CMSC 657: Introduction to Quantum Information Processing
Lecture 19

Instructor: Daniel Gottesman

Fall 2024

1 Stabilizer Codes

1.1 Pauli Group

The Pauli group P_n consists of the tensor products of I, X, Y, and Z on n qubits, with overall phase ± 1, $\pm i$.

- It is a *group* — closed under multiplication.
- Any element of P_n squares to $\pm I$.
- Any two elements of P_n either commute or anticommute.

We will be using the Pauli group a lot in this lecture.

1.2 Stabilizer of the 9-Qubit Code

For the 9-qubit code, how do we measure the error syndrome? Within each set of three qubits, we must see if the first two and last qubits are the same or different in the standard basis. Putting that in a more quantum-mechanical way, we are trying to see if the state is the $+1$ or -1 eigenstate of $Z \otimes Z$ on those two qubits. Thus, we get 6 operators we are measuring the eigenvalues of. Similarly to tell if the phases are the same or different, we measure the eigenvalue of a tensor product of 6 X's. We get the following list, leaving a space for I:

$$
\begin{array}{cccccccccc}
Z & Z & & & & & & & & \\
 & Z & Z & & & & & & & \\
 & & & Z & Z & & & & & \\
 & & & & Z & Z & & & & \\
 & & & & & & Z & Z & & \\
 & & & & & & & Z & Z & \\
X & X & X & X & X & X & & & & \\
 & & & X & X & X & X & X & X &
\end{array}
$$

The valid codewords are $+1$ eigenstates of all 8 of these operators. States with 1 Pauli error on them are -1 eigenstates of one or more of these operators. Note that the choice of these 8 operators is not unique. We could, for instance, have chosen $Z \otimes I \otimes Z$ on the first three qubits instead of one of the first two operators. We don't need to list it in addition to them, however, because

$$Z \otimes I \otimes Z = (Z \otimes Z \otimes I)(I \otimes Z \otimes Z), \tag{1}$$

so the eigenvalue of $Z \otimes I \otimes Z$ can be easily determined from the other two eigenvalues.

1.3 Stabilizers

In general, we can define the *stabilizer* of a code. Let T be the subspace of Hilbert space defining the code. Then the stabilizer is

$$S(T) = \{M \in P_n |\, M|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T\}. \tag{2}$$

The stabilizer defined this way is always an Abelian group:

$$MN|\psi\rangle = M|\psi\rangle = |\psi\rangle, \tag{3}$$

and similarly $NM|\psi\rangle = |\psi\rangle$. Thus, $[M, N]|\psi\rangle = 0$. For Paulis, M and N either commute or anticommute. If they anticommute, then $[M, N]$ is proportional to another Pauli and has no 0 eigenvalues. Thus, $[M, N] = 0$.

The stabilizer is a much more convenient description of the code than the original subspace. For instance, it is only polynomial in size, needing $O(n^2)$ bits to describe the subspace, whereas describing even a single state expanded in the computational basis might need 2^n complex numbers. We frequently therefore go the other way, initially writing down a stabilizer and defining the code from that.

Definition 1. *Let S be an Abelian subgroup of the Pauli group with the property that $-I \notin S$. Then S is a stabilizer and define its code space as follows:*

$$T(S) = \{|\psi\rangle \,|\, M|\psi\rangle = |\psi\rangle \ \forall M \in S\}. \tag{4}$$

Theorem 1. *When a stabilizer S has r generators, it has 2^r elements. Let $k = n - r$. Then $\dim T(S) = 2^k$, so the code encodes k qubits.*

We can understand this theorem intuitively by noting that each element of the stabilizer imposes a constraint on the code space that divides the eligible Hilbert space in half.

Note that not all quantum error-correcting codes are stabilizer codes, but many of the most interesting ones are.

1.4 Stabilizers and Error Correction

As we saw in the example of the 9-qubit code, the stabilizer can serve as a useful guide as to how to measure the error syndrome. Notice that in that case, we used Z operators to identify X errors and X operators to identify Z errors. This generalizes — suppose that we have a state with error E on it, and suppose that $M \in S$ anticommutes with E. Then let us look at the eigenvalue of $E|\psi\rangle$ for M:

$$M(E|\psi\rangle) = -EM|\psi\rangle = -E|\psi\rangle. \tag{5}$$

Whereas $|\psi\rangle$ has eigenvalue $+1$ for M, $E|\psi\rangle$ has eigenvalue -1 when $\{E, M\} = 0$. The other possibility is that E and M commute:

$$M(E|\psi\rangle) = EM|\psi\rangle = +E|\psi\rangle. \tag{6}$$

Thus, the eigenvalue of M tells us whether the error E that occurred commutes with M or anticommutes with it.

Definition 2. *The error syndrome of a state originally from a stabilizer code is the list of eigenvalues of the generators of S. (Usually we instead put 0 for eigenvalue $+1$ and 1 for eigenvalue -1.) The error syndrome of a Pauli error E is a vector of bits indexed by generators of the stabilizer, with entry 0 if E commutes with the generator and 1 if it anticommutes. That is, it is the error syndrome of a codeword with error E. Let*

$$N(S) = \{N \in P_n |\, [M, N] = 0 \ \forall M \in S\} \tag{7}$$

Thus, $N(S)$ is the set of errors that have trivial error syndrome.

Note that $S \subseteq N(S)$ always since S is Abelian. $N(S)$ consists of operators that take codewords to codewords, since any state with trivial error syndrome is a codeword by the definition of $T(S)$.

Theorem 2. *$N(S) \setminus S$ is the set of errors that cannot be detected by the code S. All other errors can be detected.*

It is clear that an error outside $N(S)$ can be detected because it has non-trivial error syndrome. Why are the undetectable errors $N(S) \setminus S$ instead of $N(S)$? Well, if an error E is in S, then $E|\psi\rangle = |\psi\rangle$ for all codewords. Thus, it acts like the identity on codewords, so is not really an error. Thus, $N(S) \setminus S$ is the set of Paulis that map codewords to *different* codewords. Another way of thinking about them is they are the logical operators.

If we want to correct errors, not just detect them, we need to differentiate between different errors by their error syndromes.

Theorem 3. *S can correct the set $\mathcal{E}$ of errors iff $E^\dagger F \notin N(S) \setminus S \ \forall E, F \in \mathcal{E}$.*

Proof. E and F have the same syndrome iff $E^\dagger F$ has trivial syndrome iff $E^\dagger F \in N(S)$. Thus, if $E^\dagger F \notin N(S)$, we can distinguish the errors by their error syndrome.

$E^\dagger F \in S$ iff $E|\psi\rangle = F|\psi\rangle$ for all $|\psi\rangle \in T(S)$. Thus, if $E^\dagger F \in S$, E and F act the same way on codewords and don't need to be distinguished.

If $E^\dagger F \in N(S) \setminus S$, therefore, E and F cannot be distinguished by error syndrome and act differently on the codewords. In particular, they differ by a logical operator so our inability to distinguish them causes a fatal ambiguity for error correction. □

Definition 3. *The* distance *of a stabilizer code is the minimum weight of an element of $N(S) \setminus S$. A QECC is* degenerate *if S contains a non-trivial element of weight less than the distance; otherwise the code is* non-degenerate*. A code with n physical qubits, k logical qubits, and distance d is described as an $[[n, k, d]]$ code.*

In order to correct t general errors, we should have a code that has distance $d = 2t + 1$. (E and F both have weight up to t, so $E^\dagger F$ has weight at most $2t$. If there are no elements of weight $2t$ or less in $N(S) \setminus S$, we know that $E^\dagger F \notin N(S) \setminus S$.)

Because elements of $N(S)$ are operations that take codewords to codewords, they are *logical operations*, corresponding to transformations of the encoded qubits. When the errors do one of them, that is bad, but they are also useful to perform fault-tolerant gates on encoded qubits. Those that are in S just do the logical identity. You will show in the homework that two Paulis in $N(S)$ are the same logical operation if they are in the same coset of S in $N(S)$. It turns out that the group of cosets $N(S)/S$ is isomorphic to the Pauli group P_k on the k logical qubits.

1.5 Example Stabilizer Codes

Example 1 (Five-qubit code)**.** *This is a $[[5, 1, 3]]$ code.*

$$\begin{array}{ccccc} X & Z & Z & X & I \\ I & X & Z & Z & X \\ X & I & X & Z & Z \\ Z & X & I & X & Z \end{array}$$

The code is cyclic, but the fifth cyclic permutation is a product of these four generators. There are 5 qubits, so 15 one-qubit errors, plus the identity makes 16 possible errors. There are $16 = 2^4$ possible error syndromes, and all errors have different syndromes.

The logical Paulis in this case can be taken to be $\overline{X} = X \otimes X \otimes X \otimes X \otimes X$ and $\overline{Z} = Z \otimes Z \otimes Z \otimes Z \otimes Z$. $\overline{Y}$ is the product of these two.