Two-qubit Stabilizer Circuits with Recovery I: Existence

Wim van Dam
Department of Computer Science, Department of Physics, University of California, Santa Barbara, CA, USA
vandam@ucsb.edu
https://orcid.org/0000-0001-7852-6158

Raymond Wong
Department of Computer Science, University of California, Santa Barbara, CA, USA
rwong@ucsb.edu

Abstract

In this paper, we further investigate the many ways of using stabilizer operations to generate a single qubit output from a two-qubit state. In particular, by restricting the input to certain product states, we discover probabilistic operations capable of transforming stabilizer circuit outputs back into stabilizer circuit inputs. These secondary operations are ideally suited for recovery purposes and require only one extra resource input to proceed. As a result of reusing qubits in this manner, we present an alternative to the original state preparation process that can lower the overall costs of executing a two-qubit stabilizer procedure involving non-stabilizer resources.

2012 ACM Subject Classification Theory of computation → Quantum computation theory

Keywords and phrases stabilizer circuit, recovery circuit, magic state

Digital Object Identifier 10.4230/LIPIcs.TQC.2018.7

Acknowledgements This material is based upon work supported by the National Science Foundation under Grants No. 0917244 and 1719118.

1 Introduction

There has been significant progress to building quantum computers. We can protect qubits with quantum codes, and we can combat the spread of errors with fault-tolerance; high thresholds approaching 1% [17] is already within reach. Rather, one of the central challenges is in the efficient handling of noise, where it is necessary to strike a delicate balance between quality and cost. Currently many physical qubits are required to achieve this desired level of protection on a logical qubit [10], but this comprises only one part of a larger problem. The fact remains that most fault-tolerant schemes are constrained to a finite number of native operations, so there is a limit to the type of computations that we can perform. This usually consists of stabilizer operations – Clifford group unitaries, Pauli measurements, and ancilla $|0\rangle$ preparation – which are efficiently simulable on classical computers and capable of producing highly entangled states. Unfortunately, stabilizer operations by themselves are not universal, placing a premium on any non-stabilizer resource added to a circuit.

Magic state distillation is one solution addressing this inherent limitation of stabilizer operations [4]. It works as follows: prepare imperfect "magic states," measure certain stabilizer code syndrome operators, then postselect on some target outcome. The process is repeated recursively until the qubits are at a high enough quality to consume: the magic states are injected into quantum circuits to implement quantum gates outside the Clifford group of operations. Despite being quite resource intensive in the early days, numerous proposals over the last few years have progressively increased the efficiency of distilling magic states [3, 7, 8, 12, 19], although the overall format more or less remains the same. Interestingly, stabilizer operations are enough to perform the distillation, which is a testament to their versatility. Then given a supply of non-Clifford gates, we may employ any number of pre-existing synthesis algorithms to approximate unitaries over this basis. Previous work has already succeeded in producing solutions able to generate sequences for single qubit rotations in an optimal fashion [15, 16, 22, 23]. A recent one even suggests a kind of distill-and-synthesis hybrid to reduce resource usage even further: a factor of 3 savings with quadratic error suppression is possible over traditional distill-then-synthesize methods [5, 6].

The creativity that went into designing these distillation protocols is one reason motivating our broader study of stabilizer operations. Other uses include procedures for distilling multiple types of magic qubits [7, 8, 12, 18], as well as implementing phase rotations with low depth circuits. Some notable examples of the latter are contained in [9] and [13], both of which feature the same stabilizer circuit to perform the operation. The differences lie in the pre-computed ancillae injected into the circuit, where Duclos-Cianci and Svore [9] additionally demonstrated how to use the same circuit to create other resource qubits. At any rate, though simple, both displayed the advantages of having a large set of non-homogeneous states at our disposal, and all that is required is a two-qubit stabilizer circuit.

Inspired by the magic state model to universal quantum computation, we consider general two-to-one stabilizer procedures that take a two-qubit state and produce a single qubit output using stabilizer operations only. Our intent is to explore these processes from a different angle, outside the realm of state distillation, and simply examine their behavior on more arbitrary input. And though our problem size is small, we discover some encouraging ideas that are worth pursuing for larger settings. Some limits on distilling two-qubit states are already discussed in [21]. Instead, we refine the implementation details first provided by Reichardt [21] to identify three circuit configurations characterizing all such two-to-one procedures. These three forms suggest that in addition to Pauli measurements and postselection, single qubit Clifford gates and at most one CNOT or SWAP are enough to realize any stabilizer procedure acting on two qubits. When the input set is further confined to certain product states, we discover an interesting connection between stabilizer circuits of the single CNOT variety – "interacting" circuits in our dictionary. That is, there are "recovery circuits" that can recuperate a product state input from a corrupted stabilizer circuit output. Informally our main result (Theorem 12) states the following.

Main Result (informal): *For any interacting two-to-one stabilizer procedure there exist recovery circuits, and all such recovery circuits are equivalent to one-and-another and hence have the same probability of recovery.*

The magic state injection process is one good area for utilizing such a recovery technique. We end the article with a few numerical experiments showcasing the benefits of the derived recovery protocols.

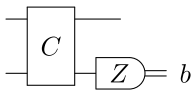


Figure 1 A postselected two-to-one stabilizer circuit (C, b) consists of a stabilizer circuit component C and a postselected bit value b.

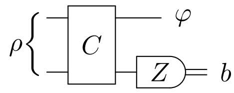


Figure 2 The qubit $\varphi = \Phi_b(C, \rho)$ is the output of a postselected two-to-one stabilizer circuit (C, b) on the two-qubit input ρ.

2 Preliminaries

This section provides an overview of the elementary stabilizer operations and basic concepts. The single qubit Pauli matrices are

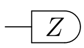
$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{1}$$

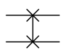
They satisfy not only the identities $X^2 = Y^2 = Z^2 = I$ and $XY = iZ$, but they also form a basis for the space of 2×2 Hermitian matrices. We can expand any single qubit density matrix φ in terms of Pauli matrices using the expression $\varphi = (I + xX + yY + zZ)/2$. If we collect the three previous coefficients, then $(x, y, z) \in \mathbb{R}^3$ is the *Bloch vector* of φ.

An n-qubit stabilizer circuit is limited to certain quantum gates and measurements. It may use elements from the Clifford group $\mathcal{C}(n)$, and it may apply measurements in the Z-basis. The Clifford group is generated by the Controlled-NOT (CNOT), Hadamard (H), and Phase (P) operators:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \qquad P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}. \tag{2}$$

A stabilizer circuit thus contains entirely of CNOT, H, and P gates. For the values of n we are concerned with, $\mathcal{C}(1)$ and $\mathcal{C}(2)$ have sizes 24 and 11520, respectively, modulo global phases. The circuit diagram for a Z-measurement is given by the left image below:





while the right image represents a qubit SWAP. A Clifford circuit is a stabilizer circuit that excludes measurements and implements a Clifford group unitary only.

3 Postselected Two-to-One Stabilizer Circuits

We revisit the study of stabilizer reductions from [21] to derive Lemma 4. Part of the novelty that Lemma 4 brings is the realization of recovery circuits described in the next section. We first introduce some terminology and notation to more concisely capture Reichardt's observations in [21] to present our result.

An n-to-1 stabilizer reduction is a procedure that accepts an n-qubit state and generates a single qubit output using stabilizer operations only. This means all post-measurement activities are also restricted to classical control over stabilizer operations. Reichardt showed that any reduction can be standardized to a particular form: an application of a Clifford unitary on n qubits, followed by a projection of qubits 2 to n onto a computational basis state [21]. Since our focus is on $n = 2$, we have the following definition.

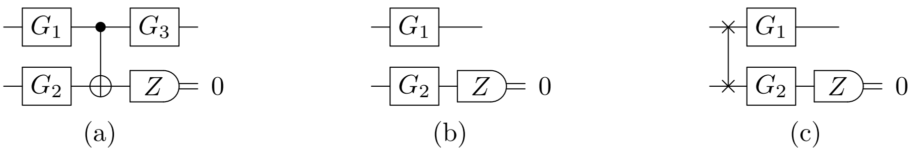


Figure 3 Any stabilizer procedure generating one qubit from two can be described by a postselected circuit (C, b) resembling circuit (a), circuit (b), or circuit (c). The choice of single qubit Clifford gates G_1, G_2, and G_3 depend on C and the postselected measurement b. Circuit (a) is known as an interacting postselected circuit; the precise definition is provided in Section 4.

▶ **Definition 1** (postselected two-to-one stabilizer circuit)**.** A *postselected two-to-one stabilizer circuit* (C, b) is a two-qubit quantum circuit that implements a Clifford unitary C, followed by a Z-measurement on the second qubit with an outcome $b \in \{0, 1\}$.

▶ **Definition 2** (probability and output)**.** Let (C, b) be a postselected two-to-one stabilizer circuit and let ρ be a two-qubit state. Then the *probability* Q_b of outcome b on the transformed state $C\rho C^\dagger$ is $Q_b(C, \rho) = \mathrm{Tr}((I \otimes \langle b|)C\rho C^\dagger(I \otimes |b\rangle))$. If $Q_b(C, \rho) > 0$, then the *output* Φ_b of a postselected circuit (C, b) on an input ρ is

$$\Phi_b(C, \rho) = \frac{(I \otimes \langle b|)C\rho C^\dagger(I \otimes |b\rangle)}{Q_b(C, \rho)}. \tag{3}$$

At times, we may say *run circuit* C, which translates to an application of the unitary C on the input ρ, followed by a Z-measurement on the second qubit. This is often followed by details on what course of action to take conditional on b (or $1 - b$). The term *circuit* C thus references the stabilizer circuit piece only of the postselected circuit, including the measurement at the end. The next definition describes what it means for postselected circuits to produce similar outputs.

▶ **Definition 3** (equivalent postselected two-to-one stabilizer circuits)**.** Two postselected two-to-one stabilizer circuits (C_1, b_1) and (C_2, b_2) are *Clifford equivalent*, $(C_1, b_1) \sim (C_2, b_2)$, if and only if there is a single qubit Clifford gate G such that for all two-qubit states ρ, we have the equality

$$(I \otimes \langle b_1|)C_1\rho C_1^\dagger(I \otimes |b_1\rangle) = G(I \otimes \langle b_2|)C_2\rho C_2^\dagger(I \otimes |b_2\rangle)G^\dagger. \tag{4}$$

Note that a Clifford equivalence implies that the probabilities of observing a b_1 or b_2 are the same for the two circuits i.e. $Q_{b_1}(C_1, \rho) = Q_{b_2}(C_2, \rho)$. We say two postselected circuits are simply *equivalent*, $(C_1, b_1) \equiv (C_2, b_2)$, if and only if $G = I$ in Equation 4.

We may alter the circuits using $|b_2\rangle = X|1 - b_2\rangle$ in Equation 4 so that both postselect on the same value. As we mentioned before, any two-to-one stabilizer reduction can be achieved through a postselected two-to-one stabilizer circuit. Despite $|\mathcal{C}(2)| = 11520$, the number of actual reductions we need to consider is 30: one for each nontrivial two-qubit Pauli, plus the bit [21]. As such, we can introduce three forms in the following lemma to represent all postselected circuits (C, b). The proof is provided in Appendix A.

▶ **Lemma 4.** *For every postselected two-to-one stabilizer circuit (C, b), there exist single qubit Clifford gates G_1 and G_2 such that either $(C, b) \sim (I \otimes G_1, 0)$, or $(C, b) \sim ((I \otimes G_1)\mathrm{SWAP}, 0)$, or $(C, b) \sim (\mathrm{CNOT}(G_1 \otimes G_2), 0)$.*

▶ **Corollary 5.** *If a postselected two-to-one stabilizer circuit (C, b) is Clifford equivalent to $(C', 0)$, where $C' = I \otimes G_1$, or $C' = (I \otimes G_1)\mathrm{SWAP}$, or $C' = \mathrm{CNOT}(G_1 \otimes G_2)$, and G_1 and G_2 are single qubit Clifford gates, then $(C, 1 - b) \sim ((I \otimes X)C', 0)$.*

Due to Lemma 4, we have a remarkably much easier time studying postselected circuits. We may substitute (C, b) with another that likely uses fewer gates but behaves in exactly the same way. Because there are many identities on Pauli operators and Clifford gates, G_1 and G_2 are not unique e.g. $((\text{CNOT}(Z \otimes I), 0) \equiv ((Z \otimes I)\text{CNOT}, 0) \sim (\text{CNOT}, 0)$. Of the 30 reductions available, it is easy to see that there are 18 varieties of $(\text{CNOT}(G_1 \otimes G_2), 0)$, and 6 each for $(I \otimes G_1, 0)$ and $((I \otimes G_1)\text{SWAP}, 0)$. If we want to separate the circuits by the stricter kind of equivalence "$\equiv$", the number of classes is multiplied by 24 e.g. $18 \cdot 24 = 432$ for $((G_3 \otimes I)\text{CNOT}(G_1 \otimes G_2), 0)$, since there are $|\mathcal{C}(1)| = 24$ choices of G_3.

4 Recovery Circuits

A quantum circuit involving measurements likely has outcomes that we prefer over others. If we are less than fortunate, convention dictates that we discard the output and rerun the circuit on new input instances until we succeed. This is not much of an issue when the initial overhead is low, but can become problematic otherwise. If the cost associated with state preparation is a barrier to large computations, any method that alleviates this burden is highly desirable. It turns out when ρ is a tensor product state, i.e. $\rho = \varphi \otimes |\psi\rangle\langle\psi|$, we have an alternative: there exist operations capable of reusing an undesirable output to try and recovery φ.

This input requirement means the only circuit configuration of Lemma 4 worth considering is $(\text{CNOT}(G_1 \otimes G_2), 0)$. We can easily see that when $(C, b) \sim (I \otimes G_1, 0)$, the output of (C, b) on $\varphi_1 \otimes \varphi_2$ is essentially φ_1. The output is always an input, and the same is similarly true for all circuits $(C, b) \sim ((I \otimes G_1)\text{SWAP}, 0)$.

▶ **Definition 6** (interacting postselected circuit)**.** A postselected two-to-one stabilizer circuit (C, b) is *interacting* if and only if there are single qubit Clifford gates G_1 and G_2 such that $(C, b) \sim (\text{CNOT}(G_1 \otimes G_2), 0)$. We say circuit C is *interacting* if and only if $(C, 0)$ is interacting.

With that, we define the notion of a recovery circuit. For convenience, we use ψ in place $|\psi\rangle\langle\psi|$ throughout the remainder of our discussion on recovery circuits.

▶ **Definition 7** (recovery circuit)**.** Let (C, b) be an interacting postselected circuit. A postselected two-to-one stabilizer circuit (C', b') is a *recovery circuit* of (C, b) if and only if for all two-qubit states $\varphi \otimes \psi$, we have $\varphi = \Phi_{b'}(C', \Phi_{1-b}(C, \varphi \otimes \psi) \otimes \psi)$.

Notice that an input qubit to (C', b') is the output of $(C, 1-b)$ on $\varphi \otimes \psi$. In this context, if b is more desirable than $1 - b$, then we say circuit C is *successful* upon measuring b on $C(\varphi \otimes \psi) C^\dagger$. Otherwise circuit C is *unsuccessful*, and the recovery circuit provides a second chance at obtaining the output of (C, b) on $\varphi \otimes \psi$. The presumption is that the implementation of C' is far simpler to pursue than the original method to prepare φ. Our next lemma presents one way on how to design such a recovery circuit to (C, b).

▶ **Lemma 8.** *Every interacting postselected circuit (C, b) has a recovery circuit.*

Proof. Let $(C, b) \sim (\text{CNOT}(G_1 \otimes G), 0)$, where G_1 and G are single qubit Clifford gates. By Corollary 5, we know $(C, 1-b) \sim (\text{CNOT}(G_1 \otimes G), 1)$, which means there is a single qubit Clifford gate G_2 such that $(C, 1-b) \equiv ((G_2^\dagger \otimes I)\text{CNOT}(G_1 \otimes G), 1)$. We shall show that $((G_1^\dagger \otimes I)\text{CNOT}(G_2 \otimes G), 0)$ is a recovery circuit of (C, b). Figure 4 includes reference diagrams to aid comprehension.

If the input to circuit C is $\varphi_1 \otimes \psi$, consider $\varphi_1' \otimes \psi' = G_1 \varphi_1 G_1^\dagger \otimes G \psi G^\dagger$. Let (x_1, y_1, z_1) be the Bloch vector of φ_1' and (x, y, z) be the Bloch vector of $|\psi'\rangle$. For ease of notation, we

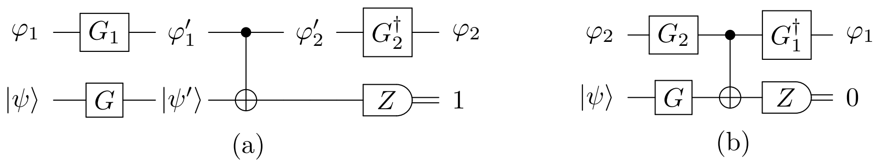


Figure 4 Suppose $(C, 1-b) \equiv ((G_2^\dagger \otimes I)\mathrm{CNOT}(G_1 \otimes G), 1)$. This equivalence allows us to study $(C, 1-b)$ via its substitute in (a) and come up with the recovery circuit in (b). We include intermediate states like φ_1' and $\varphi_2' = G_2\varphi_2 G_2^\dagger$ in (a) to signify stages in the circuit.

define outputs $\varphi_2' = \Phi_1(\mathrm{CNOT}, \varphi_1' \otimes \psi')$ and $\varphi_2 = G_2^\dagger \varphi_2' G_2 = \Phi_{1-b}(C, \varphi_1 \otimes \psi)$. Then the Bloch vector (x_2, y_2, z_2) of φ_2' becomes

$$x_2 = \frac{x_1 x + y_1 y}{1 - z_1 z}, \qquad y_2 = \frac{y_1 x - x_1 y}{1 - z_1 z}, \qquad z_2 = \frac{z_1 - z}{1 - z_1 z}. \tag{5}$$

Now suppose $\varphi_3 = \Phi_0(\mathrm{CNOT}(G_2 \otimes G), \varphi_2 \otimes \psi)$. For postselected circuits with one CNOT, the equations for computing the output's Bloch vector are essentially the same:

$$x_3 = \frac{x_2 x - y_2 y}{1 + z_2 z}, \qquad y_3 = \frac{y_2 x + x_2 y}{1 + z_2 z}, \qquad z_3 = \frac{z_2 + z}{1 + z_2 z}, \tag{6}$$

where (x_3, y_3, z_3) represents the Bloch vector of φ_3. Using $x^2 + y^2 + z^2 = 1$, we can show

$$x_3 = \frac{x_1 x^2 + x y_1 y - x y_1 y + x_1 y^2}{1 - z_1 z + z_1 z - z^2} = x_1. \tag{7}$$

Likewise, $y_3 = y_1$ and $z_3 = z_1$, which means $\varphi_3 = \varphi_1' = G_1 \varphi_1 G_1^\dagger$. The circuit $((G_1^\dagger \otimes I)\mathrm{CNOT}(G_2 \otimes G), 0)$ is therefore a recovery circuit of (C, b). ◀

Between (C, b) and its recovery circuit $((G_1^\dagger \otimes I)\mathrm{CNOT}(G_2 \otimes G), 0)$, there is a relatively straightforward relationship between the probability that circuit C would have been successful and the probability that circuit $C' = (G_1^\dagger \otimes I)\mathrm{CNOT}(G_2 \otimes G)$ will be successful.

▶ **Corollary 9.** *Let $\varphi_1 \otimes \psi$ be a two-qubit state and let $C' = (G_1^\dagger \otimes I)\mathrm{CNOT}(G_2 \otimes G)$ be a two-qubit Clifford unitary such that $(C', 0)$ is a recovery circuit of (C, b). Then*

$$Q_0(C', \Phi_{1-b}(C, \varphi_1 \otimes \psi) \otimes \psi) = \frac{(1 - z^2)/4}{1 - Q_b(C, \varphi_1 \otimes \psi)} \tag{8}$$

where $z = \langle\psi|G^\dagger Z G|\psi\rangle$.

Proof. We assume for simplicity that $C = \mathrm{CNOT}$ and $b = 0$, which implies $G_1 = G_2 = G = I$. Let $z_1 = \mathrm{Tr}(Z\varphi_1)$ and $z = \langle\psi|Z|\psi\rangle$. Also let $\varphi_2 = \Phi_1(C, \varphi_1 \otimes \psi)$. Then

$$Q_1(C, \varphi_1 \otimes \psi) = \frac{1 - z_1 z}{2}, \quad z_2 = \mathrm{Tr}(Z\varphi_2) = \frac{z_1 - z}{1 - z_1 z}. \tag{9}$$

The probability of recovering φ_1 is now clear:

$$Q_0(C', \varphi_2 \otimes \psi) = \frac{1 + z_2 z}{2} = \frac{1 - z_1 z + z_1 z - z^2}{4\left(\frac{1 - z_1 z}{2}\right)} = \frac{(1 - z^2)/4}{1 - Q_0(C, \varphi_1 \otimes \psi)} \tag{10}$$

since the circuits perform a single measurement. ◀

Another implication of the proof to Lemma 8 is that $\Phi_{1-b}(C, \varphi_1 \otimes \psi)$ is always φ_1, up to a single qubit Clifford gate, whenever $|\psi\rangle$ is an eigenstate of X, Y, or Z (a stabilizer qubit). Under these circumstances, the behavior of (C, b) on these types of inputs is actually no different than non-interacting circuits. Hence it does not warrant the use of a circuit $C' = (G_1^\dagger \otimes I)\text{CNOT}(G_2 \otimes G)$ to try and perform a recovery because the qubit is basically φ_1. It is also quite evident by now that there is only one type of recovery circuit, especially given our construction in Lemma 8.

▶ **Lemma 10.** *All recovery circuits are interacting postselected circuits.*

Proof. Let (C, b) be an interacting postselected circuit and suppose (C', b') is a recovery circuit of (C, b). If (C', b') is not an interacting postselected circuit, then $(C', b') \sim (I \otimes G, 0)$ or $(C', b') \sim ((I \otimes G)\text{SWAP}, 0)$, where G is a single qubit Clifford gate. We can easily find a two-qubit state $\varphi \otimes \psi$ such that (C', b') fails to recover φ on the input $\Phi_{1-b}(C, \varphi \otimes \psi) \otimes \psi$. ◀

Lastly, it should not come as a surprise that more than one recovery circuit of (C, b) exists. Even so, we can guarantee that not any one recovery circuit will outperform another.

▶ **Lemma 11.** *Let (C, b) be an interacting postselected circuit, and let $C'' = (G_2^\dagger \otimes I)\text{CNOT}(G_1 \otimes G)$ be a two-qubit Clifford unitary such that $(C, 1-b) \equiv (C'', 1)$. Then (C', b') is a recovery circuit of (C, b) if and only if $(C', b') \equiv ((G_1^\dagger \otimes I)\text{CNOT}(G_2 \otimes G), 0)$.*

Proof. In the reverse direction, equivalence of postselected stabilizer circuits means both produce the exact same output at the same success rate for all two-qubit states ρ. This certainly includes all two-qubit product states $\varphi_2 \otimes \psi$, where φ_2 is the output of $(C, 1-b)$ on another input $\varphi_1 \otimes \psi$.

In the forward direction, Lemmas 14 and 15 in the appendices do most of the job: $(C', b') \sim ((G_1^\dagger \otimes I)\text{CNOT}(G_2 \otimes G), 0)$. We just need to prove equivalence. We look back at the definition of Clifford equivalent postselected circuits, where we must have a single qubit Clifford gate G' such that

$$(G' \otimes \langle b'|)C'\rho C'^\dagger(G'^\dagger \otimes |b'\rangle) = (G_1^\dagger \otimes \langle 0|)\text{CNOT}(G_2 \otimes G)\rho(G_2^\dagger \otimes G^\dagger)\text{CNOT}(G_1 \otimes |0\rangle) \quad (11)$$

for all two-qubit states ρ. If it is indeed the case that they are strictly Clifford equivalent i.e. $G' \neq I$, then (C', b') cannot have been a recovery circuit of (C, b) because the output from (C', b') on ρ will be rotated by $G'^\dagger$. Thus the two must be equivalent (with "$\equiv$"). ◀

From Lemmas 8 and 11, we reach our main result, with Corollary 13 as an immediate consequence to our theorem.

▶ **Theorem 12.** *Every interacting postselected circuit (C, b) has a recovery circuit (C', b'). Moreover, all recovery circuits of (C, b) are equivalent to (C', b').*

▶ **Corollary 13.** *Every recovery circuit (C', b') has its own recovery circuit (C'', b'').*

5 Example Routines Featuring Recovery Circuits

Recovery circuits appear in the literature, where the use cases for our recovery operation seem more pertinent to state injection and implementing non-Clifford operations than to state distillation itself. For instance, the programmable ancilla rotation (PAR) of [13] uses qubits of the type $|\theta\rangle = (|0\rangle + e^{i\theta}|1\rangle)/\sqrt{2}$ and an interacting circuit CNOT to rotate $|q\rangle = \alpha|0\rangle + \beta|1\rangle$

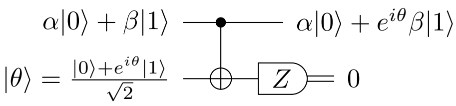


Figure 5 Procedure with the postselected circuit $(\text{CNOT}, 0)$ from [13] to rotate $\alpha|0\rangle+\beta|1\rangle$ by θ about the Z-axis.

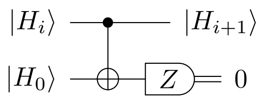


Figure 6 The same circuit $(\text{CNOT}, 0)$ appears in [9] to produce "ladder" qubits $|H_{i+1}\rangle$ from $|H_i\rangle \otimes |H_0\rangle$, where $H|H_0\rangle = |H_0\rangle$.

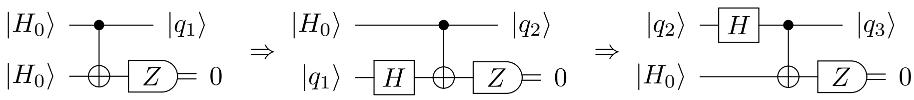


Figure 7 Approach to generate $|q_3\rangle$ with three postselected circuits and four $|H_0\rangle$ states. This qubit appears in [9] (as $|\psi_0^0\rangle$) to help create more diverse "ladder" qubits. If we measure 1 at any of the three steps, then we restart from the first circuit on the left with two new $|H_0\rangle$ copies. Adding recovery for the last two-qubit circuit additionally improves the average $|H_0\rangle$ cost.

about the Z-axis by an angle θ. This is demonstrated in Figure 5. On the chance that the Z-measurement returns 1, then instead of $|q+\theta\rangle = \alpha|0\rangle + e^{i\theta}\beta|1\rangle$, the output becomes $|q-\theta\rangle = \alpha|0\rangle + e^{-i\theta}\beta|1\rangle$, which is $|q\rangle$ rotated by $-\theta$. Jones et. al [13] suggest pairing $|q-\theta\rangle$ with $|2\theta\rangle$ as a direct line to $|q+\theta\rangle$, but we can alternatively break this down into two smaller steps if $|\theta\rangle$ are the only states available. We first run the CNOT circuit on $|q-\theta\rangle \otimes |\theta\rangle$. If we measure 0, then we recover $|q\rangle$, and we proceed with rerunning circuit CNOT on $|q\rangle \otimes |\theta\rangle$.

The method in [9] is similar. It uses the same interacting circuit with a single CNOT to obtain "ladder" qubit states of the kind

$$|H_i\rangle = \cos(\theta_i)\,|0\rangle + \sin(\theta_i)\,|1\rangle,\ \cot(\theta_i) = \cot^{i+1}(\pi/8) \tag{12}$$

for $i \geq 0$. The production starts by supplying two copies of the magic state $H|H_0\rangle = |H_0\rangle$ to the circuit, as seen in Figure 6. Each time we gain a new state $|H_i\rangle$, we reuse the qubit to try and create the next $|H_{i+1}\rangle$. If the attempt fails, then the output of $(\text{CNOT}, 1)$ on $|H_i\rangle \otimes |H_0\rangle$ is $|H_{i-1}\rangle$. Given that the recovery circuit of $(\text{CNOT}, 0)$ is itself, the method to recover $|H_i\rangle$ from $|H_{i-1}\rangle \otimes |H_0\rangle$ is no different than the procedure to create it.

Another example is provided in Figure 7. Here, we show our recovery technique improves the average magic $|H_0\rangle$ cost to produce

$$|q_3\rangle = \cos(\phi_3)|0\rangle + \sin(\phi_3)|1\rangle, \quad \cos(2\phi_3) = \frac{6+5\sqrt{2}}{6+6\sqrt{2}}, \quad 2\phi_3 \approx 0.4456. \tag{13}$$

This qubit participates in the same ladder routine of [9] to generate more varied ladder states. Duclos-Cianci and Svore's method [9] leads to an average cost 12.5 $|H_0\rangle$ states, but we find $|q_3\rangle$ is also obtainable following the procedure in Figure 7. As such, we may consider incorporating a recovery step at one or two places to try and optimize our magic state usage. Simulations of the process in Figure 7 without recovery report an average 10.04 $|H_0\rangle$ qubits, but adding recovery for the final stabilizer circuit brings the number down slightly to 9.45. Although the reduction is small, the Section 6 experiments suggest the potential is greater when the relative cost increases between $|q_2\rangle$ and $|H_0\rangle$.

In general, if we start with the two-qubit state $\varphi \otimes \psi$, then φ is allowed to be mixed, and it can even be part of a larger entangled system. As a quick demonstration, suppose we have the situation as illustrated in the left circuit of Figure 8. Let (C', b') be a recovery circuit of (C, b) and let

$$U\rho U^\dagger = \frac{1}{2^n}\left(\mathbf{P}_I \otimes I + \mathbf{P}_X \otimes X + \mathbf{P}_Y \otimes Y + \mathbf{P}_Z \otimes Z\right) \tag{14}$$

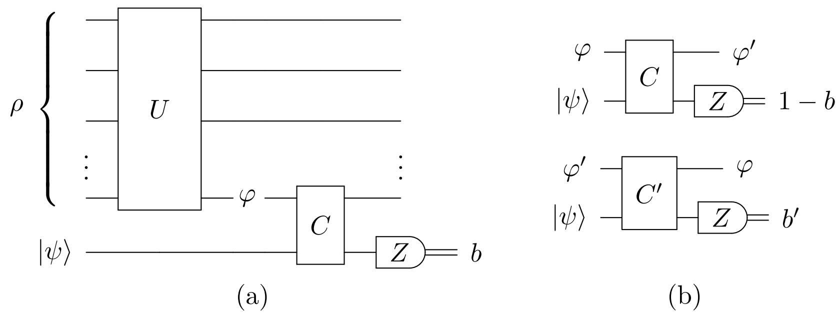


Figure 8 Recovery circuits are also applicable when one of the qubits is entangled with another system. In (a), we trace out all but the n-th qubit of $U\rho U^\dagger$ to get $\varphi \otimes \psi$ as input to circuit C. If we measure $1-b$ as pictured in the top circuit of (b), then we execute circuit C' on $\varphi' \otimes \psi$ to try and recover φ. We succeed with the recovery if we measure b'.

where $\mathbf{P}_L$ are Pauli operator sums on the first $n-1$ qubits. While the proof to Lemma 8 is generalizable to include the unused portions $\mathbf{P}_L$ of the entangled state, the math is simpler and works out the same if we trace out the first $n-1$ qubits, keeping only the last qubit $\varphi = \mathrm{Tr}_{1,n-1}\left(U\rho U^\dagger\right)$ that we need for the two-qubit circuit. If we are unlucky, then qubit n becomes $\varphi' = \Phi_{1-b}(C, \varphi \otimes \psi)$, but we can try to regain φ by executing circuit C' on $\varphi' \otimes \psi$. If the recovery is successful, then we have another opportunity at the output $\Phi_b(C, \varphi \otimes \psi)$. In all likelihood, this is a less lengthy process than preparing another ρ and running the circuit of U again; by some estimates, a synthesis of U over a universal gate set may require an exponential number of gates [11]. This is a stark contrast to C', which uses one CNOT with possibly a couple more single qubit Clifford gates.

6 Experimentation with Recovery Circuits

Consider a two-qubit Clifford unitary C_1 and a two-qubit state $\varphi \otimes \psi$. Suppose we have a target outcome of b_1; the intent is to produce output $\Phi_{b_1}(C_1, \varphi \otimes \psi)$. Then by Corollary 13, we can define a depth k protocol to be a procedure on $k-1$ postselected circuits (C_1, b_1), ..., (C_{k-1}, b_{k-1}) such that (C_{i+1}, b_{i+1}) is the recovery circuit of (C_i, b_i). We start by running circuit C_1 on $\varphi \otimes \psi$. If circuit C_1 is successful i.e. we measure b_1, then no recovery attempts are necessary and we declare success. Otherwise, we enlist circuit C_2 to try and obtain φ. More generally, if circuit C_i is successful, then we recover an input qubit to circuit C_{i-1}; if not, we run circuit C_{i+1} to recover an input qubit to circuit C_i.

The value of k represents a stopping point in our protocol: when circuit C_{k-1} is unsuccessful, we declare failure, discard the output, and restart with a new copy $\varphi \otimes \psi$ to circuit C_1. Thus this process on $k-1$ circuits is nothing more than a classical random walk on $k+1$ integers $\{0, \ldots, k\}$, where the walk begins at location 1, a step onto 0 signifies success, and a step onto k means failure. The success probability of circuit C_i is the probability of a left step from i to $i-1$ and is determined recursively by Equation 8 in Corollary 9. A step in either direction consumes one $|\psi\rangle$.

We conduct simulations of this process to obtain a better idea for N_k, the expected number of $|\psi\rangle$ resources needed to create one $\Phi_{b_1}(C_1, \varphi \otimes \psi)$ with our depth k protocol. Let d be the cost to prepare a single instance of φ relative to the cost of $|\psi\rangle$. Then the cost of one execution or trial is the same as d plus the number of $|\psi\rangle$ qubits used before halting, regardless of declaring success or fail. The costs from all trials are averaged to obtain N_k.

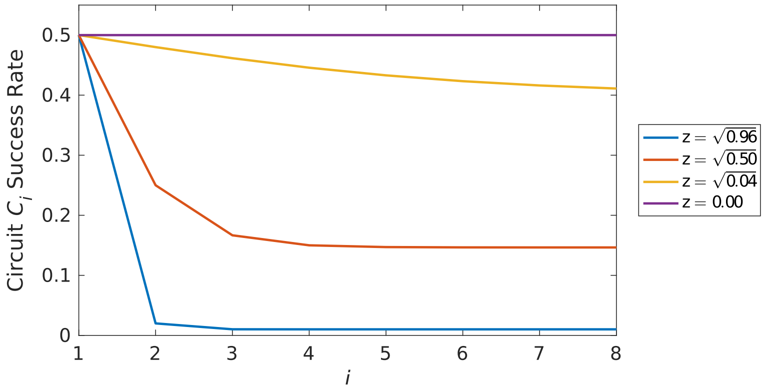


Figure 9 The success probability between circuit C_i and circuit C_{i+1} defined recursively in Corollary 9 drops more dramatically as z moves closer to 1. This leads to a greater expected cost N_k of our protocol since the recovery is less likely to succeed relative to other choices of z. On the other end of the spectrum, the success probability of each circuit C_i is uniform when $z = 0$.

We compare this against the expected cost without recovery ($k = 2$), which is

$$N_2 = \frac{d+1}{Q_{b_1}(C_1, \varphi \otimes \psi)}. \tag{15}$$

We assume for the sake of simplicity that $(C_1, b_1) = (\text{CNOT}, 0)$, which means $(C_2, b_2) = (\text{CNOT}, 0)$, and so forth for the other $k - 3$ recovery circuits.

We further assume that $Q_0(\text{CNOT}, \varphi \otimes \psi) = 1/2$. Since we fix the first success probability, N_k is dependent on the parameter $z = \langle\psi|Z|\psi\rangle$ that appears in the recovery success rate Equation 8. Technically, we need a different φ with each choice of $|\psi\rangle$ to maintain $Q_0(\text{CNOT}, \varphi \otimes \psi) = 1/2$ and the same output $\Phi_0(\text{CNOT}, \varphi \otimes \psi)$. Usually different φ means different costs d, but we will ignore this momentarily and assume the preparation overhead d for each φ is the same for the purposes of a broader comparison of N_k across different $|\psi\rangle$ qubits. In the first set of experiments, we include only one recovery circuit ($k = 3$). The following table summarizes the expected costs for four samples of z obtained over the course of 100000 trials:

d	N_2	$N_3: z = \sqrt{0.96}$	$N_3: z = \sqrt{0.50}$	$N_3: z = \sqrt{0.04}$	$N_3: z = 0$
10^{-1}	2.2	3.20	3.18	3.15	3.15
10^0	4.0	4.99	4.75	4.51	4.50
10^1	22	22.7	20.5	18.2	18.0
10^2	202	200.4	177.9	155.1	157.7
10^3	2002	1988.9	1750.7	1521.9	1498.7
10^4	20002	19816.4	17488.0	15215.4	14998.7

The first row with $d = 0.1$ should be interpreted as φ being cheaper to prepare than $|\psi\rangle$. We clearly see an improvement when factoring in recovery in the face of large relative preparation overhead between φ and $|\psi\rangle$. We also see a trend of lower costs as z grows smaller, when $|\psi\rangle$ is moving closer to the XY-plane in the Bloch sphere. This is due to the differences in the recovery success rate at circuit C_2, which are 0.02, 0.25, 0.48, and 0.5, respectively.

In the second batch of experiments, we maintain $d = 1000$ but vary the number of circuits parameterized by k. Again, $Q_0(\text{CNOT}, \varphi \otimes \psi) = 1/2$ and we run 100000 trials. Data for N_k is compiled together in the table below, starting with $k = 3$:

k	$N_k: z = \sqrt{0.96}$	$N_k: z = \sqrt{0.50}$	$N_k: z = \sqrt{0.04}$	$N_k: z = 0$
3	1981.7	1753.2	1522.9	1501.6
4	1982.9	1720.5	1372.2	1336.9
5	1982.4	1716.5	1302.9	1255.2
6	1987.5	1710.9	1266.6	1206.2
7	1982.5	1715.3	1246.7	1174.7
10	1991.7	1717.0	1221.5	1120.8
20	2002.5	1727.3	1220.2	1072.9
30	2006.3	1734.6	1231.4	1064.5
40	2023.5	1743.7	1240.8	1066.3

Observe that the value of N_k continues to lower noticeably for some of the $|\psi\rangle$ cases as more circuits are added before increasing again. This behavior is no surprise since at some point, the penalty to sustain the recovery process will exceed the overhead of repeating the computation. If we look at the success probabilities for the first eight circuits of the protocol for each of the four z samples in Figure 9, we also see the success rates decrease to some lower boundary as i increases, with the exception of when $z = 0$. The drop in probabilities from circuit C_1 to circuit C_3 is quite significant when z is close to 1 (and $1 - z^2$ is small), so the chance of recovery at circuit C_3 is only slightly larger than 0. This explains why there is no apparent change in N_k between one recovery circuit ($k = 3$) versus two ($k = 4$) for the case $z = \sqrt{0.96}$. The ideal situation is to know beforehand how many circuits to include to minimize resource usage.

7 Conclusion

We have shown two-qubit stabilizer circuits require nothing more than a few Clifford gates to perform a job. These simplifications shed light into the complementary nature between interacting circuits. Despite measurements generally being irreversible, we find an exception when handling a two-qubit product state $\varphi \otimes \psi$. That is, we can use $|\psi\rangle$ in conjunction with a specific circuit to salvage the expensive resource qubit φ. What direct effects the recovery operation will have on larger, more complex distillation schemes is unclear. At the moment, we are only able to recognize a small number of applications that involve injecting a non-stabilizer resource state into a computation.

To better gauge the utility of recovery circuits, one direction we may pursue is a more detailed and thorough examination of the depth k protocol in Section 6. In particular, there is an optimal number of circuits to employ that uses the fewest number of resources in expectation on each invocation. As we saw earlier, the behavior of our protocol is akin to that of a (possibly non-uniform) random walk. This modeling of probabilistic circuits is nothing new (see [1, 9, 13]). One matter we need to keep in mind is the costs of attaining qubits φ and $|\psi\rangle$. The amount of work that went into preparing φ should exceed that of $|\psi\rangle$ in order for the recovery to be cost effective, which stems from the fact that we need a copy of $|\psi\rangle$ to operate each circuit. The random walk techniques in [14] should also prove useful for gathering a more precise cost estimate.

Since our two-qubit setting is appropriate for only a limited number of scenarios, a natural follow-up is whether something resembling recovery circuits can easily be extended to larger stabilizer circuits. This question has been answered to an extent for the Clifford+T gate set in [1, 2, 20], where we can treat $|\psi\rangle = HP^\dagger|H_0\rangle$ to perform a non-Clifford $\pi/4$ phase rotation T. The goal in [1, 2, 20] uses a multiqubit circuit of Clifford+T gates to approximate an arbitrary single qubit unitary U up to some error ϵ. If the measurements are unfavorable, then there is a backup operation that either returns the qubits to the initial state, or directly tries to approximate U using a secondary circuit. It is worth investigating whether there exist conditions that enable larger stabilizer circuits to exhibit the recovery feature we demonstrated here on general $|\psi\rangle$ resources.

References

1 Alex Bocharov, Martin Roetteler, and Krysta M. Svore. Efficient synthesis of probabilistic quantum circuits with fallback. *Phys. Rev. A*, 91:052317, May 2015. doi:10.1103/PhysRevA.91.052317.

2 Alex Bocharov, Martin Roetteler, and Krysta M. Svore. Efficient Synthesis of Universal Repeat-Until-Success Quantum Circuits. *Phys. Rev. Lett.*, 114:080502, Feb 2015. doi:10.1103/PhysRevLett.114.080502.

3 Sergey Bravyi and Jeongwan Haah. Magic-state distillation with low overhead. *Phys. Rev. A*, 86:052329, Nov 2012. doi:10.1103/PhysRevA.86.052329.

4 Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal clifford gates and noisy ancillas. *Phys. Rev. A*, 71:022316, Feb 2005. doi:10.1103/PhysRevA.71.022316.

5 Earl T. Campbell and Mark Howard. Unified framework for magic state distillation and multiqubit gate synthesis with reduced resource cost. *Phys. Rev. A*, 95:022316, Feb 2017. doi:10.1103/PhysRevA.95.022316.

6 Earl T. Campbell and Mark Howard. Unifying Gate Synthesis and Magic State Distillation. *Phys. Rev. Lett.*, 118:060501, Feb 2017. doi:10.1103/PhysRevLett.118.060501.

7 Earl T Campbell and Joe O'Gorman. An efficient magic state approach to small angle rotations. *Quantum Science and Technology*, 1(1):015007, 2016. URL: http://stacks.iop.org/2058-9565/1/i=1/a=015007.

8 Guillaume Duclos-Cianci and David Poulin. Reducing the quantum-computing overhead with complex gate distillation. *Phys. Rev. A*, 91:042315, Apr 2015. doi:10.1103/PhysRevA.91.042315.

9 Guillaume Duclos-Cianci and Krysta M. Svore. Distillation of nonstabilizer states for universal quantum computation. *Phys. Rev. A*, 88:042325, Oct 2013. doi:10.1103/PhysRevA.88.042325.

10 Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland. Surface codes: Towards practical large-scale quantum computation. *Phys. Rev. A*, 86:032324, Sep 2012. doi:10.1103/PhysRevA.86.032324.

11 Brett Giles and Peter Selinger. Exact synthesis of multiqubit Clifford+T circuits. *Phys. Rev. A*, 87:032332, Mar 2013. doi:10.1103/PhysRevA.87.032332.

12 Jeongwan Haah, Matthew B. Hastings, D. Poulin, and D. Wecker. Magic State Distillation with Low Space Overhead and Optimal Asymptotic Input Count. *Quantum*, 1:31, Oct 2017. doi:10.22331/q-2017-10-03-31.

13 N Cody Jones, James D Whitfield, Peter L McMahon, Man-Hong Yung, Rodney Van Meter, Alán Aspuru-Guzik, and Yoshihisa Yamamoto. Faster quantum chemistry simulation on fault-tolerant quantum computers. *New Journal of Physics*, 14(11):115023, 2012. URL: http://stacks.iop.org/1367-2630/14/i=11/a=115023.

14 J.G. Kemény and J.L. Snell. *Finite markov chains*. University series in undergraduate mathematics. Springer-Verlag New York, 1976.

15 Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. Asymptotically Optimal Approximation of Single Qubit Unitaries by Clifford and T Circuits Using a Constant Number of Ancillary Qubits. *Phys. Rev. Lett.*, 110:190502, May 2013. doi:10.1103/PhysRevLett.110.190502.

16 Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates. *Quantum Information and Computation*, 13(7-8):607–630, 2013. URL: `http://arxiv.org/abs/1206.5236`.

17 E. Knill. Quantum computing with realistically noisy devices. *Nature*, 434, Mar 2005. `doi:10.1038/nature03350`.

18 Andrew J. Landahl and Chris Cesare. Complex instruction set computing architecture for performing accurate quantum Z rotations with less magic, Feb 2013. `arXiv:1302.3240`.

19 Adam Meier, Bryan Eastin, and Emanuel Knill. Magic-state distillation with the four-qubit code. *Quantum Information and Computation*, 13:195–209, 2013. URL: `http://arxiv.org/abs/1204.4221`.

20 Adam Paetznick and Krysta M. Svore. Repeat-Until-Success: Non-determistic decomposition of single-qubit unitaries. *Quantum Info. Comput.*, 14(15-16):1277–1301, Nov 2014. URL: `http://arxiv.org/abs/1311.1074`.

21 Ben Reichardt. Quantum universality by state distillation. *Quantum Information and Computation*, 9:1030–1052, 2009. URL: `http://arxiv.org/abs/quant-ph/0608085v2`.

22 Neil J. Ross. Optimal ancilla-free Clifford+V approximation of z-rotations. *Quantum Information and Computation*, 15(11-12):932–950, 2015. URL: `http://arxiv.org/abs/1409.4355`.

23 Neil J. Ross and Peter Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. *Quantum Information and Computation*, 16(11-12):901–953, 2016. URL: `http://www.rintonpress.com/xxqic16/qic-16-1112/0901-0953.pdf`.

A Proof of Lemma 4

Similar to a single qubit, a two-qubit density matrix ρ can be expressed as a real combination of two-qubit Pauli operators $\sigma_{jk} = \sigma_j \otimes \sigma_k$, where $\sigma_0 = I$, $\sigma_1 = X$, $\sigma_2 = Y$, and $\sigma_3 = Z$ e.g. $\sigma_{13} = X \otimes Z$. We omit the tensor product and use σ_{jk} for notation reasons. We define $\mathcal{P}_\pm = \{\pm\sigma_{jk} \mid j \neq 0 \text{ and } k \neq 0\}$ to be a set of nontrivial two-qubit Pauli operators.

To prove Lemma 4, we start by rewriting Equation 4 in Definition 3 as

$$C_1\Pi_1\rho\Pi_1C_1^\dagger = (G \otimes I)C_2\Pi_2\rho\Pi_2C_2^\dagger(G^\dagger \otimes I) \tag{16}$$

where $\Pi_1 = C_1^\dagger(I \otimes |b_1\rangle\langle b_1|)C_1$ and $\Pi_2 = C_2^\dagger(I \otimes |b_2\rangle\langle b_2|)C_2$ are projection operators. Reichardt [21] showed that Equation 16 holds for some single qubit Clifford G on all states ρ if $\Pi_1 = \Pi_2$. In our two-qubit case, there are only 30 cases of $\Pi_1 = \Pi_2$. We make some refinements here to make the ideas in [21] a little more digestible in our notation.

▶ **Lemma 14.** *Let (C_1, b_1) and (C_2, b_2) be postselected two-to-one stabilizer circuits. If $\Pi = C_1^\dagger(I \otimes |b_1\rangle\langle b_1|)C_1 = C_2^\dagger(I \otimes |b_2\rangle\langle b_2|)C_2$, then $(C_1, b_1) \sim (C_2, b_2)$.*

Proof. Note that $2(I \otimes |b_j\rangle\langle b_j|) = \sigma_{00} + (-1)^{b_j}\sigma_{03}$. Let $2\Pi = \sigma_{00} + \lambda_{03}$, where $\lambda_{03} \in \mathcal{P}_\pm$, and let λ_{10}, λ_{20}, $\lambda_{30} \in \mathcal{P}_\pm$ be two-qubit Pauli operators such that $[\lambda_{03}, \lambda_{10}] = [\lambda_{03}, \lambda_{20}] = [\lambda_{03}, \lambda_{30}] = 0$ and $i\lambda_{30} = \lambda_{10}\lambda_{20}$. Let ρ be a two-qubit state. Then

$$\Pi\rho\Pi = \frac{1}{8}\left(w\sigma_{00} + w\lambda_{03} + x\lambda_{10} + x\lambda_{13} + y\lambda_{20} + y\lambda_{23} + z\lambda_{30} + z\lambda_{33}\right) \tag{17}$$

where $\lambda_{k3} = \lambda_{03}\lambda_{k0}$ and $x = \mathrm{Tr}((\lambda_{10} + \lambda_{13})\rho)$. The coefficients w, y, z are determined similarly with $\sigma_{00} + \lambda_{03}$, $\lambda_{20} + \lambda_{23}$, and $\lambda_{30} + \lambda_{33}$, respectively. Our starting condition

$C_j \lambda_{03} C_j^\dagger = (-1)^{b_j} \sigma_{03}$ implies

$$C_j \lambda_{10} C_j^\dagger, C_j \lambda_{20} C_j^\dagger \in \{\, \sigma_{10}, (-1)^{b_j} \sigma_{13}, -\sigma_{10}, (-1)^{b_j+1} \sigma_{13}, \\ \sigma_{20}, (-1)^{b_j} \sigma_{23}, -\sigma_{20}, (-1)^{b_j+1} \sigma_{23}, \\ \sigma_{30}, (-1)^{b_j} \sigma_{33}, -\sigma_{30}, (-1)^{b_j+1} \sigma_{33} \,\}. \quad (18)$$

This means there are single qubit Clifford gates G_j to permute the operators in a way that

$$(G_j \otimes I) C_j \lambda_{10} C_j^\dagger (G_j^\dagger \otimes I) \in \{\, \sigma_{10}, (-1)^{b_j} \sigma_{13} \,\} \quad (19)$$

$$(G_j \otimes I) C_j \lambda_{20} C_j^\dagger (G_j^\dagger \otimes I) \in \{\, \sigma_{20}, (-1)^{b_j} \sigma_{23} \,\}. \quad (20)$$

The value of $(G_j \otimes I) C_j \lambda_{30} C_j^\dagger (G_j^\dagger \otimes I)$ is fixed given the other two. Our unnormalized post-measurement states $\rho_j' = (G_j \otimes I) C_j \Pi \rho \Pi C_j^\dagger (G_j^\dagger \otimes I)$ are now

$$\rho_j' = \frac{1}{4} (wI + xX + yY + zZ) \otimes |b_j\rangle\langle b_j|. \quad (21)$$

The first qubit of ρ_1' and ρ_2' are the same after G_1 and G_2. Therefore $(C_1, b_1) \sim (C_2, b_2)$. ◀

We now have the tools to prove Lemma 4. Note that a Clifford equivalence $(C_1, b_1) \sim (C_2, b_2)$ is invariant with respect to Clifford circuits that execute prior to circuits C_1 and C_2 i.e. $(C_1, b_1) \sim (C_2, b_2)$ if and only if $(C_1 U, b_1) \sim (C_2 U, b_2)$ for any Clifford unitary U.

Proof. We partition the 15 Pauli operators σ_{jk} into the following sets:

$$\mathcal{P}_A = \{\sigma_{jk} \mid j,k \in \{1,2,3\}\}, \qquad \mathcal{P}_B = \{\sigma_{01}, \sigma_{02}, \sigma_{03}\}, \qquad \mathcal{P}_C = \{\sigma_{10}, \sigma_{20}, \sigma_{30}\}. \quad (22)$$

We look at σ_{33} first. Suppose there is a bit b' such that $C \sigma_{33} C^\dagger = (-1)^{b'} \sigma_{03}$. For readability, set $C' = \text{CNOT}$. Knowing $C' \sigma_{33} C'^\dagger = \sigma_{03}$, we obtain $(C, b) \sim (\text{CNOT}, b + b' \bmod 2)$ from Lemma 14. For the remaining $\sigma_{jk} \in \mathcal{P}_A$, suppose $C \sigma_{jk} C^\dagger = \pm \sigma_{03}$. Choose single qubit Clifford gates G_1 and G_2 such that $(G_1 \otimes G_2) \sigma_{jk} (G_1^\dagger \otimes G_2^\dagger) = \sigma_{33}$. Define $C'' = C(G_1^\dagger \otimes G_2^\dagger)$. Then $C'' \sigma_{33} C''^\dagger = (-1)^{b'} \sigma_{03}$ for some b'. The rest follows from previous arguments to conclude $(C''(G_1 \otimes G_2), b) = (C, b) \sim (\text{CNOT}(G_1 \otimes G_2), b + b' \bmod 2)$.

For the operator $\sigma_{03} \in \mathcal{P}_B$, assume $C \sigma_{03} C^\dagger = (-1)^{b'} \sigma_{03}$. Then $(C, b) \sim (\sigma_{00}, b + b' \bmod 2)$. Coverage of the other five from $\mathcal{P}_B$ and $\mathcal{P}_C$ is similar to the above.

To finish, suppose $(C, b) \sim (I \otimes G, b + b' \bmod 2)$, where G is a single qubit Clifford gate. If $b + b' \bmod 2 = 1$, then $(C, b) \sim (I \otimes G, 1) \equiv (I \otimes XG, 0)$. The same applies when $(C, b) \sim ((I \otimes G)\text{SWAP}, 1)$. If $(C, b) \sim (\text{CNOT}(G_1 \otimes G_2), 1)$, then we include $(I \otimes X)\text{CNOT}(G_1 \otimes G_2) = \text{CNOT}(G_1 \otimes XG_2)$. The other case $b + b' \bmod 2 = 0$ follows directly from Lemma 14. ◀

B Additional Material on Recovery Circuits

We may use the following to help us determine when two recovery circuits are Clifford equivalent. In particular, it dispels concerns that there may be two recovery circuits where one has a better chance of succeeding than the other. We use the same notation for two-qubit Paulis σ_{jk} and $\mathcal{P}_\pm$ as in Appendix A.

▶ **Lemma 15.** *Let (C_1, b_1) be a recovery circuit of an interacting postselected circuit (C, b). If (C_2, b_2) is also a recovery circuit of (C, b), then $C_1^\dagger (I \otimes |b_1\rangle\langle b_1|) C_1 = C_2^\dagger (I \otimes |b_2\rangle\langle b_2|) C_2$.*

Proof. It is easier to prove the contrapositive. Specifically, we show the recovery from (C_2, b_2) will fail on one particular pair of qubits φ_2 and $|\psi\rangle$, although many exist that are equally as good. Suppose $\Pi_2 = C_2^\dagger(I \otimes |b_2\rangle\langle b_2|)C_2$. Let $2\Pi_2 = \sigma_{00} + \lambda_{03}$, where $\lambda_{03} \in \{\pm\sigma_{jk} \mid j,k \in \{1,2,3\}\}$, and let λ_{30} and λ_{33} be two-qubit Pauli operators from $\mathcal{P}_\pm$ such that $[\lambda_{03}, \lambda_{30}] = 0$ and $\lambda_{03} = \lambda_{30}\lambda_{33}$. The qubits φ_2 and $|\psi\rangle$ we choose shall have Bloch vectors

$$\varphi_2\colon\ (x_2, y_2, z_2) = \left(\sqrt{\frac{2}{17}}, \sqrt{\frac{5}{17}}, \sqrt{\frac{10}{17}}\right), \qquad |\psi\rangle\colon\ (x, y, z) = \left(\sqrt{\frac{1}{11}}, \sqrt{\frac{3}{11}}, \sqrt{\frac{7}{11}}\right). \tag{23}$$

Let φ_1 be a qubit so that $\varphi_2 = \Phi_{1-b}(C, \varphi_1 \otimes \psi)$. Let $\varphi_1' = \Phi_{b_2}(C_2, \varphi_2 \otimes \psi)$.

To prove the recovery by (C_2, b_2) will fail, we merely need to verify that the Bloch vectors from all 18 choices of λ_{03} are different, which implies $\varphi_1' \neq \varphi_1$ whenever $C_1^\dagger(I \otimes |b_1\rangle\langle b_1|)C_1 \neq \Pi_2$. We track the coefficients $a_{jk} = \mathrm{Tr}(\lambda_{jk}(\varphi_2 \otimes \psi))$. Then

$$\mathrm{Tr}\left(\Pi_2\left(\varphi_2 \otimes \psi\right)\Pi_2\right) = \frac{1 + a_{03}}{2}, \quad \mathrm{Tr}\left(\lambda_{30}\Pi_2\left(\varphi_2 \otimes \psi\right)\Pi_2\right) = \frac{a_{30} + a_{33}}{2}, \tag{24}$$

yielding $v = (a_{30} + a_{33})/(1 + a_{03})$ as a Bloch vector component of φ_1'. The most convenient choices for λ_{30} and λ_{33} are tensor products with the identity e.g. $\lambda_{03} = -\sigma_{33}$, $\lambda_{30} = \sigma_{30}$, $\lambda_{33} = -\sigma_{03}$, and $\lambda_{03} = \sigma_{11}$, $\lambda_{30} = \sigma_{10}$, $\lambda_{33} = \sigma_{01}$, which means that $a_{03} = a_{30}a_{33}$. If we look at the coefficients from the first example with $\lambda_{03} = -\sigma_{33}$, then $a_{30} = z_2$ and $a_{33} = -z$. We get the following components for each of the positive possibilities for λ_{03}:

λ_{03}	a_{03}	λ_{30}	a_{30}	λ_{33}	a_{33}	v
σ_{11}	x_2x	σ_{10}	x_2	σ_{01}	x	0.5841
σ_{12}	x_2y	σ_{10}	x_2	σ_{02}	y	0.7338
σ_{13}	x_2z	σ_{10}	x_2	σ_{03}	z	0.8957
σ_{21}	y_2y	σ_{20}	y_2	σ_{01}	x	0.7252
σ_{22}	y_2y	σ_{20}	y_2	σ_{02}	y	0.8296
σ_{23}	y_2z	σ_{20}	y_2	σ_{03}	z	0.9354
σ_{31}	z_2x	σ_{30}	z_2	σ_{01}	x	0.8678
σ_{32}	z_2y	σ_{30}	z_2	σ_{02}	y	0.9205
σ_{33}	z_2z	σ_{30}	z_2	σ_{03}	z	0.9708

and the following for each of the negative possibilities for λ_{03}:

λ_{03}	a_{03}	λ_{30}	a_{30}	λ_{33}	a_{33}	v
$-\sigma_{11}$	$-x_2x$	σ_{10}	x_2	$-\sigma_{01}$	$-x$	0.0463
$-\sigma_{12}$	$-x_2y$	σ_{10}	x_2	$-\sigma_{02}$	$-y$	-0.2183
$-\sigma_{13}$	$-x_2z$	σ_{10}	x_2	$-\sigma_{03}$	$-z$	-0.6260
$-\sigma_{21}$	$-y_2y$	σ_{20}	y_2	$-\sigma_{01}$	$-x$	0.2879
$-\sigma_{22}$	$-y_2y$	σ_{20}	y_2	$-\sigma_{02}$	$-y$	0.0280
$-\sigma_{23}$	$-y_2z$	σ_{20}	y_2	$-\sigma_{03}$	$-z$	-0.4501
$-\sigma_{31}$	$-z_2x$	σ_{30}	z_2	$-\sigma_{01}$	$-x$	0.6055
$-\sigma_{32}$	$-z_2y$	σ_{30}	z_2	$-\sigma_{02}$	$-y$	0.4083
$-\sigma_{33}$	$-z_2z$	σ_{30}	z_2	$-\sigma_{03}$	$-z$	-0.0792

Neither are any of the values v the same if we multiple each one by -1, which may come about from an application of a single qubit Pauli on the output. Thus our statement holds. ◀