Lecture 7. Quantum circuits and the stabilizer formalism

Pedram Roushan, Google Quantum AI

Started: April 2025, last modified: August 25, 2025

CONTENTS

ABSTRACT

The familiar languages of quantum mechanics are the differential equations of Schrödinger and the matrix mechanics of Heisenberg. However, influenced by computer scientists, researchers have developed a new language to help understand quantum computations provided by the quantum circuit model, which is a generalization of the classical circuit model based on Boolean logical operations. We can use a quantum circuit to depict qubits' initialization, evolution, and measurement. Quantum circuits are useful tools independent of the physical implementation; hence, the ease of communication.

Stabilizer circuits are a rich subset of quantum circuits that displays many interesting features of quantum computation, such as entanglement and teleportation, and are central to quantum error correction, but are not universal and can be simulated using an efficient algorithm. The stabilizer formalism has played a large part in research in quantum computing theory since its development in 1996. Stabilizer circuits can be thought of as an "easy subset" of quantum circuits, and the goal of this part is to develop an intuitive understanding of the evolution of a quantum state through these circuits.

1. A BRIEF HISTORICAL REVIEW OF QUANTUM COMPUTATION

The principles of quantum mechanics, which govern all known natural phenomena, were discovered in 1925. Over the past century, this foundational breakthrough has enabled a deep understanding of the physical world-from molecules and materials to elementary particles and beyond. No equally transformative advancement in fundamental science has occurred since. Until recently, most of what we have learned about the quantum world has come from studying the behavior of individual particles-such as a single electron propagating as a wave through a crystal, unaffected by barriers that would obstruct classical particles. Mastering this single-particle physics has empowered us to explore nature in unprecedented ways and to develop technologies of the *first quantum revolution*-technologies that have profoundly reshaped our lives.

We are entering a new era of quantum science-one that moves beyond individual particles to the coordinated behavior of many. When particles such as electrons or atoms become entangled, they form complex quantum states that cannot be understood in terms of their parts alone. These highly entangled systems exhibit behaviors that are often intractable for classical computers and stretch the limits of existing theoretical frameworks. This opens opportunities for discovery and innovation. Most significantly, the ability to engineer and control such

complexity paves the way for quantum computers capable of solving problems that are far beyond the reach of today's classical machines. We are at the threshold of the *second quantum revolution*.

The idea of a quantum computer emerged over 40 years ago, when researchers sought to merge the principles of quantum mechanics with another transformative framework of the 20th century: information theory. This convergence gave rise to a new field-quantum information science-which fundamentally reshaped our understanding of computation, information, and their deep ties to the physical laws. It also led to groundbreaking applications, including radically new algorithms and communication protocols. What began as a theoretical insight has since grown into a vibrant discipline, driving both foundational advances and the development of powerful new technologies.

Information theory, which includes the foundations of both computer science and communications, abstracted away the physical world so effectively that it became possible to talk about the major issues within computer science and communications, such as the efficiency of an algorithm or the robustness of a communication protocol, without understanding details of the physical devices used for the computation or the communication. This ability to ignore the underlying physics proved extremely powerful and its success can be seen in the ubiquity of the computing and communications devices around us. The abstraction away from the physical had become such a part of the intellectual landscape that the assumptions behind it were almost forgotten. At its heart, until recently, information sciences have been firmly rooted in classical mechanics.

Throughout the last century, quantum mechanics has played an increasingly important role in the development of more efficient computing technologies. It underpins the operation of classical computers and communication devices, from transistors and lasers to the latest hardware innovations that boost speed and power while reducing the size of components. Until recently, however, the influence of quantum mechanics was limited to the low-level implementation of such technologies; it had little to no impact on how computation or communication was conceptualized or studied.

In the early 1980s, a few researchers began to realize that quantum mechanics had unexpected implications for information processing. C. Bennett and G. Brassard, building on ideas from S. Wiesner, demonstrated that the non-classical properties of quantum measurement could be used to establish a cryptographic key with provable security. Around the same time, R. Feynman, Y. Manin, and others observed that certain quantum phenomena-particularly those involving entangled particles-could not be efficiently simulated by a classical Turing machine. This insight led to speculation that these uniquely quantum effects might be harnessed to accelerate computation, pushing it beyond the limitations of classical systems.

Quantum information processing, a field that includes quantum computing, quantum cryptography, quantum communications, and quantum games, explores the implications of using quantum mechanics instead of classical mechanics to model information and its processing. Quantum computing is not about changing the physical substrate on which computation is done from classical to quantum, but rather changing the notion of computation itself. The change starts at the most basic level: the fundamental unit of computation is no longer the bit, but rather the quantum bit or qubit. Classical computers make use of quantum mechanics, but they compute using bits, not qubits. For this reason, they are not considered quantum computers. Placing computation on a quantum mechanical foundation led to the discovery of faster algorithms, novel cryptographic mechanisms, and improved communication protocols.

The field of quantum information processing developed slowly in the 1980s and early 1990s as a small group of researchers worked out a theory of quantum information and quantum information processing. D. Deutsch developed a notion of a quantum mechanical Turing machine. D. Bernstein, V. Vazirani, and A. Yao improved upon his model and showed that a quantum Turing machine could simulate a classical Turing machine. The standard quantum circuit model was then defined, which led to an understanding of quantum complexity in terms of a set of basic quantum transformations called quantum gates. These gates are theoretical constructs that may or may not have direct analogs in the physical components of an actual quantum computer.

In the early 1990s, researchers developed the first truly quantum algorithms. Despite the probabilistic nature of quantum mechanics, these initial algorithms produced correct answers with certainty. They improved upon classical approaches by solving, in polynomial time and with certainty, problems that classical algorithms could only solve in polynomial time with high probability. Although the practical impact of these results was initially unclear, they were of great theoretical significance-they offered the first concrete evidence that quantum computation could be more powerful than classical computation for certain tasks.

These breakthroughs drew the attention of many researchers, including Peter Shor, who in 1994 astonished the scientific community with a polynomial-time quantum algorithm for factoring integers. This was a landmark achievement, as factoring had long been a problem of practical importance. For years, the absence of an effi-

cient classical solution led many to believe that no such algorithm existed, a belief strong enough that it formed the foundation of cryptographic systems like RSA. While it is still unknown whether a classical polynomial-time factoring algorithm exists, Shor's result demonstrated that quantum computers could potentially outperform classical ones for a problem of real-world relevance.

While Shor's result sparked a lot of interest, doubts as to its practical significance remained. Quantum systems are notoriously fragile. Key properties, such as quantum entanglement, are easily disturbed by environmental influences that cause the quantum states to decohere. In addition, properties of quantum mechanics, such as the impossibility of reliably copying an unknown quantum state, made it look unlikely that effective error-correction techniques could ever be found. For these reasons, it seemed unlikely that reliable quantum computers could be built. Luckily, in spite of serious and widespread doubts as to whether quantum information processing could ever be practical, the theory itself proved to be so tantalizing that researchers continued to explore it. In 1996 Shor and R. Calderbank, and independently A. Steane, saw a way to finesse the seemingly show-stopping problems of quantum decoherence and developed quantum error correction techniques. Today, quantum error correction is arguably the most mature area of quantum information processing.

While to some degree the ultimate practicality of quantum computing and quantum information remains uncertain, still, no known physical principles rule out the construction of a large-scale quantum computers. However long it takes to build them-or however broad their applications-quantum information processing has already reshaped our understanding of quantum physics, clarifying key concepts like measurement and entanglement. While the practical consequences of this insight are hard to predict, uniting the two most influential scientific theories of the twentieth century-quantum mechanics and information theory-is sure to have lasting effects on technological and intellectual progress in the twenty-first century.

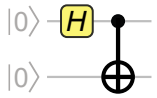
2. QUANTUM CIRCUIT MODEL OF COMPUTATION

Next we discuss the quantum circuit models. A quantum circuit is often illustrated schematically by a circuit diagram, where the wires are shown as horizontal lines and we imagine the quantum state of qubits propagating along the wires from left to right in time. A quantum gate acting on n qubits has the input of qubits; carried to it by n wires, and n other wires carry the output qubits away from the gate. The gates are usually shown in rectangular blocks. We will restrict attention to unitary quantum gates (which are also reversible).

A quantum computation consists of the following actions on a set of n qubits: an initialization, a quantum algorithm, and a final measurement. All of these steps can be captured by a quantum circuit diagram. Circuits in electronics show connections in space. Quantum circuits show connections between qubits in space and operations performed on them in time. Each qubit is spatially separated from the others, with time moves from left to right.

3. STABILIZERS, PAULI GROUP, AND TABLEAU REPRESENTATION

A quantum state (technically, a "pure state") is a unit vector in Hilbert-space describing the state of a quantum system. A qubit is the simplest quantum system. It's a two-level system (we label the levels $|0\rangle$ and $|1\rangle$), with an amplitude for $|0\rangle$ and an amplitude for $|1\rangle$. For instance here is a circuit that makes a Bell state. The initial state of qubits is $|00\rangle$ and the final state is $|00\rangle + |11\rangle$.



Here we focus on Clifford gates, which are

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}, \quad CNOT = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}, \quad S = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}, \tag{1}$$

A unitary U *stabilizes* a pure state $|\psi\rangle$ if $U|\psi\rangle = |\psi\rangle$, i.e., if $|\psi\rangle$ is an eigenvector of U with eigenvalue $+1$. Note that phase does matter here, so, if $U'|\psi\rangle = -|\psi\rangle$ or $U'|\psi\rangle = i|\psi\rangle$, then U' does *not* stabilize $|\psi\rangle$.

The stabilizer group of $|\psi\rangle$, Stab $(|\psi\rangle)$, is the set of all unitaries that stabilize a state $|\psi\rangle$.

Exercise 1. Show that $X_1X_2X_3$, Z_1Z_2, and Z_2Z_3 are three independent stabilizers of $|\psi\rangle = |000\rangle + |111\rangle$. The Stab$(|\psi\rangle)$ has 8 elements. These three stabilizers act as their generators. Find all 8 stabilizers of $|\psi\rangle$.

A stabilizer state is a state that has n *independent* stabilizer unitary operations. A stabilizer state is uniquely defined with its unitary operations. For stabilizer states we only need to look at the intersection of Stab$(|\psi\rangle)$ with a group known as the *Pauli group*. For one qubit, the Pauli group is the group generated by the Pauli matrices:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2}$$

Within the group, we have

Pauli matrix	I	X	Z	Y
State(s) Stabilized	all states	$\|+\rangle$	$\|0\rangle$	$\|i\rangle$

We can generalize the Pauli group of 1 qubit to P_n, the Pauli group on n qubits. Elements of P_n have the following form:

$$b\,(P_1 \otimes P_2 \otimes \ldots \otimes P_n) \tag{3}$$

where P_1, through P_n are elements of the single-qubit Pauli group $\{I, X, Y, Z\}$, and $b \in \{1, -1, i, -i\}$.

Elements of P_n can also be represented using "tableaus". These are matrices consisting of two $n \times n$ blocks of 1s and 0s. In a tableau, each Pauli matrix is represented by two-bit strings. Each row in the matrix represents a generator of P_n. One of the bits of the two bit string is placed in the left matrix (X-block or X-matrix), and the other in the right matrix.

Pauli matrix	I	X	Z	Y
bit-string	00	10	01	11

This effectively creates the following scheme: the presence of a 1 in the i-th entry of a row indicates the presence of a X in the i-th component of the element of P_n, and a 0 indicates the absence of an X. Similarly, for the right block (Z-block), the presence of a 1 in the i-th entry of the row indicates the presence of a Z in the i-th component of the element of P_n, and a 0 indicates the absence of an Z. If there is a 1 in the i-th entries of both the left and right blocks, this indicates a Y in the i-th component of the element of P_n. For example, the generating set $\{Z_1X_2X_3I_4Y_5, X_1Y_2Z_3X_4X_5\}$ would be represented as

$$\left[\begin{array}{ccccc|ccccc} 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \end{array}\right] \quad \begin{array}{l} Z_1X_2X_3I_4Y_5 \\ X_1Y_2Z_3X_4X_5 \end{array} \tag{4}$$

and their product is represented as

$$\left[\begin{array}{ccccc|ccccc} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right] \quad Y_1Z_2Y_3X_4Z_5 \tag{5}$$

Notice that multiplying two elements together is done by simply bitwise XOR-ing the 2n-bit strings, which is simply mod 2 addition of the digits.

4. EVOLUTION OF STABILIZER STATES IN CLIFFORD CIRCUITS

Next we discuss a theorem and a set of rules that allows us to understand how a given quantum states evolves with a simple class of circuits. Note that Stab$(|\psi\rangle) \cap \mathcal{P}_n$, being an intersection of two groups, is itself a group, which we call the *Pauli stabilizer group* of $|\psi\rangle$.

The Clifford group contains operators that conjugate Paulis into Paulis; its generating set consists of $\{H, S, CNOT\}$.

A stabilizer circuit consists solely of elements from the Clifford group.

Gottesman-Knill Theorem. Let $|\psi\rangle$ be a n-qubit stabilizer state for which the intersection of its stabilizer group with $\mathcal{P}_n$ contains 2^n elements, i.e. $|\text{Stab}(|\psi\rangle) \cap \mathcal{P}_n| = 2^n$, then $|\psi\rangle$ is reachable from the $|0\rangle^{\otimes n}$ state using only the clifford gates.

Note that such $|\psi\rangle$ states are uniquely determined by the group $\text{Stab}(|\psi\rangle) \cap \mathcal{P}_n$. As a result of this theorem, if we know the Pauli stabilizer group of a state, we know the state itself. How useful is this representation for algorithms? Since an n-qubit stabilizer state has a Pauli stabilizer group of size 2^n, with elements that are (2n+1)-bit strings, it may initially seem that keeping track of a Pauli stabilizer group is no easier than keeping track of a vector of amplitudes. However, there is an easier way to keep track of a group than to just keep track of all of its elements, namely by keeping track of its *generators*. For an n-qubit state, we only need n independent generators to keep track of its Pauli stabilizer group, since n linearly independent elements will generate a group of size 2^n.

A few examples will illustrate this point. Let's just list the action of Clifford gates on various stabilizers.

To apply H to the i-th qubit:

- Swap the i-th column of the X-matrix with the i-th column of the Z-matrix.

To apply S to the i-th qubit:

- Bitwise XOR the i-th column of the X-matrix into the i-th column of the Z-matrix.

To apply CNOT with the i-th qubit as control and the j-th as target:

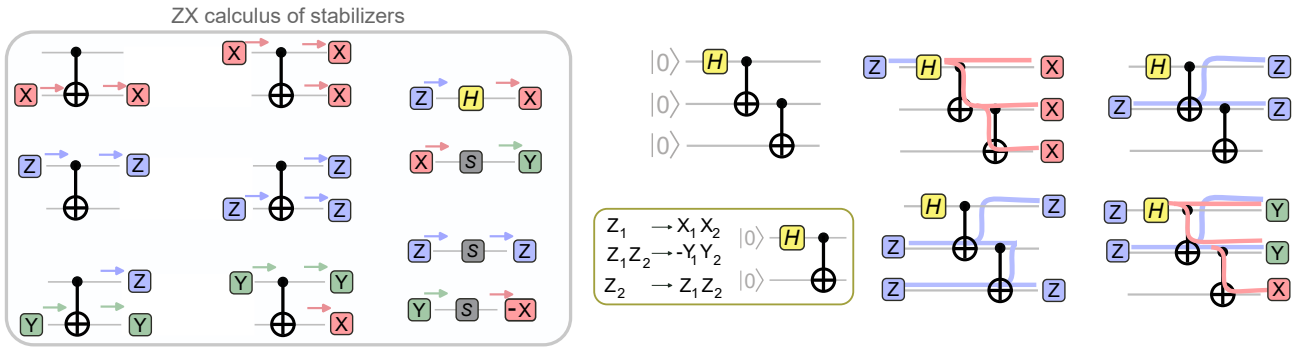
- Bitwise XOR the i-th column of the X-matrix into the j-th column of the X-matrix.
- Bitwise XOR the j-th column of the Z-matrix into the i-th column of the Z-matrix.

Keeping track of the stabilizers by updating tableau is a common practice for error correction applications. It gives the final stabilizers and the bitstrings (without sign) in the final evolved state. Here we are interested to know the exact wavefunction after evolution under U. The final state $|\psi_f\rangle$ is

$$|\psi_f\rangle = \prod^{n} \frac{I + S_j}{2} |\psi_{ref}\rangle \tag{6}$$

where S_j s are an independent set of stabilizers and $|\psi_{ref}\rangle$ is a state that we could identify to be a stabilized by one of the S_j s. Clearly we need to deal with exponentially many terms and is not optimal; depending what question we like to answer, there are ways around it.

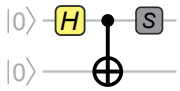
Exercise 2. If S_0 is a stabilizer of initial state $|\psi_0\rangle$, show that $US_0U^\dagger$ is a stabilizer of the final state $|\psi_f\rangle = U|\psi_0\rangle$



Exercise 3. Prove the stabilizer evolution relation above shown in the box above.

5. CLIFFORD CIRCUITS EXAMPLES USING TABLEAU

The Clifford group contains operators that conjugate Paulis into Paulis, and its generating set of operators consists of $\{H, S, CNOT\}$. A stabilizer circuit consists solely of elements from the Clifford group. Here we focus on Clifford circuits and by tracking the stabilizer states of initial state, we arrive at the final state.



Let's test this all out by keeping track of the tableau for the circuit above. Since we are interested to know the final quantum state and not the general act of this circuit, we can only focus on the effect of the circuit on a set of generators of the stabilizer states for the given initial state. We start with the state $|00\rangle$, which has the tableau representation:

$$\left[\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right] \begin{array}{c} Z_1 \\ Z_2 \end{array} \tag{7}$$

Applying the Hadamard to the first qubit swaps the first columns of the X-matrix and Z-matrix:

$$\left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right] \begin{array}{c} X_1 \\ Z_2 \end{array} \tag{8}$$

One could convert this back into the generators by saying that the current state is the one generated by $+X_1$ and Z_2. Indeed, these operators generate the stabilizer group for $|+\rangle\,|0\rangle$. To apply the CNOT gate, we bitwise XOR the first column of the X-matrix into the second column of the X-matrix, and likewise bitwise XOR the second column of the Z-matrix into the first column of the Z-matrix :

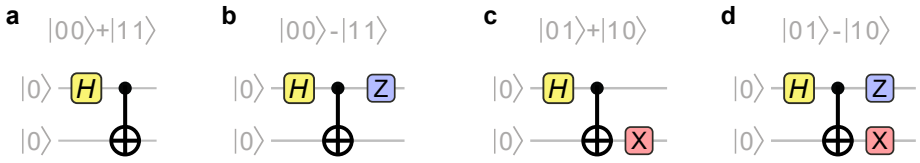
$$\left[\begin{array}{cc|cc} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right] \begin{array}{c} X_1X_2 \\ Z_1Z_2 \end{array} \tag{9}$$

The generators corresponding to this tableau are $\{X_1X_2, Z_1Z_2\}$, which are indeed the stabilizer generators for a Bell pair, as expected. Finally, we apply the S-gate by bitwise XORing the first column of the X-matrix into the first column of the Z-matrix :

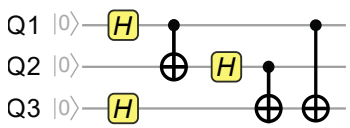
$$\left[\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right] \begin{array}{c} Y_1X_2 \\ Z_1Z_2 \end{array} \tag{10}$$

This final tableau corresponds to the generators $\{Y_1X_2, Z_1Z_2\}$, which are the stabilizers for the state $|00\rangle + i\,|11\rangle$.

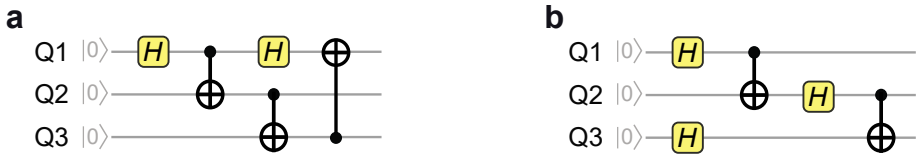
Exercise 4. Show that each circuit below gives the associated Bell pair written on top of it.



Exercise 5. Given the initial state $|000\rangle$, find a generative of the final stabilizers of the circuit below.



Exercise 6. Given the initial state $|000\rangle$, find a generative of the final stabilizers of the circuits below. What could good choice of $|\psi_{ref}\rangle$ in each case.



6. SOLUTIONS TO SOME THE EXERCISES

Exercise 1.

Since $X_1X_2X_3$ and Z_1Z_2 and Z_2Z_3 are independent, product of their projection gives the sum of all stabilizers $(I + X_1X_2X_3)(I + Z_1Z_2)(I + Z_2Z_3)$

Exercise 2.

$$S_0|\psi_0\rangle = +|\psi_0\rangle \quad \text{and} \quad |\psi_f\rangle = U|\psi_0\rangle \quad \rightarrow \quad |\psi_f\rangle = U\,S_0\,|\psi_0\rangle \quad \rightarrow \quad |\psi_f\rangle = U\,S_0\,U^\dagger|\psi_f\rangle \tag{11}$$

Exercise 3. leave to the readrers.

Exercise 4.

Two independent stabilizers of the initial states are Z_1 and Z_2.

Z_1 evolves to a) X_1X_2, b) -X_1X_2, c) X_1X_2, d) -X_1X_2.

Z_2 evolves to a) Z_1Z_2, b) Z_1Z_2, c) -Z_1Z_2, d) -Z_1Z_2.

A reference state (a state that is stabilized by one of the final stabilizers) is
a) $|00\rangle$, b) $|00\rangle$, c) $|10\rangle$, d) $|10\rangle$.

$$a. \quad |\psi_f\rangle = (I + X_1X_2)(I + Z_1Z_2)|00\rangle = (I + X_1X_2)|00\rangle = |00\rangle + |11\rangle \tag{12}$$

$$b. \quad |\psi_f\rangle = (I - X_1X_2)(I + Z_1Z_2)|00\rangle = (I - X_1X_2)|00\rangle = |00\rangle - |11\rangle \tag{13}$$

$$c. \quad |\psi_f\rangle = (I + X_1X_2)(I - Z_1Z_2)|10\rangle = (I + X_1X_2)|10\rangle = |01\rangle + |10\rangle \tag{14}$$

$$d. \quad |\psi_f\rangle = (I - X_1X_2)(I - Z_1Z_2)|10\rangle = (I - X_1X_2)|10\rangle = |10\rangle - |01\rangle \tag{15}$$

Exercise 5.

$$\text{Initial state} \left[\begin{array}{ccc|ccc} 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \\ 0&0&0&0&0&1 \end{array}\right] \begin{array}{c} Z1 \\ Z_2 \\ Z_3 \end{array} \qquad \text{final state} \left[\begin{array}{ccc|ccc} 1&0&1&0&1&0 \\ 0&1&1&1&0&0 \\ 0&0&1&0&0&0 \end{array}\right] \begin{array}{c} X_1Z_2X_3 \\ Z_1X_2X_3 \\ X_3 \end{array} \tag{16}$$

Exercise 6.

For **a**, starting with $\{Z_1, Z_2, Z_3\}$ one gets $\{-Y_1X_2Y_3, X_1Z_2, Z_2Z_3\}$. For **b**, starting with $\{Z_1, Z_2, Z_3\}$ one arrives at $\{X_1Z_2, Z_1X_2X_3, X_3\}$ for final stabilizers. Given these final stabilizers for **b**, a single bitstring cannot be a reference state.

APPENDIX A. REVIEW OF SINGLE QUBIT OPERATIONS

Pauli operators and Single Qubit gates are

$$X=\begin{bmatrix}0&1\\1&0\end{bmatrix},\quad Y=\begin{bmatrix}0&-i\\i&0\end{bmatrix},\quad Z=\begin{bmatrix}1&0\\0&-1\end{bmatrix},\quad S=\begin{bmatrix}1&0\\0&i\end{bmatrix},\quad XYZ=i,\quad XZX=-Z\,. \tag{17}$$

Single qubit θ-rotation around ϕ-axis in the xy-plane, and matrix exponentiation when $A^2=I$

$$R(\theta,\phi)=\begin{bmatrix}\cos(\theta/2)&-i\,e^{-i\phi}\sin(\theta/2)\\-i\,e^{i\phi}\sin(\theta/2)&\cos(\theta/2)\end{bmatrix},\qquad \exp(-i\theta A)=\cos(\theta)I-\sin(\theta)A \tag{18}$$

when $\phi=0$, *i.e.* rotation around x-axis

$$R_X(\theta)=\exp\left(-i\,\frac{\theta}{2}X\right)=\begin{bmatrix}\cos(\theta/2)&-i\,\sin(\theta/2)\\-i\,\sin(\theta/2)&\cos(\theta/2)\end{bmatrix}\rightarrow R_X(\pi)=X_\pi=\exp\left(-i\,\frac{\pi}{2}X\right)=-i\begin{bmatrix}0&1\\1&0\end{bmatrix}=-iX, \tag{19}$$

when $\phi=\pi/2$, *i.e.* rotation around y-axis

$$R_Y(\theta)=Y_\theta=\exp\left(-i\,\frac{\theta}{2}Y\right)=\begin{bmatrix}\cos(\theta/2)&-\sin(\theta/2)\\\sin(\theta/2)&\cos(\theta/2)\end{bmatrix}\quad\rightarrow R_Y(\pi)=Y_\pi=\exp\left(-i\,\frac{\pi}{2}Y\right)=\begin{bmatrix}0&-1\\1&0\end{bmatrix}=-iY. \tag{20}$$

$$R_X(\pi/2)=X_{\pi/2}=\exp\left(-i\,\frac{\pi}{4}X\right)=\frac{1}{\sqrt{2}}\begin{bmatrix}1&-i\\-i&1\end{bmatrix}\quad\rightarrow X_{\pi/2}|0\rangle=\frac{|0\rangle-i|1\rangle}{\sqrt{2}}=|-\mathbf{y}\,\rangle \tag{21}$$

$$R_Y(\pi/2)=Y_{\pi/2}=\exp\left(-i\,\frac{\pi}{4}Y\right)=\frac{1}{\sqrt{2}}\begin{bmatrix}1&-1\\1&1\end{bmatrix}\quad\rightarrow Y_{\pi/2}|0\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}=|+\mathbf{x}\rangle. \tag{22}$$

Hadamard is a π rotation around the $x+z$-axis :

$$H=\frac{X+Z}{\sqrt{2}}=\exp\left(-i\frac{\pi}{2}\frac{X+Z}{\sqrt{2}}\right)=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix},\quad HZ_\theta H=X_\theta,\quad HX_\theta H=Z_\theta,\quad HYH=-Y\,. \tag{23}$$

Single qubit φ-rotation around z-axis,

$$R_Z(\varphi)=Z_\varphi=\exp\left(-i\,\frac{\varphi}{2}Z\right)=\begin{bmatrix}\exp(-i\,\varphi/2)&0\\0&\exp(i\,\varphi/2)\end{bmatrix}\quad\rightarrow Z_\pi=\begin{bmatrix}-i&0\\0&i\end{bmatrix}=-iZ,\quad Z|+\mathbf{x}\rangle=|-\mathbf{x}\rangle \tag{24}$$

Change of Basis:

$$Y_\theta=X_{-\pi/2}\,Z_\theta\,X_{\pi/2},\quad Z_\theta=Y_{-\pi/2}\,X_\theta\,Y_{\pi/2},\quad X_\theta=Y_{\pi/2}\,Z_\theta\,Y_{-\pi/2},\quad \text{for }\forall\,\theta \tag{25}$$

Single qubit gates on cardinal points and basic transformations

$$X|0\rangle=|1\rangle,\quad X|1\rangle=|0\rangle,\quad X|+\mathbf{x}\rangle=|+\mathbf{x}\rangle,\quad X|-\mathbf{x}\rangle=-|-\mathbf{x}\rangle, \tag{26}$$

$$Y|0\rangle=i|1\rangle,\quad Y|1\rangle=-i|0\rangle,\quad Y|+\mathbf{x}\rangle=-i|-\mathbf{x}\rangle,\quad Y|-\mathbf{x}\rangle=i|+\mathbf{x}\rangle, \tag{27}$$

$$Z|0\rangle=|0\rangle,\quad Z|1\rangle=-|1\rangle,\quad Z|+\mathbf{x}\rangle=|-\mathbf{x}\rangle,\quad Z|-\mathbf{x}\rangle=|+\mathbf{x}\rangle, \tag{28}$$

$$S|0\rangle=|0\rangle,\quad S|1\rangle=i|1\rangle,\quad S|+\mathbf{x}\rangle=|+\mathbf{y}\rangle,\quad S|-\mathbf{x}\rangle=|-\mathbf{y}\rangle, \tag{29}$$

$$S\,X\,S^\dagger=Y,\quad S\,Y\,S^\dagger=-X,\quad S\,Z\,S^\dagger=Z, \tag{30}$$

$$S^\dagger\,X\,S=-Y,\quad S^\dagger\,Y\,S=X,\quad S^\dagger\,Z\,S=Z, \tag{31}$$

$$H\,X\,H=Z,\quad H\,Y\,H=-Y,\quad H\,Z\,H=X, \tag{32}$$

APPENDIX B. REVIEW OF CIRCUIT BASIC OPERATIONS

1Q universal = $\{T, H\}$, Universal = Any 2Q entangling + $\{T, H\}$ = e.g. $\{H, T, CNOT\}$

Universal= T-gate + Clifford = T-gate + $\{H, S, CNOT\}$. Clifford only $\rightarrow$ effectively simulate-able

$$\text{Phase Gate} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}, \quad \phi = \begin{cases} \pi & \rightarrow Z = S^2 \\ \pi/2 & \rightarrow S = T^2 \\ \pi/4 & \rightarrow T = \sqrt{S} \end{cases}, \quad SZS^\dagger = Z, \quad HZH = X. \tag{33}$$

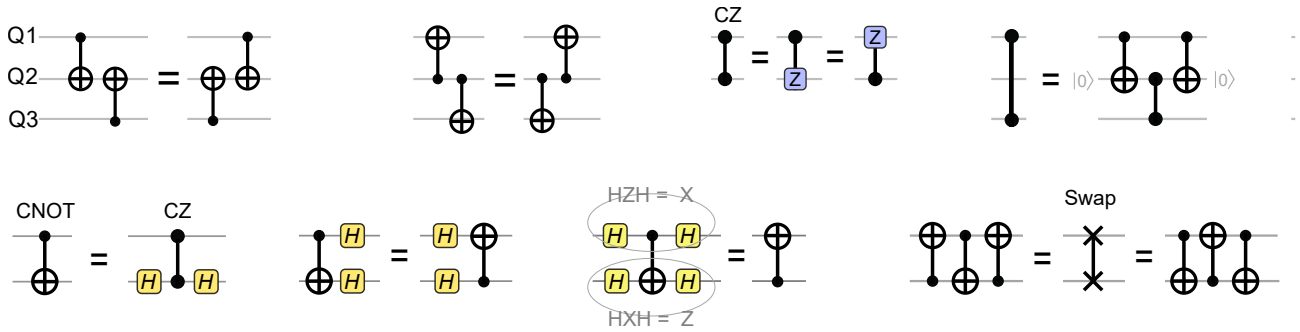


Figure 1. Commonly used single and 2 qubit manipulations.

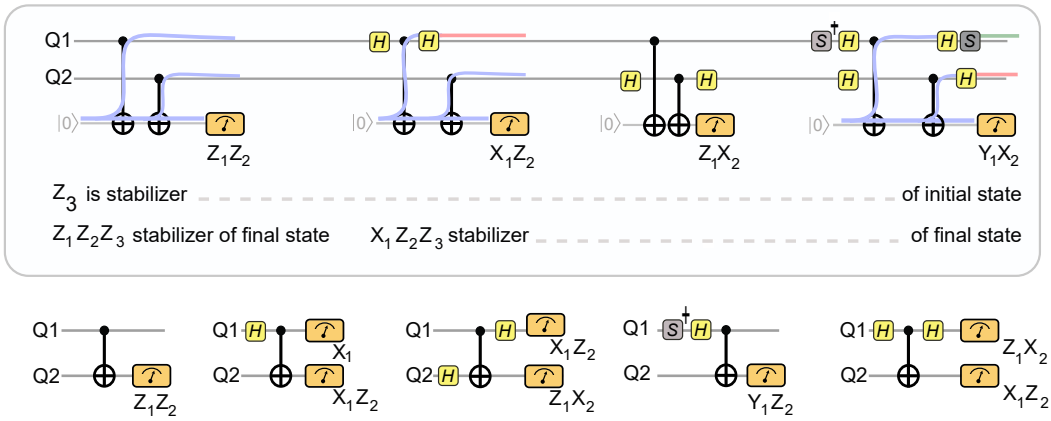


Figure 2. QND measurements