Stabilizer Formalism

A beautiful framework with origins in quantum-error correction, now central to quantum computation.

November 26, 2024

Key Definitions

- Stabilizer Gates:
  - CNOT, Hadamard, Phase Gate $P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
- Stabilizer Circuits:
  - Quantum circuits made entirely of stabilizer gates.
- Stabilizer States:
  - States generated by a stabilizer circuit starting from $|00\ldots0\rangle$.

Not Universal

- Warning: Set {CNOT, Hadamard, P} is not universal.
- Why is this surprising?
  - Hadamard: Creates superpositions.
  - CNOT: Acts on two qubits and enables entanglement (with Hadamard).
  - Phase Gate (P): Adds complex phases.
- Yet, the set {CNOT, Hadamard, P} is insufficient for universality.

- What can S demonstrate?
- Quantum protocols:
  - Quantum teleportation, BB84, Wiesner’s quantum money.
- Quantum algorithms:
  - Deutsch-Jozsa, Bernstein-Vazirani.
- Quantum error correction:
  - Shor’s 9-qubit code.

Why not universal?

- Key Limitation:
    - Operations only reach discrete states — nothing in between.
- Superposition Constraints:
    - Any n-qubit superposition assigns nonzero amplitudes to strings in a set $A \subseteq \{0,1\}^n$
    - A is always:
        - An equal superposition (with phases $\pm 1, \pm i$)
        - An affine subspace of $\mathbb{F}_2^n$

1-Qubit Case

- Using H and P, we can only reach 6 states (ignoring global phases): $|0\rangle, |1\rangle, |+\rangle, |-\rangle, |i\rangle, |-i\rangle$
- These are the 1-qubit stabilizer states.

What About Two Qubits?

- New Possibilities:
  - States like $\frac{|00\rangle + i|11\rangle}{\sqrt{2}}$ are reachable.
- Patterns Persist:
  - Always equal superpositions over a power-of-2 number of strings.
- Measurement Outcomes (in $\{|0\rangle, |1\rangle\}$ basis):
  - Always $|0\rangle$
  - Always $|1\rangle$
  - $|0\rangle$ and $|1\rangle$ with equal probabilities.

What Does This All Mean?

- Key Concept:
  - A unitary U stabilizes a pure state $|\Psi\rangle$ if $U|\Psi\rangle = |\Psi\rangle$.
    - $|\Psi\rangle$ is an eigenstate of U with eigenvalue $+1$.
- Important Note:
  - Global phase matters!
    - If $U|\Psi\rangle = -|\Psi\rangle$, then U does not stabilize $|\Psi\rangle$.
- Properties of Stabilizers:
  - If U and V stabilize $|\Psi\rangle$ then UV, VU, U^{-1}, V^{-1} and I (identity) also stabilize $|\Psi\rangle$.
  - The set of stabilizers forms a group under multiplication.

The Pauli Matrices

- Definition: The four Pauli matrices, fundamental to quantum physics.
- $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- Error Types in Quantum Error Correction:
  - No Error: $I|1\rangle = |1\rangle$
  - Bit Flip: $X|1\rangle = |0\rangle$
  - Phase Flip: $Z|1\rangle = -|1\rangle$
  - Both (Bit & Phase Flip): $Y|1\rangle = -i|0\rangle$

Properties

- Key Identities:
  - $X^2 = Y^2 = Z^2 = I$
  - $XY = iZ, YX = -iZ$
  - $YZ = iX, ZY = -iX$
  - $ZX = iY, XZ = -iY$
- Connections:
  - These relations resemble the quaternions (not a coincidence!).
  - All four matrices are unitary and Hermitian.

What Does Each Pauli Matrix Stabilize?

- I: Stabilizes everything.
- $-I$: Stabilizes nothing (global phase matters: $-I|\Psi\rangle \neq |\Psi\rangle$)
- Specific Stabilizations:
  - X: Stabilizes $|+\rangle$, $-X$ stabilizes $|-\rangle$.
  - Z: Stabilizes $|0\rangle$, $-Z$ stabilizes $|1\rangle$.
  - Y: Stabilizes $|i\rangle$, $-Y$ stabilizes $|-i\rangle$
- Conclusion: Each of the six 1-qubit stabilizer states corresponds to a Pauli matrix that stabilizes it.

Stabilizer Groups - Basics

- Definition: Given an n-qubit pure state $|\Psi\rangle$, its stabilizer group is:
    - The group of all tensor products of Pauli matrices that stabilize $|\Psi\rangle$.
- Properties:
    - Forms a group since:
        - Pauli matrices are closed under multiplication.
        - Stabilization of $|\Psi\rangle$ is closed under group operations.
    - Abelian: Stabilizer groups are always commutative.
- Examples:
    - Stabilizer group of $|0\rangle$: $\{I, Z\}$
    - Stabilizer group of $|+\rangle$: $\{I, X\}$
    - Stabilizer group of $|0\rangle \otimes |+\rangle$: $\{II, IX, ZI, ZX\}$ (Omitting $\otimes$ for simplicity)

Stabilizer Group - Bell State Example

- Stabilizer Group of Bell State $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$:
  - XX: Stabilizes the state (symmetry under X-flip).
  - $-YY$: Similarly stabilizes the state.
  - ZZ: Obtained by component-wise multiplication: $XX \cdot (-YY) = -(iZ)(iZ) = ZZ$
- Result: The stabilizer group is $\{II, XX, -YY, ZZ\}$
- For $\frac{|00\rangle - |11\rangle}{\sqrt{2}}$, stabilizer group is $\{II, -XX, YY, ZZ\}$

Characterization of Stabilizer States

- Fact: For n-qubit states, the stabilizer states are exactly those with a stabilizer group of size 2^n.
- Examples:
  - 1-qubit stabilizer states: Stabilizer group has 2 elements.
  - 2-qubit stabilizer states: Stabilizer group has 4 elements.
- Significance: This offers a structural characterization of stabilizer states:
  - Independent of stabilizer circuits.
  - Reflects the invariant preserved by stabilizer circuits.

Generating Sets for Stabilizer Groups

- Key Question: How can we succinctly specify the stabilizer group G of an n -qubit stabilizer state (size 2^n)?
- Answer: The stabilizer group G is always generated by n elements, which are $\pm$ tensor products of Pauli matrices.
  - To specify G, it suffices to provide n such generators.
- Example: Stabilizer group of the Bell pair $\{II, XX, -YY, ZZ\}$
  - Generating set 1: $\{XX, ZZ\}$
  - Generating set 2: $\{XX, -YY\}$

Storage Efficiency of Stabilizer Formalism

- Storing a Generating Set:
  - Each generator requires $2n + 1$ bits:
    - 2 bits for each of the n Pauli matrices.
    - 1 bit for the $\pm$ sign.
  - Total storage for n generators: $n(2n+1) = 2n^2 + n = O(n^2)$
- Comparison:
  - Storing the full amplitude vector or stabilizer group: $\sim 2^n$ bits.
  - Exponential savings achieved using stabilizer formalism.
- Conclusion: This efficiency demonstrates the power of the stabilizer formalism in quantum computation.

The Gottesman–Knill Theorem

- Theorem: There is a polynomial-time classical algorithm to simulate any stabilizer circuit acting on an initial stabilizer state (e.g., $|00\ldots0\rangle$).
- Capabilities:
  - Compute probabilities of measurement outcomes.
  - Simulate measurement outcomes using random bits.
- Implication:
  - Positive: Efficient simulation of stabilizer circuits.
  - Negative: Stabilizer circuits alone cannot provide superpolynomial quantum speedups.
- How It Works:
  - Track the stabilizer group's generators.
  - Update the generators for each gate (CNOT, Hadamard, Phase) or measurement.

The Gottesman–Knill Algorithm

- Initial Stabilizer Representation: For $|00\ldots0\rangle$:
  - Stabilizer group includes $II\ldots I$, implied by default.
  - Generating set: $ZIII\ldots I, IZII\ldots I, IIZI\ldots I, \ldots, IIII\ldots Z$
- Tableau Representation
  - Use two $n \times n$ binary matrices:
    - X Matrix: Tracks X or Y
    - Z Matrix: Tracks Z or Y

Gate Operations in Tableau Representation

- Rules for Gate Updates:
- Hadamard Gate (H) on i-th qubit:
  - Swap the i-th column of the X and Z matrices.
- Phase Gate (P) on i-th qubit:
  - XOR i-th column of the X matrix into the Z matrix.
- CNOT Gate:
  - Control i, target j:
    - XOR i-th column of X into j-th column of X.
    - XOR j-th column of Z into i-th column of Z.

Measurements and Observations

- Measurement in $\{ |0\rangle, |1\rangle \}$ Basis:
  - Determinate outcome if i-th column of the X matrix is all 0's.
- Why?
  - Columns indicate commutation relationships; all 0's in X implies only Z acts, ensuring definite outcomes.
- Efficiency:
  - Tracks stabilizers efficiently.
  - Skips signs unless the specific outcome is needed.

Rank of the X Matrix and Basis States

- Fact: For a stabilizer state, the number of basis states with nonzero amplitudes is 2^k, where k is the rank of the X matrix.
- Example 1: If rank$(X) = 0$, only a single basis state (e.g., $|0000\rangle$) has a nonzero amplitude.
- Example 2…