Lecture 3: Stabilizer states and Clifford circuits

Computational aspects of quantum simulation
ENS de Lyon

2026

Abstract

We complete the stabilizer formalism begun in Lecture 2 by introducing tableaux, Clifford circuits, Pauli measurements, and the Gottesman–Knill simulation algorithm. The emphasis is on making the simulation procedure explicit: how signs are stored and updated, how Pauli measurements modify a stabilizer group, and why the resulting classical algorithm samples exactly from the circuit's output distribution.

Learning objectives. After this lecture, students should be able to:

- encode stabilizer generators in a binary tableau and update their signs;
- update stabilizer descriptions under Clifford gates and Pauli measurements;
- state and prove the Gottesman–Knill theorem;
- carry out the exact classical simulation of a concrete adaptive Clifford computation.

Main message. Efficient simulation is a closure phenomenon. Stabilizer states have concise Pauli descriptions; Clifford gates and Pauli measurements preserve those descriptions, including under adaptive classical control. The simulator therefore follows the quantum computation using only a polynomial-size list of signed Pauli generators.

Contents

Consider the two-qubit states

$$|\psi\rangle = \frac{|00\rangle + i|11\rangle}{\sqrt{2}}, \qquad |\phi\rangle = \frac{|00\rangle + e^{i\pi/4}|11\rangle}{\sqrt{2}}.$$

(a) Verify that Z_1Z_2 and X_1Y_2 are independent commuting Hermitian Paulis and that both stabilize $|\psi\rangle$. Conclude that $|\psi\rangle$ is a stabilizer state, and list the four elements of its stabilizer group.

(b) Prove that $|\phi\rangle$ is not a stabilizer state. First show that a Pauli stabilizing $|\phi\rangle$ must preserve the set of computational-basis strings $\{00, 11\}$. Up to sign, it must therefore be one of

$$II,\ ZI,\ IZ,\ ZZ,\ XX,\ XY,\ YX,\ YY.$$

Determine which signed operators in this list stabilize $|\phi\rangle$, and show that there cannot be two independent stabilizer generators.

Solution

Part (a). Each of Z_1Z_2 and X_1Y_2 is Hermitian. On the two components of $|\psi\rangle$,

$$Z_1Z_2|00\rangle = |00\rangle, \qquad Z_1Z_2|11\rangle = |11\rangle,$$

and hence $Z_1Z_2|\psi\rangle = |\psi\rangle$. Moreover,

$$X_1Y_2|00\rangle = i|11\rangle, \qquad X_1Y_2(i|11\rangle) = |00\rangle,$$

so $X_1Y_2|\psi\rangle = |\psi\rangle$.

The two operators commute: on qubit 1, Z anticommutes with X, and on qubit 2, Z anticommutes with Y; the two minus signs cancel. They are independent because neither is the identity and they have different Pauli labels. Finally,

$$(Z_1Z_2)(X_1Y_2) = (Z_1X_1)(Z_2Y_2) = (iY_1)(-iX_2) = Y_1X_2.$$

Thus

$$S(\psi) = \{I,\ Z_1Z_2,\ X_1Y_2,\ Y_1X_2\}.$$

It has two independent commuting generators and therefore size 2^2, so $|\psi\rangle$ is a two-qubit stabilizer state.

Part (b). Put $\omega = e^{i\pi/4}$, so

$$|\phi\rangle = \frac{|00\rangle + \omega|11\rangle}{\sqrt{2}}.$$

A Pauli maps every computational-basis vector to another computational-basis vector up to phase. If a signed Pauli stabilizes $|\phi\rangle$, the support of the resulting state must still be exactly $\{00, 11\}$. Its pattern of X-components must therefore either flip neither bit or flip both bits. This gives precisely the eight unsigned candidates in the question.

For the diagonal candidates,

$$ZZ|\phi\rangle = |\phi\rangle, \qquad ZI|\phi\rangle = IZ|\phi\rangle = \frac{|00\rangle - \omega|11\rangle}{\sqrt{2}}.$$

Thus among their signed versions only $+II$ and $+ZZ$ stabilize $|\phi\rangle$.

It remains to check the operators that flip both bits. We have

$$XX|\phi\rangle = \frac{\omega|00\rangle + |11\rangle}{\sqrt{2}}, \qquad YY|\phi\rangle = -\frac{\omega|00\rangle + |11\rangle}{\sqrt{2}}.$$

Neither vector is $\pm|\phi\rangle$, because that would require $\omega^2 = 1$. Similarly,

$$XY|\phi\rangle = YX|\phi\rangle = \frac{-i\omega|00\rangle + i|11\rangle}{\sqrt{2}}.$$

This is not $\pm|\phi\rangle$, because such an equality would require $\omega^2 = -1$, whereas $\omega^2 = i$. Checking equality up to a sign is enough: if $P|\phi\rangle = -|\phi\rangle$, then $-P$ would be the signed Pauli that stabilizes the state.

Consequently the only Pauli stabilizers of $|\phi\rangle$ are I and Z_1Z_2. A pure two-qubit stabilizer state must have a stabilizer group of size 4, generated by two independent commuting Hermitian Paulis. No such second generator exists for $|\phi\rangle$, so $|\phi\rangle$ is not a stabilizer state.

2 From stabilizer groups to tableaux

We continue the stabilizer discussion from Lecture 2 by making the concise Pauli-generator representation algorithmic.

2.1 The tableau representation

For a pure stabilizer state $|\psi\rangle$, the full Pauli stabilizer

$$S(\psi) = \{g \in \mathcal{P}_N : g|\psi\rangle = |\psi\rangle\}$$

is the unique stabilizer group of size 2^N that stabilizes $|\psi\rangle$. It does not, however, have a unique ordered list of independent generators. This is analogous to a vector space having many possible bases: different independent generating sets for the same group describe the same state. A tableau records one such choice.

Write

$$g_i = (-1)^{\sigma_i} P(a_i, b_i)$$

for each generator. The sign σ_i is essential state information: from $g_i|\psi\rangle = |\psi\rangle$, we obtain

$$P(a_i, b_i)|\psi\rangle = (-1)^{\sigma_i}|\psi\rangle.$$

Thus (a_i, b_i) specifies the Pauli observable, while σ_i specifies whether the state lies in its $+1$ or -1 eigenspace. This is not a global phase of $|\psi\rangle$; changing the sign of a generator generally changes the stabilized state.

For example, the unsigned label $(a, b) = (0, 1)$ specifies Z, but

σ	a	b
0	0	1

stabilizes $|0\rangle$,

σ	a	b
1	0	1

stabilizes $|1\rangle$.

Without the sign column these states would have the same tableau, and a simulator could not determine whether a measurement of Z has outcome $+1$ or -1.

Placing the N signed generators in rows gives the $N \times (2N + 1)$ binary array

$$\left[\ \sigma \mid A \mid B\ \right],$$

called a stabilizer tableau. Swapping two rows merely reorders the generators. For $i \neq j$, the replacement

$$g_i \longleftarrow g_i g_j$$

also preserves the generated group: the new generator is in the old group, and the inverse replacement is the same operation because $g_j^2 = I$. On binary labels this operation adds row j to row i modulo two, but the new sign must be computed as well.

Multiplying signed rows. Consider two Hermitian Paulis

$$g_1 = (-1)^{\sigma_1} P(a_1, b_1), \qquad g_2 = (-1)^{\sigma_2} P(a_2, b_2),$$

and put

$$a = a_1 \oplus a_2, \qquad b = b_1 \oplus b_2,$$

where $\oplus$ denotes componentwise addition modulo two. Recall that

$$P(a,b) = i^{a\cdot b} X^a Z^b, \qquad X^a = \bigotimes_{j=1}^{N} X_j^{a_j}, \quad Z^b = \bigotimes_{j=1}^{N} Z_j^{b_j}.$$

We now compute the phase in the product explicitly. Moving every Z from the first Pauli past every X from the second Pauli gives

$$Z^{b_1} X^{a_2} = (-1)^{b_1\cdot a_2} X^{a_2} Z^{b_1} = i^{2b_1\cdot a_2} X^{a_2} Z^{b_1}.$$

Therefore

$$\begin{aligned} P(a_1,b_1)P(a_2,b_2) &= i^{a_1\cdot b_1 + a_2\cdot b_2} X^{a_1} Z^{b_1} X^{a_2} Z^{b_2} \\ &= i^{a_1\cdot b_1 + a_2\cdot b_2 + 2b_1\cdot a_2} X^{a_1} X^{a_2} Z^{b_1} Z^{b_2} \\ &= i^{a_1\cdot b_1 + a_2\cdot b_2 + 2b_1\cdot a_2} X^{a} Z^{b} \\ &= i^{a_1\cdot b_1 + a_2\cdot b_2 - a\cdot b + 2b_1\cdot a_2} P(a,b). \end{aligned}$$

Multiplying by the two input signs thus gives

$$g_1 g_2 = (-1)^{\sigma_1+\sigma_2} i^{\kappa} P(a,b),$$

where

$$\kappa = a_1\cdot b_1 + a_2\cdot b_2 - a\cdot b + 2b_1\cdot a_2 \pmod 4.$$

The dot products in this formula are evaluated as ordinary integer sums before reducing κ modulo 4. In particular, $a\cdot b$ is computed using the bits of $a = a_1 \oplus a_2$ and $b = b_1 \oplus b_2$, not by adding the other three dot products over the integers.

Let us also see directly why commutation makes κ even. Reducing the formula for κ modulo two removes the last term. Since $a = a_1 + a_2$ and $b = b_1 + b_2$ when these vectors are viewed over $\mathbb{F}_2$,

$$\begin{aligned} \kappa &\equiv a_1\cdot b_1 + a_2\cdot b_2 - (a_1+a_2)\cdot(b_1+b_2) \pmod 2 \\ &\equiv -a_1\cdot b_2 - a_2\cdot b_1 \pmod 2 \\ &\equiv a_1\cdot b_2 - b_1\cdot a_2 \pmod 2. \end{aligned}$$

The last expression is precisely the symplectic product of the two labels. It vanishes exactly when the two Paulis commute. Hence commuting Paulis have $\kappa \equiv 0 \pmod 2$, so the representative of κ modulo four is either 0 or 2. Equivalently, the product of two commuting Hermitian operators is Hermitian, so its phase relative to the Hermitian operator $P(a,b)$ must be $i^{\kappa} \in \{+1,-1\}$.

Thus, when g_1 and g_2 commute, as tableau generators do, their product can again be written in signed Hermitian form:

$$g_1 g_2 = (-1)^{\sigma} P(a,b), \qquad \sigma = \sigma_1 + \sigma_2 + \frac{\kappa}{2} \pmod 2.$$

Thus *tracking the sign* means applying this update to the sign bit in addition to adding the a- and b-labels modulo two. If the two Paulis anticommute, then κ is odd and their product has phase $\pm i$; this case does not occur when one row of a stabilizer tableau is multiplied by another. Computing the label and sign of a product of two full rows takes $O(N)$ bit operations.

Testing membership in the generated group. Let us now give an explicit method for deciding signed group membership. Let

$$S = \langle g_1, \ldots, g_N \rangle, \qquad g_i = (-1)^{\sigma_i} P(a_i, b_i),$$

where the generators are independent and commuting, and consider the candidate Hermitian Pauli

$$Q = (-1)^s P(a', b'), \qquad s \in \mathbb{F}_2.$$

Here (a', b') is the binary label of Q, while s is its sign bit. To test whether $Q \in S$, proceed as follows.

1. Ignore the candidate sign temporarily and solve the binary linear system

$$\sum_{i=1}^{N} \lambda_i a_i = a', \qquad \sum_{i=1}^{N} \lambda_i b_i = b', \qquad \lambda_i \in \mathbb{F}_2.$$

   This can be done by Gaussian elimination on the $2N$-bit generator labels.

2. If the system has no solution, no product of the generators has label (a', b'), and therefore $Q \notin S$.

3. If the system has a solution, compute the signed product

$$h = \prod_{i:\lambda_i=1} g_i$$

   one selected generator at a time. Represent the running product as $h = (-1)^\rho P(\alpha, \beta)$ and initialize $(\alpha, \beta, \rho) = (0, 0, 0)$, corresponding to $h = I$ and use the algorithm we discussed for multiplying signed rows to update.

4. Compare the computed sign ρ with the candidate sign s. Then

$$Q \in S \quad \Longleftrightarrow \quad \rho = s.$$

   If $\rho \neq s$, the generated element is $h = -Q$, so $-Q \in S$ but $Q \notin S$. The two cannot both belong to a stabilizer group, because that would imply $-I \in S$.

Because the generator labels are independent, the solution λ, when it exists, is unique. The linear system decides membership up to sign; the explicit product and its sign update decide membership in the signed group.

Two tableaux for the Bell state. Using $\sigma = 0$ for a positive sign and $\sigma = 1$ for a negative sign, the generators X_1X_2 and Z_1Z_2 give

σ	a_1	a_2	b_1	b_2
0	1	1	0	0
0	0	0	1	1

.

Replacing the second row by the product of the two rows replaces Z_1Z_2 by $(Z_1Z_2)(X_1X_2) = -Y_1Y_2$, and yields

σ	a_1	a_2	b_1	b_2
0	1	1	0	0
1	1	1	1	1

.

Both tableaux generate $\{I, X_1X_2, Z_1Z_2, -Y_1Y_2\}$, so both represent $|\Phi^+\rangle$. Notice that adding the two unsigned row labels produces the label of Y_1Y_2, while signed-row multiplication produces $-Y_1Y_2$. This is exactly the information supplied by tracking the sign. It also shows that a measurement of Y_1Y_2 on $|\Phi^+\rangle$ has the deterministic outcome -1.

3 Clifford circuits

Definition 3.1 (Clifford group)**.** *The N-qubit Clifford group is the normalizer of the Pauli group:*

$$\mathcal{C}_N = \{U : U\mathcal{P}_N U^\dagger = \mathcal{P}_N\}.$$

A Clifford circuit is a circuit composed of Clifford gates.

The one-qubit Hadamard and phase gates are

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

Together with CNOT, they generate the Clifford group up to global phase. A constructive proof is given in Appendix A. Their action by conjugation is determined by

U	$UXU^\dagger$	$UYU^\dagger$	$UZU^\dagger$
H	Z	$-Y$	X
S	Y	$-X$	Z

and, for a CNOT with control c and target t,

$$X_c \mapsto X_c X_t, \qquad Z_c \mapsto Z_c, \qquad X_t \mapsto X_t, \qquad Z_t \mapsto Z_c Z_t.$$

The images of products are obtained by multiplication, with the sign retained.

Proposition 3.2 (Closure of stabilizer states under Clifford gates)**.** *If $S = \langle g_1, \ldots, g_N\rangle$ stabilizes $|\psi\rangle$ and U is a Clifford unitary, then $U|\psi\rangle$ is stabilized by*

$$USU^\dagger = \langle Ug_1U^\dagger, \ldots, Ug_NU^\dagger\rangle.$$

The generators remain independent and commuting. In particular, a local Clifford gate updates a stabilizer tableau in $O(N)$ bit operations.

Proof. If $g|\psi\rangle = |\psi\rangle$, then

$$(UgU^\dagger)(U|\psi\rangle) = U|\psi\rangle.$$

Hence a Clifford gate updates a stabilizer state by conjugating each tableau row. The displayed rules update only the columns of the acted-on qubits and the sign bit. Updating all N generators therefore takes $O(N)$ elementary bit operations per one- or two-qubit gate, and the tableau remains of size $O(N^2)$. □

For example, for a single row the action of H_j swaps a_j and b_j, and flips the sign when $a_j = b_j = 1$, in agreement with $HYH = -Y$. The action of S_j replaces b_j by $b_j + a_j \pmod 2$, and again flips the sign in the case $(a_j, b_j) = (1, 1)$. The CNOT rule is obtained directly from the four images displayed above, including any sign needed to return to the canonical Hermitian representative $P(a, b)$.

Tableau update for Bell-state preparation. The state $|00\rangle$ has generators Z_1, Z_2, hence tableau

$$T_0 = \begin{array}{c|cc|cc} \sigma & a_1 & a_2 & b_1 & b_2 \\ \hline 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}.$$

Applying H_1 sends Z_1 to X_1 and leaves Z_2 unchanged:

$$T_1 = \begin{array}{c|cc|cc} \sigma & a_1 & a_2 & b_1 & b_2 \\ \hline 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}.$$

A CNOT from qubit 1 to qubit 2 sends X_1 to X_1X_2 and Z_2 to Z_1Z_2, giving

$$T_2 = \begin{array}{c|cc|cc} \sigma & a_1 & a_2 & b_1 & b_2 \\ \hline 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{array}.$$

This is the Bell-state tableau, consistently with $\mathrm{CNOT}_{1\to 2}\, H_1|00\rangle = |\Phi^+\rangle$.

4 Measuring a Pauli observable

Let $S = \langle g_1, \ldots, g_N\rangle$ stabilize the pure state $|\psi\rangle$, and let M be a Hermitian Pauli observable with eigenvalues ± 1. Since $M^2 = I$, its $+1$ and -1 eigenspaces have orthogonal projectors

$$\Pi_+ = \frac{I+M}{2}, \qquad \Pi_- = \frac{I-M}{2}.$$

Indeed, $\Pi_\pm^2 = \Pi_\pm$, $\Pi_+\Pi_- = 0$, $\Pi_+ + \Pi_- = I$, and $M\Pi_\pm = \pm\Pi_\pm$. Thus measuring the observable M means performing the two-outcome projective measurement $\{\Pi_+, \Pi_-\}$. More uniformly, for an outcome $\mu \in \{+1, -1\}$, write

$$\Pi_\mu = \frac{I+\mu M}{2}.$$

The Born rule then gives

$$\Pr[\mu] = \langle\psi|\Pi_\mu|\psi\rangle = \frac{1+\mu\langle\psi|M|\psi\rangle}{2}.$$

When this probability is nonzero, the corresponding post-measurement state is $\Pi_\mu|\psi\rangle/\sqrt{\Pr[\mu]}$.

Proposition 4.1 (Measurement rule for a stabilizer state)**.** *Exactly one of the following cases occurs.*

(i) If M commutes with every generator, then $M|\psi\rangle = \mu|\psi\rangle$ for a uniquely determined $\mu \in \{+1, -1\}$. The outcome is deterministic and the stabilizer group is unchanged.

(ii) If M anticommutes with at least one generator, then the outcomes $+1$ and -1 each have probability $1/2$. After obtaining outcome μ, one can update the generators by row multiplications and by replacing one anticommuting generator with μM.

Both the outcome probabilities and the post-measurement stabilizer group can be computed in polynomial time from the tableau.

Proof. **Deterministic case.** Suppose that M commutes with every generator. Then $M|\psi\rangle$ is also stabilized by every element of S. The stabilized space is one-dimensional, so $M|\psi\rangle = \mu|\psi\rangle$ for some $\mu \in \{+1, -1\}$.

The tableau also determines μ efficiently and explicitly. Write

$$g_i = (-1)^{\sigma_i} P(a_i, b_i), \qquad M = (-1)^{\tau} P(a_M, b_M).$$

Because $M|\psi\rangle = \mu|\psi\rangle$, the Pauli μM stabilizes $|\psi\rangle$ and therefore belongs to its full stabilizer group $S = \langle g_1, \ldots, g_N\rangle$. We use the procedure for testing membership of M in the stabilizer group. If it is, then $\mu = +1$, else $\mu = -1$.

Random case. Suppose instead that M anticommutes with at least one generator, and choose one such generator g_a. Then

$$\langle\psi|M|\psi\rangle = \langle\psi|g_a M g_a|\psi\rangle = -\langle\psi|M|\psi\rangle = 0.$$

Thus the two outcomes each have probability $1/2$. After sampling $\mu \in \{+1, -1\}$, define, for every $i \neq a$,

$$h_i = \begin{cases} g_i, & \text{if } g_i \text{ commutes with } M, \\ g_i g_a, & \text{if } g_i \text{ anticommutes with } M. \end{cases}$$

and replace g_a by μM.

Here is why this update is correct. Each h_i commutes with M: when both g_i and g_a anticommute with M, their product commutes with it. The h_i's commute with one another because they are products of elements of the abelian group S. They also stabilize $|\psi\rangle$ and commute with M, and therefore stabilize the normalized post-measurement state

$$|\psi_\mu\rangle = \frac{(I + \mu M)|\psi\rangle}{\sqrt{2}}.$$

The new generator μM stabilizes this state as well. The set $\{h_i : i \neq a\}$ remains independent because it was obtained by invertible row operations before removing the pivot row. Moreover, μM cannot be generated by the h_i's: every such product lies in S and commutes with g_a, whereas M anticommutes with g_a. Thus the updated list contains N independent commuting generators and uniquely specifies $|\psi_\mu\rangle$. □

Measuring one qubit of a Bell state. Start from $S = \langle X_1X_2, Z_1Z_2\rangle$ and measure $M = Z_1$. The operator X_1X_2 anticommutes with M, whereas Z_1Z_2 commutes with it. The outcome μ is therefore uniform in $\{+1, -1\}$. Choose X_1X_2 as the pivot and replace it by μZ_1; the second generator is unchanged. For $\mu = +1$, the new stabilizers Z_1, Z_1Z_2 specify $|00\rangle$. For $\mu = -1$, the stabilizers $-Z_1, Z_1Z_2$ specify $|11\rangle$, exactly as expected.

5 Clifford circuits can be simulated efficiently

A unitary Clifford circuit has the form

$$C = G_m G_{m-1} \cdots G_1,$$

where each G_j is an H, S, or CNOT gate and G_1 acts first. If the input is a stabilizer state, then every prefix $G_j \cdots G_1$ produces another stabilizer state. Rather than storing its 2^N amplitudes, we

can therefore store N signed Pauli generators and update them gate by gate. If Pauli measurements are interspersed with the gates, the measurement rule of the preceding section shows that the state conditioned on the outcomes remains a stabilizer state as well. This closure property is the reason Clifford computation admits an efficient exact classical simulation.

A two-qubit Clifford circuit. Consider

$$C = S_2 \,\mathrm{CNOT}_{1\to 2}\, H_1$$

acting on $|00\rangle$, with the rightmost gate acting first. At the level of state vectors,

$$|00\rangle \overset{H_1}{\longmapsto} |+\rangle|0\rangle \overset{\mathrm{CNOT}_{1\to 2}}{\longmapsto} \frac{|00\rangle + |11\rangle}{\sqrt{2}} \overset{S_2}{\longmapsto} \frac{|00\rangle + i|11\rangle}{\sqrt{2}}, \qquad |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

The same computation can be followed using only two stabilizer generators:

$$\begin{aligned} \langle Z_1, Z_2\rangle &\overset{H_1}{\longmapsto} \langle X_1, Z_2\rangle \\ &\overset{\mathrm{CNOT}_{1\to 2}}{\longmapsto} \langle X_1X_2, Z_1Z_2\rangle \\ &\overset{S_2}{\longmapsto} \langle X_1Y_2, Z_1Z_2\rangle. \end{aligned}$$

Thus the circuit prepares the stabilizer state studied in the exercise at the beginning of the lecture, without ever requiring a list of all amplitudes.

The simulation theorem below applies to a slightly more general class: Pauli measurements can be performed during the computation and the following operations can depend on the outcomes.

Theorem 5.1 (Gottesman–Knill [1, 2])**.** *A polynomial-size circuit with a stabilizer-state input, Clifford gates given over H, S, and CNOT, measurements of Hermitian Pauli observables specified by their binary labels and signs, and polynomial-time classical control depending on earlier measurement outcomes can be sampled exactly by a classical randomized algorithm in polynomial time.*

Classical simulation algorithm. Maintain a tableau for the quantum state conditioned on the measurement outcomes generated so far.

1. Initialize the tableau with a given independent generating set for the input stabilizer state. For the common input $|x\rangle$, use the rows $(-1)^{x_j} Z_j$, for $j = 1, \dots, N$.
2. Read the next instruction selected by the classical controller.
   (a) For a Clifford gate U, replace every row g_i by $U g_i U^\dagger$, using the update rules of Section 3.
   (b) For a measurement of a Hermitian Pauli M, first compute which rows anticommute with M. If there are none, solve the binary linear system of Section 4 for the coefficients λ_i, compute the signed product $h = \prod_{i:\lambda_i=1} g_i$, and compare its sign with that of M to obtain the deterministic eigenvalue. If there is an anticommuting row, choose one as the pivot g_a, draw $\mu \in \{+1, -1\}$ uniformly, multiply g_a into every other row that anticommutes with M, replace g_a by μM, and output μ.
3. Give each generated outcome to the classical controller and continue until the computation halts. Return the complete measurement transcript, or the designated output bits.

Proof. Fix a transcript prefix h generated by the simulator. We prove the following invariant by induction over the circuit instructions: conditioned on the history h, the tableau contains N

independent commuting generators whose unique common $+1$ eigenstate is exactly the conditional quantum state of the circuit.

The invariant holds initially by the definition of the input stabilizer state. For example, $(-1)^{x_j} Z_j |x\rangle = |x\rangle$ for every j, so the stated initial tableau describes $|x\rangle$.

Suppose next that the controller selects a Clifford gate U. If the old rows are $g_1, \ldots, g_N$, the simulator replaces them by $Ug_1U^\dagger, \ldots, Ug_NU^\dagger$. Each new row is a Pauli because U is Clifford. Conjugation is an invertible homomorphism, so it preserves all multiplication relations, and hence preserves independence and pairwise commutation. Finally,

$$(Ug_iU^\dagger)U|\psi\rangle = Ug_i|\psi\rangle = U|\psi\rangle,$$

so the new rows stabilize the state after the gate. They are still N independent generators, and therefore their common $+1$ eigenspace is one-dimensional. The invariant is preserved.

Now suppose that the controller requests measurement of M. If every row commutes with M, Section 4 shows that M has a definite eigenvalue μ on the current state. The linear-system and sign computation returns this same μ, so the simulator outputs the Born-probability-one outcome. The conditional quantum state and the tableau are unchanged.

If some row anticommutes with M, Section 4 shows that the two Born probabilities are both $1/2$. The simulator makes exactly this random choice. For the chosen outcome μ, the row update produces N independent commuting generators for $|\psi_\mu\rangle = (I + \mu M)|\psi\rangle/\sqrt{2}$, which is precisely the quantum state conditioned on that outcome. Thus the invariant also holds after a random measurement.

It remains to bound the resources. The tableau contains N rows of $2N + 1$ bits, so it uses $O(N^2)$ space. An elementary H, S, or CNOT update changes only constantly many entries in each of the N rows and takes $O(N)$ bit operations. For a measurement, testing all commutators takes $O(N^2)$ operations. In the deterministic case, a straightforward binary linear-system solve and sign reconstruction take $O(N^3)$ time. In the random case, at most $N - 1$ row multiplications of length $O(N)$ are needed, so the update takes $O(N^2)$ time. A polynomial number of circuit instructions is therefore simulated in polynomial time and space. □

6 Summary

A pure stabilizer state is specified by N independent commuting signed Pauli generators. A tableau stores these generators in $O(N^2)$ bits. The binary labels determine commutation and group membership up to sign, while the sign column determines the actual stabilized eigenspaces.

Clifford conjugation maps Pauli generators to Pauli generators. Measuring a Hermitian Pauli either reveals a deterministic eigenvalue, found by signed group membership, or gives a uniform random outcome and replaces one anticommuting generator. Both operations preserve a polynomial-size stabilizer description. Iterating these updates gives the exact Gottesman–Knill sampling algorithm, even when later Clifford operations depend on earlier measurement outcomes.

7 Optional training exercises

These exercises are not part of the assignment.

1. The state $|+i\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$ is stabilized by Y. Write its one-row tableau. Update the tableau after applying H, and identify the resulting state up to global phase.

2. Consider the three commuting Paulis

$$X_1 Z_2, \qquad Z_1 X_2 Z_3, \qquad Z_2 X_3.$$

Verify that they are independent and hence define a three-qubit stabilizer state. Measure Z_2: determine whether the outcome is random or deterministic and give valid post-measurement generators for both possible outcomes.

3. Show that

$$\mathrm{CZ}_{1,2} = H_2 \, \mathrm{CNOT}_{1\to 2} \, H_2$$

is a Clifford gate. Derive its action on X_1, Z_1, X_2, Z_2, and use those rules to prepare the stabilizer state of the preceding exercise from $|+++\rangle$ with two adjacent controlled-Z gates.

8 Assigned exercise: an adaptive Clifford computation

Consider the following computation on the input $|00\rangle$:

$$|00\rangle \xrightarrow{H_1} \xrightarrow{\mathrm{CNOT}_{1\to 2}} \xrightarrow{S_2} .$$

Next measure X_1, and denote the outcome by $\mu \in \{+1, -1\}$. If $\mu = -1$, apply the unitary $Z_1 Z_2$; if $\mu = +1$, do nothing. Finally measure Y_2, with outcome $\nu \in \{+1, -1\}$.

Give a complete stabilizer simulation of this adaptive computation.

(a) Starting from the generators Z_1, Z_2, update the tableau through the three gates and show that the state immediately before the first measurement is stabilized by

$$X_1 Y_2, \qquad Z_1 Z_2.$$

(b) Use the Pauli-measurement rule to show that μ is uniform. For each value of μ, give two independent signed generators for the post-measurement state.

(c) Apply the classically controlled correction. Show, using signed row multiplication where needed, that after the correction both branches have the same stabilizer group

$$\langle X_1, Y_2 \rangle.$$

(d) Determine the conditional distribution of ν, and hence the complete joint distribution of the transcript (μ, ν).

(e) Identify the final two-qubit state.

A Why H, S, and CNOT generate the Clifford group

The definition of $\mathcal{C}_N$ as a normalizer inside the full unitary group includes $e^{i\theta}U$ whenever it includes U. Consequently, a finite gate set cannot generate every global phase. The appropriate statement is therefore generation *up to global phase*, which is also the physically relevant notion for quantum circuits.

Theorem A.1 (Generation of the Clifford group)**.** *For every $U \in \mathcal{C}_N$, there is a circuit C over one-qubit H and S gates and two-qubit CNOT gates such that*

$$U = e^{i\theta}C$$

for some $\theta \in \mathbb{R}$.

Proof. The proof has two parts. We first synthesize the action of U on Pauli labels, ignoring signs. We then correct the remaining signs by a Pauli operator.

1. The action on Pauli labels is symplectic. Let ε_j be the j-th standard basis vector of $\mathbb{F}_2^N$, and define

$$e_j = (\varepsilon_j, 0), \qquad f_j = (0, \varepsilon_j).$$

These are respectively the labels of X_j and Z_j. They form a symplectic basis: $\omega(e_j, f_k) = \delta_{jk}$, while all pairings between two e's or two f's vanish.

Conjugation by a Clifford maps Paulis to Paulis. After quotienting out their phases, it therefore induces an invertible linear map

$$F_U : \mathbb{F}_2^{2N} \longrightarrow \mathbb{F}_2^{2N}.$$

Conjugation preserves commutation and anticommutation, so

$$\omega(F_U v, F_U w) = \omega(v, w) \qquad \text{for all } v, w \in \mathbb{F}_2^{2N}.$$

Thus F_U is a symplectic transformation.

On binary labels, the three elementary gates act as follows:

gate	label update
H_j	$(a_j, b_j) \longmapsto (b_j, a_j)$
S_j	$(a_j, b_j) \longmapsto (a_j, b_j \oplus a_j)$
$\mathrm{CNOT}_{c\to t}$	$a_t \longmapsto a_t \oplus a_c, \quad b_c \longmapsto b_c \oplus b_t$

with all undisplayed coordinates unchanged. These formulas follow directly from the Pauli conjugation rules in Section 3.

2. Reduction of one symplectic pair. We prove by induction on N that the transformations above generate every symplectic transformation. Let F be symplectic and consider

$$p = F(e_1), \qquad q = F(f_1).$$

Since F is invertible, $p \neq 0$. On each qubit on which the Pauli labelled by p is nonidentity, H and S can turn the local factor into X, up to sign. Indeed, their actions permute the three nonzero single-qubit labels X, Y, Z.

We may move one of these X's to qubit 1 using

$$\mathrm{SWAP}_{1j} = \mathrm{CNOT}_{1\to j}\,\mathrm{CNOT}_{j\to 1}\,\mathrm{CNOT}_{1\to j}\,.$$

The label p is now a product of X_1 and possibly some other X_j's. For every $j > 1$ for which X_j occurs, conjugation by $\mathrm{CNOT}_{1\to j}$ removes it, because

$$X_1 X_j \longmapsto (X_1 X_j) X_j = X_1.$$

We have therefore mapped p to e_1.

Apply all these transformations to q as well. Since the symplectic pairing is preserved,

$$\omega(e_1, q) = \omega(p, q) = \omega(e_1, f_1) = 1.$$

Hence the first-qubit factor of q is Z_1 or Y_1; equivalently, its first b-coordinate is one.

We next remove the factors of q on qubits $j > 1$, without changing e_1. If the factor on qubit j is nonidentity, first use H_j and S_j to turn it into Z_j. Then conjugate by $\mathrm{CNOT}_{j\to 1}$. This CNOT fixes X_1, while its action on the relevant part of q is

$$Z_j Z_1 \longmapsto Z_j (Z_j Z_1) = Z_1.$$

Repeating this for every $j > 1$ leaves $q = Z_1$ or $q = Y_1$, up to sign. In the second case, conjugation by $H_1 S_1 H_1$ maps the label of Y_1 to that of Z_1 while fixing the label of X_1: on the first pair of bits,

$$(a_1, b_1) \longmapsto (a_1 \oplus b_1, b_1).$$

Thus we have reduced the first symplectic pair to

$$p = e_1, \qquad q = f_1.$$

3. Induction on the remaining qubits. After the preceding reduction, the current symplectic transformation fixes e_1 and f_1. It must therefore preserve their common symplectic orthogonal complement

$$W = \mathrm{span}\{e_2, \ldots, e_N, f_2, \ldots, f_N\}.$$

Indeed, for $v \in W$, symplectic invariance gives

$$\omega(Fv, e_1) = \omega(Fv, Fe_1) = \omega(v, e_1) = 0$$

and similarly $\omega(Fv, f_1) = 0$. Thus $Fv \in W$. The restriction of F to W is a symplectic transformation on $N - 1$ qubits, so the induction hypothesis reduces it using gates acting only on qubits $2, \ldots, N$.

This gives a sequence of elementary gates that reduces any symplectic transformation to the identity. Reversing that sequence synthesizes the original transformation: H and CNOT are self-inverse, while $S^{-1} = S^3$. Consequently there is a circuit C over H, S, CNOT whose unsigned action on Pauli labels is exactly F_U.

4. Recovering the Pauli signs. Set

$$V = C^\dagger U.$$

The unitary V fixes every Pauli label, although it may still change its sign. In particular, there are bits $r_j, s_j \in \mathbb{F}_2$ such that

$$V X_j V^\dagger = (-1)^{r_j} X_j, \qquad V Z_j V^\dagger = (-1)^{s_j} Z_j.$$

Consider the Hermitian Pauli

$$R = P(s, r), \qquad s = (s_1, \ldots, s_N), \quad r = (r_1, \ldots, r_N).$$

Conjugation by R multiplies X_j by $(-1)^{r_j}$ and Z_j by $(-1)^{s_j}$. Therefore RV fixes every X_j and Z_j exactly. It consequently commutes with every Pauli operator. Since the Pauli operators span the full matrix algebra on $(\mathbb{C}^2)^{\otimes N}$, the only such unitary is a scalar:

$$RV = e^{i\theta} I.$$

It follows that

$$U = e^{i\theta} C R^\dagger.$$

Finally, the Pauli correction is itself generated up to phase by H and S, because

$$Z_j = S_j^2, \qquad X_j = H_j S_j^2 H_j.$$

Absorbing $R^\dagger$ into the circuit completes the proof. □

Remark A.2. *The proof is constructive. At each induction step it uses $O(N)$ elementary gates to reduce one symplectic pair, so it also gives an $O(N^2)$-gate synthesis algorithm for a Clifford specified by its action on the Pauli generators, followed by $O(N)$ Pauli sign corrections.*

References

[1] Daniel Gottesman, *The Heisenberg Representation of Quantum Computers*, 1998.
https://arxiv.org/abs/quant-ph/9807006

[2] Scott Aaronson and Daniel Gottesman, *Improved Simulation of Stabilizer Circuits*, Physical Review A 70, 052328 (2004).
https://arxiv.org/abs/quant-ph/0406196