Two-Qubit Stabilizer Circuits with Recovery I: Existence

Wim van Dam* Raymond Wong†

March 19, 2018

Abstract

Understanding how a stabilizer circuit responds to different input is important to formulating an effective strategy for resource management. 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 ancilla to succeed. 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 any two-qubit stabilizer procedure involving non-stabilizer resources.

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% [19] 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 [11], 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 [5]. 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. The primary concern then is the large input-to-output ratio before the magic state error is low enough to be permitted in a fault-tolerant scheme. Numerous proposals over the last few years have made tremendous advances to increase the efficiencies of this technique [4, 8, 9, 14, 21], 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

*Department of Computer Science, Department of Physics, University of California, Santa Barbara, CA, USA
†Department of Computer Science, University of California, Santa Barbara, CA, USA
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 \[17, 18, 24, 25\]. 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 \[6, 7\].

The creativity that went into designing these distillation protocols is one reason motivating our study of stabilizer operations. Other uses include procedures for distilling multiple types of magic qubits \[8, 9, 14, 20\], as well as implementing phase rotations with low depth circuits. Some notable examples of the latter are contained in \[10\] and \[15\], both of which feature the same stabilizer circuit to perform the operation. The differences lie in the pre-computed ancillas injected into the circuit, where Duclos-Cianci and Svore \[10\] 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-homogenous states at our disposal, and all that is required is a two-qubit stabilizer circuit.

Here we consider general two-to-one stabilizer procedures that take a two-qubit state and produces 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. Some limits on distilling two-qubit states are already discussed in \[23\]. Instead, we refine the implementation details first provided by Reichardt \[23\] to identify three circuit configurations characterizing all such procedures. These three forms suggest that in addition to Pauli measurements and postselection, single qubit Clifford gates and at most one \textsc{CNOT} or \textsc{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 \textsc{CNOT} variety: there are “recovery circuits” that can recuperate a product state input from a corrupted stabilizer circuit output. For our main result, we show that any two-to-one stabilizer procedure realizable by one \textsc{CNOT} has a recovery circuit, and that every recovery circuit to this procedure has the same probability of recovery, which means any will suffice to install as part of a larger computation. We end with a few experiments showcasing the benefits of recovery circuits.

2 Preliminaries

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

\[
I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.
\]

They satisfy not only the identities

\[
X^2 = Y^2 = Z^2 = I, \quad XY = iZ, \quad YZ = iX, \quad ZX = iY
\]

but they also form a basis for the space of $2 \times 2$ Hermitian matrices. We can expand any single qubit density matrix $\varphi$ in terms of Pauli matrices using the expression

\[
\varphi = \frac{1}{2} \left( I + xX + yY + zZ \right).
\]

If we collect the coefficients above, then $(x, y, z) \in \mathbb{R}^3$ is the Bloch vector of $\varphi$. 

2
A postselected two-to-one stabilizer circuit $(C, b)$ consists of a stabilizer circuit component $C$ and a postselected bit value $b$. (b) 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 $\rho$.

A $n$-qubit stabilizer circuit is limited to certain quantum gates and measurements. It may use elements from the Clifford group $C(n)$, 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:

\[
\begin{align*}
\text{CNOT} &= \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
\end{bmatrix}, \\
H &= \frac{1}{\sqrt{2}} \begin{bmatrix}
1 & 1 \\
1 & -1 \\
\end{bmatrix}, \\
P &= \begin{bmatrix}
1 & 0 \\
0 & i \\
\end{bmatrix}. \\
\end{align*}
\]

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

\[
\begin{array}{c}
Z \\
\end{array}
\]

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 [23] to derive Lemma 1. Part of the novelty that Lemma 1 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 [23] to present our result.

A $n$-to-1 stabilizer reduction is a procedure that accepts a $n$-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 [23]. Since our focus is on $n = 2$, we have the following definition.

**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 $\rho$ be a two-qubit state. Then the probability $Q_b$ of outcome $b$ on the transformed state $C\rho C^\dagger$ is

\[
Q_b(C, \rho) = \text{Tr}((I \otimes \langle b \rangle)C\rho C^\dagger(I \otimes |b\rangle)).
\]
If $Q_b(C,\rho) > 0$, then the output $\Phi_b$ of a postselected circuit $(C, b)$ on an input $\rho$ is

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

(6)

At times, we may say circuit $C$ to reference the stabilizer circuit piece only of the postselected circuit, which includes the measurement at the end. This allows us to use language about how we may use or run the circuit $C$ and is often followed by details on what course of action to take conditional on $b$ (or $1-b$). 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 $\rho$, we have the equality

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

(7)

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 7.

We may also alter the circuits using $|b_2\rangle = X|1-b_2\rangle$ in Equation 7 so that both postselect on the same value.

As we mentioned earlier, 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 23. 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 1.** For every postselected two-to-one stabilizer circuit $(C, b)$, there exists single qubit Clifford gates $G_1$ and $G_2$ such that either $(C, b) \sim (I \otimes G_1,0)$, or $(C, b) \sim ((I \otimes G_1)\text{SWAP},0)$, or $(C, b) \sim (\text{CNOT}(G_1 \otimes G_2),0)$.

**Corollary 1.** Let $(C_{eq}, b_{eq}) \sim (C, b)$. Then $(C, 1-b)$ is Clifford equivalent to a slightly modified version $(C_{eq}', b_{eq}')$ of $(C_{eq}, b_{eq})$:

$$
\begin{array}{c|c}
(C_{eq}, b_{eq}) \sim (C, b) & (C_{eq}', b_{eq}') \sim (C, 1-b) \\
(I \otimes G_1,0) & (I \otimes XG_1,0) \\
((I \otimes G_1)\text{SWAP},0) & ((I \otimes XG_1)\text{SWAP},0) \\
(\text{CNOT}(G_1 \otimes G_2),0) & ((I \otimes X)\text{CNOT}(G_1 \otimes G_2),0)
\end{array}
$$  

(8)
Due to Lemma 1, 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. \(((CNOT(Z \otimes I), 0) \equiv ((Z \otimes I)\text{CNOT}, 0) \sim (\text{CNOT}, 0)\). 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, 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 \(|C(1)| = 24\) 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 \(\rho\) 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 \(\varphi\).

This input requirement means the only circuit configuration of Lemma 1 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 \(\varphi_1\). 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 4** (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. As a matter of convenience, we use \(\psi\) in place \(|\psi\rangle\langle \psi|\) throughout the remainder of our discussion on recovery circuits.

**Definition 5** (recovery circuit). Let \((C, b)\) be an interacting postselected circuit. Then 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

\[
\varphi = \Phi_{\psi} (C', \Phi_{1-b}(C, \varphi \otimes \psi) \otimes \psi) \, .
\] (9)

Notice that an input qubit to \((C', b')\) is \(\Phi_{1-b}(C, \varphi \otimes \psi)\), the output from the circuit that postselects on the opposite outcome. 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 \(\varphi \otimes \psi\) by using a presumably much simpler circuit \(C'\) to recover \(\varphi\). Our next lemma presents one way on how to design such a recovery circuit to \((C, b)\).

**Lemma 2.** 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 1, we know

\[
(C, 1-b) \sim ((I \otimes X)\text{CNOT}(G_1 \otimes G), 0) \equiv (\text{CNOT}(G_1 \otimes G), 1)\, .
\] (10)
Figure 3: Suppose \((C, 1 - b) \equiv ((G_2^\dagger \otimes I) \text{CNOT}(G_1 \otimes G), 1)\). 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 \(\varphi'_1\) and \(\varphi'_2 = G_2 \varphi_2 G_2^\dagger\) in (a) to signify stages in the circuit.

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 3 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 \(\varphi'_1\) and \((x, y, z)\) be the Bloch vector of \(|\psi'\rangle\). For ease of notation, we define outputs

\[
\varphi'_2 = \Phi_1(CNOT, \varphi'_1 \otimes \psi')
\]

\[
\varphi_2 = G_2^\dagger \varphi'_2 G_2 = \Phi_{1-b}(C, \varphi_1 \otimes \psi).
\]

Then the Bloch vector \((x_2, y_2, z_2)\) of \(\varphi'_2\) becomes

\[
x_2 = \frac{x_1 x + y_1 y}{1 - z_1 z}, \quad y_2 = \frac{y_1 x - x_1 y}{1 - z_1 z}, \quad z_2 = \frac{z_1 - z}{1 - z_1 z}.
\]

Now suppose \(\varphi_3 = \Phi_0(CNOT(G_2 \otimes G), \varphi_2 \otimes \psi)\). For postselected circuits that are basically a single \(\text{CNOT}\), the equations for computing the output’s Bloch vector are essentially the same:

\[
x_3 = x_2 - \frac{y_2 y}{1 + z_2 z}, \quad y_3 = \frac{y_2 x + x_2 y}{1 + z_2 z}, \quad z_3 = \frac{z_2 + z}{1 + z_2 z},
\]

where \((x_3, y_3, z_3)\) represents the Bloch vector of \(\varphi_3\). Using \(x^2 + y^2 + z^2 = 1\), we can show

\[
x_3 = \frac{x_1 x^2 + x_1 y - x_1 y + x_1 y^2}{1 - z_1 z + z_1 z - z^2} = x_1.
\]

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 \(((G_1^\dagger \otimes I) \text{CNOT}(G_2 \otimes G), 0)\) is therefore a recovery circuit of \((C, b)\).

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

**Corollary 2.** Let \(\varphi_1 \otimes \psi\) be a two-qubit state and let \(C' = (G_1^\dagger \otimes I) \text{CNOT}(G_2 \otimes G)\) be a two-qubit Clifford unitary such that \((C', 0)\) is a recovery circuit of \((C, b)\). Then

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

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

$$Q_1(C, \varphi_1 \otimes \psi) = \frac{1 - z_1 z}{2}.$$  

Similarly, $z_2 = \text{Tr}(Z\varphi_2) = \frac{z_1 - z}{1 - z_1 z}$. The probability of recovering $\varphi_1$ is now clear:

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

since the circuits perform a single measurement. \qed

Another implication of the proof to Lemma 2 is that $\Phi_{1-b}(C, \varphi_1 \otimes \psi)$ is always $\varphi_1$, 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 $(C_1 \otimes I)\text{CNOT}(G_2 \otimes G)$ to try and perform a recovery because the qubit is basically $\varphi_1$. It is also quite evident by now that there is only one type of recovery circuit, especially given our construction in Lemma 2.

Lemma 3. 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 $\varphi$ on the input $\Phi_{1-b}(C, \varphi \otimes \psi) \otimes \psi$. \qed

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 4. Let $(C, b)$ be an interacting postselected circuit, and let $C'' = (G_1^4 \otimes I)\text{CNOT}(G_1 \otimes G)$ be a two-qubit Clifford unitary such that $(C, 1-b) \equiv (C'', 1-b'')$. Then $(C', b')$ is a recovery circuit of $(C, b)$ if and only if $(C', b') \equiv ((G_1^4 \otimes I)\text{CNOT}(G_2 \otimes G), b'')$.

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

In the forward direction, Lemmas 5 and 6 in the Appendices do most of the job: $(C', b') \sim ((G_1^4 \otimes I)\text{CNOT}(G_2 \otimes G), b'')$. 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

$$(I \otimes \langle b'\rangle)C'_{\rho}C'^\dagger(I \otimes |b'\rangle) = (G \otimes \langle b''\rangle)C''_{\rho}C''^\dagger(G^4 \otimes |b''\rangle)$$  

for all two-qubit states $\rho$. 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 $\rho$ will be rotated by $G$. Thus the two must be equivalent (with “$\equiv$”).

\end{document}
Figure 4: The postselected circuit \((\text{CNOT}, 0)\) appears in both [10] and [15], with each one supplying a different input set to circuit \(\text{CNOT}\). The qubit \(|H_0\rangle\) in (a) is the +1 eigenstate of \(H\), and the process of generating \(|H_{i+1}\rangle\) in [10] starts with \(|H_0\rangle \otimes |H_0\rangle\). For (b), a qubit \(|\gamma\rangle\) leads to a +\(\gamma\) Z-rotation on the first qubit \(\alpha|0\rangle + \beta|1\rangle\) upon measuring 0.

From Lemmas 2 and 4 we reach our main result, with Corollary 3 as an immediate consequence to our theorem.

**Theorem 1.** 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 3.** Every recovery circuit \((C', b')\) has its own recovery circuit \((C'', b'')\) with \(b'' = b'\).

**Proof.** The first claim is a given since recovery circuits are interacting postselected circuits themselves by Lemma 3. If the recovery circuit \((C'', b'')\) already satisfies \(b'' = b'\), then we are done. Otherwise, \(b'' = 1 - b'\), so \((C'', b'') \equiv ((I \otimes X)C'', b')\).

### 5 Example Routines Featuring Recovery Circuits

Recovery circuits appear in the literature. The procedure of [10] uses an interacting circuit with a single \(\text{CNOT}\) to obtain “ladder” qubit states of the kind

\[
|H_i\rangle = \cos (\theta_i) |0\rangle + \sin (\theta_i) |1\rangle, \quad \cot (\theta_i) = \cot^{i+1} (\pi/8)
\]

for \(i \geq 0\). The production starts by supplying two copies of the magic state \(|H_0\rangle = H|H_0\rangle\) to the \(\text{CNOT}\) circuit in Figure 4a. Each time we gain a new state \(|H_i\rangle\), we can reuse the qubit in an attempt to 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.

The programmable ancilla rotation (PAR) of [15] is similar. It uses qubits of the kind

\[
|\gamma\rangle = \frac{|0\rangle + e^{i\gamma}|1\rangle}{\sqrt{2}}
\]

to rotate \(|q\rangle = \alpha|0\rangle + \beta|1\rangle\) about the Z-axis by an angle \(\gamma\), demonstrated in Figure 4b. The PAR routine uses the same interacting circuit \(\text{CNOT}\) to achieve this task. On the chance that the Z-measurement returns 1, then instead of \(|q + \gamma\rangle = \alpha|0\rangle + e^{i\gamma}|1\rangle\), the output becomes \(|q - \gamma\rangle = \alpha|0\rangle + e^{-i\gamma}|1\rangle\), which is \(|q\rangle\) rotated by \(-\gamma\). Jones et al. [15] suggest pairing \(|q - \gamma\rangle\) with \(|2\gamma\rangle\) as a direct line to \(|q + \gamma\rangle\), but we can alternatively break this down into two smaller steps if \(|\gamma\rangle\) are the only states available. We first run the \(\text{CNOT}\) circuit on \(|q - \gamma\rangle \otimes |\gamma\rangle\). If we measure 0, then we recover \(|q\rangle\), and we proceed with rerunning circuit \(\text{CNOT}\) on \(|q\rangle \otimes |\gamma\rangle\).

In addition to pure qubits, our notation for the two-qubit state \(\varphi \otimes \psi\) throughout the previous section indicates that \(\varphi\) is allowed to be mixed, and it can even be part of a larger entangled system.
Figure 5: Recovery circuits also work 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 $\varphi$. We succeed with the recovery if we measure $b'$.

As a quick demonstration, suppose we have the situation as illustrated in Figure 5a. Let $(C', b')$ be the recovery circuit of $(C, b)$ and let

$$U\rho U^\dagger = \frac{1}{2^n} (P_I \otimes I + P_X \otimes X + P_Y \otimes Y + P_Z \otimes Z)$$

where $P_L$ are Pauli operator sums on the first $n-1$ qubits. While the proof to Lemma 2 is generalizable to include the unused portions $P_L$ 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 $\varphi = \text{Tr}_{1,n-1} (U\rho U^\dagger)$ 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 $\varphi$ 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 $\rho$ 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 [12]. 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 3, we can define a depth $k$ protocol to be a procedure on $k-1$ postselected circuits $(C_1, b_1), \ldots, (C_{k-1}, b_{k-1})$ such that $(C_i, b_i)$ is the recovery circuit of $(C_{i-1}, b_{i-1})$. 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 $\varphi$. 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 \([17]\) in Corollary \([2]\). 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 \( \Phi_k(C_1, \varphi \otimes \psi) \) with our depth \( k \) protocol. Let \( d \) be the cost to prepare a single instance of \( \varphi \) 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 tallied together and divided by the number of successful trials to obtain \( N_k \). We compare this against the expected cost without recovery (\( k = 2 \)), which is

\[
N_2 = \frac{d + 1}{Q_{b_1}(C_1, \varphi \otimes \psi)}.
\]

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 \([17]\). Technically, we need a different \( \varphi \) with each choice of \(|\psi\rangle\) to maintain \( Q_0(\text{CNOT}, \varphi \otimes \psi) = 1/2 \) and the same output \( \Phi_0(C_1, \varphi \otimes \psi) \). Usually different \( \varphi \) means different costs \( d \), but we will ignore this momentarily and assume the preparation overhead \( d \) for each \( \varphi \) 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 \( \varphi \) 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 \( \varphi \) 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          |
Figure 6: The success probability between circuit $C_i$ and circuit $C_{i+1}$ defined recursively in Corollary 2 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 $z = 0$.

Observe that the value of $N_k$ continue to lower noticeably for some of $|\psi\rangle$ 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 seven circuits of the protocol for each of the four $z$ samples in Figure 6, 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 $\varphi$.

One natural follow-up is whether something resembling recovery circuits exist for larger stabilizer circuits that is distinct from stabilizer error correcting code procedures. This question has been answered to an extent for the Clifford+$T$ gate set in [2, 3, 22], where we can treat $|\psi\rangle = HP^\dagger|H_0\rangle$ to perform a non-Clifford $\pi/4$ phase rotation

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}.$$  \hspace{1cm} (26)

The goal in [2, 3, 22] uses a multiqubit circuit of Clifford+$T$ gates to approximate an arbitrary single qubit unitary $U$ up to some error $\epsilon$. 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 exists conditions that enable larger
stabilizer circuits to exhibit the recovery feature we demonstrated here on general $|\psi\rangle$ resources.

Another direction that we may pursue is a more detailed and thorough examination of the depth
$k$ protocol. 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 in Section 6, 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 [2, 10, 15]). One matter we need to keep in mind is the costs of attaining
qubits $\varphi$ and $|\psi\rangle$. The amount of work that went into preparing $\varphi$ 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 [15] should also prove useful for gathering a
more precise cost estimate. From there, we could gain better insight into the overall capabilities
and limitations of stabilizer circuits acting on non-stabilizer input.

References

[1] A. Bocharov, Y. Gurevich, and K. M. Svore, “Efficient decomposition of single-qubit gates
into $v$ basis circuits,” Phys. Rev. A, vol. 88, p. 012313, Jul 2013. [Online]. Available:
http://link.aps.org/doi/10.1103/PhysRevA.88.012313

[2] A. Bocharov, M. Roetteler, and K. M. Svore, “Efficient synthesis of probabilistic quantum
circuits with fallback,” Phys. Rev. A, vol. 91, p. 052317, May 2015. [Online]. Available:
https://link.aps.org/doi/10.1103/PhysRevA.91.052317

[3] ——, “Efficient synthesis of universal repeat-until-success quantum circuits,” Phys. Rev.
Lett., vol. 114, p. 080502, Feb 2015. [Online]. Available: http://link.aps.org/doi/10.1103/
PhysRevLett.114.080502

[4] S. Bravyi and J. Haah, “Magic-state distillation with low overhead,” Phys. Rev. A, vol. 86, p.
052329, Nov 2012. [Online]. Available: http://dx.doi.org/10.1103/PhysRevA.86.052329

[5] S. Bravyi and A. Kitaev, “Universal quantum computation with ideal clifford gates
and noisy ancillas,” Phys. Rev. A, vol. 71, p. 022316, Feb 2005. [Online]. Available:
https://link.aps.org/doi/10.1103/PhysRevA.71.022316

[6] E. T. Campbell and M. Howard, “Unified framework for magic state distillation and
multiqubit gate synthesis with reduced resource cost,” Phys. Rev. A, vol. 95, p. 022316, Feb
2017. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.95.022316

[7] ——, “Unifying gate synthesis and magic state distillation,” Phys. Rev. Lett., vol. 118,
p. 060501, Feb 2017. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.118.
060501

[8] E. T. Campbell and J. OGorman, “An efficient magic state approach to small angle
rotations,” Quantum Science and Technology, vol. 1, no. 1, p. 015007, 2016. [Online].
Available: http://stacks.iop.org/2058-9565/1/i=1/a=015007

[9] G. Duclos-Cianci and D. Poulin, “Reducing the quantum-computing overhead with complex
gate distillation,” Phys. Rev. A, vol. 91, p. 042315, Apr 2015. [Online]. Available:
https://link.aps.org/doi/10.1103/PhysRevA.91.042315
[10] G. Duclos-Cianci and K. M. Svore, “Distillation of nonstabilizer states for universal quantum computation,” *Phys. Rev. A*, vol. 88, p. 042325, Oct 2013. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.88.042325

[11] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, “Surface codes: Towards practical large-scale quantum computation,” *Phys. Rev. A*, vol. 86, p. 032324, Sep 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.86.032324

[12] B. Giles and P. Selinger, “Exact synthesis of multiqubit clifford+t circuits,” *Phys. Rev. A*, vol. 87, p. 032332, Mar 2013. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.87.032332

[13] D. Gottesman, “Stabilizer codes and quantum error correction,” Ph.D. dissertation, California Institute of Technology, 1997, http://arxiv.org/abs/quant-ph/9705052.

[14] J. Haah, M. B. Hastings, D. Poulin, and D. Wecker, “Magic State Distillation with Low Space Overhead and Optimal Asymptotic Input Count,” *Quantum*, vol. 1, p. 31, Oct. 2017. [Online]. Available: https://doi.org/10.22331/q-2017-10-03-31

[15] N. C. Jones, J. D. Whitfield, P. L. McMahon, M.-H. Yung, R. V. Meter, A. Aspuru-Guzik, and Y. Yamamoto, “Faster quantum chemistry simulation on fault-tolerant quantum computers,” *New Journal of Physics*, vol. 14, no. 11, p. 115023, 2012. [Online]. Available: http://stacks.iop.org/1367-2630/14/i=11/a=115023

[16] J. Kemény and J. Snell, *Finite markov chains*, ser. University series in undergraduate mathematics. Springer-Verlag New York, 1976.

[17] V. Kluchnikov, D. Maslov, and M. Mosca, “Asymptotically optimal approximation of single qubit unitaries by clifford and t circuits using a constant number of ancillary qubits,” *Phys. Rev. Lett.*, vol. 110, p. 190502, May 2013. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.110.190502

[18] ———, “Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates,” *Quantum Information and Computation*, vol. 13, no. 7-8, pp. 607–630, 2013. [Online]. Available: http://arxiv.org/abs/1206.5236

[19] E. Knill, “Quantum computing with realistically noisy devices,” *Nature*, vol. 434, Mar 2005. [Online]. Available: https://arxiv.org/abs/quant-ph/0410199

[20] A. J. Landahl and C. Cesare, “Complex instruction set computing architecture for performing accurate quantum z rotations with less magic,” Feb 2013. [Online]. Available: https://arxiv.org/abs/1302.3240

[21] A. Meier, B. Eastin, and E. Knill, “Magic-state distillation with the four-qubit code,” *Quantum Information and Computation*, vol. 13, pp. 195–209, 2013. [Online]. Available: http://arxiv.org/abs/1204.4221

[22] A. Paetznick and K. M. Svore, “Repeat-until-success: Non-deterministic decomposition of single-qubit unitaries,” *Quantum Info. Comput.*, vol. 14, no. 15-16, pp. 1277–1301, Nov. 2014. [Online]. Available: http://arxiv.org/abs/1311.1074
where \( \Pi \) and \( i \lambda \).  

**Lemma 5.**  
In our two-qubit case, there are only 30 cases of \( \Pi \)

Similar to a single qubit, a two-qubit density matrix

A Proof of Lemma 1

To prove Lemma 1, we start by rewriting Equation 7 in Definition 3 as

\[
C_1 \Pi_1 \rho \Pi_1 C_1^T = (G \otimes I) C_2 \Pi_2 \rho \Pi_2 C_2^T (G^T \otimes I)
\]

(27)

where \( \Pi_1 = C_1^T (I \otimes |b_1\rangle \langle b_1|) C_1 \) and \( \Pi_2 = C_2^T (I \otimes |b_2\rangle \langle b_2|) C_2 \) are projection operators. Reichardt showed that Equation 27 holds for some single qubit Clifford \( G \) on all states \( \rho \) 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 Reichardt a little more digestible in our notation.

**Lemma 5.** Let \((C_1, b_1)\) and \((C_2, b_2)\) be postselected two-to-one stabilizer circuits. If

\[
C_1^T (I \otimes |b_1\rangle \langle b_1|) C_1 = \Pi = C_2^T (I \otimes |b_2\rangle \langle b_2|) C_2,
\]

(28)

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 \(\lambda_{10}, \lambda_{20}, \lambda_{30} \in \mathcal{P}_\pm\) 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 \(\rho\) be a two-qubit state. Then

\[
\Pi \rho \Pi = \frac{1}{8} (w \sigma_{00} + w \lambda_{03} + x \lambda_{10} + x \lambda_{13} + y \lambda_{20} + y \lambda_{23} + z \lambda_{30} + z \lambda_{33})
\]

(29)

where \(\lambda_{k3} = \lambda_{03} \lambda_{k0}\) and \(x = \text{Tr}(\lambda_{10} + \lambda_{13})\rho\). 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 \(C_j \lambda_{03} C_j^T = (-1)^{b_j} \sigma_{03}\) implies

\[
C_j \lambda_{10} C_j^T, C_j \lambda_{20} C_j^T \in \{ \sigma_{10}, (-1)^{b_j} \sigma_{13}, -\sigma_{10}, (-1)^{b_j} + 1 \sigma_{13}, \sigma_{20}, (-1)^{b_j} \sigma_{23}, -\sigma_{20}, (-1)^{b_j} + 1 \sigma_{23}, \sigma_{30}, (-1)^{b_j} \sigma_{33}, -\sigma_{30}, (-1)^{b_j} + 1 \sigma_{33} \}. 
\]

(30)
This means there are single qubit Clifford gates $G_j$ to permute the operators in a way that

\[(G_j \otimes I)C_j\lambda_1\lambda_2C_j^{-1}(G_j^\dagger \otimes I) \in \{ \sigma_{10}, (-1)^b\sigma_{13} \} \] (31)

\[(G_j \otimes I)C_j\lambda_2\lambda_3C_j^{-1}(G_j^\dagger \otimes I) \in \{ \sigma_{20}, (-1)^b\sigma_{23} \}. \] (32)

The value of $(G_j \otimes I)C_j\lambda_3\lambda_0C_j^{-1}(G_j^\dagger \otimes I)$ is fixed given the other two. Our unnormalized post-measurement states $\rho_j' = (G_j \otimes I)C_j\Pi\rho_jG_j^\dagger(G_j^\dagger \otimes I)$ are now

\[\rho_j' = \frac{1}{4}(wI + xX + yY + zZ) \otimes |b_j\rangle\langle b_j|. \] (33)

The first qubit of $\rho_1'$ and $\rho_2'$ are the same after $G_1$ and $G_2$. Therefore $(C_1, b_1) \sim (C_2, b_2)$. \(\square\)

We now have the tools available to prove Lemma 1. 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 $(C_1U, b_1) \sim (C_2U, b_2)$ for any Clifford unitary $U$.

**Proof.** We partition the 15 Pauli operators $\sigma_{jk}$ into the following sets:

\[\mathcal{P}_A = \{ \sigma_{jk} \mid j, k \in \{1, 2, 3\} \}, \quad \mathcal{P}_B = \{ \sigma_{01}, \sigma_{02}, \sigma_{03} \}, \quad \mathcal{P}_C = \{ \sigma_{10}, \sigma_{20}, \sigma_{30} \}. \] (34)

We look at $\sigma_{33}$ 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 $(C, b) \sim (\text{CNOT}, b + b' \mod 2)$ from Lemma 5.

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 $(C'', (G_1 \otimes G_2), b) = (C, b) \sim (\text{CNOT}(G_1 \otimes G_2), b + b' \mod 2)$.

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

To finish, suppose $(C, b) \sim (I \otimes G, b + b' \mod 2)$, where $G$ is a single qubit Clifford gate. If $b + b' \mod 2 = 1$, 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 $b + b' \mod 2 = 0$ follows directly from Lemma 5. \(\square\)

## 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 $\sigma_{jk}$ and $\mathcal{P}_{\pm}$ as in Appendix A.

**Lemma 6.** 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 $\psi_2$ and $|\psi\rangle$, although many exists 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 $\lambda_{03} \in \mathcal{P}_{\pm}$, and let $\lambda_{30}$ and $\lambda_{33}$ be
two-qubit Pauli operators from \( P_{\pm} \) such that \([\lambda_{03}, \lambda_{30}] = 0\) and \(\lambda_{03} = \lambda_{30}\lambda_{33}\). The qubits \(\varphi_2\) and \(|\psi\rangle\) we choose shall have Bloch vectors

\[
\varphi_2: (x_2, y_2, z_2) = \left(\sqrt{\frac{2}{17}}, \sqrt{\frac{5}{17}}, \sqrt{\frac{10}{17}}\right), \quad |\psi\rangle: (x, y, z) = \left(\sqrt{\frac{1}{11}}, \sqrt{\frac{3}{11}}, \sqrt{\frac{7}{11}}\right). \tag{35}
\]

Let \(\varphi_1\) 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 \(\lambda_{03}\) 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 \(a_{jk} = \text{Tr}(\lambda_{jk}(\varphi_2 \otimes \psi))\). Then

\[
\text{Tr} (\Pi_2 (\varphi_2 \otimes \psi) \Pi_2) = \frac{1 + a_{03}}{2}, \quad \text{Tr} (\lambda_{30} \Pi_2 (\varphi_2 \otimes \psi) \Pi_2) = \frac{a_{30} + a_{33}}{2}, \tag{36}
\]
yielding \(v = \frac{a_{30} + a_{33}}{1 + a_{03}}\) as a Bloch vector component of \(\rho'_1\). The most convenient choices for \(\lambda_{30}\) and \(\lambda_{33}\) are tensor products with one 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 possibility of \(\lambda_{03}\):

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

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

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