Introduction to quantum information processing

Stabilizer codes

Brad Lackey

15 November 2016

OUTLINE

LAST TIME...

- The Steane code as a CSS-code has generators:

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

and

$$G_2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

- G_2 is also the parity check matrix for G_1,
- so G_2 is used to compute the all the syndomes.

OUTLINE

The Pauli group

The Pauli group is defined to be:

$$\mathcal{P}_n = \{c\sigma_1 \otimes \cdots \otimes \sigma_n \ : \ \sigma_j \in \{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\},\ c \in \{\pm 1, \pm i\}\}.$$

From $\sigma_x\sigma_y = -i\sigma_z$ we have

Lemma

Two elements of $\mathcal{P}_n$ either commute or anticommute.

Definition

Let S be an Abelian subgroup of $\mathcal{P}_n \setminus \{-\mathbb{1}\}$. The *stabilizer code* of S is

$$C(S) = \{|\psi\rangle \ : \ M|\psi\rangle = |\psi\rangle \text{ for all } M \in S\}.$$

Basic idea: S is the set of syndrome operators for the code.

- $-\mathbb{1}$ does not have a $+1$ eigenvalues and so is not useful for syndromes.

CHECK ROWS

To any element $M = \alpha\sigma_1 \otimes \cdots \otimes \sigma_n$ we associate a row

$$(x_1 x_2 \cdots x_n | z_1 z_2 \cdots z_n) \in \mathbb{F}_2^n$$

where the x and z bits are computed as

$$x_j = \begin{cases} 1 & \text{if } \sigma_j = \sigma_x \text{ or } \sigma_y \\ 0 & \text{if } \sigma_j = \mathbb{1} \text{ or } \sigma_z \end{cases}$$

$$z_j = \begin{cases} 1 & \text{if } \sigma_j = \sigma_y \text{ or } \sigma_z \\ 0 & \text{if } \sigma_j = \mathbb{1} \text{ or } \sigma_x. \end{cases}$$

This is called the *check row* and denoted $c(M)$. The coefficient α is ignored!

Lemma

$c(M_1 M_2) = c(M_1) + c(M_2)$.

Consequently: generators of S correspond to (linear) bases of $c(S)$.

- We can use Gaussian elimination to find generating sets.

EXAMPLE: THE STEANE CODE

In the Steane code, both X-checks and Z-checks are computed by:

$$G_2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$S = \langle X_1X_3X_5X_7,\ X_2X_3X_6X_7,\ X_4X_5X_6X_7,\ Z_1Z_3Z_5Z_7,\ Z_2Z_3Z_6Z_7,\ Z_4Z_5Z_6Z_7 \rangle.$$

Here $\langle \cdot \rangle$ mean "generated by." In fact, S has 64 elements.

- The check rows of S are the rows of the matrix:

$$\left(\begin{array}{ccccccc|ccccccc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

The Normalizer

Definition

Let S be stabilizer group. Its *normalizer* is

$$N(S) = \{P \in \mathcal{P}_n \ : \ MP = PM \text{ for all } M \in S\}.$$

This is usually called the *centralizer*. But these are the same:

- The normalizer is usually $P \in \mathcal{P}_n$ such that $P^{-1}MP \in S$ for all $M \in S$.
- Since elements of $\mathcal{P}_n$ either commute or anticommute, we have

$$P^{-1}MP = \pm P^{-1}PM = \pm M.$$

- So if both $M, P^{-1}MP \in S$ then since $-M \notin S$ we must have $MP = PM$.

The normalizer plays two important roles for stabilizer codes:

- it defines *logical* Pauli operators on the code, and
- it characterizes uncorrectable Pauli errors.

OUTLINE

PAULI ERRORS

From Assignment 5, #3, we need only focus on correction Pauli errors, E.

- *Claim*: for $|\psi\rangle \in C(S)$, we have $E|\psi\rangle$ is eigenvector of any $M \in S$.
- *Proof*: $M(E|\psi\rangle) = \pm E(M|\psi\rangle) = \pm(E|\psi\rangle)$.
- *Recall*: the eigenvalue is the syndrome, so we get syndromes directly.

Let $\{M_\alpha\}_{\alpha=1}^{n-k}$ be a generating set for a stabilizer S.

- The *syndrome vector* of $E \in \mathcal{P}_n$ is $\vec{s}(E) = (s_\alpha(E)) \in \{\pm 1\}^{n-k}$,
- where it can be computed from $EM_\alpha = s_\alpha(E) \cdot M_\alpha E$.
- Syndromes satisfy: $s_\alpha(E_1 E_2) = s_\alpha(E_1) \cdot s_\alpha(E_2)$.
- The eigenprojection for a general vector $\vec{v} = (v_\alpha) \in \{\pm 1\}^{n-k}$ is

$$\Pi_{\vec{v}} = \frac{1}{2^{n-k}} \prod_{\alpha=1}^{n-k} (\mathbb{1} - v_\alpha M_\alpha).$$

The normalizer $N(S)$ is the set of Pauli operators with all $+1$ syndromes.

SYNDROME MEASUREMENTS

Lemma

We have $\{\Pi_{\vec{v}}\}_{\vec{v}\in\{\pm 1\}^{n-k}}$ *is a P.O.V.M.*

Proof: We have

$$\begin{aligned}\sum_{\vec{v}\in\{\pm 1\}^{n-k}} (\mathbb{1} + v_\alpha M_\alpha) &= \prod_{\alpha=1}^{n-k} \sum_{v_\alpha=\pm 1} (\mathbb{1} + v_\alpha M_\alpha) \\ &= \prod_{\alpha\in A} 2\cdot\mathbb{1} \;=\; 2^{n-k}\cdot\mathbb{1}.\end{aligned}$$

Therefore, $\sum_{\vec{v}\in\{\pm 1\}^{n-k}} \Pi_{\vec{v}\in\{\pm 1\}^{n-k}} = \frac{1}{2^{n-k}}\cdot 2^{n-k}\cdot\mathbb{1}$. □

For a general vector $\vec{v} = (v_\alpha) \in \{\pm 1\}^{n-k}$ define the syndrome space:

- $C_{\vec{v}} = \text{image}(\Pi_{\vec{v}})$. (Note: $C(S) = C_{(+1,\cdots,+1)}$.)

SYNDROME SPACES AND ERROR RECOVERY

Theorem

For a Pauli error E, we have $E : C(S) \to C_{\vec{s}(E)}$ unitarily.

Proof: We claim $E\Pi_{C(S)} = \Pi_{\vec{s}(E)}E$, which follows from:

$$\frac{1}{2^{n-k}} E \prod_{\alpha} (\mathbb{1} + M_\alpha) = \frac{1}{2^{n-k}} \left(\prod_{\alpha} (\mathbb{1} + s_\alpha(E) M_\alpha) \right) \cdot E.$$

Thus $E|\psi\rangle = \Pi_{s(E)} E|\psi\rangle$ for $|\psi\rangle \in C(S)$, and so $E|\psi\rangle \in C_{s(E)}$. □

Here's the error correction process:

1. Begin with $|\psi\rangle \in C(S)$. Error results in $E|\psi\rangle$.
2. Measure $\{\Pi_{\vec{v}}\}_{\vec{v} \in \{\pm 1\}^{n-k}}$.
3. The result is $\vec{v} = \vec{s}(E)$ with certainty as $E|\psi\rangle \in C_{\vec{s}(E)}$.
4. After measurement state is still $E|\psi\rangle$. Apply $E^\dagger$.

OUTLINE

STABILIZERS VERSUS NORMALIZERS

Let S be a stabilizer group. Recall:

- The normalizer is $N(S) = \{P \in \mathcal{P}_n \ : \ MP = PM \text{ for all } M \in S\}$.
- Since S is Abelian (all elements commute), $S \subseteq N(S)$.
- The syndrome of any $E \in N(S)$ is $(+1, \ldots, +1)$.

Therefore, any $E \in N(S)$ maps $E : C(S) \to C(S)$

What does this mean for error correction?

- If $E \in S$, then $E|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in C(S)$ (so no error).
- It turns out, if $E|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in C(S)$, then $E \in S$.
  - We won't prove this because we didn't developed the needed machinery:
  - one characterizes S and $N(S)$ using "augmented check matrices."

Consequently, if $E \in N(S) \setminus S$ then $E|\psi\rangle \neq |\psi\rangle$ for some $|\psi\rangle \in C(S)$.

- So if E is unintentional: this is an error.
- If E is intentional: we performed an quantum operation on our encoded data. More on this topic next time.

QUANTUM ERROR CORRECTION CONDITION

Theorem

Let S be a stabilizer group and $N(S)$ its normalizer. The stabilizer code $C(S)$ can correct Pauli errors $\{E_j\}_{j=1}^r$ if for each $j \neq k$ we have $E_j^\dagger E_k \notin N(S) \setminus S$.

Proof: If $E_j^\dagger E_k \in S$ then $\Pi_{C(S)} E_j^\dagger E_k \Pi_{C(S)} = \Pi_{C(S)}$. If $E_j^\dagger E_k \notin N(S)$ then it anticommutes with some generator M_α of S. So,

$$E_j^\dagger E_k \Pi_{C(S)} = \frac{1}{2^{n-k}} E_j^\dagger E_k \prod_\beta (\mathbb{1} + M_\beta) = \frac{1}{2^{n-k}} (\mathbb{1} - M_\alpha) E_j^\dagger E_k \prod_{\beta \neq \alpha} (\mathbb{1} + M_\beta).$$

But,

$$\Pi(\mathbb{1} - M_\alpha) = \frac{1}{2^{n-k}} \prod_{\beta \neq \alpha} (\mathbb{1} + M_\beta)(\mathbb{1} + M_\alpha)(\mathbb{1} - M_\alpha) = \mathbf{0}.$$

Thus, $\Pi_{C(S)} E_j^\dagger E_k \Pi_{C(S)} = \mathbf{0}$. From the QECC we can correct $\{E_j\}_{j=1}^r$. □

Distance

Corollary

If every element in $N(S) \setminus S$ involves at least d Pauli operators, then $C(S)$ can correct $t = \lfloor \frac{d-1}{2} \rfloor$ errors.

Proof: If any E_j has at most t Pauli operators, then ${E_j}^\dagger E_k$ has at most $2t \leq d$. Therefore, ${E_j}^\dagger E_k \notin N(S) \setminus S$. □

The d in this results is called the *distance* of the stabilizer code.

- This allows one to find how many errors a quantum code can correct.

However, if possible, it's easier to show each error has a unique syndrome:

- if $\vec{s}(E_j) \neq \vec{s}(E_k)$ then
- some α has $s_\alpha(E_j^\dagger E_k) = s_\alpha(E_j) \cdot s_\alpha(E_k) = -1$,
- hence $E_j^\dagger E_k \notin N(S)$.
- So the theorem shows we can correct $\{E_j\}$.

NEXT TIME...

- Fault-tolerate error-correction and quantum computation.