CS 599 P1: Introduction to Quantum Computation   Boston University, Fall 2025
Instructor: Alexander Poremba

LECTURE # 22: STABILIZER FORMALISM

In the previous lectures, we encountered concrete quantum error-correcting codes such as the 9-qubit Shor code and saw how more general CSS codes can be constructed from pairs of classical linear codes. While these constructions are extremely powerful, they can sometimes obscure the underlying mathematical structure that all such quantum codes share.

In this lecture, we introduce the *stabilizer formalism*. This formalism provides a clean, algebraic framework for describing and analyzing a large family of quantum error-correcting codes, including the Shor code and all CSS codes as special cases. Conceptually, stabilizer codes allow us to define a quantum code not by explicitly writing down its codewords, but instead by specifying a collection of *symmetries* that all valid code states must obey.

1 Background: Group theory

Since the stabilizer formalism is inherently group-theoretic, we begin by recalling a few basic definitions.

Groups. A *group* $(G, \cdot)$ is a set G together with a binary operation $\cdot$ satisfying the following axioms:

- **Closure:** For all $g, h \in G$, the product $g \cdot h$ is also in G.
- **Associativity:** For all $g, h, k \in G$, we have $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.
- **Identity element:** There exists an element $e \in G$ such that $g \cdot e = e \cdot g = g$ for all $g \in G$.
- **Inverse:** For every $g \in G$, there exists an element $g^{-1} \in G$ such that

$$g \cdot g^{-1} = g^{-1} \cdot g = e.$$

Groups arise naturally whenever we study symmetries, transformations, or sets of operators closed under multiplication.

Abelian groups. A group G is called *abelian* if the group operation is commutative:

$$g \cdot h = h \cdot g \qquad \forall g, h \in G.$$

As we will see, commutativity will be a crucial requirement for stabilizer groups.

Generating sets. A subset $S \subseteq G$ is called a *generating set* if every element of G can be written as a finite product of elements of S and their inverses. Intuitively, generators are the "basic building blocks" from which the entire group can be constructed.

Example (roots of unity). Let $\omega = e^{2\pi i/n}$. The set

$$G = \{1, \omega, \omega^2, \dots, \omega^{n-1}\}$$

forms an abelian group under multiplication. In fact, this group is generated by the single element ω.

Group actions. Let G be a group and X a set. A *group action* of G on X is a map

$$G \times X \to X, \qquad (g, x) \mapsto g \cdot x$$

such that

- $e \cdot x = x$ for all $x \in X$,
- $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$.

In quantum information, the most important example is a group of operators acting on quantum states.

Stabilizer subgroups. Given an action of G on X and a particular element $x \in X$, the *stabilizer subgroup* of x is defined as

$$\mathrm{Stab}(x) = \{g \in G : g \cdot x = x\}.$$

That is, it consists of all group elements that leave x unchanged. This notion will later be applied to quantum states.

2 Quantum error-correcting codes

We now recall the basic definition of a quantum code.

Definition. An $[[n, k]]$ quantum error-correcting code uses *redundancy* to encode k *logical* qubits into a larger Hilbert space consisting of n *physical* qubits such that

$$|\psi\rangle \in (\mathbb{C}^2)^{\otimes k} \quad \longmapsto \quad |\overline{\psi}\rangle \in (\mathbb{C}^2)^{\otimes n}.$$

The image of this embedding is a 2^k-dimensional subspace of the 2^n-dimensional Hilbert space, called the *codespace*. The purpose of the encoding is to protect the logical information against physical noise.

Example: the 9-qubit Shor code. The Shor code encodes a single logical qubit into 9 physical qubits. Its logical basis states are

$$|\overline{0}\rangle = \frac{1}{2^{3/2}}\big(\,|000\rangle + |111\rangle\,\big)^{\otimes 3},$$
$$|\overline{1}\rangle = \frac{1}{2^{3/2}}\big(\,|000\rangle - |111\rangle\,\big)^{\otimes 3}.$$

Here, an arbitrary logical state $\alpha\,|0\rangle + \beta\,|1\rangle$ is encoded as

$$|\overline{\psi}\rangle = \alpha\,|\overline{0}\rangle + \beta\,|\overline{1}\rangle\,.$$

Rather than thinking of these states as complicated superpositions, the stabilizer formalism will allow us to describe them via symmetry conditions.

3 Stabilizer symmetries

The stabilizer approach is based on the observation that many important quantum states can be uniquely characterized as simultaneous eigenstates of a set of commuting operators. Before we formally define what a quantum stabilizer code is, let us first begin with an insightful example.

Example (Bell-state symmetries). Consider the two-qubit Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

A direct calculation shows that

$$(X \otimes X)\,|\Phi^+\rangle = |\Phi^+\rangle\,, \qquad (Z \otimes Z)\,|\Phi^+\rangle = |\Phi^+\rangle\,.$$

Interestingly, the Bell pair $|\Phi^+\rangle$ is a $+1$ eigenstate of both $X \otimes X$ and $Z \otimes Z$—despite the fact that X and Z are not diagonal in the same basis and do not commute, i.e. $[X, Z] = XZ - ZX \neq 0$.

Although X and Z anti-commute, the two-qubit operators $X \otimes X$ and $Z \otimes Z$ do in fact commute:

$$(X \otimes X)(Z \otimes Z) = (XZ) \otimes (XZ) = (ZX) \otimes (ZX) = (Z \otimes Z)(X \otimes X).$$

The two minus signs cancel, allowing us to simultaneously diagonalize $X \otimes X$ and $Z \otimes Z$ in the same basis. The notion of *simultaneous diagonalization* is in fact a much more general principle in linear algebra.

Fact: Simultaneous diagonalization

If two Hermitian operators commute, then they can be diagonalized in the same orthonormal basis; that is, there exists an orthonormal basis consisting of simultaneous eigenvectors of both operators.

In the case of $X \otimes X$ and $Z \otimes Z$, their simultaneous eigendecomposition is given by the Bell basis:

Bell state	$X \otimes X$	$Z \otimes Z$
$\lvert\Phi^+\rangle$	$+1$	$+1$
$\lvert\Phi^-\rangle$	-1	$+1$
$\lvert\Psi^+\rangle$	$+1$	-1
$\lvert\Psi^-\rangle$	-1	-1

Each Bell state is uniquely identified by its eigenvalues under $X \otimes X$ and $Z \otimes Z$; for example, we can immediately see that the Bell pair $|\Phi^+\rangle$ is the *unique* two-qubit state which carries a $+1$ symmetry under both $X \otimes X$ and $Z \otimes Z$. This idea is precisely what gives rise to the quantum stabilizer formalism: instead of characterizing a quantum code by explicitly writing down its codewords, it suffices to specify a collection of symmetries that all valid code states must obey. The symmetries of the quantum stabilizer formalism are defined via Pauli operators, which form a group under multiplication.

The Pauli group. The single-qubit Pauli group is defined as

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}.$$

By inspection, we can see that $\mathcal{P}_1$ contains 16 elements.

The n-qubit Pauli group $\mathcal{P}_n$ consists of all n-fold tensor products of Pauli operators, together with overall phases $\{\pm 1, \pm i\}$. It is straightfoward to see that $\mathcal{P}_n$ is of size

$$|\mathcal{P}_n| = 4^{n+1}.$$

Properties of Pauli operators

- Any two n-qubit Pauli operators either commute or anti-commute.
- Every Pauli operator has eigenvalues contained in $\{\pm 1, \pm i\}$.

4 Quantum stabilizer codes

We are now ready to formally define stabilizer codes.

Definition. An $[[n, k]]$ *stabilizer code* is specified by an abelian subgroup of the n-qubit Pauli group, i.e.,

$$\mathcal{S} \subset \mathcal{P}_n \,,$$

such that $-I \notin \mathcal{S}$. The associated codespace is defined as

$$\mathcal{C} = \{|\overline{\psi}\rangle \in (\mathbb{C}^2)^{\otimes n} : S\,|\overline{\psi}\rangle = (+1)\,|\overline{\psi}\rangle \,,\ \forall S \in \mathcal{S}\}.$$

That is, valid code states are precisely those states that are stabilized by every element of $\mathcal{S}$.

Dimension of the codespace. If the stabilizer group $\mathcal{S}$ has $n-k$ independent generators, each consisting of an n-qubit Pauli operator, then it contains 2^{n-k} elements. Intuitively, each independent stabilizer condition halves the dimension of the Hilbert space, so the codespace has dimension

$$\dim(\mathcal{C}) = \frac{2^n}{2^{n-k}} = 2^k.$$

Here, we are relying on the following well-known fact about the generators of a finite group.

Generators of a finite group

A group of size $|G|$ can be generated by at most $\log_2 |G|$ independent generators.

Therefore, a stabilizer group $\mathcal{S}$ with $n - k$ stabilizer generators describes an $[[n, k]]$ quantum code.

4.1 Examples of quantum stabilizer codes.

Let us now consider two examples of stabilizer codes.

Trivial stabilizer code. The stabilizer

$$\mathcal{S} = \langle Z_1, Z_2, \ldots, Z_{n-k} \rangle$$

fixes the first $n-k$ qubits to $|0\rangle$. A stabilizer tableau is

	1	2	$\cdots$	$n-k$	$n-k+1$	$\cdots$	n
Z_1	Z	I	$\cdots$	I	I	$\cdots$	I
Z_2	I	Z	$\cdots$	I	I	$\cdots$	I
$\vdots$			$\ddots$				
Z_{n-k}	I	I	$\cdots$	Z	I	$\cdots$	I

The Shor code. The 9-qubit Shor code has 8 stabilizer generators. A convenient tableau representation is

	1	2	3	4	5	6	7	8	9
Z_1Z_2	Z	Z	I	I	I	I	I	I	I
Z_2Z_3	I	Z	Z	I	I	I	I	I	I
Z_4Z_5	I	I	I	Z	Z	I	I	I	I
Z_5Z_6	I	I	I	I	Z	Z	I	I	I
Z_7Z_8	I	I	I	I	I	I	Z	Z	I
Z_8Z_9	I	I	I	I	I	I	I	Z	Z
$X_1 \cdots X_6$	X	X	X	X	X	X	I	I	I
$X_4 \cdots X_9$	I	I	I	X	X	X	X	X	X

5 Error Detection and Correction in Stabilizer Codes

Let us now briefly explain how quantum errors are detected and corrected in the stabilizer formalism.

Let $\mathcal{P}_n$ denote the n-qubit Pauli group, and let $\mathcal{S} \subset \mathcal{P}_n$ be an abelian stabilizer group generated by $n-k$ independent Pauli operators $\{S_1, \ldots, S_{n-k}\}$, none of which being equal to $-I$. The codespace is

$$\mathcal{C} = \{|\overline{\psi}\rangle \in (\mathbb{C}^2)^{\otimes n} : S\,|\overline{\psi}\rangle = (+1)\,|\overline{\psi}\rangle\,,\ \forall S \in \mathcal{S}\}.$$

Let $|\overline{\psi}\rangle \in \mathcal{C}$ be a logical state and let $E \in \mathcal{P}_n$ represent a Pauli error acting on the physical qubits.

5.1 Commutation Relations with Stabilizers

Since both E and each stabilizer generator S_i are Pauli operators, they either commute or anticommute:

$$[S_i, E] = 0 \quad \text{or} \quad \{S_i, E\} = 0.$$

where $\{S_i, E\} = S_iE + ES_i$ is the anti-commutator. If E commutes with S_i, then

$$S_i(E\,|\overline{\psi}\rangle) = E\,|\overline{\psi}\rangle\,,$$

and the measurement outcome of S_i remains $+1$. If instead E anticommutes with S_i, then

$$S_i(E\,|\overline{\psi}\rangle) = -E\,|\overline{\psi}\rangle\,,$$

so the measurement outcome of S_i is flipped from $+1$ to -1.

Thus, an error E maps the codespace either onto itself or onto an orthogonal eigenspace of the stabilizer generators.

5.2 Syndrome Measurement

Measuring all $n-k$ stabilizer generators produces a classical bit string

$$\mathbf{s}(E) = (s_1, \ldots, s_{n-k}) \in \{0,1\}^{n-k},$$

called the *error syndrome*, where

$$s_i = \begin{cases} 0, & \text{if } [S_i, E] = 0, \\ 1, & \text{if } \{S_i, E\} = 0. \end{cases}$$

Equivalently, $s_i = 1$ indicates that the measurement outcome of S_i is -1.

Importantly, the syndrome depends only on the commutation relations between E and the stabilizer generators. In particular, if E and E' differ by a stabilizer, then they produce the same syndrome.

5.3 Stabilizer Decoding

The task of decoding is to infer a suitable correction operator from the measured syndrome.

Stabilizer Decoding Problem

Given: A stabilizer group $\mathcal{S}$ and a measured syndrome $\mathbf{s} \in \{0,1\}^{n-k}$.

Promise: The physical error has sufficiently low weight.

Goal: Find a Pauli operator $\widehat{E} \in \mathcal{P}_n$ consistent with $\mathbf{s}$, up to multiplication by an element of $\mathcal{S}$.

The decoder outputs a correction operator $C(\mathbf{s})$ such that $C(\mathbf{s})E \in \mathcal{S}$ whenever the true error E lies within the correctable error set.

5.4 Recovery and Logical Errors

Applying the correction operator yields

$$C(\mathbf{s})E\,|\overline{\psi}\rangle = S\,|\overline{\psi}\rangle$$

for some $S \in \mathcal{S}$. Since stabilizers act trivially on the codespace,

$$S\,|\overline{\psi}\rangle = |\overline{\psi}\rangle\,,$$

and the original logical state is restored, up to an irrelevant global phase.

If instead $C(\mathbf{s})E$ differs from the identity by a nontrivial logical operator, then the recovery induces a logical error. A stabilizer code is said to *correct* a set of errors $\mathcal{E}$ if for all $E, E' \in \mathcal{E}$,

$$E^\dagger E' \notin \mathcal{N}(\mathcal{S}) \setminus \mathcal{S},$$

where $\mathcal{N}(\mathcal{S})$ denotes the normalizer of the stabilizer group.

Remark. Because stabilizer codes are generally *degenerate*, multiple distinct Pauli errors may act identically on the codespace. Consequently, decoding aims only to identify the error up to stabilizers, rather than uniquely determining the physical error.