6.443/8.371/18.436 Quantum Information Science II Lecture 5

Stabilizers

Aram Harrow February 20, 2018

In this lecture we discuss:

- Stabilizer subgroups and subspaces
- Example
- Projectors onto stabilizer subspaces
- $\mathbb{F}_2$ linear algebra perspective
- Logical operations and undetectable errors

5.1 Stabilizer subgroups and subspaces

Stabilizer codes are an important class of quantum codes whose construction is analogous to classical linear codes.

Let P_n be the real valued group of matrices $\pm\{I, X, iY, Z\}$ as the basis. Note that this is a group, because it is closed under multiplication and contains inverses. However, it is not commuting. $p \in P_n$ can be written as $(-1)^a X^b Z^c$, where $b = (b_1, \cdots, b_n)^T$, $c = (c_1, \cdots, c_n)^T$ and $X^b = X_1^{b_1} X_2^{b_2} \cdots X_n^{b_n}$. These Paulis are going to be the parity check.

Our code will be defined in terms of a "stabilizer group" $S \leq P_n$. The stabilizer subspace is $V_S = \{|\psi\rangle : g|\psi\rangle = |\psi\rangle, \forall g \in S\}$. In order that S stabilizes a non-trivial vector space, two conditions must be satisfied:

1. the elements of S commute (S is an abelian subgroup of P_n), and
2. $-I$ is not an element of S.

In general $\forall g, h \in P_n$, $gh = \pm hg$. For 2, obviously the only solution to $(-I)|\psi\rangle = |\psi\rangle$ is $|\psi\rangle = 0$. For 1, suppose that $g, h \in S$ and $\{g, h\} = 0$, then $gh + hg = 0$ leads to the result that $-I \in S$. This is because if $\{g, h\} = 0$ then $S \ni ghgh = -ghhg = -I$.

The basic idea of stabilizer formalism is that many quantum states can be more easily described by working with the operators that stabilize them than by working explicitly with the state itself.

5.2 Examples

1. $V_S = \text{span}\{|00\rangle\}$: $S = \{II, IZ, ZI, ZZ\} = \langle IZ, ZI\rangle$. $\langle IZ, ZI\rangle$ means that S is generated by IZ, ZI.
2. $V_S = \text{span}\{\frac{|00\rangle+|11\rangle}{\sqrt{2}}\}$: $S = \langle XX, ZZ\rangle$.
3. $V_S = \text{span}\{|001\rangle\}$: $S = \langle ZII, -IZI, -IIZ\rangle$.
4. $V_S = \text{span}\{|000\rangle, |111\rangle\}$ from the repetition code. Then $S = \langle ZZI, IZZ\rangle$.
5. $V_S = \text{span}\{|+++\rangle, |---\rangle\}$. Then $S = \langle XXI, IXX\rangle$.
6. V_S is the 9 qubit Shor code. Then $S = \langle Z_1Z_2, Z_2Z_3, Z_5Z_5, Z_5Z_6, Z_1Z_2, Z_6Z_8, Z_8Z_9, X_1 \ldots, X_6, X_4 \ldots X_9\rangle$.

5.3 Stabilizer subspace projectors

Let $\Pi_S := \text{Proj}(V_S)$ be the projector onto the subspace V_S. We claim that

Claim 1.

$$\Pi_S = \frac{1}{|S|}\sum_{g\in S} g$$

Proof. First observe that if $g \in S$ then

$$g\Pi_S = \Pi_S. \tag{5.1}$$

To see this we calculate

$$g\sum_{h\in S} h = \sum_{h\in S} gh = \sum_{h'=gh\in S} h'. \tag{5.2}$$

This uses the fact that g acts on S by permuting its elements. The same idea works for any group.

From (5.1) we have that $\Pi_S^\dagger \Pi_S = \Pi_S$ implying that Π_S is indeed a projector. Note that if $g \in S$ then $g^\dagger \in S$ and therefore $g^\dagger \Pi_S = \Pi_S$ and therefore $\Pi_S^\dagger \Pi_S = \Pi_S$. Hence the Π_S is a projector and has eigenvalues 0 or 1.

Next we show that $\text{Im}\,\Pi_S = V_S$. Indeed for any $|\psi\rangle$ and any $g \in S$ we have $g\Pi_S|\psi\rangle = \Pi_S|\psi\rangle$, implying that $\Pi_S|\psi\rangle \in V_S$. Hence $Im\Pi_S \subseteq V_S$. Next if $|\psi\rangle \in V_S$ then $\Pi_S|\psi\rangle = |\psi\rangle$ and therefore $V_S \subseteq \Pi_S$. This completes the proof. □

We can use this to calculate the dimension. Let $|S| = 2^\ell$ with generators $S = \langle s_1, \ldots, s_\ell\rangle$. Indeed

$$\dim V_S = \text{tr}\,\Pi_S = \frac{1}{|S|}\sum_{g\in S}\text{tr}\, g = \frac{1}{2^\ell}\sum_{g\in S} 2^n\delta_{g,I} = 2^{n-\ell}, \tag{5.3}$$

Note that

$$g \in S \iff g = s_1^{a_1}\ldots s_n^{a_n}, a_1, \ldots, a_n \in \{0,1\}^n$$

Therefore, we can write Π_S in another way, as

$$\Pi_S = \frac{1}{2^\ell}\sum_{a\in\mathbb{F}_2^\ell} s_1^{a_1}\cdots s_\ell^{a_\ell} = \prod_{i=1}^{\ell}\sum_{a_i=0,1}\frac{s^{a_i}}{2} = \prod_{i=1}^{\ell}\left(\frac{I+s_i}{2}\right). \tag{5.4}$$

For example, $\frac{I+Z}{2} = |0\rangle\langle 0|$ and $\frac{I-Z}{2} = |1\rangle\langle 1|$.

5.4 The $\mathbb{F}_2$-linear algebra perspective

If $p \in P_n$ then we can write $p = (-1)^a X^b Z^c$ for $a \in \mathbb{F}_2, b, c \in \mathbb{F}_2^n$. If $q = (-1)^{a'} X^{b'} Z^{c'}$ then

$$pq = (-1)^{a+a'} X^b Z^c X^{b'} Z^{c'}. \tag{5.5}$$

Let's look at the middle two terms

$$Z^c X^{b'} = Z_1^{c_1}\cdots Z_n^{c_n} X_1^{b'_1}\cdots X_n^{b'_n} = X^{b'} Z^c (-1)^{\langle b', c\rangle}. \tag{5.6}$$

Thus we have

$$pq = (-1)^{a+a'+\langle b', c\rangle} X^{b+b'} Z^{c+c'}. \tag{5.7}$$

This is as though we represent p, q by the vectors $\begin{pmatrix} a \\ b \\ c \end{pmatrix}, \begin{pmatrix} a' \\ b' \\ c' \end{pmatrix}$ which simply add when we multiply p, q except there is an extra phase of $\langle b', c\rangle$. If we choose the other ordering a similar calculation shows

$$qp = (-1)^{a+a'+\langle b, c'\rangle} X^{b+b'} Z^{c+c'}. \tag{5.8}$$

Putting this together we have

$$pq = (-1)^{\langle c,b'\rangle + \langle b,c'\rangle} qp. \tag{5.9}$$

This phase can be thought of as coming from the *symplectic inner product* between $\begin{pmatrix} b \\ c \end{pmatrix}$ and $\begin{pmatrix} b' \\ c' \end{pmatrix}$.

$$\langle c, b'\rangle + \langle b, c'\rangle = \begin{pmatrix} b^T & c^T \end{pmatrix} \begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix} \begin{pmatrix} b' \\ c' \end{pmatrix} = \begin{pmatrix} b^T & c^T \end{pmatrix} \Lambda \begin{pmatrix} b' \\ c' \end{pmatrix}, \tag{5.10}$$

where $\Lambda := \begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix}$. Finally we have a simple linear-algebraic way of describing when Pauli matrices commute or anticommute. p, q commute iff $\begin{pmatrix} b \\ c \end{pmatrix} \perp \begin{pmatrix} b' \\ c' \end{pmatrix}$. Here $\perp$ is with respect to the symplectic inner product defined by Λ.

We can use this linear algebra framework to talk about S as a subspace of $\mathbb{F}_2^{2n}$. if we neglect phases. Since the code properties don't depend on these phases, this can be a good way to investigate the properties of the code.

Let's return to undetected errors. If S is a stabilizer group, let $L(S)$ be the subspace of $\mathbb{F}_2^n$ corresponding to S. Then the above discussion implies that

$$L(N(S)) = L(S)^{\perp}. \tag{5.11}$$

5.5 Detecting errors and logical operators

Recall the classical check matrix H. We have that $x \in C_{cl} \iff Hx = 0$. Now if we add the bit flip error e we have that $x + e$ is undetectable if $H(x + e) = He = 0$. We have the same for the stabilizer codes. Therefore undetected errors are exactly the codes. For any two $A, B \in P_n$ we have $AB = \pm BA$; i.e. they either commute (+) or anti-commute (-). Suppose $|\psi\rangle \in V_S$ and $E \in P_n$. Then

$$E|\psi\rangle \in V_S \quad \Leftrightarrow \quad gE|\psi\rangle = E|\psi\rangle \ \forall g \in S. \tag{5.12}$$

Since g, E are both Paulis they either commute or anticommute. So if $gE|\psi\rangle = E|\psi\rangle$ for all $g \in S$ then E is an "undetected error". It leaves the state within V_S while possibly changing it. (Note that this includes the possibility that $E \in S$ and so E acts trivially. Also we call this an "error" although it might be been an intended change.) On the other hand if E anticommutes with some $g \in V_S$ then it is a "detected error" and it maps V_S to an orthogonal subspace. The set of undetected errors is also called the "normalizer" group of S and its denoted

$$N(S) = \{g : gh = hg \forall h \in S\}. \tag{5.13}$$

Note that since S is abelian we have $S \leq N(S)$; however in general $N(S)$ can be larger.