CHAPTER 10

Learning Stabilizer States

We now introduce an important family of states that lies at the boundary between classical and quantum computation: **stabilizer states**. A salient property of these states is that they can be highly entangled, yet they are *classically simulable* in the sense that one can sample from the probability distribution encoded by their amplitudes using classical computation – this is the content of the *Gottesman-Knill theorem*, which we will not prove in this course [GOT98]. Indeed as we will see in the next lecture, they offer a useful yardstick by which to quantify the extent to which a given quantum computation is truly quantum. Stabilizer states also come with rich algebraic structure and are characterized by their symmetries. This structure makes them particularly useful for robustly encoding quantum information to be resilient to noise, and for this reason they play a central role in the field of *quantum error correction*.

In this lecture, we continue the theme of learning structured classes of states by giving an efficient algorithm for learning stabilizer states, due to Montanaro [Mon07]. Unlike the algorithms we saw for shallow circuit states and Gibbs states, this algorithm will heavily exploit the algebraic structure native to stabilizer states. This will also give us our first glimpse at a powerful and ubiquitous primitive: **Bell sampling**.

1. Stabilizer State Basics

Stabilizer states can be defined either in terms of the quantum circuits that prepare them, or in terms of the symmetries that they possess.

Definition 165 (Clifford group)**.** *The **Clifford group** $\mathcal{C}_n$ on n qubits is the group of unitaries U for which $UPU^{-1} \in \mathcal{P}_n$ for all $P \in \mathcal{P}_n$. One choice of gates generating $\mathcal{C}_n$ are Hadamard, phase, and CNOT:*

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

*We will refer to elements of $\mathcal{C}_n$ as **Clifford circuits** as they can be built out of these gates.*

Definition 166 (Stabilizer states – Clifford circuit formulation)**.** *A state $|\psi\rangle$ is a* stabilizer state *if it can be written as $|\psi\rangle = U|0^n\rangle$ for $U \in \mathcal{C}_n$.*

Lemma 167 (Symmetry formulation)**.** *A state $|\psi\rangle$ is a stabilizer state if and only if there are exactly 2^n commuting Pauli operators $P \in \{\pm I, \pm X, \pm Y, \pm Z\}^{\otimes n}$ that* stabilize *$|\psi\rangle$, that is, for which $P|\psi\rangle = |\psi\rangle$.*

PROOF. Suppose $|\psi\rangle = U|0^n\rangle$ for $U \in \mathcal{C}_n$. There are exactly 2^n Paulis P for which $P|0^n\rangle = |0^n\rangle$, namely $P \in \{I, Z\}^{\otimes n}$. Because U is Clifford, for every $P \in \mathcal{P}_n$ we have $UP = P_U U$ for a unique $P_U \in \mathcal{P}_n$. Therefore, for each $P \in \{I, Z\}^{\otimes n}$,

$$P_U|\psi\rangle = P_U U|0^n\rangle = UP|0^n\rangle = U|0^n\rangle = |\psi\rangle \ ,$$

so there are exactly 2^n Paulis that stabilize $|\psi\rangle$. Furthermore, they commute because they stabilize $|\psi\rangle$ and all Paulis either commute or anti-commute with each other.

For the converse, we provide a sketch of the proof. Let $P_1, \ldots, P_n \in G$ be a set of generators for the abelian group consisting of stabilizers of $|\psi\rangle$, and let $Z_1, \ldots, Z_n$ denote the Z operators on qubits $1, \ldots, n$. Each P_j can be expressed as $\prod_i Z_i^{a_{ij}}$, so we can effectively perform Gaussian elimination to obtain $U \in \mathcal{C}_n$ for which $UP_iU^{-1} = Z_i$ for all i (the details for this are provided in Lemma 177). As $P_i|\psi\rangle = |\psi\rangle$, we have that

$$U|\psi\rangle = UP_i|\psi\rangle = Z_iU|\psi\rangle \ ,$$

so $U|\psi\rangle$ is stabilized by all Paulis in $\{I, Z\}^{\otimes n}$. Therefore, $|\psi\rangle = U^\dagger|\phi\rangle$ for $|\phi\rangle \in \{|0\rangle, |1\rangle\}^{\otimes n}$, and thus $|\psi\rangle = U'|0^n\rangle$ for some $U' \in \mathcal{C}_n$. □

The group of Paulis stabilizing a stabilizer state is important enough to merit a name:

Definition 168. *Given a stabilizer state $|\psi\rangle$, the group of 2^n Pauli operators P for which $P|\psi\rangle = |\psi\rangle$ is called the **stabilizer group** of $|\psi\rangle$, denoted* $\mathrm{Stab}(|\psi\rangle)$.

Example 169. *As we saw in the proof above, the simplest stabilizer state is $|0^n\rangle$, whose stabilizer group is $\{I, Z\}^{\otimes n}$. More generally, any state which is a product of single-qubit states from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |i\rangle, |-i\rangle\}$ is a stabilizer state.*

Another example to keep in mind is the n-qubit cat state $\frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$, which can be prepared starting from $|0^n\rangle$ by applying H to one qubit and then taking CNOTs with all of the remaining qubits.

There is a third formulation of stabilizer states in terms of their amplitudes in the computational basis:

Lemma 170. *If $|\psi\rangle$ is stabilizer, then it is equal, up to phase, to*

$$\frac{1}{\sqrt{|A|}} \sum_{x \in A} i^{\ell(x)} (-1)^{q(x)} |x\rangle \tag{62}$$

for some affine subspace $A \subseteq \mathbb{F}_2^n$, linear function $\ell : \mathbb{F}_2^n \to \mathbb{F}_2$, and quadratic function $q : \mathbb{F}_2^n \to \mathbb{F}_2$.

PROOF SKETCH. This follows by direct calculation by inducting on the number of gates in the Clifford circuit preparing $|\psi\rangle$. It is not hard to see that applying phase or CNOT gates will respectively modify ℓ and linearly transform A. The trickiest part to verify is that applying a Hadamard gate to a state of the form Eq. (62) results in another state of the same form but with A, ℓ, and q all modified. The complete calculation is provided in Appendix A of [**VDN10**]. □

In fact the converse holds, though we will not prove or use this.

2. Symplectic Vector Spaces – A First Glimpse

When ρ is pure, the distribution over measurement outcomes under Bell sampling has a useful characterization. It will be convenient to adopt the following mapping between Pauli operators and bitstrings.

Definition 171 (Bijection between Paulis and strings)**.** *Given a string* $\vec{s} = (s_{1,1}, \ldots, s_{1,n}, s_{2,1}, \ldots, s_{2,n}) \in \mathbb{F}_2^{2n}$*, define*

$$P_{\vec{s}} \triangleq \bigotimes_{j=1}^{n} i^{s_{1,j} \cdot s_{2,j}} X_j^{s_{1,j}} Z_j^{s_{2,j}} .$$

Every $P \in \mathcal{P}_n$ *can then be written as* $\phi \cdot P_{\vec{s}}$ *for some phase* $\phi \in \{\pm 1, \pm i\}$*.*

With this identification, we can naturally associate to every element of $\mathrm{Stab}(|\psi\rangle)$ a string as follows:

Definition 172 (Unsigned stabilizer group)**.** *The* ***unsigned stabilizer group*** *of a stabilizer state* $|\psi\rangle$*, denoted* $\mathrm{Weyl}(|\psi\rangle)$*, is the set of* $\vec{s} \in \mathbb{F}_2^{2n}$ *for which either* $P_{\vec{s}}|\psi\rangle = |\psi\rangle$ *or* $P_{\vec{s}}|\psi\rangle = -|\psi\rangle$*. Note that the elements of* $\mathrm{Weyl}(|\psi\rangle)$ *and* $\mathrm{Stab}(|\psi\rangle)$ *are in one-to-one correspondence up to sign.*[1]

In fact the mapping in Definition 171 has even richer structure: commutation relations between Pauli operators correspond to linear algebraic relations between their associated vectors in $\mathbb{F}_2^{2n}$ equipped with the *symplectic* inner product.

Definition 173 (Symplectic inner product)**.** *Given* $\vec{s}, \vec{t} \in \mathbb{F}_2^{2n}$ *with entries*

$$\vec{s} = (s_{1,1}, \ldots, s_{1,n}, s_{2,1}, \ldots, s_{2,n})$$
$$\vec{t} = (t_{1,1}, \ldots, t_{1,n}, t_{2,1}, \ldots, t_{2,n}) ,$$

their ***symplectic inner product****, which we will denote by* $[\vec{s}, \vec{t}]$*, is given by*

$$[\vec{s}, \vec{t}] = \sum_{j=1}^{n} (s_{1,j} t_{2,j} + s_{2,j} t_{1,j}) .$$

Our motivation for using this notation is the following elegant fact:

Lemma 174 (Commutation as symplectic orthogonality)**.** *For any* $\vec{s}, \vec{t} \in \mathbb{F}_2^{2n}$*,* $[\vec{s}, \vec{t}] = 0$ *(resp. 1) if and only if* $P_{\vec{s}}$ *and* $P_{\vec{t}}$ *commute (resp. anti-commute).*

Proof. It suffices to show this at the level of a single qubit. Let $s = (s_1, s_2)$ and $t = (t_1, t_2)$, so that $P_s = i^{s_1 s_2} X^{s_1} Z^{s_2}$ and $P_t = i^{t_1 t_2} X^{t_1} Z^{t_2}$. Then

$$P_s P_t - P_t P_s = i^{s_1 s_2 + t_1 t_2} (X^{s_1} Z^{s_2} X^{t_1} Z^{t_2} - X^{t_1} Z^{t_2} X^{s_1} Z^{s_2}) .$$

It can be verified that the first term in the parentheses is $(-1)^{s_2 t_1} \cdot X^{s_1 + t_1} Z^{s_2 + t_2}$, and likewise the second term is $(-1)^{s_1 t_2} \cdot X^{s_1 + t_1} Z^{s_2 + t_2}$. So the above expression is zero if and only $s_2 t_1 = s_1 t_2$. □

Definition 175. *A subspace* $T \subseteq \mathbb{F}_2^{2n}$ *is* ***isotropic*** *if* $[\vec{s}, \vec{t}] = 0$ *for all distinct* $\vec{s}, \vec{t} \in T$*.*

[1] However, be wary that despite the terminology, the unsigned stabilizer group is not necessarily a group – for example, consider the stabilizer group $\{II, XX, -YY, ZZ\}$, for which the corresponding unsigned stabilizer group $\{II, XX, YY, ZZ\}$ is not closed under multiplication.

Lemma 176. *For any (abelian) subgroup $G \subseteq \mathcal{P}_n$, the corresponding strings form an (isotropic) subspace of $\mathbb{F}_2^{2n}$. Conversely, any (isotropic) subspace of $\mathbb{F}_2^{2n}$ corresponds to an (abelian) subgroup $G \subseteq \mathcal{P}_n$.*

Proof. This equivalence follows immediately from Lemma 174 and the fact that $P_{\vec{s}}P_{\vec{t}}$ and $P_{\vec{s}\oplus\vec{t}}$ are equal to each other up to phase for any strings $\vec{s}, \vec{t}$. □

This symplectic structure will be especially useful in the next lecture. For now, the most important takeaway from the association between $\{I, X, Y, Z\}^{\otimes n}$ and $\mathbb{F}_2^{2n}$ is that it allows us to efficiently and classically perform manipulations of Pauli operators. This will allow us to flesh out the details in the proof sketch of the second part of Lemma 167.

Lemma 177. *Given a collection of vectors $\vec{s}^1, \ldots, \vec{s}^m \in \mathbb{F}_2^{2n}$ which are mutually orthogonal with respect to the symplectic inner product, there is an $O(n^3)$-time classical algorithm that outputs a minimal subset $S \subseteq [m]$ such that $\{P_{\vec{s}^j}\}_{j\in S}$ generates all of $\{P_{\vec{s}^j}\}_{j\in[m]}$. If $|S| = n$, the algorithm additionally outputs a classical description of a Clifford circuit $U \in \mathcal{C}_n$ for which the corresponding stabilizer state is $U|0^n\rangle$, and for which $UP_{\vec{s}^j}U^{-1} = Z_j$ for all j.*

The proof of this can be skipped upon first reading, as it essentially amounts to Gaussian elimination.

Proof. This amounts to finding a *basis* for the rows of the matrix

$$M = \left(\begin{array}{ccc|ccc} s^1_{1,1} & \cdots & s^1_{1,n} & s^1_{2,1} & \cdots & s^1_{2,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ s^m_{1,1} & \cdots & s^m_{1,n} & s^m_{2,1} & \cdots & s^m_{2,n} \end{array}\right).$$

We will refer to the submatrix on the left (resp. right) of the divider as the "X block" (resp. "Z block"). We can find a row basis for M via Gaussian elimination. More specifically, we can apply column operations to this matrix to place it in reduced column echelon form, with nonzero columns within the Z block. This is done by a combination of (1) swapping columns within the X block, (2) swapping a column in the X block with a corresponding column in the Z block, (3) adding columns in the X block to the corresponding columns in the Z block, and (4) adding the i-th column in both the X and Z blocks to the j-th column in both blocks respectively for various i, j. (1) corresponds to SWAPs which can be implemented with Clifford gates, (2) can be implemented with H gates, (3) can be implemented with phase gates, and (4) can be implemented with CNOT gates. Note that these column operations do not change the commutation relations among the Paulis associated to the rows.

The first part of the lemma then follows by selecting the rows of the resulting matrix corresponding to the identity block in reduced column echelon form. The second part of the lemma follows from the fact that if this block is $n \times n$, it occupies the entire Z block, and the X block is zero. Because the stabilizer state associated to this matrix is simply $|0^n\rangle$, the Clifford circuit U in the lemma statement can be read off from the sequence of gates that were used to implement the above column operations. □

The upshot is that in order to learn a classical description of a stabilizer state, it suffices to learn a classical description of its stabilizer group. This is what we will do in the rest of the lecture.