k)}$) noise reduces to stochastic Pauli-X, Y and Z errors happening before the noisy operations. More formally:

Lemma 4. [Twirling the noise]. *(Proof in Section 5.5.1.) Suppose that all single-qubit gates in all the circuits implemented in our protocol are noiseless, and that state preparation, measurements and two-qubit gates suffer noise of the type type N1. Summed over the random numbers $\alpha_{i,j}^{(k)}$, $\alpha_{i,j}'^{(k)}$ and $\gamma_{i,j}^{(k)}$, the joint state of the target and the traps at the end of the protocol is*

$$\begin{aligned}
&\rho_{\text{out}}\big(\mathcal{U}_1^{(1)}, \dots, \mathcal{U}_m^{(v+1)}\big) \\
&= \sum_{\overline{s}^{(1)},\dots,\overline{s}^{(v+1)}} \; \sum_{\mathcal{P}_0^{(1)},\dots,\mathcal{P}_m^{(v+1)}} \frac{\text{prob}\big(\mathcal{P}_0^{(1)}, \dots, \mathcal{P}_m^{(v+1)}\big)}{2^{n(v+1)}} \times \\
&\bigotimes_{k=1}^{v+1} \langle +|^{\otimes n} \Big[\mathcal{Z}^{\overline{s}^{(k)}} \mathcal{P}_m^{(k)} \mathcal{U}_m^{(k)} \circ_{j=1}^{m-1} \Big(\mathcal{CZ}_j \mathcal{P}_j^{(k)} \mathcal{U}_j^{(k)} \Big) \circ \mathcal{P}_0^{(k)} \big(\rho_{\text{in}}\big) \Big] |+\rangle^{\otimes n} \times \\
&\Big(\otimes_i \, Z_i^{s_i^{(k)}} |+\rangle_i \langle +| Z_i^{s_i^{(k)}} \Big)
\end{aligned} \tag{5.14}$$

where $\rho_{\text{in}} = \otimes_i |+\rangle_i \langle +|$, $\overline{s}^{(k)} = (s_1^{(k)}, \dots, s_n^{(k)})$ is a binary string representing the *output of the k-th circuit,* $\mathcal{Z}^{\overline{s}^{(k)}}(\rho) = \otimes_i Z_i^{s_i^{(k)}} \rho Z_i^{s_i^{(k)}}$ *and* $\mathrm{prob}\big(\mathcal{P}_0^{(1)}, \ldots, \mathcal{P}_m^{(v+1)}\big)$ *is the joint probability of a collection of Pauli errors* $\mathcal{P}_0^{(1)}, \ldots, \mathcal{P}_m^{(v+1)}$ *affecting the system, with* $\mathcal{P}_1^{(k)}, \ldots, \mathcal{P}_{m-1}^{(k)} \in \{\mathcal{I}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}\}^{\otimes n}$ *and* $\mathcal{P}_0^{(k)}, \mathcal{P}_m^{(k)} \in \{I, \mathcal{Z}\}^{\otimes n}$ *for all k.*

This Lemma is the counterpart of Lemma 1 (Twirl for Bob's deviations, page 32), with the difference that the Pauli Twirl is now operated using the single-qubit gates rather than state preparation. Twirling noise using single-qubit gates was first done in Ref. [68] for Markovian noise, and here we show that this result holds also if the noise creates correlations in time.

Having reduced arbitrary non-local noise to Pauli errors via the QOTP, we then show that our trap circuits detect *all* Pauli errors with probability larger than zero. We prove the following Lemma:

Lemma 5. [Traps lemma]. *(Proof in Section 5.5.2.) For any collection of Pauli errors* $\mathcal{P}_0, \ldots, \mathcal{P}_m$ *affecting a trap circuit, summing over all possible single-qubit gates in the trap circuit (i.e. over all possible sets* $\{U_{i,j}\}$ *output by Routine 4), the probability that the trap circuit outputs* $\overline{s} = \overline{0}$ *is at most 3/4.*

We can now finally calculate ε. To do so, suppose that noise afflicts $\widetilde{v} \in \{1, \ldots, v+1\}$ circuits. In this case, the probability $p(E_1 \wedge E_2|\widetilde{v})$ of the events E_1 *the noise afflicts the target circuit* and E_2 *the noise is not detected* when noise afflicts $\widetilde{v}$ circuits equals

$$p(E_1 \wedge E_2|\widetilde{v}) = p(E_1|\widetilde{v})\; p(E_2|E_1 \wedge \widetilde{v}) \tag{5.15}$$

Since the noise does not depend on the choice of single-qubit gates (cfr. Lemma 4), the noise has probability $p(E_1|\widetilde{v}) = \widetilde{v}/(v+1)$ of afflicting the target circuit. Moreover, due to Lemma 5 we have

$$p(E_2|E_1 \wedge \widetilde{v}) \leq \left(\frac{3}{4}\right)^{\widetilde{v}-1} \tag{5.16}$$

Finally, maximizing $p(E_1 \wedge E_2|\widetilde{v})$ over $\widetilde{v}$ yields

$$\varepsilon = \max_{\widetilde{v}}\; p(E_1 \wedge E_2|\widetilde{v}) \approx \frac{1.7}{v+1}, \text{ for } \widetilde{v} = 3\ . \tag{5.17}$$

This proves $p(E_1 \wedge E_2|\widetilde{v}) \leq \kappa/(v+1) = \varepsilon$ with $\kappa \approx 1.7$. □

We now relax the assumption of noiseless single-qubit gates and generalize our results to noise of the form N2. We assume that all the rounds of single-qubit gates suffer bounded noise, i.e. that for all circuits $k = 1, \ldots, v+1$ and bands

$j = 1, \ldots, m$, a noisy implementation of the round of single-qubit gates is (cfr. Figure 5.4 for notation)

$$\widetilde{\mathcal{U}}_j^{\prime\prime(k)} = \mathcal{E}_j^{(k)}(\mathcal{U}_j^{\prime\prime(k)} \otimes \mathcal{I}_E) \tag{5.18}$$

with $\mathcal{E}_j^{(k)} = (1 - r_j^{(k)})\mathcal{I}_{SE} + r_j^{(k)}\mathcal{E}_j^{\prime(k)}$ for some arbitrary CPTP map $\mathcal{E}_j^{\prime(k)}$ acting on both system and environment and for some number $0 \leq r_j^{(k)} < 1$. We refer to the number $r_j^{(k)}$ as "error rate" of $\mathcal{U}_j^{\prime\prime(k)}$. Since each $\mathcal{U}_j^{\prime\prime(k)}$ is chosen at random (depending on whether circuit k is the target or a trap and on the QOTP) and since noise in single-qubit gates is potentially gate-dependent (condition N2), let us indicate with $r_{\text{max, } j}^{(k)}$ the maximum error rate of single-qubit gates in band j of circuit k, the maximum being taken over all possible choices of $\mathcal{U}_j^{\prime\prime(k)}$.

We can now state Theorem 7:

Theorem 7. [Credibility with noisy single-qubit gates]. *Our protocol with v trap circuits can accredit the outputs of a noisy quantum computer affected by noise of the form* N1 *and* N2 *with*

$$\varepsilon = g\frac{\kappa}{v+1} + \; 1 \; - g \; , \tag{5.19}$$

where $\kappa = 3(3/4)^2 \approx 1.7$ and $g = \prod_{j,k}(1 - r_{\text{max, } j}^{(k)})$.

Proof. To calculate ε for the protocol with noisy single-qubit gates we use that $\mathcal{E}_j^{(k)} = (1 - r_{\text{max, } j}^{(k)})\mathcal{I}_{SE} + r_{\text{max, } j}^{(k)}\mathcal{Q}_j^{(k)}$, where $\mathcal{Q}_j^{(k)}$ is a CPTP map encompassing the system and the environment. We can then rewrite the state of the system at the end of the protocol as

$$\rho_{\text{out}}^{\star} = g\rho_{\text{out}} + \big(1 - g\big)\widetilde{\rho}_{\text{out}} \tag{5.20}$$

where ρ_{out} is the state of the system at the end of a protocol run with noiseless single-qubit gates—which by Theorem 6 is of the form of Equation 5.3 with $b \leq \kappa/(v+1)$—and $\widetilde{\rho}_{\text{out}}$ is a quantum state containing the effects of noise in single-qubit gates. Expressing $\widetilde{\rho}_{\text{out}}$ as

$$\widetilde{\rho}_{\text{out}} = h \; \widetilde{\tau}_1^{\text{tar}} \otimes |\text{acc}\rangle\langle\text{acc}| + (1 - h) \; \widetilde{\tau}_2^{\text{tar}} \otimes |\text{rej}\rangle\langle\text{rej}| \; , \tag{5.21}$$

where ${\widetilde{\tau}_1}^{\text{tar}}$ and ${\widetilde{\tau}_2}^{\text{tar}}$ are arbitrary states for the target and $0 \leq h \leq 1$, we thus have

$$\rho^{\star}_{\text{out}}{=}g\Bigg[b\ \tau'^{\text{ tar}}_{\text{out}} \otimes |\text{acc}\rangle\langle\text{acc}| + (1-b)\Bigg(l\ \sigma^{\text{tar}}_{\text{out}} \otimes |\text{acc}\rangle\langle\text{acc}| + (1-l)\tau^{\text{tar}}_{\text{out}} \otimes |\text{rej}\rangle\langle\text{rej}|\Bigg)\Bigg]$$
$$+ (1-g)\Bigg[h\ {\widetilde{\tau}_1}^{\text{tar}} \otimes |\text{acc}\rangle\langle\text{acc}| + (1-h)\ {\widetilde{\tau}_2}^{\text{tar}} \otimes |\text{rej}\rangle\langle\text{rej}|\Bigg]$$

Thus, the probability that the target is in the wrong state and the flag bit is in the state $|\text{acc}\rangle$ is $gb + (1-g)h \leq g\kappa/(v+1) + (1-g)h$, where we used that $b \leq \kappa/(v+1)$ from Theorem 6. This probability reaches its maximum for $h = 1$, therefore we have $\varepsilon = g\kappa/(v+1) + 1 - g$. □

Note that if $r^{(k)}_{\max,j} \leq r_0 \ll 1$, then

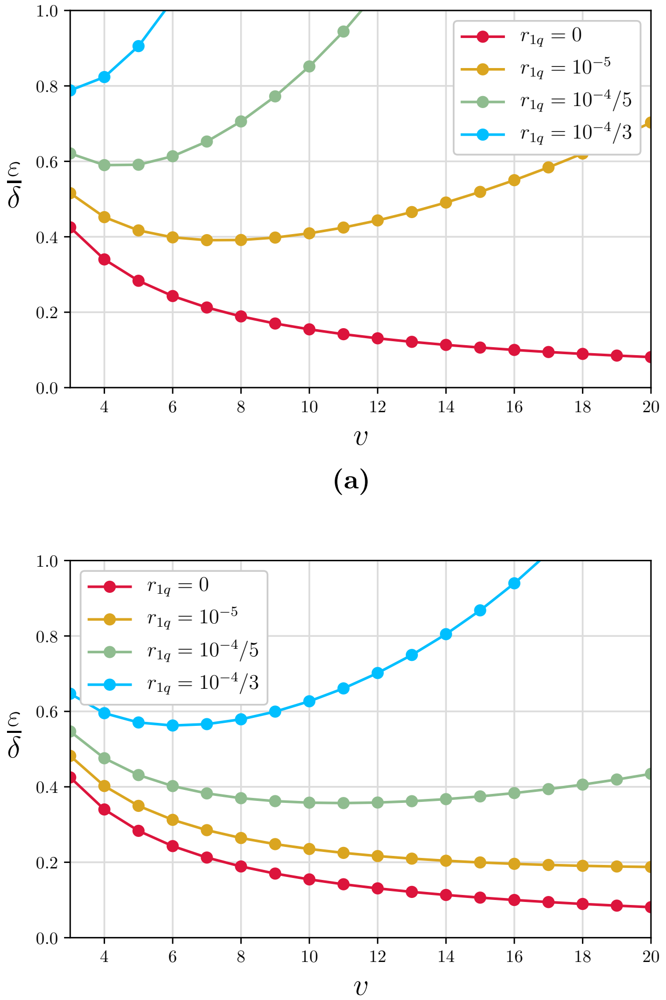
$$g \geq \prod_{k=1}^{v+1}\prod_{j=1}^{m}(1-r_0) \approx 1 - m(v+1)r_0 + O(r_0^2). \tag{5.22}$$

Thus, if $r_0 \ll 1/m(v+1)$, then $g \approx 1$ and $\varepsilon \approx 1.7/(v+1)$.

It is worth noting that our Theorem 6 also holds if single-qubit gates suffer unbounded noise, provided that this noise is gate-independent. Indeed, if $\mathcal{E}^{(k)}_j = \mathcal{E}$ does not depend on the parameters in $\mathcal{U}''^{(k)}_j$ (cfr. Figure 5.4 for notation), using $\mathcal{E}^{(k)}_j\mathcal{CZ}_j\mathcal{F}^{(k)}_j = \mathcal{CZ}_j\mathcal{F}'^{(k)}_j$ (with $\mathcal{F}'^{(k)}_j = \mathcal{CZ}^{-1}_j\mathcal{E}^{(k)}_j\mathcal{CZ}_j\mathcal{F}^{(k)}_j$) we can factor this noise into that of $\mathcal{CZ}_j$ and prove $\varepsilon = \kappa/(v+1)$ with the same arguments used in Theorem 6. Similarly, we also expect our Theorem 7 to hold if noise in single-qubit gates has a *weak* gate-dependence, as is the case for some of the protocols centered around randomized benchmarking [37]. We leave the analysis of weakly gate-dependent noise to future works.

5.4 Utility of the accreditation protocol

In this Section we consider a target circuit containing $n = 60$ qubits and $m = 22$ bands. We analyze the utility of the accreditation protocol by calculating the ratio $\varepsilon/\text{prob(acc)}$—which is the bound on the variation distance provided by our protocol, cfr. Equation 5.5 on page 56 —for different values of v, assuming that all the circuits undergo Pauli noise (Section 2.4, page 14). We assume that all the single-qubit gates introduce a single-qubit Pauli error with probability r_{1q}, all the two-qubit gates introduce a two-qubit Pauli error with probability r_{2q} and SPAM errors occur with probability r_s. We set $r_{2q} = 4r_{1q}$ and $r_s = 20r_{1q}$ as in Google Sycamore (Table 1.1, page 2).



(a)

(b)

Figure 5.5: Values of ε/δ (the bound on the variation distance provided by our accreditation protocol, cfr. Inequality 5.24; lower is better) as a function of the number v of trap circuits, for different values of single-qubit error rates r_{1q}. In **(a)** we assume that the single-qubit gates suffer gate-dependent noise and calculate g as in Equation 5.25, in **(b)** we assume that they suffer gate-independent noise and set $g = 1$.

Under the assumption of Pauli noise, using Equation 2.24 (page 14) we can lower-bound prob(acc) by

$$\delta := \left((1 - r_{1q})^{60\times 22} (1 - 4r_{1q})^{20\times 21} (1 - 20r_{1q})^{60} \right)^{v} \leq \text{prob(acc)} \; . \tag{5.23}$$

This yields (cfr. Equation 5.5 and Theorem 7)

$$\frac{1}{2}\sum_{\overline{s}}\left|p_{\text{noiseless}}(\overline{s})-p_{\text{noisy}}(\overline{s})\right|\leq\frac{\varepsilon}{\delta}=\frac{g\kappa/(v+1)+1-g}{\delta}\ , \tag{5.24}$$

where $\kappa\approx 1.7$ and

$$g=\big(1-r_{1q}\big)^{60\times 22\times(v+1)} \text{ if noise depends on single-qubit gates} \tag{5.25}$$

$$g=1 \text{ if noise does not depend on single-qubit gates.} \tag{5.26}$$

In Figure 5.5 we plot ε/δ as a function of the number v of trap circuits and for various error rates r_{1q}. As it can be seen, the various curves in the Figure are convex: as the number v of traps is increased, the curves initially decrease, then achieve a minimum and eventually start increasing with v. This is because the denominator δ (the probability that all the v traps accept) decreases with v. All the points in the curve are valid upper-bounds on the variation distance, and the smallest value of ε/δ corresponds to the best bound that can be provided by the accreditation protocol. To obtain the best bound, the user of our protocol can implement the protocol many times for different values of v and reproduce curves of the type in Figure 5.5.

In Figure 5.6 we plot the best bound that can be provided by our protocol as a function of the error r_{1q}. As it can be seen, the best bound increases with r_{1q} and eventually reaches 1. Since the variation distance is smaller than 1 by definition (cfr. page 12), we say that our accreditation protocol is *useful* when the best bound is below 1 and *useless* otherwise.

In Figure 5.6 we see that if single-qubit gates suffer gate-dependent noise (brown solid line), our accreditation protocol is useful for $r_{1q}\lesssim 4.5\times 10^{-5}$. This value is $\approx$ 30 times smaller than that in Google Sycamore (where $r_{1q}\approx 1.5\times 10^{-3}$, cfr. 1.1 in page 2). Instead, if single-qubit gates suffer gate-independent noise (blue solid line), our accreditation protocol is useful for $r_{1q}\lesssim 6.5\times 10^{-5}$. This value is $\approx$ 20 times smaller than that in Google Sycamore. In both cases, our accreditation protocol provides a significant improvement over the protocol in Chapter 4, that is useful if the error rates are reduced by a factor $\approx$ 1500 as compared to Google Sycamore (Section 4.6).

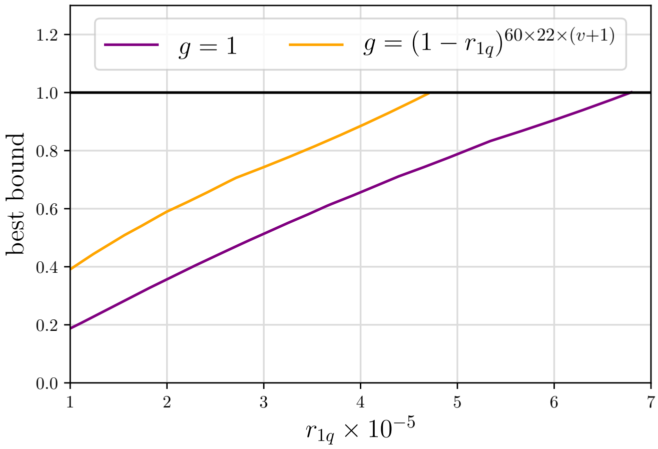


Figure 5.6: Best bound that can be provided by our accreditation protocol as a function of the number v of trap circuits, for different values of single-qubit error rates r_{1q} and g. If single-qubit gates suffer gate-dependent noise (orange line), our accreditation protocol is useful for error rates below $r_{1q} \approx 4.5 \times 10^{-5}$ (x-coordinate of the intersection between orange and black lines), which is ≈ 30 times smaller than in Google Sycamore (where $r_{1q} \approx 1.5 \times 10^{-3}$). If single-qubit gates suffer gate-dependent noise (purple line), our accreditation protocol is useful for error rates below $r_{1q} \approx 6.5 \times 10^{-5}$ (x-coordinate of the intersection between purple and black lines), which is ≈ 20 times smaller than r_{1q} in Google Sycamore.

5.5 Proofs

In this Section we present the proofs of the theorems contained in this Chapter.

5.5.1 Proof of Lemma 4 (Twirling the noise)

We begin by presenting the proof of Lemma 4.

Proof. (Lemma 4 is stated on page 63) We start proving the lemma for the case where we run a single circuit ($v = 0$), and then we generalize to multiple circuits ($v > 0$). Including all the purifications in the environment, we can rewrite the noise as unitary matrices acting on system and environment (for clarity we write these unitaries in bold font). Doing this, for a fixed choice of gates $\mathcal{U}''_j, \dots, \mathcal{U}''_m$ (which depend on the choice of gates $\mathcal{U}_1, \dots, \mathcal{U}_m$ and on all the random bits $\alpha_{i,j}, \alpha'_{i,j}, \gamma_i$, cfr. Routine 4), the state of the system before the measurement becomes (Figure 5.7)

$$\rho(\mathcal{U}''_1, \dots, \mathcal{U}''_m) = \mathrm{Tr}_{\mathrm{E}}\Big[\mathbf{M}\; U''_m \widehat{cZ}_{m-1}\mathbf{F}_{m-1}U''_{m-1} \dots \widehat{cZ}_1 \mathbf{F}_1 U''_1 \mathbf{R}\Big(\rho_{\mathrm{in}} \otimes \rho_E\Big)\mathbf{R}^\dagger \dots \mathbf{M}^\dagger\Big]\;, \tag{5.27}$$

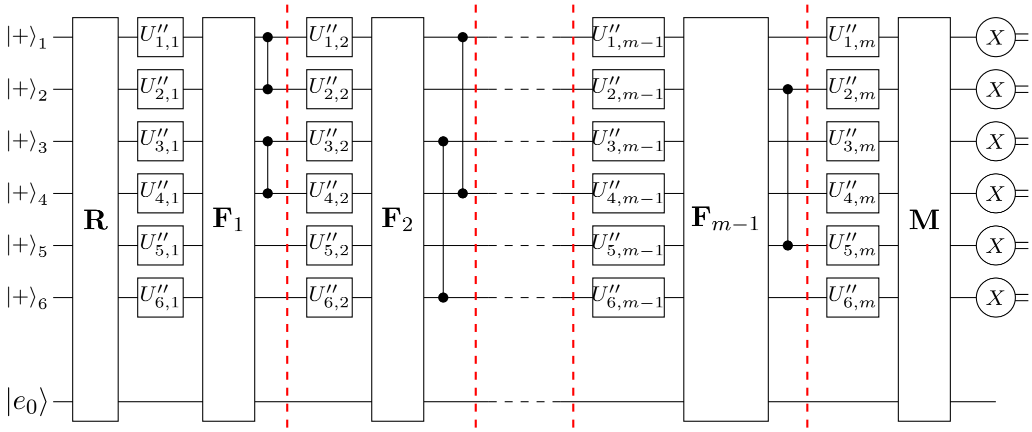


Figure 5.7: Noisy implementation of the 6-qubit target circuit in Figure 1.1. The noise in state preparation is described by the unitary $\mathbf{R}$, that in the measurements by $\mathbf{M}$, that in the cZ-gates in a band $j = 1, \ldots, m-1$ by $\mathbf{F}_j$. All these unitaries act simultaneously on the system and on the environment (initially in the ground state $|e_0\rangle$).

$\langle e_{k_2}\|\mathbf{R}\|e_0\rangle = \sum_{\mu_1} \eta^{(R)}_{k_2,0,\mu_1} P_{\mu_1}$	$\langle e_0\|\mathbf{R}^\dagger\|e_{l_2}\rangle = \sum_{\nu_1} \eta^{*(R)}_{l_2,0,\nu_1} P_{\nu_1}$
$\langle e_{k_1}\|\mathbf{F}_1\|e_{k_2}\rangle = \sum_{\mu_2} \eta^{(F)}_{k_1,k_2,\mu_2} P_{\mu_2}$	$\langle e_{l_2}\|\mathbf{F}_1^\dagger\|e_{l_1}\rangle = \sum_{\nu_2} \eta^{*(F)}_{l_1,l_2,\nu_2} P_{\nu_2}$
$\langle e_p\|\mathbf{M}\|e_{k_1}\rangle = \sum_{\mu_3} \eta^{(M)}_{p,k_1,\mu_3} P_{\mu_3}$	$\langle e_{l_1}\|\mathbf{M}^\dagger\|e_p\rangle = \sum_{\nu_3} \eta^{*(M)}_{p,l_1,\nu_3} P_{\nu_3}$

Table 5.1. Operators appearing in Equation 5.29 rewritten in Pauli basis. $P_\mu \in \{I, X, Y, Z\}^{\otimes n}$ are n-fold tensor products of Pauli operators acting on the system and $\eta^{(R)}_{k_2,0,\mu_1}$, $\eta^{(F)}_{k_1,k_2,\mu_2}$ and $\eta^{(M)}_{k_p,k_1,\mu_3}$ are complex numbers.

where $\rho_{\text{in}} = \otimes_{i=1}^{n} |+\rangle_i\langle+|$, $\rho_E = |e_0\rangle\langle e_0|$ is the initial state of the environment, $U''_j = \otimes_{i=1}^{n} U''_{i,j}$ are the gates returned by Routine 4, the unitary matrix $\mathbf{R}$ represents the noise in state preparation, the unitary matrix $\mathbf{M}$ represents the noise in the measurements, $\widehat{cZ}_j\mathbf{F}_j$ is the noisy round of entangling gates in a band j and $\text{Tr}_\text{E}[\,\cdot\,]$ is the trace over the environment.

For simplicity, we first prove our result for a circuit with $m = 2$ bands and generalize to $m > 2$ bands later. Defining an orthonormal basis $\{|e_p\rangle\langle e_p|\}$ for the environment, the state in Equation 5.27 becomes

$$\rho(\mathcal{U}''_1, \mathcal{U}''_2) = \sum_p \langle e_p|\mathbf{M}\; U''_2\widehat{cZ}_1\mathbf{F}_1 U''_1\mathbf{R}\big(\rho_{\text{in}} \otimes |e_0\rangle\langle e_0|\big)\mathbf{R}^\dagger\; U''^\dagger_1\mathbf{F}^\dagger_1\widehat{cZ}_1 U''^\dagger_2\mathbf{M}^\dagger|e_p\rangle\;. \tag{5.28}$$

Introducing resolutions of the identity on the environment before and after every noise operator, we have

$$\rho(\mathcal{U}_1'',\mathcal{U}_2'') = \sum_{\substack{p\\ k_1,k_2,l_1,l_2}} \Big[\langle e_p|\mathbf{M}|e_{k_1}\rangle\; U_2''\widehat{cZ}_1\langle e_{k_1}|\mathbf{F}_1|e_{k_2}\rangle U_1''\langle e_{k_2}|\mathbf{R}|e_0\rangle\Big]\big(\rho_{\text{in}}\big)\Big[h.c.\Big]\ , \tag{5.29}$$

where we indicated as *h.c.* the Hermitian conjugate of the quantity in squared parenthesis. We used $\sum_k |e_k\rangle\langle e_k| = I_E$ and $\langle e_k|V_S|e_{k'}\rangle = V_S\delta_{k,k'}$, which is valid for every operator V_S acting only on the system. The operators $\langle e_p|\mathbf{M}|e_{k_1}\rangle$, $\langle e_{k_1}|\mathbf{F}_1|e_{k_2}\rangle$, $\langle e_{k_2}|\mathbf{R}|e_0\rangle$, $\langle e_0|\mathbf{R}^\dagger|e_{l_2}\rangle$, $\langle e_{l_2}|\mathbf{F}_1^\dagger|e_{l_1}\rangle$, $\langle e_{l_1}|\mathbf{M}^\dagger|e_p\rangle$ act only on the system, hence they can be rewritten in Pauli basis as in Table 5.1.

We thus obtain

$$\begin{aligned}\rho(\mathcal{U}_1'',\mathcal{U}_2'') = \sum_{\substack{p,k_1,k_2,l_1,l_2\\ \mu_1,\mu_2,\mu_3\\ \nu_1,\nu_2,\nu_3}} &\left(\eta^{(R)}_{k_2,0,\mu_1}\eta^{(F)}_{k_1,k_2,\mu_2}\eta^{(M)}_{p,k_1,\mu_3}\eta^{*(R)}_{l_2,0,\nu_1}\eta^{*(F)}_{l_1,l_2,\nu_2}\eta^{*(M)}_{p,l_1,\nu_3}\right)\times\\ &\times P_{\mu_3}U_2''\widehat{cZ}_1 P_{\mu_2}U_1''P_{\mu_1}\big(\rho_{\text{in}}\big)P_{\nu_1}U_1''^\dagger P_{\nu_2}\widehat{cZ}_1 U_2''^\dagger P_{\nu_3}\ .\end{aligned} \tag{5.30}$$

We will now describe how to apply the Pauli twirl Lemmas iteratively, in the order the operations apply on the input. Therefore, we start by showing how to eliminate terms of the sum where $\mu_1 \neq \nu_1$. Since X stabilizes $|+\rangle$ states, we can rewrite ρ_{in} as $\big(\otimes_i X_i^{\gamma_i}\big)\rho_{\text{in}}\big(\otimes_i X_i^{\gamma_i}\big)$. Moreover, using $U_1'' = U_1'\big(\otimes_i X_i^{\gamma_i}\big)$, cfr. Routine 3, the above state becomes

$$\begin{aligned}\rho(\mathcal{U}_1'',\mathcal{U}_2'') = \sum_{\substack{p,k_1,k_2,l_1,l_2\\ \mu_1,\mu_2,\mu_3\\ \nu_1,\nu_2,\nu_3}} &\left(\eta^{(R)}_{k_2,0,\mu_1}\eta^{(F)}_{k_1,k_2,\mu_2}\eta^{(M)}_{p,k_1,\mu_3}\eta^{*(R)}_{l_2,0,\nu_1}\eta^{*(F)}_{l_1,l_2,\nu_2}\eta^{*(M)}_{p,l_1,\nu_3}\right)\times\\ \times P_{\mu_3}U_2''\widehat{cZ}_1 P_{\mu_2}U_1'\big(\otimes_i X_i^{\gamma_i}\big)P_{\mu_1}\big(\otimes_i X_i^{\gamma_i}\big)\big(\rho_{\text{in}}\big)&\big(\otimes_i X_i^{\gamma_i}\big)P_{\nu_1}\big(\otimes_i X_i^{\gamma_i}\big)U_1'^\dagger P_{\nu_2}\widehat{cZ}_1 U_2''^\dagger P_{\nu_3}\ .\end{aligned} \tag{5.31}$$

Summing over all possible γ_i and applying the Restricted Pauli Twirl (the Pauli-X components of both P_{μ_1} and P_{ν_1} stabilize ρ_{in} and can thus be ignored), we obtain a factor δ_{μ_1,ν_1}, and thus the above state becomes

$$\begin{aligned}\rho(\mathcal{U}_1',\mathcal{U}_2'') =&\frac{1}{2^n}\sum_{\{\gamma_i\}}\rho(\mathcal{U}_1'',\mathcal{U}_2'')\\ =&\sum_{\substack{p,k_1,k_2,l_1,l_2\\ \mu_1,\mu_2,\mu_3\\ \nu_2,\nu_3}}\left(\eta^{(R)}_{k_2,0,\mu_1}\eta^{(F)}_{k_1,k_2,\mu_2}\eta^{(M)}_{p,k_1,\mu_3}\eta^{*(R)}_{l_2,0,\mu_1}\eta^{*(F)}_{l_1,l_2,\nu_2}\eta^{*(M)}_{p,l_1,\nu_3}\right)\times\\ &\times P_{\mu_3}U_2''\widehat{cZ}_1P_{\mu_2}U_1'P_{\mu_1}\big(\rho_{\text{in}}\big)P_{\mu_1}U_1'^{\dagger}P_{\nu_2}\widehat{cZ}_1U_2''^{\dagger}P_{\nu_3}\ .\end{aligned}\tag{5.32}$$

To operate a Pauli twirl on P_{μ_2} and P_{ν_2}, we rewrite U_1' as $\big(\otimes_i Z^{\alpha_{i,1}}X^{\alpha'_{1,i}}\big)U_1$ and $U_2''\widehat{cZ}_1$ as $U_2'\widehat{cZ}_1\big(\otimes_i X^{\alpha'_{1,i}}Z^{\alpha_{i,1}}\big)$, cfr. Routine 3. Summing over $\alpha_{i,1}$ and $\alpha'_{i,1}$ and using the Pauli Twirl, we obtain δ_{μ_2,ν_2}, and thus

$$\begin{aligned}\rho(\mathcal{U}_1,\mathcal{U}_2') =&\frac{1}{2^{2n}}\sum_{\{\alpha_{i,1}\},\{\alpha'_{i,1}\}}\rho(\mathcal{U}_1',\mathcal{U}_2'')\\ =&\sum_{\substack{p,k_1,k_2,l_1,l_2\\ \mu_1,\mu_2,\mu_3\\ \nu_3}}\left(\eta^{(R)}_{k_2,0,\mu_1}\eta^{(F)}_{k_1,k_2,\mu_2}\eta^{(M)}_{p,k_1,\mu_3}\eta^{*(R)}_{l_2,0,\mu_1}\eta^{*(F)}_{l_1,l_2,\mu_2}\eta^{*(M)}_{p,l_1,\nu_3}\right)\times\\ &\times P_{\mu_3}U_2'\widehat{cZ}_1P_{\mu_2}U_1P_{\mu_1}\big(\rho_{\text{in}}\big)P_{\mu_1}U_1^{\dagger}P_{\mu_2}\widehat{cZ}_1U_2'^{\dagger}P_{\nu_3}\ .\end{aligned}\tag{5.33}$$

To operate a Pauli twirl on P_{μ_3} and P_{ν_3} we write the state of the system after the measurements:

$$\begin{aligned}\rho_{\text{meas}}(\mathcal{U}_1,\mathcal{U}_2') =& \frac{1}{2^n}\sum_{\{s_i\}}\otimes_i\Big(\langle+|_iZ_i^{s_i}\ \rho(\mathcal{U}_1,\mathcal{U}_2')\ Z_i^{s_i}|+\rangle_i\Big)\ Z_i^{s_i}|+\rangle_i\langle+|Z_i^{s_i}\\ =&\frac{1}{2^n}\sum_{\substack{p,k_1,k_2,l_1,l_2\\ \mu_1,\mu_2,\mu_3,\nu_3\\ s_1,\dots,s_n}}\left(\eta^{(R)}_{k_2,0,\mu_1}\eta^{(F)}_{k_1,k_2,\mu_2}\eta^{(M)}_{p,k_1,\mu_3}\eta^{*(R)}_{l_2,0,\mu_1}\eta^{*(F)}_{l_1,l_2,\mu_2}\eta^{*(M)}_{p,l_1,\nu_3}\right)\times\\ &\times\langle+|^{\otimes n}\big(\otimes_i Z_i^{s_i}\big)P_{\mu_3}U_2'\widehat{cZ}_1P_{\mu_2}U_1P_{\mu_1}\big(\rho_{\text{in}}\big)P_{\mu_1}U_1^{\dagger}P_{\mu_2}\widehat{cZ}_1U_2'^{\dagger}P_{\nu_3}\big(\otimes_i Z_i^{s_i}\big)|+\rangle^{\otimes n}\\ &\times\otimes_iZ_i^{s_i}|+\rangle_i\langle+|Z_i^{s_i}\end{aligned}\tag{5.34}$$

Since $U_2' = \big(\otimes_i X_i^{\alpha'_{i,2}}Z_i^{\alpha_{i,2}}\big)U_2$ and $|+\rangle^{\otimes n} = \otimes_iX_i^{\alpha''_{i,2}}|+\rangle^{\otimes n}$, summing over $\{\alpha'_{i,2}\}$ and using the Restricted Pauli Twirl (the Pauli-X components of both P_{μ_3} and P_{ν_3}

stabilize $|+\rangle^{\otimes n}$ and can thus be ignored) we obtain δ_{μ_3,ν_3}:

$$\rho_{\text{meas}}\big(\mathcal{U}_1,\mathcal{U}_2\big) = \frac{1}{2^n}\sum_{\alpha'_{i,2}} \rho_{\text{meas}}\big(\mathcal{U}_1,\mathcal{U}'_2\big)$$

$$= \frac{1}{2^n}\sum_{\substack{p,k_1,k_2,l_1,l_2\\ \mu_1,\mu_2,\mu_3,\nu_3\\ s_1,\dots,s_n}} \Big(\eta^{(R)}_{k_2,0,\mu_1}\eta^{(F)}_{k_1,k_2,\mu_2}\eta^{(M)}_{p,k_1,\mu_3}\eta^{*(R)}_{l_2,0,\mu_1}\eta^{*(F)}_{l_1,l_2,\mu_2}\eta^{*(M)}_{p,l_1,\mu_3}\Big)$$

$$\times \langle+|^{\otimes n}\big(\otimes_i\, Z_i^{s_i\oplus\alpha_{i,2}}\big)P_{\mu_3}U_2\widehat{cZ}_1P_{\mu_2}U_1P_{\mu_1}\big(\rho_{\text{in}}\big)P_{\mu_1}U_1^\dagger P_{\mu_2}\widehat{cZ}_1U_2^\dagger P_{\mu_3}\big(\otimes_i\, Z_i^{s_i\oplus\alpha_{i,2}}\big)|+\rangle^{\otimes n}$$

$$\times \otimes_i Z_i^{s_i}|+\rangle_i\langle+|Z_i^{s_i} \tag{5.35}$$

Finally, after the classical post-processing (which replaces the outputs s_i with $s_i \oplus \alpha_{i,2}$), average over $\{\alpha_{i,2}\}$ yields the outcome state

$$\rho_{\text{out}}\big(\mathcal{U}_1,\ \mathcal{U}_2\big) = \frac{1}{2^n}\sum_{\{\alpha_{i,2}\}}\frac{1}{2^n}\sum_{\substack{p,k_1,k_2,l_1,l_2\\ \mu_1,\mu_2,\mu_3\\ s_1,\dots,s_n}} \Big(\eta^{(R)}_{k_2,0,\mu_1}\eta^{(F)}_{k_1,k_2,\mu_2}\eta^{(M)}_{p,k_1,\mu_3}\eta^{*(R)}_{l_2,0,\mu_1}\eta^{*(F)}_{l_1,l_2,\mu_2}\eta^{*(M)}_{p,l_1,\mu_3}\Big)$$

$$\times \langle+|^{\otimes n}\big(\otimes_i\, Z_i^{s_i\oplus\alpha_{i,2}}\big)P_{\mu_3}U_2\widehat{cZ}_1P_{\mu_2}U_1P_{\mu_1}\big(\rho_{\text{in}}\big)P_{\mu_1}U_1^\dagger P_{\mu_2}\widehat{cZ}_1U_2^\dagger\big(\otimes_i\, Z_i^{s_i\oplus\alpha_{i,2}}\big)P_{\mu_3}|+\rangle^{\otimes n}$$

$$\times \otimes_i Z_i^{s_i\oplus\alpha_{i,2}}|+\rangle_i\langle+|Z_i^{s_i\oplus\alpha_{i,2}}$$

$$= \frac{1}{2^n}\sum_{\substack{\mu_1,\mu_2,\mu_3\\ s_1,\dots,s_n}}\Big(\sum_{p,k_1,k_2,l_1,l_2}\eta^{(R)}_{k_2,0,\mu_1}\eta^{(F)}_{k_1,k_2,\mu_2}\eta^{(M)}_{p,k_1,\mu_3}\eta^{*(R)}_{l_2,0,\mu_1}\eta^{*(F)}_{l_1,l_2,\mu_2}\eta^{*(M)}_{p,l_1,\mu_3}\Big)$$

$$\times \langle+|^{\otimes n}\big(\otimes_i\, Z_i^{s_i}\big)P_{\mu_3}U_2\widehat{cZ}_1P_{\mu_2}U_1P_{\mu_1}\big(\rho_{\text{in}}\big)P_{\mu_1}U_1^\dagger P_{\mu_2}\widehat{cZ}_1U_2^\dagger P_{\mu_3}\big(\otimes_i\, Z_i^{s_i}\big)|+\rangle^{\otimes n}$$

$$\times \otimes_i Z_i^{s_i}|+\rangle_i\langle+|Z_i^{s_i}$$

$$= \frac{1}{2^n}\sum_{\substack{\mu_1,\mu_2,\mu_3\\ s_1,\dots,s_n}}\phi_{\mu_1,\mu_2,\mu_3}$$

$$\times \langle+|^{\otimes n}\big(\otimes_i\, Z_i^{s_i}\big)P_{\mu_3}U_2\widehat{cZ}_1P_{\mu_2}U_1P_{\mu_1}\big(\rho_{\text{in}}\big)P_{\mu_1}U_1^\dagger P_{\mu_2}\widehat{cZ}_1U_2^\dagger P_{\mu_3}\big(\otimes_i\, Z_i^{s_i}\big)|+\rangle^{\otimes n}$$

$$\times \otimes_i Z_i^{s_i}|+\rangle_i\langle+|Z_i^{s_i}\ , \tag{5.36}$$

where

$$\begin{aligned}\phi_{\mu_1,\mu_2,\mu_3} = &\sum_{p,k_1,k_2,l_1,l_2} \eta^{(R)}_{k_2,0,\mu_1}\eta^{(F)}_{k_1,k_2,\mu_2}\eta^{(M)}_{p,k_1,\mu_3}\eta^{*(R)}_{l_2,0,\mu_1}\eta^{*(F)}_{l_1,l_2,\mu_2}\eta^{*(M)}_{p,l_1,\mu_3}\\ =&\sum_p \left| \sum_{k_1,k_2} \eta^{(R)}_{k_2,0,\mu_1}\eta^{(F)}_{k_1,k_2,\mu_2}\eta^{(M)}_{p,k_1,\mu_3}\right|^2 \geq 0 \end{aligned} \tag{5.37}$$

and $\sum_{\mu_1,\mu_2,\mu_3} \phi_{\mu_1,\mu_2,\mu_3} = 1$. $\rho_{\text{out}}\big(\mathcal{U}_1,\, \mathcal{U}_2\big)$ is therefore a convex combination of quantum states and ϕ_{μ_1,μ_2,μ_3} can be seen as the joint probability of Pauli errors P_{μ_1}, P_{μ_2} and P_{μ_3}. This can be rewritten as

$$\begin{aligned}\rho_{\text{out}}\big(\mathcal{U}_1,\mathcal{U}_2\big) = &\sum_{\substack{\mathcal{P}_0,\mathcal{P}_1,\mathcal{P}_2\\ s_1,\dots,s_n}} \frac{\text{prob}\big(\mathcal{P}_0,\mathcal{P}_1,\mathcal{P}_2\big)}{2^n} \langle+|^{\otimes n}\Big[\mathcal{Z}^{\overline{s}}\mathcal{P}_2\,\mathcal{U}_2\,\mathcal{C}\mathcal{Z}_1\;\mathcal{P}_1\,\mathcal{U}_1\;\mathcal{P}_0\big(\rho_{\text{in}}\big)\Big]|+\rangle^{\otimes n}\\ &\times \otimes_i Z_i^{s_i}|+\rangle_i\langle+|Z_i^{s_i}\;,\end{aligned} \tag{5.38}$$

where $\mathcal{P}_0, \mathcal{P}_2 \in \{\mathcal{I},\mathcal{Z}\}^{\otimes n}$, $\mathcal{P}_1 \in \{\mathcal{I},,\mathcal{X},\mathcal{Y},\mathcal{Z}\}^{\otimes n}$ and $\text{prob}\big(\mathcal{P}_0,\mathcal{P}_1,\mathcal{P}_2\big)$ is the joint probability of Pauli errors $\mathcal{P}_0,\mathcal{P}_1,\mathcal{P}_2$. Finally,

$$\rho_{\text{out}}\big(\mathcal{U}_1,\mathcal{U}_2\big) = \sum_{\substack{\mathcal{P}_0,\mathcal{P}_1,\mathcal{P}_2\\ s_1,\dots,s_n}} \frac{\text{prob}(\overline{s}^{(1)},\dots,\overline{s}^{(v+1)}|\mathcal{P}_0^{(1)},\dots,\mathcal{P}_m^{(v+1)})}{2^n} \;\Big(\otimes_i\, Z_i^{s_i}|+\rangle_i\langle+|Z_i^{s_i}\Big)\;, \tag{5.39}$$

where

$$\begin{aligned}&\text{prob}(\overline{s}^{(1)},\dots,\overline{s}^{(v+1)}|\mathcal{P}_0^{(1)},\dots,\mathcal{P}_m^{(v+1)}) \\ =&\text{prob}\big(\mathcal{P}_0^{(1)},\dots,\mathcal{P}_m^{(v+1)}\big)\langle+|^{\otimes n}\Big[\mathcal{Z}^{\overline{s}}\mathcal{P}_2\,\mathcal{U}_2\,\mathcal{C}\mathcal{Z}_1\;\mathcal{P}_1\,\mathcal{U}_1\;\mathcal{P}_0\big(\rho_{\text{in}}\big)\Big]|+\rangle^{\otimes n}\;.\end{aligned} \tag{5.40}$$

This concludes the proof for the protocol with $v = 0$ and $m = 2$.

The generalization to a protocol with $v = 0$ and $m > 2$ is straightforward. Starting from the state in Equation 5.27, one can use the same arguments as for the 2-band circuit. To generalize to multiple circuits ($v > 0$), we start by noticing that the circuits are implemented in series, hence the noise can only affect one circuit at a time. Starting from here and using the same arguments as above, one can finally obtain Equation 5.14. □

5.5.2 Proof of Lemma 5 (Traps lemma)

In this Section we show the proof of Lemma 5.

Proof. (Lemma 5 is stated on page 64) For a given collection of Pauli errors $\{\mathcal{P}_j\}_{j=0}^{m}$ affecting a trap circuit, the state of the trap circuit after the measurements is of the form

$$\rho_{\text{out}}^{\text{trap}}(\{\mathcal{P}_j\}) = \frac{1}{M_1 \times \cdots \times M_{m-1}} \sum_{\mathcal{U}_1,\cdots,\mathcal{U}_m} \mathcal{P}_m \mathcal{U}_m \circ \left(\circ_{j=1}^{m-1} \mathcal{CZ}_j \mathcal{P}_j \mathcal{U}_j \right) \circ \mathcal{P}_0(\rho_{\text{in}}^{\text{trap}}) \ , \tag{5.41}$$

where $\rho_{\text{in}}^{\text{trap}} = \otimes_{i=1}^{n} |+\rangle_i\langle+|$, $\mathcal{CZ}_j$ is the entangling operation in band j, $\mathcal{P}_0, \mathcal{P}_m \in \{\mathcal{I}, \mathcal{Z}\}^{\otimes n}$, $\mathcal{P}_j \in \{\mathcal{I}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}\}^{\otimes n}$ for all $j = 1, \ldots, m$ and M_j is the number of choices of $\mathcal{U}_j$. Note that each number M_j depends on the number of qubits connected by a cZ in band j of the trap circuit, cfr. Routine 4.

In a trap circuit the gate $\mathcal{U}_1$ in the first band is of the form $\mathcal{U}_1 = \mathcal{V}_1 \mathcal{H}^t$, where $\mathcal{V}_1$ implements a gate from $\{H, S\}^{\otimes n}$ (cfr. Step 2.1 of Routine 4) and $\mathcal{H}^t$ is the round of Hadamard gates activated at random (cfr. Step 3 of Routine 4). Similarly, for all $j = 2, \ldots, m-1$, $\mathcal{U}_j$ implements a gate belonging to the set $\{I, HS^\dagger, SH\}^{\otimes n}$. These gates undo the gates in previous band and implement new ones (cfr. Step 2.1 Routine 4 and Figure 6.2), thus we can write them as $\mathcal{U}_j = \mathcal{V}_j \mathcal{V}_{j-1}^{-1}$—with each $\mathcal{V}_j$ implementing a gate from the set $\{H, S\}^{\otimes n}$. Finally, the gate $\mathcal{U}_m$ in the last band is of the form $\mathcal{U}_m = \mathcal{H}^t \mathcal{V}_{m-1}^{-1}$, where $\mathcal{V}_{m-1}^{-1}$ implements a gate from $\{H, S^\dagger\}^{\otimes n}$ and undoes the gate in band $m-1$ (cfr. Step 2.2 of Routine 4). Using this, we obtain

$$\rho_{\text{out}}^{\text{trap}}(\{\mathcal{P}_j\}) = \frac{1}{2(N_1 \times \cdots \times N_{m-1})} \sum_{\substack{t=0,1 \\ \mathcal{V}_1,\cdots,\mathcal{V}_{m-1}}} \mathcal{P}_m \mathcal{H}^t \circ \left(\circ_{j=1}^{m-1} \mathcal{V}_j^{-1} \mathcal{CZ}_j \mathcal{P}_j \mathcal{V}_j \right) \circ \mathcal{H}^t \mathcal{P}_0(\rho_{\text{in}}^{\text{trap}}) \ , \tag{5.42}$$

where N_j is the number of possible choices of $\mathcal{V}_j$.

Using that $\mathcal{V}_j^{-1} \mathcal{CZ}_j \mathcal{V}_j = \mathcal{CX}_j$ is a tensor product of cX gates, the above state can also be rewritten as

$$\rho_{\text{out}}^{\text{trap}}(\{\mathcal{P}_j\}) = \frac{1}{2(N_1 \times \cdots \times N_{m-1})} \sum_{\substack{t=0,1 \\ \mathcal{V}_1,\cdots,\mathcal{V}_{m-1}}} \mathcal{P}_m \mathcal{H}^t \circ \left(\circ_{j=1}^{m-1} \mathcal{CX}_j \mathcal{V}_j^{-1} \mathcal{P}_j \mathcal{V}_j \right) \circ \mathcal{H}^t \mathcal{P}_0(\rho_{\text{in}}^{\text{trap}}) \ . \tag{5.43}$$

Notice that each $\mathcal{CX}_j$ carries an implicit dependency on $\mathcal{V}_j$ (the orientation of the cX gates depends on $\mathcal{V}_j$, cfr. Figure 6.2).

The probability that the trap outputs $\overline{s} = \overline{0}$ is

$$\text{prob}\big(\overline{s} = \overline{0} \mid \{\mathcal{P}_j\}\big) = \langle + |^{\otimes n} \rho_{\text{out}}^{\text{trap}}\big(\{\mathcal{P}_j\}\big) | + \rangle^{\otimes n} \ . \tag{5.44}$$

To upper-bound this probability by 3/4, we first consider “1-band” collections of errors, namely collections $\{\mathcal{P}_j\}$ such that $\mathcal{P}_{j_0} \neq \mathcal{I}$ for some $j_0 \in \{0, \dots, m\}$ and $\mathcal{P}_j = \mathcal{I}$ for all other $j \neq j_0$. For these collections, we prove that the probability that the output of the trap is the correct one $\overline{s} = \overline{0}$ is smaller than 1/2:

$$\text{prob}(\overline{s} = \overline{0} \mid \text{1-band coll.}) \leq \frac{1}{2} \tag{5.45}$$

We prove this in Statement 1.

Next, we consider “2-band” collections of errors. We obtain

$$\text{prob}(\overline{s} = \overline{0} \mid \text{2-band coll.}) \leq \frac{3}{4} \tag{5.46}$$

We prove this in Statement 2. To obtain this bound, we *move* the two errors towards each other (i.e. we commute them with all the gates in the middle) and subsequently *merge* them, rewriting them as a single Pauli operator. The resulting Pauli operator is the identity $\mathcal{I}$ with probability c, or is a different operator with probability $1 - c$. In the former case, the errors have canceled out with each other, while in the latter they have reduced to a 1-band collection. Importantly, in Statement 2 we prove that $c \leq 1/2$. This yields

$$\begin{aligned}
&\text{prob}(\overline{s} = \overline{0} \mid \text{2-band coll.}) \\
=&(1 - c)\text{prob}(\overline{s} = \overline{0} \mid \text{1-band coll.}) + c \ \text{prob}(\overline{s} = \overline{0} \mid \text{no error}) \\
\leq&\frac{1 - c}{2} + c = \frac{1}{2} + \frac{c}{2} \ ,
\end{aligned} \tag{5.47}$$

where we used $\text{prob}(\overline{s} = \overline{0} \mid \text{no error}) = 1$ and $\text{prob}(\overline{s} = \overline{0} \mid \text{1-band coll.}) \leq 1/2$. Maximizing over $c \in [0, 1/2]$, we find

$$\text{prob}(\overline{s} = \overline{0} \mid \text{2-band coll.}) \leq \max_{0 \leq c \leq \frac{1}{2}} \left(\frac{1}{2} + \frac{c}{2}\right) = \frac{3}{4} \tag{5.48}$$

Finally, we generalise to collections affecting more than two bands. For three-band collections, again we move two of these Pauli operators towards each other and merge them. Doing this, the 3-band collection reduces to a 1-band collection with probability $c \leq 1/2$ or to a 2-band one with probability $1 - c$. Thus, using the above results, we have

$$\begin{aligned}
&\text{prob}(\overline{s}=\overline{0} \mid \text{3-band coll.})\\
=&(1-c)\text{prob}(\overline{s}=\overline{0} \mid \text{2-band coll.}) + c\ \text{prob}(\overline{s}=\overline{0} \mid \text{1-band coll.})\\
\leq&\frac{3(1-c)}{4}+\frac{c}{2} \leq \max_{0\leq c\leq \frac{1}{2}} \left(\frac{3(1-c)}{4}+\frac{c}{2}\right) = \frac{3}{4}
\end{aligned} \tag{5.49}$$

This argument can be iterated: at any fixed h, if $\text{prob}(\overline{s}=\overline{0} \mid (h{-}2)\text{-band coll.}) \leq 3/4$ and $\text{prob}(\overline{s}=\overline{0} \mid (h{-}1)\text{-band coll.}) \leq 3/4$, then it can be easily shown that $\text{prob}(\overline{s}=\overline{0} \mid h\text{-band coll.}) \leq 3/4$. We now complete the proof by proving Statement 1 and Statement 2.

Statement 1. *For all 1-band collections of error we have*

$$\text{prob}(\overline{s}=\overline{0} \mid \text{1-band coll.}) \leq \frac{1}{2}\ . \tag{5.50}$$

Proof. Single-band collections are defined as follows:

$$\mathcal{P}_j \neq \mathcal{I} \text{ for } j = j_0 \in \{0,\cdots,m\}\ ,\ \mathcal{P}_j = \mathcal{I} \text{ for all } j \neq j_0. \tag{5.51}$$

If $j_0 = 0$, using $cX\,|{+}{+}\rangle = |{+}{+}\rangle$ and $cX|00\rangle = |00\rangle$, we have

$$\begin{aligned}
\text{prob}\big(\overline{s}=\overline{0} \mid \{\mathcal{P}_j\}\big) =&\frac{1}{2}\sum_{t=0,1} \langle +|^{\otimes n}\mathcal{H}^t \circ \left(\circ_{j=1}^{m}\, \mathcal{C}\mathcal{X}_j\right) \circ \mathcal{H}^t \mathcal{P}_0 |+\rangle^{\otimes n}\\
=&\langle +|^{\otimes n}\mathcal{P}_0|+\rangle^{\otimes n} = 0\ ,
\end{aligned} \tag{5.52}$$

since $\mathcal{P}_0 \neq \mathcal{I} \in \{\mathcal{I},\mathcal{Z}\}^{\otimes n}$, and the same happens if $j_0 = m$.

If $1 \leq j_0 \leq m-1$, we have

$$\text{prob}\big(\overline{s}=\overline{0} \mid \{\mathcal{P}_j\}\big) = \frac{1}{N_{j_0}}\sum_{\mathcal{V}_{j_0}} \frac{1}{2}\sum_{t=0,1} \langle +|^{\otimes n}\mathcal{H}^t \mathcal{V}_{j_0}^{-1}\mathcal{P}_{j_0}\mathcal{V}_{j_0}\mathcal{H}^t|+\rangle^{\otimes n}\ , \tag{5.53}$$

where we used again that $cX\,|{+}{+}\rangle = |{+}{+}\rangle$ and $cX|00\rangle = |00\rangle$. Notice that $\langle +|^{\otimes n}\mathcal{P}|+\rangle^{\otimes n} = 0$ for all Pauli operators P whose Pauli-Z component is non-trivial, therefore $\sum_t \langle +|^{\otimes n}\mathcal{H}^t\mathcal{P}\mathcal{H}^t|+\rangle^{\otimes n}/2 \leq 1/2$ for all $\mathcal{P} \in \{\mathcal{I},\mathcal{X},\mathcal{Y},\mathcal{Z}\}^{\otimes n}/\mathcal{I}$. This yields

$$\text{prob}\big(\overline{s}=\overline{0} \mid \{\mathcal{P}_j\}\big) \leq \frac{1}{N_{j_0}}\sum_{\mathcal{V}_{j_0}} \frac{1}{2} \leq \frac{1}{2}\ , \tag{5.54}$$

where we used that $\mathcal{V}_{j_0}^{-1}\mathcal{P}_{j_0}\mathcal{V}_{j_0}$ is a Pauli operator for any $\mathcal{V}_{j_0}$. □

Statement 2. *For all 2-band collections of errors error we have*

$$\mathrm{prob}(\overline{s} = \overline{0} \mid \text{2-band coll.}) \leq \frac{3}{4} \ . \tag{5.55}$$

Proof. Two-band collections are defined as follows:

$$\mathcal{P}_j \neq \mathcal{I} \text{ for } j = j_1, j_2 \in \{0, \cdots, m\} \text{ (with } j_1 < j_2) \ , \ \mathcal{P}_j = \mathcal{I} \text{ for all } j \neq j_1, j_2. \tag{5.56}$$

We can distinguish four classes of 2-band collections:

1) Errors in state preparation and entangling gates, i.e. $j_1 = 0$ and $1 \leq j_2 \leq m - 1$.
2) Errors in entangling gates and measurements, i.e. $1 \leq j_1 \leq m - 1$ and $j_2 = m$.
3) Errors in two different entangling gates, i.e. $1 \leq j_1 < j_2 \leq m - 1$.
4) Errors in state preparation and measurements, i.e. $j_1 = 0$ and $j_2 = m$.

Errors in class 1 yield $\overline{s} = \overline{0}$ with probability at most 3/4. To prove this, we start by rewriting this probability as

$$\begin{aligned}\mathrm{prob}\big(\overline{s} = \overline{0} \mid \{P_j\}\big) = &\frac{1}{2(N_1 \times \cdots \times N_{m-1})} \sum_{\substack{t=0,1 \\ \mathcal{V}_1, \cdots, \mathcal{V}_{m-1}}} \langle + |^{\otimes n} \mathcal{H}^t \Bigg(\circ_{j=j_2}^{m-1} \mathcal{CX}_j \Bigg) \mathcal{V}_{j_2}^{-1} \mathcal{P}_{j_2} \mathcal{V}_{j_2} \\ &\circ \Bigg(\circ_{j=1}^{j_2-1} \mathcal{CX}_j \Bigg) \mathcal{H}^t \mathcal{P}_0 \big(\rho_{\text{in}}^{\text{trap}}\big) | + \rangle^{\otimes n} \\ = &\frac{1}{2(N_1 \times \cdots \times N_{m-1})} \sum_{\substack{t=0,1 \\ \mathcal{V}_1, \cdots, \mathcal{V}_{m-1}}} \langle + |^{\otimes n} \mathcal{H}^t \mathcal{V}_{j_2}^{-1} \mathcal{P}_{j_2} \mathcal{V}_{j_2} \Bigg(\circ_{j=1}^{j_2-1} \mathcal{CX}_j \Bigg) \mathcal{H}^t \mathcal{P}_0 \big(\rho_{\text{in}}^{\text{trap}}\big) | + \rangle^{\otimes n} \ ,\end{aligned} \tag{5.57}$$

where we used $cX \, |{+}{+}\rangle = |{+}{+}\rangle$ and $cX|00\rangle = |00\rangle$. We now start from the case $j_2 = 1$. We then note that (i) if $n = 1$ (single-qubit circuit), all $\mathcal{P}_1 \in \{\mathcal{X}, \mathcal{Y}, \mathcal{Z}\}$ and all $\mathcal{P}_0 = \mathcal{Z}$ lead to

$$\mathrm{prob}\big(\overline{s} = \overline{0} \mid \{P_j\}, \text{ 1 qubit}\big) = \frac{1}{2} \sum_{t=0,1} \frac{1}{N_1} \sum_{\mathcal{V}_1 \in \{\mathcal{H}, \mathcal{S}\}} \langle + | \mathcal{H}^t \mathcal{V}_1^{-1} \mathcal{P}_1 \mathcal{V}_1 \mathcal{H}^t \mathcal{P}_0 \big(\rho_{\text{in}}^{\text{trap}}\big) | + \rangle \leq \frac{3}{4} \ , \tag{5.58}$$

and (ii) if $n = 2$ (two-qubit circuit) and in band 1 the two qubits are connected by

cZ, all $\mathcal{P}_1 \neq \mathcal{I} \in \{\mathcal{I}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}\}^{\otimes 2}$ and all $\mathcal{P}_0 \neq \mathcal{I} \in \{\mathcal{I}, \mathcal{Z}\}^{\otimes 2}$ lead to

$$\begin{aligned}&\text{prob}\big(\overline{s} = \overline{0} \mid \{P_j\},\, 2\text{ qubits}\big)\\ =&\frac{1}{2N_1} \sum_{\substack{t=0,1\\ \mathcal{V}_1 \in \{\mathcal{H}\otimes\mathcal{S}, \mathcal{S}\otimes\mathcal{H}\}}} \langle + |^{\otimes 2} \mathcal{H}^t \mathcal{V}_1^{-1} \mathcal{P}_1 \mathcal{V}_1 \mathcal{H}^t \mathcal{P}_0 \big(\rho_{\text{in}}^{\text{trap}}\big) | + \rangle^{\otimes 2} \leq \frac{3}{4}\ . \end{aligned} \tag{5.59}$$

The above inequalities for $n = 1$ and $n = 2$ can be proven using that H maps $\{X, Y, Z\}$ into $\{Z, Y, X\}$ under conjugation and S maps $\{X, Y, Z\}$ into $\{Y, X, Z\}$ under conjugation (apart from unimportant global phases). Extension to more than two qubits is as follows: If $\text{prob}\big(\overline{s} = \overline{0} \mid \{P_j\}\ , n_0 \text{ qubits}\big) \leq 3/4$, then tensoring one more qubit yields

$$\begin{aligned}&\text{prob}\big(\overline{s} = \overline{0} \mid \{P_j\},\, n_0+1\text{ qubits}\big) =\\ &\frac{1}{2N_1} \sum_{\substack{t=0,1\\ \mathcal{V}_1}} \Big(\langle + |^{\otimes n_0} \mathcal{H}^t_{1,\dots,n_0} \mathcal{V}^{-1}_{1|1,\dots,n_0} \mathcal{P}_{1|1,\dots,n_0} \mathcal{V}_{1|1,\dots,n_0} \mathcal{H}^t_{1,\dots,n_0} \mathcal{P}_{0|1,\dots,n_0} \big(\rho_{\text{in}}^{\text{trap}}\big) | + \rangle^{\otimes n_0} \times\\ &\langle + | \mathcal{H}^t_{n_0+1} \mathcal{V}^{-1}_{1|n_0+1} \mathcal{P}_{1|n_0+1} \mathcal{V}_{1|n_0+1} \mathcal{H}^t_{n_0+1} \mathcal{P}_{0|n_0+1} \big(\rho_{\text{in}}^{\text{trap}}\big) | + \rangle \Big)\ ,\end{aligned} \tag{5.60}$$

where $\mathcal{H}^t_{1,\dots,n_0}, \mathcal{V}_{1|1,\dots,n_0}, \mathcal{P}_{1|1,\dots,n_0}$ and $\mathcal{P}_{0|1,\dots,n_0}$ are the components of $\mathcal{H}^t, \mathcal{V}_1, \mathcal{P}_1$ and $\mathcal{P}_0$ acting on qubits $\{1, \dots, n_0\}$ and $\mathcal{H}^t_{n_0+1}, \mathcal{V}_{1|n_0+1}, \mathcal{P}_{1|n_0+1}$ and $\mathcal{P}_{0|n_0+1}$ the components acting on qubit $n_0 + 1$. Using that if $A_h, B_h \geq 0\ \forall\ h$, then $\sum_h A_h B_h \leq \sum_h A_h \sum_h B_h$, we obtain

$$\begin{aligned}&\text{prob}\big(\overline{s} = \overline{0} \mid \{P_j\},\, n_0+1\text{ qubits}\big) \leq\\ &\frac{1}{2} \sum_{t=0,1} \frac{1}{N_1} \sum_{\mathcal{V}_1} \Big(\langle + |^{\otimes n_0} \mathcal{H}^t_{1,\dots,n_0} \mathcal{V}^{-1}_{1|1,\dots,n_0} \mathcal{P}_{1|1,\dots,n_0} \mathcal{V}_{1|1,\dots,n_0} \mathcal{H}^t_{1,\dots,n_0} \mathcal{P}_{0|1,\dots,n_0} \big(\rho_{\text{in}}^{\text{trap}}\big) | + \rangle^{\otimes n_0} \Big)\\ &\times \frac{1}{2} \sum_{t=0,1} \frac{1}{N_1} \sum_{\mathcal{V}_1} \Big(\langle + | \mathcal{H}^t_{n_0+1} \mathcal{V}^{-1}_{1|n_0+1} \mathcal{P}_{1|n_0+1} \mathcal{V}_{1|n_0+1} \mathcal{H}^t_{n_0+1} \mathcal{P}_{0|n_0+1} \big(\rho_{\text{in}}^{\text{trap}}\big) | + \rangle \Big)\\ &\leq \frac{3}{4} \times \frac{3}{4} \leq \frac{3}{4}\ ,\end{aligned} \tag{5.61}$$

Tensoring two qubits connected by cZ yields the same bound, and this concludes the proof by induction for $j_2 = 1$. If $j_2 \in \{1, \dots, m-1\}$ the proof is similar, but the Pauli operator $\mathcal{V}_{j_2}^{-1} \mathcal{P}_{j_2} \mathcal{V}_{j_2}$ must be commuted with $\mathcal{CX}_1, \dots, \mathcal{CX}_{j_2-1}$ (where we remember that each $\mathcal{CX}_j$ depends on $\mathcal{V}_j$). At fixed $\mathcal{V}_1, \dots, \mathcal{V}_{j_2-1}$ it can be shown (with the same arguments as used for $j_2 = 1$, i.e. considering first the cases $n = 1$ and $n = 2$ and then generalizing to $n > 2$) that summations over $\mathcal{V}_{j_2}$ and t yield an upper-bound of 3/4. The upper-bound on $\text{prob}\big(\overline{s} = \overline{0} \mid \{P_j\},\, n_0 + 1 \text{ qubits}\big)$ follows

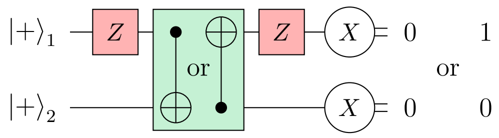


Figure 5.8: In this example, $\mathcal{P}_0 = \mathcal{P}_1 = Z_1$ (red gates) and $t = 0$. Due to identities 5.65, commuting $\mathcal{P}_1$ with the entangling gate (green box, cX gate with random orientation) make the two errors cancel out if qubit 1 is the control qubit. On the contrary, if qubit 1 is the target qubit, the errors do not cancel and cause a bit-flip of output s_1. Thus, for $t = 0$ these errors are detected with probability 1/2. The same can be proven for $t = 1$ using identities 5.66, as well as for all other errors $\mathcal{P}_0, \mathcal{P}_1$.

by summing over all possible values of $\mathcal{V}_1, \ldots, \mathcal{V}_{j_2-1}$.

Errors in class 2 yield $\overline{s} = \overline{0}$ with probability at most 3/4. This can be proven with the same arguments as for errors in class 1.

Errors in class 3 yield $\overline{s} = \overline{0}$ with probability at most 3/4. To see this, consider first the case where the errors affect neighboring bands ($j_2 = j_1 + 1$), which yields

$$\begin{aligned}&\text{prob}\big(\overline{s} = \overline{0} \mid \{\mathcal{P}_j\}\big)\\ =&\frac{1}{2}\sum_{t=0,1}\frac{1}{N_{j_1}N_{j_1+1}}\sum_{\mathcal{V}_{j_1},\mathcal{V}_{j_1+1}}\langle +|^{\otimes n}\mathcal{H}^t\mathcal{V}_{j_1+1}^{-1}\mathcal{P}_{j_1+1}\mathcal{V}_{j_1+1}\mathcal{V}_{j_1}^{-1}\mathcal{P}_{j_1}\mathcal{V}_{j_1}\mathcal{H}^t|+\rangle^{\otimes n} \leq \frac{3}{4}\end{aligned} \tag{5.62}$$

As for errors in class 1, this can be shown by proving that the bound holds for the single-qubit case and the two-qubit one, and then using induction. If the errors affect two non-neighboring bands ($j_2 \neq j_1 + 1$), we have

$$\begin{aligned}&\text{prob}\big(\overline{s} = \overline{0} \mid \{\mathcal{P}_j\}\big)\\ =&\frac{1}{2}\sum_{t=0,1}\frac{1}{N_{j_1}N_{j_2}}\sum_{\mathcal{V}_{j_1},\mathcal{V}_{j_2}}\langle +|^{\otimes n}\mathcal{H}^t\mathcal{V}_{j_2}^{-1}\mathcal{P}_{j_2}\mathcal{V}_{j_2}\Big(\circ_{j=j_1+1}^{j_2-1}\mathcal{CX}_j\Big)\mathcal{V}_{j_1}^{-1}\mathcal{P}_{j_1}\mathcal{V}_{j_1}\mathcal{H}^t|+\rangle^{\otimes n} \leq \frac{3}{4}\end{aligned} \tag{5.63}$$

To prove the inequality, one can commute $\mathcal{V}_{j_1}^{-1}\mathcal{P}_{j_1}\mathcal{V}_{j_1}$ (which is a Pauli operator) with the entangling operation and use the same arguments as for $j_2 = j_1 + 1$. □

Finally, errors in class 4 yield

$$
\begin{aligned}
&\mathrm{prob}\big(\bar{s}=\bar{0}\mid\{P_j\}\big)\\
=&\frac{1}{2(N_1\times\cdots\times N_{m-1})}\sum_{\substack{t=0,1\\ \mathcal{V}_1,\cdots,\mathcal{V}_{m-1}}}\langle+|^{\otimes n}\mathcal{P}_m\mathcal{H}^t\circ\left(\circ_{j=1}^{m-1}\mathcal{C}\mathcal{X}_j\right)\circ\mathcal{H}^t\mathcal{P}_0\big(\rho_{\mathrm{in}}^{\mathrm{trap}}\big)|+\rangle^{\otimes n}\leq\frac{1}{2}
\end{aligned}
\tag{5.64}
$$

To see this, consider first the case $t=0$, and consider commuting $\mathcal{P}_0\in\{\mathcal{I},\mathcal{Z}\}^{\otimes n}/\mathcal{I}$ with all the gates in the circuit. Since all these gates are cX gates with random orientation, the identities

$$
\begin{aligned}
cX(Z_1\otimes I_2)&=(Z_1\otimes I_2)cX\\
cX(I_1\otimes Z_2)&=(Z_1\otimes Z_2)cX\\
cX(Z_1\otimes Z_2)&=(I_1\otimes Z_2)cX
\end{aligned}
\tag{5.65}
$$

ensure that every time time that a Pauli-Z error is commuted with a cX, this error becomes another error, chosen at random from two possible ones—Figure 5.8. This can be used to prove that if $t=0$, errors in class 4 are detected with probability larger than 1/2. The same considerations apply to the case $t=1$, where the identities

$$
\begin{aligned}
cX(X_1\otimes I_2)&=(X_1\otimes X_2)cX\\
cX(I_1\otimes X_2)&=(I_1\otimes X_2)cX\\
cX(X_1\otimes X_2)&=(X_1\otimes I_2)cX
\end{aligned}
\tag{5.66}
$$

must be used instead of identities 5.65. □

Chapter 6

Improving the accreditation protocol based on empirical evidence on the noise

The accreditation protocol in Chapter 5 requires implementing circuits with no more qubits and gates than the target circuit. Thus, it is ready for implementation on current NISQ devices. However, before it can become useful for accreditation of computations that are classically non-simulable, our protocol requires that further improvements on the hardware be made (Section 5.4).

Other protocols (such as protocols based on tomography [33–35] and randomized benchmarking [36–45], protocols for noise modelling [48] and some protocols for error correction [87] and fault-tolerant quantum computing [27, 88]) typically assume less general noise models, such as Markovian and time-independent noise (Section 3.3). Importantly, recent experiments [16, 45] have provided empirical evidence that these noise models provide a good approximation of the experimental noise. Motivated by this empirical evidence, it is reasonable to ask how the accreditation protocol may be improved if a less general noise model is assumed.

6.1 Summary of the results

In this Chapter we present a modification to the accreditation protocol that we name "single-run accreditation protocol". In this modification, the accreditation protocol in Chapter 5 is implemented one time with $v \gg 1$ trap circuits. The

[1] This Chapter presents unpublished results.

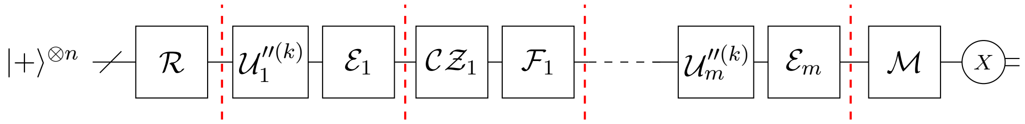


Figure 6.1: Schematic illustration of a noisy implementation of circuit $k \in \{1, \dots, v+1\}$ in the single-run accreditation protocol. All the boxes represent CPTP maps. $\mathcal{E}_j\mathcal{U}_j^{\prime\prime(k)}$ is a noisy implementation of the j-th round of single-qubit gates with gate-independent noise, $\mathcal{F}_j\mathcal{CZ}_j$ is a noisy implementation of the j-th round of cZ gates, $\mathcal{R}$ is the noise in state preparation and $\mathcal{M}$ is the noise in measurements.

single-run protocol returns the outputs of the target circuit and the number of traps $T_{\text{rej}} \in [0, v]$ that yield an incorrect output $\overline{s} \neq \overline{0}$.

We make the following assumptions about the noise (Figure 6.1):

A1. A noisy implementation of a unitary gate $\mathcal{G} : \rho \to G\rho G^\dagger$ is $\mathcal{E}_\mathcal{G}\mathcal{G}$, where $\mathcal{E}_\mathcal{G}$ is a (potentially gate-dependent) CPTP map.

A2. Rounds of single-qubit gates suffer gate-independent noise.

A3. Errors in a trap circuit never cancel with each other.

We show that under these assumptions, it is possible to upper-bound the variation distance of the outputs of the target circuit as

$$\frac{1}{2}\sum_{\overline{s}} \left|p_{\text{noiseless}}(\overline{s}) - p_{\text{noisy}}(\overline{s})\right| \leq 2\text{prob}(\overline{s} \neq \overline{0}) \ , \tag{6.1}$$

where $\{p_{\text{noiseless}}(\overline{s})\}$ and $\{p_{\text{noisy}}(\overline{s})\}$ are the noiseless and noisy probability distributions of the outputs and $\text{prob}(\overline{s} \neq \overline{0})$ is the probability that a trap returns an incorrect output. By Hoeffding's inequality we have $|\text{prob}(\overline{s} \neq \overline{0}) - T_{\text{rej}}/v| \leq \theta$ with confidence greater than $1 - 2\text{exp}\big(-2v\theta^2\big)$, where $\theta \in [0, 1]$ is a tunable parameter connecting the confidence to the bound. Therefore, we can bound the variation distance as

$$\frac{1}{2}\sum_{\overline{s}} \left|p_{\text{noiseless}}(\overline{s}) - p_{\text{noisy}}(\overline{s})\right| \leq 2(T_{\text{rej}}/v + \theta) \tag{6.2}$$

with confidence greater than $1 - 2\text{exp}\big(-2v\theta^2\big)$.

The single-run accreditation protocol is scalable and ready for implementation on NISQ devices, as well as the original accreditation protocol. Testing circuits rather than gates, it can detect noise that may be missed by the protocols based on tomography [33–35] and randomized benchmarking [36–45], such as spatially correlated or time-dependent noise. Moreover, with numerical studies presented in Section 6.3.1 we show that the single-run protocol provides a tighter bound on the variation distance than the original protocol (Figure 6.3). As a consequence, the single-run protocol requires lesser improvements on the hardware to become useful for accreditation of classically non-simulable computations (Figures 6.4).

Unlike the original accreditation protocol, the single-run protocol requires running a large number $v \gg 1$ of traps. This is because in the single-run protocol the aim is estimating prob($\overline{s} \neq \overline{0}$) via T_{rej}/v, hence many traps are required in order to obtain a *good* estimate. Instead, in the original accreditation protocol the output of the target is accepted only if *all* the traps return the correct output, hence large values of v yield prob(acc)$\approx$ 0 and useless bounds on the variation distance (cfr. Equation 5.5 on page 56).

The single-run accreditation protocol relies on the assumptions A1, A2 and A3, which are absent in the original accreditation protocol. A1 and A2 are standard assumptions for protocols centered around tomography [33–35] and randomized benchmarking [36–45] and are motivated by empirical evidence about experimental noise [16]. A3 is motivated by the observation that error cancellation in a trap circuit is likely to be a rare event, unless the quantum computer is actively trying to fool the user (Section 6.2.3).

We demonstrate the single-run accreditation protocol by implementing it on the IBMQ Ourense device [18]. We show that it correctly upper-bounds the variation distance of target circuits containing $2, 3$ and 4 qubits and up to 7 bands. Being scalable, ready for implementation and robust to noise models that are standardly assumed by other protocols, the single-run accreditation protocol represents the state-of-the-art of circuit characterization.

This Chapter is organized as follows. In Section 6.2 we provide a description of the single-run accreditation protocol and prove the bound in the inequality 6.2. In Section 6.3 we analyze the utility of the single-run accreditation protocol for NISQ devices. In Section 6.4 we provide the results of the experimental demonstration on IBMQ Ourense.

6.2 The single-run accreditation protocol

In this Section we present the single-run accreditation protocol and prove the main claims of the Chapter. We begin with a description of the protocol.

Box 6.1. Single-run accreditation protocol.

Input:

- A target circuit that takes as input n qubits in the state $|+\rangle$, contains only single-qubit gates and cZ gates arranged in m bands and ends with Pauli-X measurements (Figure 1.1).
- The number v of trap circuits, a number $\theta \in [0, 1]$.

Routine:

1. Choose a random number $v_0 \in \{1, \ldots, v + 1\}$ and define $\{U_{i,j}^{(v_0)}\} = \{U_{i,j}\}$, where $\{U_{i,j}\}$ is the set of single-qubit gates in the target circuit.

2. For $k = 1, \ldots, v + 1$: If $k \neq v_0$ (trap circuit), run Routine 4 and obtain the set of single-qubit gates $\{U_{i,j}^{(k)}\}$ for the k-th trap circuit.

3. For $k = 1, \ldots, v + 1$: Run Routine 3 and obtain $\{U_{i,j}^{\prime\prime(k)}\}$, together with the bit-string $(\alpha_{1,m}^{(k)}, \ldots \alpha_{n,m}^{(k)})$.

4. For $k = 1, \ldots, v + 1$:

   4.1 Create a state $\rho_{\text{in}} = \otimes_{i=1}^{n} |+\rangle_i \langle +|$.

   4.2 Implement circuit k with single-qubit gates from the set $\{U_{i,j}^{\prime\prime(k)}\}$ and obtain output $\overline{s}^{(k)} = (s_1^{(k)}, \ldots, s_n^{(k)})$. Next, for all $i = 1, \ldots, n$, recompute $s_i^{(k)}$ as $s_i^{(k)} \oplus \alpha_{i,m}^{(k)}$.

5. Initialize a number $T_{\text{rej}} = 0$. Then, for $k = 1, \ldots, v + 1$: if $\overline{s}^{(k)} \neq \overline{0}$ and $k \neq v_0$ (trap circuit), set $T_{\text{rej}} = T_{\text{rej}} + 1$.

Output: The output $\overline{s}^{(v_0)}$ of the target circuit and the number $2(T_{\text{rej}} + \theta)$.

6.2.1 Description of the protocol

The single-run accreditation protocol is provided in Box 6.1. It takes as input a classical description of the target circuit, the number v of trap circuits and a number $\theta \in [0,1]$. Steps 1-4 in the single-run protocol coincide with Steps 1-4 of the original accreditation protocol (Box 5.1). In Step 5, the routine is ended by counting the number $T_{\text{rej}} \in [0, v]$ of trap circuits that have returned an incorrect output $\overline{s} \neq \overline{0}$. Finally, the single-run protocol returns the outputs of the target circuit and the number $2(T_{\text{rej}}/v + \theta)$.

6.2.2 Proof of Inequality 6.2

In this Section we prove the bound in Inequality 6.2.

Proof. (Inequality 6.2). To obtain the bound in Inequality 6.2 we proceed as follows:

Step 1: We show that under assumptions A1 and A2, the total probability of error $p_e \in [0,1]$ in the target circuit equals that in the trap circuits[1].

Step 2: We show that under assumption A3, Hoeffding Inequality [86] allows bounding p_e as $p_e \leq 2(T_{\text{rej}}/v + \theta)$ with confidence greater than $1 - 2\text{exp}\big(-2v\theta^2\big)$.

Overall, indicating with $\rho_{\text{noisy}}^{(\text{target})}$ ($\rho_{\text{noiseless}}^{(\text{target})}$) the state of the system at the end of a noisy (noiseless) implementation of the target circuit, the steps above prove the following chain of inequalities:

$$\frac{1}{2}\sum_{\overline{s}} \big|p_{\text{noiseless}}(\overline{s}) - p_{\text{noisy}}(\overline{s})\big| = D\big(\rho_{\text{noiseless}}^{(\text{target})}, \rho_{\text{noisy}}^{(\text{target})}\big) \leq p_e \leq 2(T_{\text{rej}}/v + \theta) \ , \tag{6.3}$$

where the last inequality is satisfied with probability greater than $1 - 2\text{exp}\big(-2v\theta^2\big)$.

We now elaborate each of the above steps.

Step 1: Using A1, we write the state of the system at the end of the target circuit as

$$\rho_{\text{noisy}}^{(\text{target})} = \mathcal{M}\ \mathcal{E}_m \mathcal{U}_m \mathcal{F}_{m-1} c\mathcal{Z}_{m-1} \dots \mathcal{F}_1 c\mathcal{Z}_1 \mathcal{E}_1 \mathcal{U}_1 \mathcal{R}\big(\rho_{\text{in}}\big) \ , \tag{6.4}$$

where $\rho_{\text{in}} = \otimes_{i=1}^{n} |+\rangle_i\langle+|$, $\mathcal{R}$ is the noise in state preparation, $\mathcal{E}_j\mathcal{U}_j$ is a noisy implementation of the round of single-qubit gates in band j, $\mathcal{F}_j c\mathcal{Z}_j$ is a noisy implementation of the round of cZ gates in band j, $\mathcal{M}$ is the final measurement (measurement

[1] Note that the noise afflicting target and trap circuits can be treated as probabilistic Pauli errors, cfr. Lemma 4 (Twirling the noise) on page 63.

noise is inside $\mathcal{E}_m$). Using A2 we can rewrite $\rho_{\text{out}}^{(\text{target})}$ as

$$\rho_{\text{noisy}}^{(\text{target})} = \mathcal{M}\mathcal{E}_m\mathcal{U}_m\mathcal{F}'_{m-1}c\mathcal{Z}_{m-1}\ldots\mathcal{F}'_1c\mathcal{Z}_1\mathcal{U}_1\mathcal{R}\big(\rho_{\text{in}}\big) \ , \tag{6.5}$$

where $\mathcal{F}'_j = \mathcal{F}_jc\mathcal{Z}_j\mathcal{E}_jc\mathcal{Z}_j$, and where all the maps $\mathcal{R}, \mathcal{F}'_1, \ldots, \mathcal{F}'_{m-1}, \mathcal{E}_m$ do not depend on rounds of single-qubit gates.

The trap circuits contain the same input state, two-qubit gates and measurements as the target circuit. Therefore, using A1 and A2 a noisy implementation of a trap circuit yields

$$\rho_{\text{noisy}}^{(\text{trap})} = \mathcal{M}'\mathcal{E}_m\mathcal{W}_m\mathcal{F}'_{m-1}c\mathcal{Z}_{m-1}\ldots\mathcal{F}'_1c\mathcal{Z}_1\mathcal{W}_1\mathcal{R}\big(\rho_{\text{in}}\big) \ , \tag{6.6}$$

where $\mathcal{W}_j$ is the round of single-qubit gates in the j-th band of the trap and the CPTP maps $\mathcal{R}, \mathcal{F}'_1, \ldots, \mathcal{F}'_{m-1}, \mathcal{E}_m$ are the same as in Equation 6.5.

Applying the QOTP (Routine 3 in Chapter 5) to target and trap circuits we obtain

$$\rho_{\text{noisy}}^{(\text{target})} = \sum_{\mathcal{P}_0,\ldots,\mathcal{P}_m} \text{prob}(\mathcal{P}_0,\ldots,\mathcal{P}_m)\ \mathcal{M}\mathcal{P}_m\mathcal{U}_m\mathcal{P}_{m-1}c\mathcal{Z}_{m-1}\ldots\mathcal{P}_1c\mathcal{Z}_1\mathcal{U}_1\mathcal{P}_0\big(\rho_{\text{in}}\big) \tag{6.7}$$

$$\rho_{\text{noisy}}^{(\text{trap})} = \sum_{\mathcal{P}_0,\ldots,\mathcal{P}_m} \text{prob}(\mathcal{P}_0,\ldots,\mathcal{P}_m)\ \mathcal{M}\mathcal{P}_m\mathcal{W}_m\mathcal{P}_{m-1}c\mathcal{Z}_{m-1}\ldots\mathcal{P}_1c\mathcal{Z}_1\mathcal{W}_1\mathcal{P}_0\big(\rho_{\text{in}}\big) \ , \tag{6.8}$$

where $\mathcal{P}_0, \ldots, \mathcal{P}_m \in \{I, X, Y, Z\}^{\otimes n}$ are Pauli errors. Thus, the total probability of error $p_e = 1 - \text{prob}(\mathcal{I}, \ldots, \mathcal{I})$ in the target circuit is the same as that in the trap circuit.

Step 2: We rewrite $\text{prob}(\overline{s} \neq \overline{0})$ as

$$\text{prob}(\overline{s} \neq \overline{0}) = \sum_{k=1}^{m} \text{prob}(\overline{s} \neq \overline{0} \mid k\text{-band coll.}) \times \text{prob}(k\text{-band coll.}) \ , \tag{6.9}$$

where prob(k-band coll.) is the probability that a k-band collection of errors occurs (see Section 5.5.2 for a definition of k-band collection).

In Section 5.5.2 we showed that $\text{prob}(\overline{s} \neq \overline{0} \mid 1\text{-band coll.}) \geq 1/2$ (Statement 1 on page 77). For 2-band collection, under A3 (errors do not cancel) we can move the errors towards each other and merge them into a 1-band collection. Thus, due to Statement 1 we obtain $\text{prob}(\overline{s} \neq \overline{0} \mid 2\text{-band coll.}) \geq 1/2$. We can iterate this argument for all $k \in \{2, \dots, m\}$, finding $\text{prob}(\overline{s} \neq \overline{0} \mid k\text{-band coll.}) \geq 1/2$. This yields

$$\text{prob}(\overline{s} \neq \overline{0}) \geq \frac{1}{2} \sum_{k=1}^{m} \text{prob}(k\text{-band coll.}) = \frac{1}{2} p_e \tag{6.10}$$

and therefore $p_e \leq 2\text{prob}(\overline{s} \neq \overline{0})$.

Using Hoeffding's Inequality [86] we finally obtain

$$\text{prob}\left(\left| \text{prob}(\overline{s} \neq \overline{0}) - \frac{T_{\text{rej}}}{v} \right| \leq \theta \right) \geq 1 - 2\text{exp}\big(- 2v\theta^2 \big) \ , \tag{6.11}$$

which ensures that $p_e \leq 2\text{prob}(\overline{s} \neq \overline{0}) \leq 2(T_{\text{rej}}/v + \theta)$ with probability greater than $1 - 2\text{exp}\big(- 2v\theta^2 \big)$. □

6.2.3 Motivation for assumption A3

In this Section we provide evidence that error cancellation in a trap circuit is unlikely to happen. Specifically, we prove the following Theorem:

Theorem 8. *Consider a trap circuit containing n qubits and m bands. Consider the set of all 4^{nm} collections of Pauli errors $\mathcal{P}_0, \dots, \mathcal{P}_m$ that can possibly afflict the trap circuit (cfr. Equation 6.6). The fraction of collections of errors that cancel is smaller than $1/(4^n - 1)$.*

It must be noted that the statement of Theorem 8 is about the fraction of collections that cancel, not about the likelihood that errors effectively cancel. Indeed, a *malicious* quantum computer (such as the quantum computer held by a dishonest prover in verification protocols, cfr. Chapters 3 and 4) may actively introduce errors that cancel in the trap circuits. However, recent experimental evidence suggests that the noise in NISQ devices consists of uncorrelated errors [16]. Therefore, it seems reasonable to assume that NISQ devices are not malicious entities and that error cancellation in large trap circuits happens exponentially rarely.

We now provide a proof of Theorem 8:

Proof. (Theorem 8). We begin by observing that the total number of 1-band collections is $m(4^n - 1)$, however none of them cancels (Statement 1 in Chapter 5). Instead, for any $k \in \{2, \dots, m\}$, the total number of k-band collections of errors amounts to $\binom{m}{k}(4^n - 1)^k$, however only $\binom{m}{k}(4^n - 1)^{k-1}$ of these collections cancel. We now prove this claim for the case $k = 2$, then we generalize to $k > 2$.

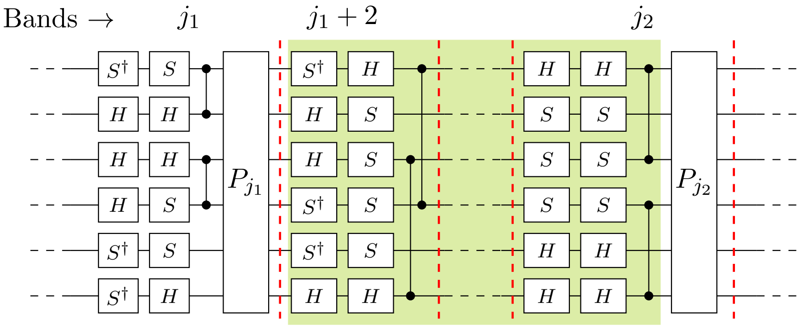

Bands →
j_1
$j_1 + 2$
j_2
$S^\dagger$ S $S^\dagger$ H H H
H H H S S S
H H H S S S
H S $S^\dagger$ S S S
$S^\dagger$ S $S^\dagger$ S H H
$S^\dagger$ H H H H H
P_{j_1}
P_{j_2}

Figure 6.2: Example of 2-band collection with errors in bands j_1 and j_2. The green box highlight the gates between the two errors, the composition of which is denoted by C.

Consider 2-band collections with errors in bands j_1 and j_2, where we assume $0 \leq j_1 < j_2 \leq m$ (Figure 6.2). Since $P_{j_1}, P_{j_2} \in \{I, X, Y, Z\}^{\otimes n}/I^{\otimes n}$, the total number of 2-band collections afflicting bands j_1 and j_2 is $(4^n - 1)^2$. Denote by C the composition of the gates in bands $j_1, \ldots, j_2$ (green box in Figure 6.2). Since C is a Clifford gate, P_{j_1} and P_{j_2} cancel if and only if $P_{j_2} = CP_{j_1}C^\dagger$, therefore only $4^n - 1$ collections cancel. Noting that there are $\binom{m}{2}$ possible choices of j_1 and j_2, the total number of 2-band collections of errors amounts to $\binom{m}{2}(4^n - 1)^2$, of which only $\binom{m}{2}(4^n - 1)$ cancel.

Generalization to $k > 2$ follows with similar arguments. Given a set of bands $j_1, \ldots, j_k$ (with $0 \leq j_1 < \ldots < j_k \leq m$), the total number of k-band collections of errors that may occur is $(4^n - 1)^k$, but it can be shown that only $(4^n - 1)^{k-1}$ cancel. Noting that there are $\binom{m}{k}$ possible choices of $j_1, \ldots, j_k$, the total number of k-band collections of errors amounts to $\binom{m}{k}(4^n - 1)^k$, of which only $\binom{m}{k}(4^n - 1)^{k-1}$ cancel.

Overall, we have

$$\begin{aligned}\frac{\text{number of collections that cancel}}{\text{total number of collections}} &= \frac{\sum\limits_{k=2}^{m} \binom{m}{k}(4^n - 1)^{k-1}}{m(4^n - 1)^n + \sum\limits_{k=2}^{m} \binom{m}{k}(4^n - 1)^k} \\ &\leq \frac{\sum\limits_{k=2}^{m} \binom{m}{k}(4^n - 1)^{k-1}}{\sum\limits_{k=2}^{m} \binom{m}{k}(4^n - 1)^k} = \frac{1}{4^n - 1} \qquad (6.12)\end{aligned}$$

□

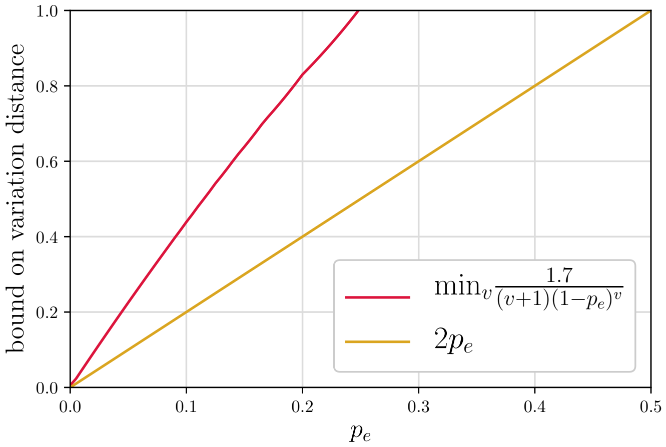


Figure 6.3: Best bound provided by the original protocol (red line) and worst-case bound provided by the single-run protocol (yellow line) as a function of the total probability of error $p_e \in [0, 1]$ in the target circuit. As it can be seen, the single-run accreditation protocol provides a smaller (hence, better) bound on the variation distance than the original protocol.

6.3 Utility of the single-run accreditation protocol

In this Section we analyze the utility of the single-run protocol for accreditation of classically non-simulable computations on NISQ devices.

6.3.1 Comparison with the original accreditation protocol

We begin by comparing the bounds on the variation distance provided by the single-run and by the original accreditation protocols as a function of the total probability of error $p_e \in [0, 1]$ in the target circuit. To do so, we now provide lower-bound and upper-bound on the number $2(T_{\text{rej}}/v + \theta)$ returned by the single-run protocol.

In Section 6.2.2 we have shown that $p_e \leq 2\text{prob}(\bar{s} \neq \bar{0})$, where $\text{prob}(\bar{s} \neq \bar{0})$ is the probability that a trap circuit returns an incorrect output (Equation 6.10). In turn, $\text{prob}(\bar{s} \neq \bar{0}) \leq p_e$ (the traps return an incorrect output only if an error has occurred). Thus,

$$p_e \leq 2\text{prob}(\bar{s} \neq \bar{0}) \leq 2p_e \ . \tag{6.13}$$

Since $\text{prob}(\bar{s} \neq \bar{0}) \approx T_{\text{rej}}/v$ for $v \gg 1$ (Equation 6.11), p_e and $2p_e$ respectively represent the best-case and worst-case upper-bounds on the variation distance provided by the single-run accreditation protocol.

In Figure 6.3 we plot $2p_e$ together with the best bound provided by the original accreditation protocol (Section 5.4). This shows that the single-run accred-

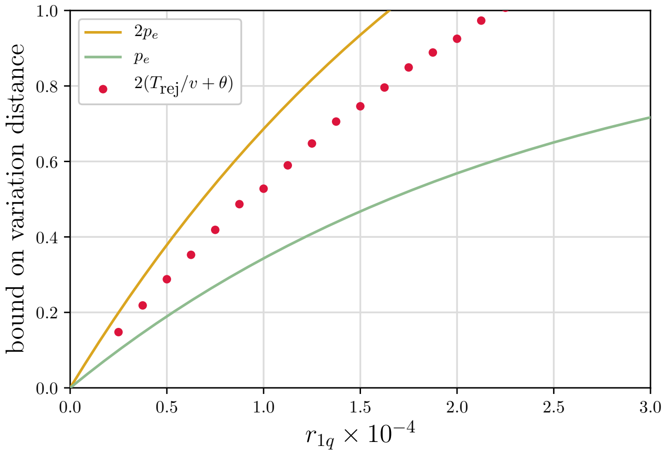


Figure 6.4: Results of our numerical studies. The red dots represent the value of $2(T_{\rm rej}/v+\theta)$ obtained with our classical simulations. We simulated $v = 18500$ noisy trap circuits (which are Clifford circuits and can be efficiently simulated classically, see Ref. [1–3] for algorithms) and calculated $T_{\rm rej}/v$. We set $\theta = 0.01$ (confidence higher than 95%). Green and yellow lines respectively represent p_e and $2p_e$ and are obtained using Equation 6.14.

itation protocol always provides tighter bounds on the variation distance than the original protocol.

6.3.2 Simulation for target circuit with 60 qubits and 22 bands

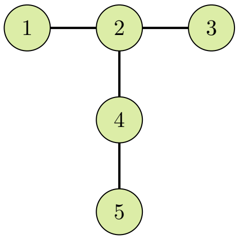
We now simulate a protocol run with target computation containing $n = 60$ qubits and $m = 22$ bands. In the simulations we assume that all the single-qubit gates introduce a single-qubit Pauli error with probability r_{1q}, all the two-qubit gates introduce a two-qubit Pauli error with probability r_{2q} and SPAM errors occur with probability r_s. We set $r_{2q} = 4r_{1q}$ and $r_s = 20r_{1q}$, as in Google Sycamore (Table 1.1).

The results of the simulations are illustrated in Figure 6.4. The red points represent the quantity $2(T_{\rm rej}/v + \theta)$ obtained by classically simulating $v = 18500$ noisy trap circuits and by setting $\theta = 0.01$ (which gives confidence higher than 95% on the bound). As expected (Section 6.3.1), these points lie between p_e and $2p_e$, where

$$p_e = 1 - \Big(1 - r_{1q}\Big)^{60\times 22}\Big(1 - 4r_{1q}\Big)^{20\times 21}\Big(1 - 20r_{1q}\Big)^{60} \qquad (6.14)$$

is the probability of error in the target circuit.

Since the variation distance is below 1 by definition (cfr. page 12), as in the previous Chapter we say that our protocol is *useful* if it provides a bound on the



(a)

One-qubit errors	Two-qubit errors	SPAM errors
Q1: 4.07×10^{-4}	Q1-Q2: 6.18×10^{-3}	Q1: 0.023
Q2: 3.17×10^{-4}	Q2-Q3: 3.17×10^{-3}	Q2: 0.022
Q3: 2.64×10^{-4}	Q2-Q4: 10.43×10^{-3}	Q3: 0.028
Q4: 5.53×10^{-4}	Q4-Q5: 6.75×10^{-3}	Q4: 0.03
Q5: 3.37×10^{-4}		Q5: 0.038

(b)

Figure 6.5: IBMQ Ourense. **(a)** Schematic illustration of the architecture. The circles represent the qubits, the edges represent the two-qubit gates. The qubits are initialized in the state $|0\rangle$ and measured in the Pauli-Z basis. Native two-qubit gates are cX gates. **(b)** Gate errors and SPAM errors (as of February 19th, 2020).

variation distance below 1 (i.e., $2(T_{\text{rej}} + \theta) < 1$), otherwise we say that it is *useless*. Figure 6.4 indicates that our single-run protocol is useful if $r_{1q} \lesssim 2 \times 10^{-4}$. This is ≈ 8 times smaller than the error rate of Google Sycamore (where $r_{1q} \approx 1.5 \times 10^{-3}$, see Table 1.1 on page 2). This provides a significant improvement over the original accreditation protocol, which will become useful if the error rates are decreased by a factor of ≈ 20 (Section 5.4 on page 66).

6.4 Experimental implementation on IBMQ Ourense

In this Section we present the results of the experimental implementation of the single-run accreditation protocol on IBMQ Ourense, a quantum computer available online on IBM's website [18]. IBMQ Ourense contains 5 superconducting qubits arranged in a T-shaped configuration (Figure 6.5). The qubits are initialized in the state $|0\rangle$ and can be individually addressed with arbitrary single-qubit gates or entangled with their nearest neighbor(s). The measurements are performed in the Pauli-Z basis.

We implement the single-run accreditation protocol for target circuits of two different types. The first type generates an n-qubit Greenberger–Horne–Zeilinger (GHZ)

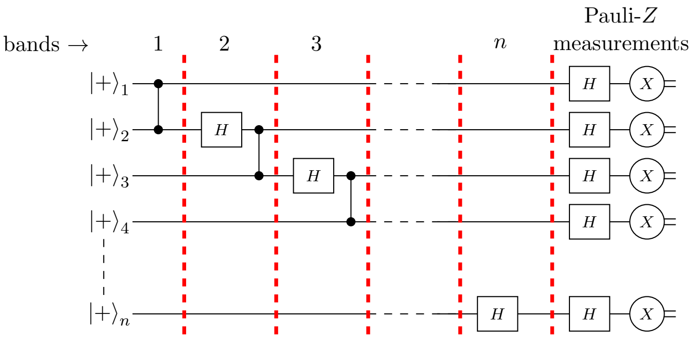


Figure 6.6: Circuit that prepares an n-qubit GHZ state and measures all the qubits in Pauli-Z basis.

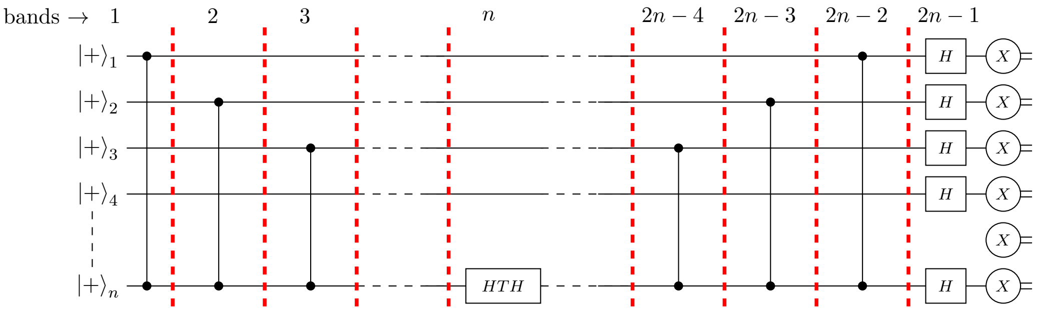


Figure 6.7: Circuit that implements the unitary evolution $\exp(-i\frac{\pi}{4}Z_1 \otimes \ldots \otimes Z_{n-1})$ on $n-1$ qubits in the state $|+\rangle$ (qubit n is an ancilla).

state [89], namely a state of the form $(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})/\sqrt{2}$, and finally measures each qubit in the Pauli-Z basis (Figure 6.6). The noiseless probability distribution of the outputs is

$$\{p_{\text{noiseless}}(\overline{s})\} = \{0.5 \text{ for } \overline{s} = (0,\ldots,0),(1,\ldots,1),\ 0 \text{ for all other } \overline{s}\}. \tag{6.15}$$

The second type of circuits (Figure 6.7) implements the unitary evolution $\exp(-i\frac{\pi}{4}Z_1 \otimes \ldots \otimes Z_{n-1})$ on $n-1$ qubits in the state $|+\rangle$ (qubit n is used as an ancilla) [69]. The noiseless probability distribution of the outputs is

$$\{p_{\text{noiseless}}(\overline{s})\} = \{0.5 \text{ for } \overline{s} = (0,\ldots,0,0),(1,\ldots,1,0),\ 0 \text{ for all other } \overline{s}\}. \tag{6.16}$$

These two types of circuits provide a florid ground for testing the single-run accreditation protocol. Since the noiseless probability distribution of their outputs is known *a priori*, it is possible (i) to calculate the variation distance between noiseless and

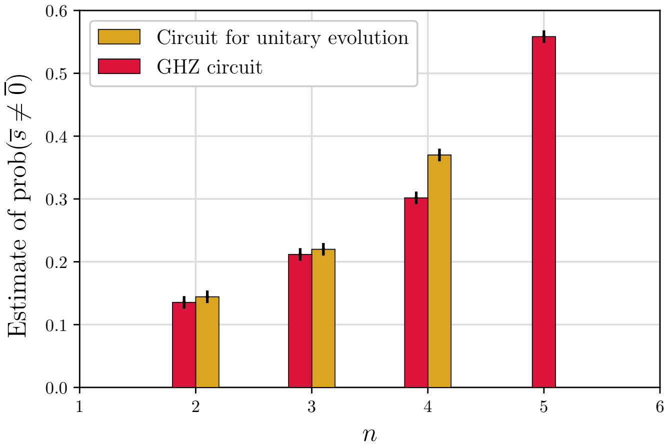


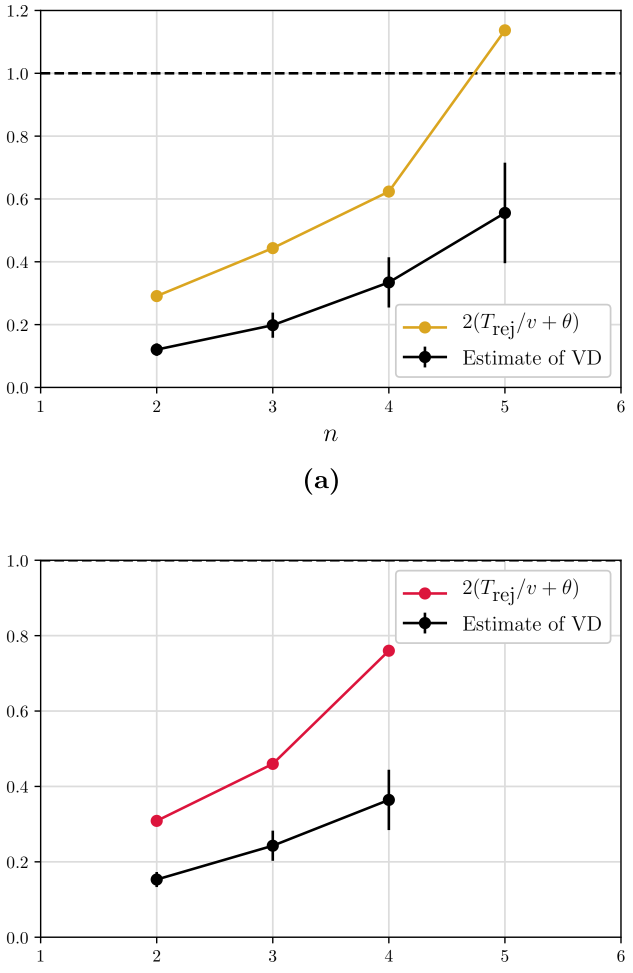
Figure 6.8: Estimates of prob($\overline{s} \neq \overline{0}$) for the circuit in Figure 6.6 (red bars) and for the circuit in Figure 6.7 (yellow bars) as a function of the number n of qubits. The bars represent T_{rej}/v obtained by implementing $v = 18500$ unique trap circuits on IBMQ Ourense. The error bars are equal to $\theta = 0.01$ (which gives confidence greater than 95%, Equation 6.11).

noisy probability distributions of the outputs *without using the accreditation protocol* and (ii) to verify that the accreditation protocol correctly upper-bounds this variation distance.

We begin by plotting the estimates of prob($\overline{s} \neq \overline{0}$) for the various circuits, obtained by implementing $v = 18500$ unique trap circuits and by calculating T_{rej}/v (Figure 6.8). Noting that the circuit for unitary evolution contains twice as many gates as the GHZ circuit (Figures 6.6 and 6.7), it can be seen that the number of qubits has a larger impact on prob($\overline{s} \neq \overline{0}$) than the number of gates. The reason may be that state preparation and measurements introduce more noise than the gates, as indicated by the calibration data (Table in Figure 6.5).

In Figure 6.9 we plot the estimates of the variation distance of the outputs of the various target circuits and the corresponding upper-bounds provided by the single-run accreditation protocol. Estimating the variation distance in Figure 6.9 requires estimating the probability distribution $\{p_{\text{noisy}}(\overline{s})\}$ of the experimental outputs. To do so, we implement each target circuit $v' \gg 1$ times and calculate the frequency $f(\overline{s})$ of each output $\overline{s}$. Hoeffding's inequality ensures that

$$\text{prob}\left(\left| p_{\text{noisy}}(\overline{s}) - f(\overline{s}) \right| \leq \theta' \right) \geq 1 - 2\exp(-2v'\theta'^{\,2}) \quad \text{for all } \overline{s}. \tag{6.17}$$



(a)

(b)

Figure 6.9: Estimates of the variation distance (black points) and upper-bound on the variation distance provided by the single-run accreditation protocol (yellow and red points) for **(a)** an n-qubit circuit of the type in Figure 6.6 **(b)** an n-qubit circuit of the type in Figure 6.7. The estimates of the variation distance are obtained by implementing each target circuit $v' = 37000$. Their error bars are equal to $2^n\theta'/2$ with $\theta' = 0.01$ (which gives confidence greater than 95%, Equation 6.18). The upper-bounds on the variation distance are obtained by implementing $v = 18500$ unique trap circuits and by setting $\theta = 0.01$ (which gives confidence greater than 95%, Equation 6.11). The figures show that our protocol correctly upper-bounds the variation distance of all the circuits considered.

Therefore, with confidence greater than $(1-2\exp(-2v'\theta'^{\,2}))^{2^n}$ we have

$$\begin{aligned}\left|\frac{1}{2}\sum_{\overline{s}}\left|p_{\text{noiseless}}(\overline{s})-p_{\text{noisy}}(\overline{s})\right|-\frac{1}{2}\sum_{\overline{s}}\left|p_{\text{noiseless}}(\overline{s})-f(\overline{s})\right|\right| &\leq \frac{1}{2}\sum_{\overline{s}}\left|p_{\text{noisy}}(\overline{s})-f(\overline{s})\right| \\ &\leq \frac{2^n\theta'}{2}\ .\end{aligned} \tag{6.18}$$

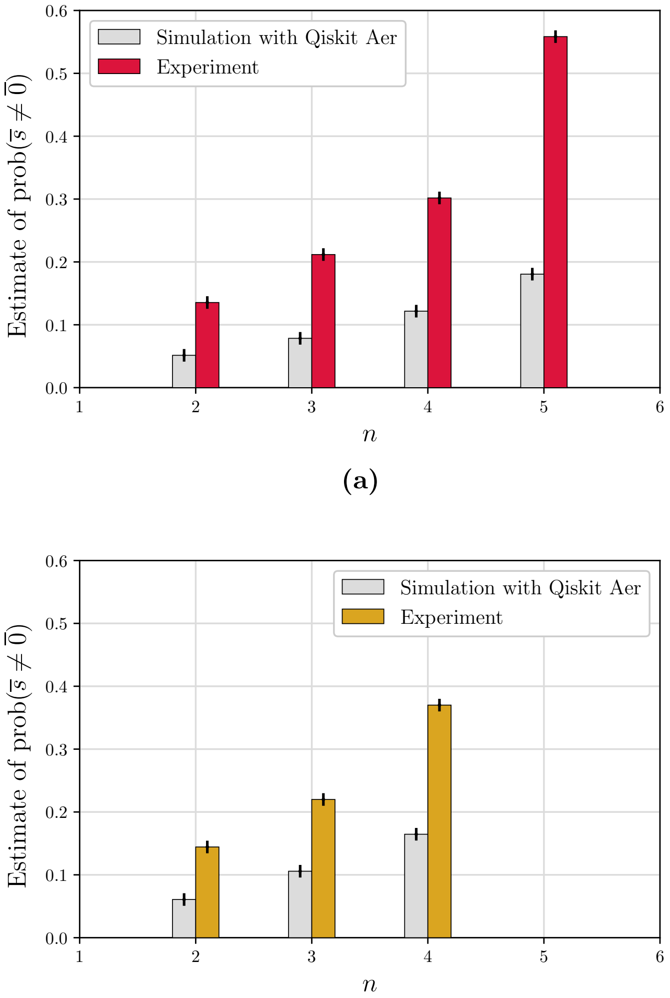
As it can be seen in Figure 6.9, our protocol correctly upper-bounds the variation distance for all the circuits containing $n=2,3,4$ qubits. For the circuit with $n=5$ (Figure 6.9a) it provides a trivial upper-bound, since the variation distance is smaller than 1 by definition [69].

Note that in Figure 6.9, each upper-bound is roughly twice as large as the corresponding estimate of the variation distance. Again, this may be explained by the fact that state preparation and measurements introduce more noise than the gates. To see this, let us assume that gate errors can be neglected. In this case:

1. SPAM errors flip some of the measurement outputs of the target circuits. Thus, for circuits of the type in Figures 6.6 and 6.7 (i.e., circuits for which $p_{\text{noiseless}}(\overline{s})$ is non-zero only for *few* outputs $\overline{s}$), $p_{\text{noisy}}(\overline{s})=(1-a)p_{\text{noiseless}}(\overline{s})+aq(\overline{s})$, where $a\approx p_e$ is the total probability of error in the circuit (defined in Section 6.2.2) and $\frac{1}{2}\sum_{\overline{s}}|p_{\text{noiseless}}(\overline{s})-q(\overline{s})|=1$. Therefore,
$$\frac{1}{2}\sum_{\overline{s}}\left|p_{\text{noiseless}}(\overline{s})-p_{\text{noisy}}(\overline{s})\right|=\frac{a}{2}\sum_{\overline{s}}\left|p_{\text{noiseless}}(\overline{s})-q(\overline{s})\right|\approx p_e\ . \tag{6.19}$$

2. Under assumption A3 (errors never cancel), SPAM errors are always detected by the traps (cfr. Statement 1 in Section 5.5.2). Therefore, $p_e=\text{prob}(\overline{s}\neq\overline{0})$ and the single-run accreditation protocol outputs $2T_{\text{rej}}/v\approx 2p_e$.

Thus, high levels of SPAM noise may be the reason why in Figure 6.9 the upper-bounds are twice as large as the corresponding estimates of the variation distance.



(a)

(b)

Figure 6.10: Estimates of prob($\overline{s} \neq \overline{0}$) for **(a)** an n-qubit circuit of the type in Figure 6.6 **(b)** an n-qubit circuit of the type in Figure 6.7. The gray bars represent T_{rej}/v obtained by classical simulating $v = 18500$ unique trap circuits on Qiskit Aer. The error bars are equal to $\theta = 0.01$ (which gives confidence greater than 95%, Equation 6.11). The red bars are those in Figure 6.8.

To conclude, we simulate the single-run accreditation protocol on Qiskit Aer, a high performance simulator provided by IBM [18]. Qiskit Aer models the experimental noise based upon the calibration data [90]. Specifically, it models the noise of single-qubit (two-qubit) gates as a single-qubit (two-qubit) depolarizing channel followed by thermal relaxation, in such a way that the gate infidelity is equal to the corresponding gate error obtained in the calibration. Moreover, it models SPAM noise as classical bit-flips of the measurement outputs, in such a way that each output is flipped with probability equal to the corresponding SPAM error obtained in the calibration.

In Figure 6.10 we compare the estimates of prob($\overline{s} \neq \overline{0}$) obtained experimentally with those obtained by using Qiskit Aer. As it can be seen, the estimates obtained in the experiments are significantly higher than those obtained with Qiskit Aer. This offers evidence that IBMQ Ourense is afflicted by noise that is missed when the gates are benchmarked individually, but is correctly captured by our trap circuits. For example a source of errors that is neglected by the Qiskit Aer simulator is cross-talk between qubits (i.e., unwanted interactions among the qubits being processed), which in recent works [91, 92] has been identified as a significant source of errors on IBMQ devices. Overall, our protocol provides a pathway to detect cross-talks, as well as other types of noise (such as system-environment interactions and time-dependent noise) that are missed by the standard noise characterization protocols.

Chapter 7

From accreditation back to verification

Inspired by verification protocols, in Chapter 5 we have provided an accreditation protocol that is ready for implementation on NISQ devices. Going full-circle, in this Chapter we investigate whether the accreditation protocol may inspire novel verification protocols. The objective of this investigation is two-fold. First, understanding why verification protocols require quantum overhead and the accreditation protocol does not. Second, understanding whether the accreditation protocol may be of use in future scenarios of delegated quantum computing.

7.1 Summary of the results

In this Chapter we provide a verification protocol (which we call "mesothetic" verification protocol, from the Greek *being in the middle*) where Alice and Bob follow the instructions of the accreditation protocol in Chapter 5. In the mesothetic protocol, Alice implements the single-qubit gates in the various circuits (target and trap) and Bob executes all the other operations (state preparation, measurements and two-qubit gates). Importantly, Alice must be able to implement all the single-qubit in each band *simultaneously*, i.e., she must possess an n-qubit memory (where n is the number of qubits in the target computation).

Being based on the accreditation protocol, the mesothetic protocol requires implementing computations with no more qubits and gates than the target computa-

[1] This Chapter presents the results of Appendix D of Ferracin, Kapourniotis, Datta, *Accrediting outputs of noisy intermediate-scale quantum computing devices*, New J. Phys. 21 113038 (2019).

tion, thus minimizing the requirements on Bob's side. However, the requirements on Alice's side are greater than in prepare-and-send [49–54, 84] or receive-and-measure [55–59] protocols, where Alice only requires a single-qubit memory. This suggests the possibility that protocols optimized for experiments (i.e., with no quantum overhead) may translate into more demanding verification protocols (i.e., with more requirements on Alice's side) and vice-versa.

Similarly to post-hoc verification protocols [56, 65], the mesothetic protocol is not blind. Indeed, Alice leaks crucial information to Bob regarding the target circuit, such as the position of the two-qubit gates. However, blindness may be required to protect the privacy of users in future delegated quantum computations [93]. Thus, we show how to turn the mesothetic protocol into a blind protocol. This requires recompiling the target circuit into a circuit with a fixed pattern of cZ gates (Figure 7.2), yielding an increase in circuit depth. Thus, the minimal overheads of the protocol must be traded in exchange for blindness.

This Chapter is organized as follows. In Section 7.2 we describe the mesothetic protocol and calculate completeness and soundness. In Section 7.3 we explain how it can be turned into a blind protocol. All the necessary definitions can be found in Section 4.2.

7.2 The mesothetic protocol

In this Section we describe the mesothetic protocol, which is provided in Box 7.1. We then calculate the completeness and soundness of the protocol.

7.2.1 Description of the protocol

We assume that Alice wants to implement a circuit of the type of Figure 1.1 with n qubits and m bands. We also assume that Alice owes a device that can receive n qubits from Bob, implement a single-qubit gate on each of them and send the qubits back to Bob. Alice's device must be able to implement all the single-qubit gates contained in the target circuit, together with $H, S, S^\dagger$ (used in trap circuits) and X, Y, Z (used for the QOTP).

The mesothetic protocol takes as input a description of the target circuit and the number v of trap circuits. After revealing to Bob the position of the cZ gates in the target circuit, in Step 1 Alice chooses a random number $v_0 \in \{1, \dots, v+1\}$ indicating what circuit will implement the target. In Step 2 she chooses the single-qubit gates for the trap circuits. Next, in Step 3 she adds the QOTP to the single-qubit gates in all the circuits.

Box 7.1. Mesothetic verification protocol.

Input:

A classical description of the target circuit and the number v of traps.

Routine:

1. Alice reveals to Bob the number of traps v and the position of the cZ gates in the target circuit. Next, Alice randomly chooses what circuit $v_0 \in \{1, \dots, v+1\}$ will be used to implement the target. Finally, she defines $\{U_{i,j}^{(v_0)}\} = \{U_{i,j}\}$, where $\{U_{i,j}\}$ is the set of single-qubit gates in the target circuit.

2. For $k \in \{1, \dots, v+1\}$: If $k \neq v_0$ (trap circuit), Alice runs Routine 4 (page 61) and obtains the set $\{U_{i,j}^{(k)}\}$ of single-qubit gates for the k-th circuit.

3. For $k \in \{1, \dots, v+1\}$: Alice runs Routine 3 (page 60) and obtains the set of gates $\{U_{i,j}''^{(k)}\}$, together with the random bits $\alpha_{i,m}^{(k)}$.

4. For all $k \in \{1, \dots, v+1\}$, Alice and Bob interact as follows:

   4.1 Bob creates n qubits in state $|+\rangle$.

   4.2 For $j \in \{1, \dots, m\}$:

      4.2.1 Bob sends all the qubits to Alice. For $i = 1, \dots, n$, Alice executes $U_{i,j}''^{(k)}$ on qubit i. Finally, Alice sends all the qubits back to Bob.

      4.2.2 Bob applies the entangling gates $\widehat{cZ}_j$ contained in the j-th band of the target circuit.

   4.3 For $i \in \{1, \dots, n\}$: Bob measures qubit i in the Pauli-X basis and stores the measurement output $s_i^{(k)}$.

5. For all $k \in \{1, \dots, v+1\}$, for all $i \in \{1, \dots, n\}$: Bob reveals to Alice the value of $s_i^{(k)}$. If if $\alpha_{i,m}^{(k)} = 1$, Alice bit-flips $s_i^{(k)}$.

6. Alice initializes a flag bit to the state $|\text{acc}\rangle = |0\rangle$. Next, for all $k = 1, \dots, v+1$: if $k \neq v_0$ (trap circuit) and $s_i^{(k)} \oplus \alpha_{i,m}^{(k)} \neq 0$ for some $i \in \{1, \dots, n\}$, Alice sets the flag bit to $|\text{rej}\rangle = |\text{acc} \oplus 1\rangle$.

Output: The outputs of the target circuit and the flag bit.

In Step 4 Alice and Bob implement all the $v+1$ circuits. To do so, they interact as follows: For all circuits $k \in \{1, \ldots, v+1\}$, in Step 4.1 Bob creates n qubits in the state $|+\rangle$. In Step 4.2, for each band $j \in \{1, \ldots, m\}$, Bob sends all the qubits to Alice; Alice implements the rounds of single-qubit gates $\otimes_{i=1}^{n} U_{i,j}^{(k)}$ and sends the qubits back to Bob; Bob implements $\widehat{cZ}_j$. In Step 4.3 Bob measures all the qubits in circuit k.

In Step 5 Bob sends Alice the results of the measurements and Alice recovers the bit-flips caused by the QOTP. Finally, in Step 6 Alice checks the outputs of the trap circuits. If all the traps output $\overline{s} = \overline{0}$, she accepts the output of the target circuit, otherwise she rejects it.

7.2.2 Completeness and soundness

We begin by computing completeness and soundness assuming that Alice's device is noiseless.

Theorem 9. *Suppose that Alice's device is noiseless. Then, for any number $v \geq 3$ of trap circuits, the mesothetic protocol is (δ, ε)-verifiable with*

$$\delta = 1 \ \text{ and } \ \varepsilon = \frac{\kappa}{v+1} \ , \tag{7.1}$$

where $\kappa = 3(3/4)^2 \approx 1.7$.

The proof of Theorem 9 relies on the following Lemma:

Lemma 6. *Suppose that Alice's device is noiseless. Summed over the random numbers $\alpha_{i,j}^{(k)}$, $\alpha_{i,j}^{\prime\,(k)}$ and $\gamma_{i,j}^{(k)}$, the state of system in Alice's register at the end of the protocol is of the form*

$$\begin{aligned}
&\rho_{\text{out}}\big(\mathcal{U}_1^{(1)}, \ldots, \mathcal{U}_m^{(v+1)}\big) \\
&= \sum_{\overline{s}^{(1)}, \ldots, \overline{s}^{(v+1)}} \ \sum_{\mathcal{P}_0^{(1)}, \ldots, \mathcal{P}_m^{(v+1)}} \frac{\text{prob}\big(\mathcal{P}_0^{(1)}, \ldots, \mathcal{P}_m^{(v+1)}\big)}{2^{n(v+1)}} \times \\
&\bigotimes_{k=1}^{v+1} \langle + |^{\otimes n} \left[\mathcal{Z}^{\overline{s}^{(k)}} \mathcal{P}_m^{(k)} \mathcal{U}_m^{(k)} \circ_{j=1}^{m-1} \left(\mathcal{CZ}_j \mathcal{P}_j^{(k)} \mathcal{U}_j^{(k)} \right) \circ \mathcal{P}_0^{(k)} \big(\rho_{\text{in}}\big) \right] | + \rangle^{\otimes n} \times \\
&\left(\otimes_i \, Z_i^{s_i^{(k)}} \, |+\rangle_i \langle + | Z_i^{s_i^{(k)}} \right)
\end{aligned} \tag{7.2}$$

where $\rho_{\text{in}} = \otimes_i |+\rangle_i \langle +|$, $\overline{s}^{(k)} = (s_1^{(k)}, \ldots, s_n^{(k)})$ is a binary string representing the output of the k-th circuit, $\mathcal{Z}^{\overline{s}^{(k)}}(\rho) = \otimes_i Z_i^{s_i^{(k)}} \rho Z_i^{s_i^{(k)}}$ and $\text{prob}\big(\mathcal{P}_0^{(1)}, \ldots, \mathcal{P}_m^{(v+1)}\big)$ *is*

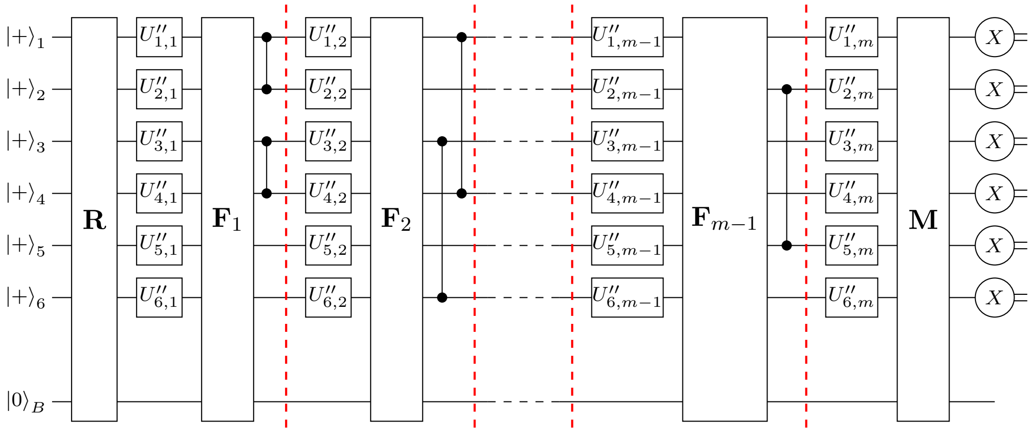


Figure 7.1: Implementation of the 6-qubit target circuit by Alice and dishonest Bob. Bob's deviations in state preparation are described by the unitary $\mathbf{R}$, those in the measurements by $\mathbf{M}$, those in the cZ-gates in a band $j = 1, \ldots, m-1$ by $\mathbf{F}_j$. All these unitaries act simultaneously on the system and on the environment (initially in the state $|0\rangle_B$).

the joint probability of a collection of Pauli errors $\mathcal{P}_0^{(1)}, \ldots, \mathcal{P}_m^{(v+1)}$ affecting the system, with $\mathcal{P}_1^{(k)}, \ldots, \mathcal{P}_{m-1}^{(k)} \in \{\mathcal{I}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}\}^{\otimes n}$ and $\mathcal{P}_0^{(k)}, \mathcal{P}_m^{(k)} \in \{I, \mathcal{Z}\}^{\otimes n}$ for all k.

Lemma 6 states that *on average* (i.e, summed over all the random numbers), the state in Alice's register at the end of the protocol is equivalent to the state that she gets when Bob is honest, but his quantum computer is afflicted by Pauli errors. This holds independent of the specific way in which Bob deviates from the instructions. Lemma 6 can thus be seen as the counterpart of Lemma 4.

We now prove Lemma 6, next we prove Theorem 9.

Proof. (Lemma 6). We start by proving the lemma for the case where Alice and Bob implement a single circuit ($v = 0$), next we generalise to multiple circuits ($v > 0$). Representing Bob's deviations as unitary matrices acting on the system and on a private register held by Bob, the state in Bob's register at the beginning of Step 4.2 (i.e., before Bob measures the qubits) is of the form (Figure 7.1)

$$\rho(\mathcal{U}_1'', \ldots, \mathcal{U}_m'') = \mathbf{M}\, U_m'' \widehat{cZ}_{m-1} \mathbf{F}_{m-1} U_{m-1}'' \ldots \widehat{cZ}_1 \mathbf{F}_1 U_1'' \mathbf{R} \Big(\rho_{\text{in}} \otimes |0\rangle_B\langle 0| \Big) \mathbf{R}^\dagger \ldots \mathbf{M}^\dagger \,, \tag{7.3}$$

where $\rho_{\text{in}} = \otimes_{i=1}^n |+\rangle_i\langle +|$, $|0\rangle_B$ is the initial state of Bob's private register, $U_j'' = \otimes_{i=1}^n U_{i,j}''$ are the gates implemented by Alice, the unitary matrix $\mathbf{R}$ represents Bob's deviations in state preparation, the unitary matrix $\mathbf{M}$ represents Bob's deviations before the measurements and $\widehat{cZ}_j \mathbf{F}_j$ is a dishonest implementation of the entangling gates in a band j.

Tracing out Bob's private register, we obtain the same state as on the r.h.s. of Equation 5.27. Thus, with the same calculations as in Lemma 4, we can prove that when Bob sends the measurement outputs to Alice and Alice undoes the QOTP (Step 5), the state in Alice register is of the form of Equation 7.2. This proves Lemma 6 for the case $v = 0$.

To generalize to multiple circuits ($v > 0$), we start by noticing that the circuits are implemented in series, hence Bob's deviations can only affect one circuit at a time. Starting from here and using the same arguments as for $v = 0$, one can finally obtain Equation 7.2. □

We can now prove Theorem 9:

Proof. (Theorem 9). Completeness $\delta = 1$ follows from the fact that Alice and Bob are implementing the accreditation protocol, which (in the absence of deviations) always returns the correct output of the target and flag bit in the state $|\text{acc}\rangle$ (Section 5.3.1).

To prove soundness $\varepsilon = \kappa/(v+1)$, we begin by using the Lemma 6, which states that all the deviations by Bob reduce to Pauli errors. We then calculate the probability $p(E_1 \wedge E_2|\widetilde{v})$ of the events E_1 *the Pauli errors afflict the target circuit* and E_2 *the Pauli errors are not detected by the traps* when the Pauli errors afflicts $\widetilde{v}$ circuits. This probability equals

$$p(E_1 \wedge E_2|\widetilde{v}) = p(E_1|\widetilde{v})p(E_2|E_1 \wedge \widetilde{v}) \tag{7.4}$$

Since the probability associated to each collection of Pauli errors does not depend on the choice of single-qubit gates (cfr. Lemma 6), the Pauli errors have probability $p(E_1|\widetilde{v}) = \widetilde{v}/(v+1)$ of afflicting the target circuit. Moreover, due to Lemma 5 we have

$$p(E_2|E_1 \wedge \widetilde{v}) \leq \left(\frac{3}{4}\right)^{\widetilde{v}-1} \tag{7.5}$$

Finally, maximizing $p(E_1 \wedge E_2|\widetilde{v})$ over $\widetilde{v}$ yields

$$\varepsilon = \max_{\widetilde{v}} \; p(E_1 \wedge E_2|\widetilde{v}) \approx \frac{1.7}{v+1}, \text{ for } \widetilde{v} = 3. \tag{7.6}$$

□

We now compute completeness and soundness in the case where Alice's device suffers bounded noise (potentially gate-dependent):

Theorem 10. *Suppose that Alice's device is affected by bounded noise, i.e. that for all circuits $k \in \{1, \dots, v+1\}$ and bands $j \in \{1, \dots, m\}$ she applies $\mathcal{E}_j^{(k)}\mathcal{U}_j^{(k)}$, where $\mathcal{E}_j^{(k)} = (1-r_j^{(k)})\mathcal{I} + r_j^{(k)}\mathcal{E'}_j^{(k)}$ for some arbitrary CPTP-map $\mathcal{E'}_j^{(k)}$ and number $0 \leq r_j^{(k)} < 1$. Then, for any number $v \geq 3$ of trap computations, the mesothetic protocol is verifiable with*

$$\delta = 1 \text{ and } \varepsilon = g\frac{\kappa}{v+1} + \ 1 \ - g \ , \tag{7.7}$$

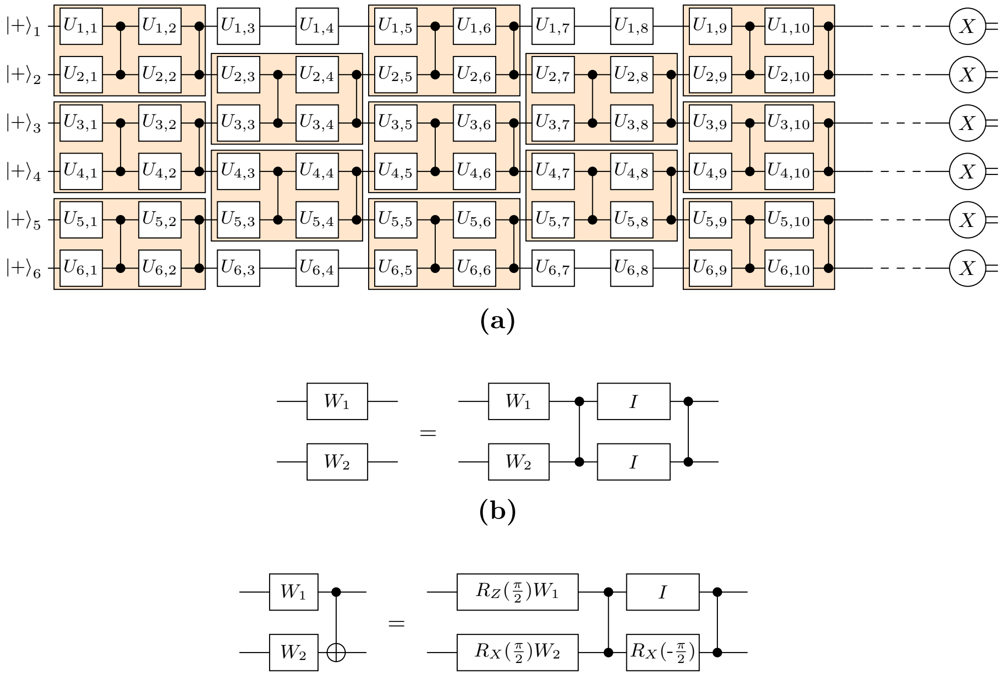
where $\kappa = 3(3/4)^2 \approx 1.7$, $g = \prod_{j,k} 1 - r_{\text{max, }j}^{(k)}$ and $r_{\text{max, }j}^{(k)}$ is the maximum error rate of the round of gates in band j of circuit k, where this maximum is taken over all choices gates for this round.

Proof. The proof of completeness is the same as for Theorem 9. To compute soundness, we denote as $\rho_{\text{out}}^{\star}$ the state in Alice's register at the end of a protocol run when Alice's device is noisy, and as ρ_{out} the state in Alice's register at the end of a protocol run when Alice's device is noiseless (Lemma 6). Indicating as $r_{\text{max, }j}^{(k)}$ the maximum error rate for gates in band j, we rewrite this noisy map as $\mathcal{E}_j^{(k)} = (1 - r_{\text{max, }j}^{(k)})I + r_{\text{max, }j}^{(k)}\mathcal{Q}_j^{(k)}$ for some other CPTP map $\mathcal{Q}_j^{(k)}$. This allows rewriting of the classical state in Alice's register at the end of the protocol as $g\rho_{\text{out}} + (1-g)\rho_{\text{out}}^{\star}$ and to obtain the upper-bound the trace distance. □

7.3 Turning the mesothetic protocol into a blind protocol

In Step 1 of the mesothetic protocol Alice reveals to Bob the position of the cZ gates in the target circuit. Thus, in its present form the mesothetic protocol cannot be considered blind, since it leaks important information about the target circuit. Nevertheless, Alice can turn the mesothetic protocol into a blind protocol by recompiling the target circuit into a circuit of the type illustrated in Figure 7.2 (which we name "circuit in normal form").

Recompiling the target circuit into a circuit in normal form makes the input to the mesothetic protocol independent of the target circuit that Alice wishes to verify. This allows proving the following Theorem:


$|+\rangle_1$ $U_{1,1}$ $U_{1,2}$ $U_{1,3}$ $U_{1,4}$ $U_{1,5}$ $U_{1,6}$ $U_{1,7}$ $U_{1,8}$ $U_{1,9}$ $U_{1,10}$ X
$|+\rangle_2$ $U_{2,1}$ $U_{2,2}$ $U_{2,3}$ $U_{2,4}$ $U_{2,5}$ $U_{2,6}$ $U_{2,7}$ $U_{2,8}$ $U_{2,9}$ $U_{2,10}$ X
$|+\rangle_3$ $U_{3,1}$ $U_{3,2}$ $U_{3,3}$ $U_{3,4}$ $U_{3,5}$ $U_{3,6}$ $U_{3,7}$ $U_{3,8}$ $U_{3,9}$ $U_{3,10}$ X
$|+\rangle_4$ $U_{4,1}$ $U_{4,2}$ $U_{4,3}$ $U_{4,4}$ $U_{4,5}$ $U_{4,6}$ $U_{4,7}$ $U_{4,8}$ $U_{4,9}$ $U_{4,10}$ X
$|+\rangle_5$ $U_{5,1}$ $U_{5,2}$ $U_{5,3}$ $U_{5,4}$ $U_{5,5}$ $U_{5,6}$ $U_{5,7}$ $U_{5,8}$ $U_{5,9}$ $U_{5,10}$ X
$|+\rangle_6$ $U_{6,1}$ $U_{6,2}$ $U_{6,3}$ $U_{6,4}$ $U_{6,5}$ $U_{6,6}$ $U_{6,7}$ $U_{6,8}$ $U_{6,9}$ $U_{6,10}$ X
(a)
W_1
W_2
=
W_1
W_2
I
I
(b)
W_1
W_2
=
$R_Z(\frac{\pi}{2})W_1$
$R_X(\frac{\pi}{2})W_2$
I
$R_X(-\frac{\pi}{2})$

(c)

Figure 7.2: Circuit in normal form. **(a)** Six-qubit example of circuit in normal form. This circuit has the same repetitive structure as the BwS. Recompiling the target circuit into a normal form of this type can always be done using the circuit identities **(b)** and **(c)**, and by adding a polynomial number of SWAP gates to the target circuit.

Theorem 11. *Suppose that Alice can apply noiseless single-qubit gates. If Alice recompiles the target circuit into a circuit in normal form, the mesothetic protocol is blind.*

Proof. To prove blindness, we notice that during the execution of the protocol Bob cannot retrieve any information about the the target circuit, apart from the number of qubits and an upper-bound on the circuit depth. Indeed, Bob's tasks are the same for all circuits (prepare the same input state, execute the same entangling gates and measure in the same basis) and these tasks do not depend on the target circuit, since this target is implemented on a circuit in normal form. Moreover, the only type of information that Bob receives from Alice during the implementation of the circuits are the qubits in Step 4.2.1, but the QOTP prevents Bob from retrieving useful information: at any $k = 1, \ldots, v+1$ and $j = 1, \ldots, m$, if Bob sends to Alice a state $\rho_j^{(k)}$, Alice returns to him the state

$$U_j''^{(k)} \rho_j^{(k)} U_j^{\dagger\prime\prime(k)} = \otimes_{i=1}^n Z^{\alpha_{i,j}^{(k)}} X^{\alpha_{i,j}'^{(k)}} \left[U_j^{(k)} P_{j-1} \rho_j^{(k)} P_{j-1} U_j^{\dagger(k)} \right] X^{\alpha_{i,j}'^{(k)}} Z^{\alpha_{i,j}^{(k)}} \ , \qquad (7.8)$$

where P_{j-1} is the Pauli operator that undoes the previous QOTP. Summing over all possible $\alpha_{i,j}^{(k)}$ and $\alpha_{i,j}^{\prime(k)}$ yields the maximally mixed state. $\square$

Chapter 8

Conclusions

NISQ devices will be useful to test the predictions of quantum mechanics and to demonstrate the building blocks of future quantum computers [23]. Moreover, they will be able to outperform current supercomputers in specific tasks, as was demonstrated in recent experiments [16]. However, due to the high levels of noise afflicting the internal components of NISQ devices, it is crucial to develop protocols able to check the correctness of their outputs.

In this thesis we have built towards such protocols. Our work begun with the optimization of some of the existing verification protocols [49, 51, 52, 55]. Specifically, in Chapter 4 we have provided two protocols that enable a verifier Alice with restricted quantum power (single-qubit state preparation or measurement) to check the outputs of a "target" quantum computation implemented by a prover Bob. Our protocols reduce the requirements on Alice's side (preparation of eight types of states as opposed to ten in previous protocols [49, 51, 52], or else measurement in four types of basis as opposed to five in previous protocols [55]). However, the requirements on Bob's side remain impractical for NISQ devices, due to the overhead in qubits and gates of our protocols.

Moving beyond the optimization of existing protocols, in Chapter 5 we have defined the concept of an *accreditation protocol*, namely a protocol that can guarantee with high confidence that the outputs of a quantum computer are close to the correct ones. We have then presented an accreditation protocol that encompasses all the limitations of NISQ devices.

The accreditation protocol in Chapter 5 returns (i) an upper-bound on the variation distance between noisy and noiseless probability distribution of the outputs of the target circuit and (ii) a confidence on the upper-bound. Unlike verification protocols [49–62, 64, 65, 84, 85], our accreditation protocol has no overhead, since it requires implementing circuits with no more qubits and gates than the target circuit. Moreover, relying on the high quality of the single-qubit gates in present NISQ devices (Table 1.1), it captures all noise afflicting state preparation, two-qubit gates and measurements.

In Chapter 6 we have presented a modified version of the accreditation protocol (named "single-run accreditation protocol") that can provide tighter bounds on the variation distance. The single-run accreditation protocol relies on more assumptions on the noise, such as Markovianity and independence from single-qubit gates. These assumptions are standard for protocols based on tomography [33–35] and randomized benchmarking [36–45] and are motivated by empirical evidence about experimental noise [16, 45]. Importantly, the single-run accreditation protocol can detect all the noise that is detected by the protocols based on tomography or randomized benchmarking, as well as noise (such as time-dependent noise) that may be missed by those protocols.

We have demonstrated our single-run accreditation protocol on the IBMQ Ourense quantum computer for circuits containing 2,3 and 4 qubits and up to 7 rounds of single- and two-qubit gates. Being readily implementable on current quantum computers, scalable and robust to standard noise models, we expect our single-run accreditation protocol to play a crucial role in computations on future quantum computers.

Coming full circle, in Chapter 7 we have shown how the accreditation protocol in Chapter 5 can be turned into a verification protocol. Specifically, we have provided a "mesothetic verification protocol" where the Alice and Bob follow the steps of the accreditation protocol. The mesothetic protocol has more requirements on Alice's side than other verification protocols [49–52, 54–62, 64, 65, 84, 85], since Alice must possess a device able to store n qubits (where n is the number of qubits in the target computation) and implement single-qubit gates on each of them. However, it minimizes the requirements for Bob, who must only implement computations containing as many qubits and gates as the target computation.

The results presented in this thesis leave several open questions for future works. The first question is how to incorporate fault-tolerance into our accreditation protocols, as has been done for some verification protocols [51, 61, 94]. Fault-tolerant protocols rely on the assumption that the noise is digitalized and localized, meaning that it can be represented by single-qubit Pauli errors afflicting each qubit independently [16, 88, 95]. Moreover, they require that the probability that such errors occur is below a certain *threshold*. If these assumptions are invalid, then fault-tolerant protocols may be unable to detect and correct errors. Therefore, it is important to devise accreditation protocols that can also check whether errors are indeed being corrected by a given fault-tolerant protocol.

Another open question regards the applicability of our accreditation protocols if the single-qubit gates suffer noise that is systematic and gate-dependent (such as gate-dependent over- or under-rotations). In its current state, the analysis of our protocol does not account for such noise. The main reason is that the QOTP (which maps coherent errors into stochastic Pauli errors) is applied at the level of the single-qubit gates. Unbounded errors that depend on the gates used to randomize arbitrary noise processes to Pauli errors are an obstacle to other works including cryptographic protocols [51] and protocols based on randomized benchmarking [36–38, 43, 45].

Finally, another open question regards the requirements of the mesothetic protocol. The mesothetic protocol minimizes the requirements for Bob. However, Alice must possess a multi-qubit qubit memory, while in all the other protocols she must possess a single-qubit memory [49–52, 54–62, 64, 65, 84, 85]. We thus ask whether it is possible to adapt our mesothetic protocol to a scenario where Alice only possesses a single-qubit memory. This may lead to the first verification protocol that has minimal requirements for both Alice and Bob.

Bibliography

[1] D. Gottesman. The Heisenberg Representation of Quantum Computers. *arXiv:quant-ph/9807006*, 1998.

[2] S. Bravyi and D. Gosset. Improved classical simulation of quantum circuits dominated by Clifford gates. *Phys. Rev. Lett. 116,250501*, 2017.

[3] R. Bennink et al. Unbiased simulation of near-Clifford quantum circuits. *Phys. Rev. A 95, 062337*, 2017.

[4] R. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics, Vol. 21, Issue 6–7, pp 467–488*, 1985.

[5] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press.*, 1994.

[6] M. Hastings, D. Wecker, B. Bauer, and M. Troyer. Improving Quantum Algorithms for Quantum Chemistry. *Quantum Info. Comput. 15, 1*, 2015.

[7] A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. Chow, and J. Gambetta. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets. *Nature volume 549, pp 242–246*, 2017.

[8] R. Babbush, N. Wiebe, J. McClean, J. McClain, H. Neven, and G. Chan. Low-Depth Quantum Simulation of Materials. *Phys. Rev. X 8, 011044*, 2018.

[9] Z. Jiang, K. Sung, K. Kechedzhi, V. Smelyanskiy, and S. Boixo. Quantum Algorithms to Simulate Many-Body Physics of Correlated Fermions. *Phys. Rev. Applied 9, 044036*, 2018.

[10] M. Bremner, A. Montanaro, and D. Shepherd. Average-case complexity versus approximate simulation of commuting quantum computations. *Phys. Rev. Lett. 117, 080501*, 2016.

[11] S. Boixo et al. Characterizing Quantum Supremacy in Near-Term Devices. *Nature Physics 14, 595-600*, 2018.

[12] X. Gao, S.-T. Wang, and L.-M. Duan. Quantum Supremacy for Simulating A Translation-Invariant Ising Spin Model. *Phys. Rev. Lett. 118, 040502*, 2017.

[13] M. Raymer et al. The US National Quantum Initiative. *Quantum Science and Technology, Volume 4, Number 2*, 2019.

[14] B. Sussman et al. Quantum Canada. *Quantum Science and Technology, Volume 4, Number 2*, 2019.

[15] P. Knight et al. UK national quantum technology programme. *Quantum Science and Technology, Volume 4, Number 4*, 2019.

[16] F. Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature volume 574, pp 505–510*, 2019.

[17] Rigetti Aspen-7 on Amazon, https://aws.amazon.com/braket/hardware-providers/Rigetti.

[18] IBM quantum experience, https://quantumexperience.ng.bluemix.net/qx/devices.

[19] P. Murali et al. Full-Stack, Real-System Quantum Computer Studies: Architectural Comparisons and Design Insights. *arXiv:1905.11349*, 2019.

[20] J. Zhang et al. Observation of a many-body dynamical phase transition with a 53-qubit quantum simulator. *Nature volume 551, pp 601–604*, 2019.

[21] K. Wright et al. Benchmarking an 11-qubit quantum computer. *Nature Communications volume 10, Article number: 5464*, 2019.

[22] E Knill, R. Laflamme, and G. Milburn. A scheme for efficient quantum computation with linear optics . *Nature, vol 409, pp 46–52*, 2000.

[23] J. Preskill. Quantum Computing in the NISQ era and beyond. *Quantum 2, 79*, 2018.

[24] A. Dimic and B. Dakic. Single-copy entanglement detection. *npj Quantum Information volume 4, Article number: 11*, 2018.

[25] A. Cervera-Lierta. Exact Ising model simulation on a quantum computer. *Quantum 2, 114*, 2018.

[26] V. Saggio et al. Experimental few-copy multipartite entanglement detection. *Nature Physics volume 15, pp 935–940*, 2019.

[27] C. Vuillot. Is error detection helpful on IBM 5Q chips ? *Quantum Information and Computation, Vol. 18, No. 11-12*, 2018.

[28] J. Wootton and D. Loss. Repetition code of 15 qubits. *Phys. Rev. A 97, 052313*, 2018.

[29] B. Villalonga et al. A flexible high-performance simulator for the verification and benchmarking of quantum circuits implemented on real hardware. *npj Quantum Information volume 5, Article number: 86*, 2019.

[30] I. Chuang and M. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box . *Journal of Modern Optics, Vol. 44, Issue 11-12*, 1997.

[31] Y. Weinstein, T. Havel, J. Emerson, and N. Boulant. Quantum process tomography of the quantum Fourier transform . *J. Chem. Phys. 121, 6117*, 2004.

[32] S. Merkel, J. Gambetta, J. Smolin, S. Poletto, and A. Corcoles. Self-consistent quantum process tomography. *Phys. Rev. A 87, 062119*, 2013.

[33] R. Blume-Kohout et al. Robust, self-consistent, closed-form tomography of quantum logic gates on a trapped ion qubit. *arXiv:1310.4492*, 2013.

[34] D Greenbaum. Introduction to Quantum Gate Set Tomography . *arxiv:1509.0292*, 2015.

[35] R. Blume-Kohout, J. Gamble, E. Nielsen, K. Rudinger, J. Mizrahi, K. Fortier, and P. Maunz. Demonstration of qubit operations below a rigorous fault tolerance threshold with gate set tomography . *Nature Communications 8, 14485*, 2017.

[36] E. Knill et al. Randomized Benchmarking of Quantum Gates. *Phys. Rev. A 77, 012307*, 2007.

[37] E. Magesan, J. Gambetta, and J. Emerson. Scalable and Robust Randomized Benchmarking of Quantum Processes. *Phys. Rev. Lett. 106, 180504*, 2011.

[38] J. Emerson et al. Symmetrised Characterisation of Noisy Quantum Processes. *Science 317, 1893-1896*, 2007.

[39] J. Wallman, M. Barnhill, and J. Emerson. Robust Characterization of Loss Rates. *Phys. Rev. Lett. 115, 060501*, 2015.

[40] A. Carignan-Dugas, J. Wallman, and J. Emerson. Characterizing universal gate sets via dihedral benchmarking. *Phys. Rev. A 92, 060302(R)*, 2015.

[41] G. Wendin. Quantum information processing with superconducting circuits: a review. *Reports on Progress in Physics*, 2017.

[42] J. Wallman, M. Barnhill, and J. Emerson. Robust characterization of leakage errors. *New J. Phys.18 04302*, 2016.

[43] J. Combes, C. Granade, C. Ferrie, and S. Flammia. Logical Randomized Benchmarking. *arXiv:1702.03688*, 2017.

[44] J. Helsen, X. Xue, L. Vandersypen, and S. Wehner. A new class of efficient randomized benchmarking protocols. *npj Quantum Information volume 5, Article number: 71*, 2019.

[45] A. Erhard et al. Characterizing Large-Scale Quantum Computers Via Cycle Benchmarking. *arXiv:1902.08543*, 2019.

[46] J. Wallman. Randomized benchmarking with gate-dependent noise. *Quantum 2, 47*, 2018.

[47] S. Merkel, E. Pritchett, and B. Fong. Randomized Benchmarking as Convolution: Fourier Analysis of Gate Dependent Errors. *arXiv:1804.05951*, 2018.

[48] M. Lilly and T. Humble. Modeling noisy quantum circuits using experimental characterization. *arXiv:2001.08653*, 2020.

[49] J. Fitzsimons and E. Kashefi. Unconditionally Verifiable Blind Computation. *Phys. Rev. A 96, 012303*, 2017.

[50] S. Barz, J. Fitzsimons, E. Kashefi, and P. Walther. Experimental verification of quantum computations. *Nature Physics 9, 727-731*, 2013.

[51] T. Kapourniotis and A. Datta. Nonadaptive fault-tolerant verification of quantum supremacy with noise. *Quantum 3, 164*, 2017.

[52] E. Kashefi and P. Wallden. Optimised resource construction for verifiable quantum computation. *J. Phys. A: Math. Theor., Volume 50, Number 14*, 2017.

[53] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev. Interactive Proofs For Quantum Computations. *arXiv:1704.04487*, 2017.

[54] A. Broadbent. How to Verify a Quantum Computation. *Theory of Computing 14(11):1-37*, 2018.

[55] M. Hayashi and T. Morimae. Verifiable measurement-only blind quantum computing with stabilizer testing. *Phys. Rev. Lett. 115, 220502*, 2015.

[56] T. Morimae and J. Fitzsimons. Post hoc verification with a single prover. *Phys. Rev. Lett. 120, 040501*, 2018.

[57] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert. Direct certification of a class of quantum simulations. *Quantum Science and Technology 2(1) 015004*, 2017.

[58] D. Markham and A. Krause. A simple protocol for certifying graph states and applications in quantum networks. *arXiv:1801.05057*, 2018.

[59] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. Fitzsimons. Resource-efficient verification of quantum computing using Serfling's bound. *npj Quantum Information volume 5, Article number: 27*, 2018.

[60] B.W. Reichardt, F. Unger, and U. Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. *arXiv:1209.0448*, 2012.

[61] A. Gheorghiu, E. Kashefi, and P. Wallden. Robustness and device independence of verifiable blind quantum computing. *New J. Phys. 17, 083040*, 2015.

[62] M. McKague. Interactive proofs for BQP via self-tested graph states. *Theory of Computing, Volume 12, Article 3, pp 1-42*, 2016.

[63] S. Goldwasser and C. Micali, S and. Rackoff. The knowledge complexity of interactive proof systems. *Proceedings of the seventeenth annual ACM symposium on Theory of computing, pp 291–304, ACM New York, NY, USA*, 1985.

[64] U. Mahadev. Classical Verification of Quantum Computations. *arXiv:1804.01082*, 2018.

[65] J. Fitzsimons and M. Hajdusek. Post hoc verification of quantum computation. *arXiv:1502.02563*, 2015.

[66] B. Terhal. Quantum supremacy, here we come. *Nature Physics 14, 530–531*, 2018.

[67] D. Aharonov, M. Ben-Or, and E. Eban. Interactive Proofs For Quantum Computations. *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 5-7, 2010. Proceedings 453–469*, 2010.

[68] J. Wallman and J. Emerson. Noise tailoring for scalable quantum computation via randomized compiling. *Phys. Rev. A 94, 052325*, 2016.

[69] M. Nielsen and I. Chuang. Quantum Computation and Quantum Information: 10th anniversary edition. *Cambridge University Press New York, NY, USA*, 2000.

[70] C. Dankert, E. Cleve, J. Emerson, and E. Livine. Exact and Approximate Unitary 2-Designs: Constructions and Applications. *Phys. Rev. A 80, 012304*, 2009.

[71] M. Mosca, A. Tapp, and R. de Wolf. Private Quantum Channels and the Cost of Randomizing Quantum Information. *arXiv:quant-ph/0003101*, 2000.

[72] A. Childs. Secure Assisted Quantum Computation. *Quantum Information and Computation 5, 456*, 2005.

[73] R. Raussendorf and H.J. Briegel. A One-Way Quantum Computer. *Phys. Rev. Lett. 86, 5188*, 2001.

[74] M. Bremner, C. Mora, and A. Winter. Are Random Pure States Useful for Quantum Computation? *Phys. Rev. Lett. 102, 190502*, 2009.

[75] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal Blind Quantum Computation. *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, pp 517-526*, 2009.

[76] L. Grover. A fast quantum mechanical algorithm for database search. *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, pp 212-219*, 1996.

[77] The Aaronson *£*25.00 Prize.

[78] Y. Sanders, J. Wallman, and B. Sanders. Bounding quantum gate error rate based on reported average fidelity. *New Journal of Physics 18 012002*, 2016.

[79] A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden. QFactory: classically-instructed remote secret qubits preparation. *arXiv:1904.06303*, 2019.

[80] V. Dunjko, J.F. Fitzsimons, C. Portmann, and R. Renner. Composable Security of Delegated Quantum Computation. *Advances in Cryptology–ASIACRYPT*, 2014.

[81] A. Gheorghiu, T. Kapourniotis, and E. Kashefi. Verification of quantum computation: An overview of existing approaches. *Theory of Computing Systems, Volume 63, Issue 4, pp 715-808*, 2018.

[82] D. Aharonov and M. Ben-Or. Fault-Tolerant Quantum Computation With Constant Error Rate. *arXiv:quant-ph/9906129v1*, 1999.

[83] V. Dunjko. Ideal quantum protocols in the non-ideal physical world. *PhD thesis*, 2012.

[84] S. Ferracin, T. Kapourniotis, and A. Datta. Reducing resources for verification of quantum computations. *Phys. Rev. A 98, 022323*, 2017.

[85] A. Natarajan and T. Vidick. Robust self-testing of many-qubit states. *arXiv:1610.03574*, 2016.

[86] W. Hoeffding. Probability Inequalities for Sums of Bounded Random Variables. *Journal of the American Statistical Association, 58 (301), pp 13–30*, 1963.

[87] P. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A 52, R2493(R)*, 1995.

[88] E. Campbell, B. Terhal, and C. Vuillot. Roads towards fault-tolerant universal quantum computation. *Nature volume 549, pp 172–179*, 2017.

[89] D. Greenberger, M. Horne, and A. Zeilinger. Going Beyond Bell's Theorem. *Bell's Theorem, Quantum Theory, and Conceptions of the Universe, pp 69-72*, 1989.

[90] Noise model in Qiskit Aer, https://qiskit-staging.mybluemix.net/documentation/aer/device_noise_simulation.html.

[91] D. McKay, A. Cross, C. Wood, and J. Gambetta. Correlated Randomized Benchmarking . *arXiv:2003.02354*, 2020.

[92] A. Winick, J. Wallman, and J. Emerson. Simulating and mitigating crosstalk . *arXiv:2006.09596*, 2020.

[93] J. Fitzsimons. Private quantum computation: An introduction to blind quantum computing and related protocols. *npj Quantum Information, Volume 3, Article number 23*, 2017.

[94] K. Fujii and M. Hayashi. Verifiable fault-tolerance in measurement-based quantum computation. *Phys. Rev. A 96, 030301*, 2017.

[95] A. Fowler, M. Mariantoni, J. Martinis, and A. Cleland. Surface codes: Towards practical large-scale quantum computation. *Phys. Rev. A 86, 032324*, 2012.