Stabilizer Formalism. (Source Nielsen & Chuang).

Note Title 5/29/2012

We will look at an important class of quantum error correcting codes called Stabilizer codes. These are analogous to classical linear codes. First we present the Stabilizer formalism. This formalism turns out to be useful in other contexts as well for understanding operations in quantum mechanics, but we will focus on its use in error correction.

Start with an example: $|4\rangle = \frac{1}{\sqrt{2}}(|100\rangle + |111\rangle)$

Notice that $X_1X_2|4\rangle = |4\rangle$ and $Z_1Z_2|4\rangle = |4\rangle$
We say that $|4\rangle$ is Stabilized by X_1X_2 & Z_1Z_2.

It turns out that $|4\rangle$ is the unique state which is stabilized by both X_1X_2 and Z_1Z_2.

We will use the set of stabilizers as a description for the space of states that are stabilized by the set. This sometimes gives a more compact description than the direct specification in the state space.

We will be mainly concerned with stabilizers which are subgroups of the Pauli group on n qubits, G_n.
For a single qubit this is:

$$G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Z, \pm iZ, \pm Y, \pm iY\}$$

G_n is the set of n-fold tensor products of Pauli matrices with multiplicative factors of ± 1 and $\pm i$.

Let S be a subgroup of G_n
Let V_S be the set of n-qubit states that are stabilized by all of S.
V_S is a vector space & S is the stabilizer for V_S.

Example: $S = \{\pm I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$

Z_1Z_2 stabilizes $|000\rangle, |111\rangle, |110\rangle, |001\rangle$ ← Subspace stabilized by Z_1Z_2 is spanned by this set.
Z_2Z_3 stabilizes $|000\rangle, |111\rangle, |100\rangle, |011\rangle$

V_S = subspace spanned by $\{|000\rangle, |111\rangle\}$

It is enough to consider just Z_1Z_2 and Z_1Z_3 because these two operations form a set of generators for S.
(Note $(Z_1Z_2)^2 = I$ and $(Z_1Z_2)(Z_2Z_3) = Z_1Z_3$)

⇒ A set of elements $g_1, \ldots, g_\ell$ of G generate group G if any element in G can be formed by a product of the g_i's.
$G = \langle g_1, \ldots, g_\ell \rangle$ ⇒ gives a compact representation of G.

We only need to check that a vector is stabilized by the generators of S to determine if the vector is in V_S.

When can a set $S \subseteq G_n$ be used to generate a stabilizer for a non-trivial V_S?

We need at least two conditions: → It turns out that these are sufficient conditions as well.
1. $-I \notin S$. $\quad -I|\psi\rangle = -|\psi\rangle = |\psi\rangle \Rightarrow |\psi\rangle = 0$
2. S is abelian

Note that any two elements $M, N \in G_n$ either commute or anti-commute. If M & N anti commute,

$$|\psi\rangle = MN|\psi\rangle = -NM|\psi\rangle = -|\psi\rangle \Rightarrow |\psi\rangle = 0.$$

(M & N anti-commute; N & M stabilize $|\psi\rangle$.)

Shor Code re-visited:

The two states that generate the code are:

$$|\bar{0}\rangle = \tfrac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$
$$|\bar{1}\rangle = \tfrac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

The stabilizer for this subspace has generators:

$M_1 = ZZI\ III\ III$
$M_2 = ZIZ\ III\ III$
$M_3 = III\ ZZI\ III$
$M_4 = III\ ZIZ\ III$
$M_5 = III\ III\ ZZI$
$M_6 = III\ III\ ZIZ$
$M_7 = XXX\ XXX\ III$
$M_8 = XXX\ III\ XXX$

We will eventually prove the following proposition.

Prop: Let $S = \langle g_1, \ldots, g_{n-k} \rangle$ be generated by $n-k$ independent and commuting elements of G_n such that $-I \notin S$. Then V_S is a 2^k-dimensional vector space.

The overall goal will be to start with a set of generators $\langle g_1, \ldots, g_{n-k} \rangle$ that satisfies the conditions of the proposition above and use the fact that V_S is a vector space of dim 2^k. We would like to use this as the codespace which will yield an $[n, k]$ code. We will use the stabilizer as a set of measurements to yield a syndrome which can then be used to detect and correct a set of errors. We will also need a means of encoding and decoding (i.e. operations that map an orthonormal basis of k-qubits to an orthonormal basis of V_S).

First we need a means of checking the conditions of the proposition:

1. S is commuting
2. $-I \notin S$
3. $g_1, \ldots, g_{n-k}$ are linearly independent.

First we introduce a useful representation of $\langle g_1, \ldots, g_e \rangle$

A check matrix is an $\ell \times 2n$ matrix

Row i corresponds to g_i.

Columns j + nj reflect the operator in g_i that operates on qubit j.

entry in col j	entry in col nj	operation on qubit j
0	0	I
1	0	X
0	1	Z
1	1	Y

If $g = IXZYX$ would correspond to row:

$r(g) = 0\,1\,0\,1\,1 \quad 0\,0\,1\,1\,0$

Note that the check matrix tells you everything about the generators of S, except the multiplicative factor $(\pm 1, \pm i)$ in front of each operator.

Also note that for two operators g, g': $r(g) + r(g') = r(gg')$

Now consider the matrix $\Lambda = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$ (I: $n \times n$ identity; 0: $n \times n$ 0's matrix.)

Let $r(g) + r(g')$ be the row representations of two operators g, g'. We have that

$$r(g)\,\Lambda\,r(g')^T = 0 \quad \text{iff} \quad g, g' \text{ commute.}$$

$$(r(g)_z, r(g)_x) \begin{pmatrix} r(g')_x \\ r(g')_z \end{pmatrix} = [r(g)_z \cdot r(g')_x] \oplus [r(g)_x \cdot r(g')_z]$$

So if the check matrix is C, we need to check that $C \Lambda C^T$ is all 0's.

Note that it is sufficient to check that the set of generators commute to ensure that all of S is commuting.

Now for conditions ② + ③ we will show that these are equivalent to the following 3 (checkable) conditions:

Ⓐ The rows of C are linearly independent.

Ⓑ $(g_i)^2 = I \quad \forall \; i \in \{1, \ldots, \ell\}$.

→ Note we can't have an all 0's row: $g_i \neq \pm I, \pm iI$.

We will show that for commuting $S = \langle g_1, \ldots, g_e \rangle$

(A), (B) $\iff$ (2) (3) $\rightarrow$ $g_1 \ldots g_e$ are independent.

$\hookrightarrow -I \notin S$

Proof $\Rightarrow$ assume (A) (B)

Suppose $g_1, \ldots, g_e$ are linearly dependent:

$$\prod_{i \neq k} (g_i)^{a_i} = g_k.$$

Since $(g_i)^2 = I$, we can assume that the exponents a_i are 0 or 1. Multiplying both sides by g_k gives:

$$g_k \prod_{i \neq k} (g_i)^{a_i} = (g_k)^2 = I.$$

$$r(g_k) + \sum_{i \neq k} a_i \, r(g_i) = 0.$$

Contradicts (1): rows of C are linearly independent.

Similarly, we can't have

$$\prod_{i} (g_i)^{a_i} = -I$$

Since this would also imply $\sum_i a_i \, r(g_i) = 0$.

Now the $\Leftarrow$ direction.

Since $g_i \in G_n$ $\quad (g_i)^2 = \pm I$ or $\pm iI$.

if $\pm iI \in S$ then $(\pm iI)^2 = -I \in S$, so $(g_i)^2 = I \quad \forall i$.

Now suppose: $\sum a_i \, r(g_i) = 0$

then $\prod_i (g_i)^{a_i} = \pm I$ or $\pm iI$ $\rightarrow$ must by I because $-I \notin S$.

$\prod_i (g_i)^{a_i} = I$ pick k s.t. $a_k = 1$

multiply each side by g_k.

$\prod_{i \neq k} (g_i)^{a_i} = g_k$ → this means we can remove g_k from $\langle g_1, \ldots, g_\ell \rangle$ and generate the same set. //

Thus, we have a mechanism to check the conditions of the above Proposition. Now we need to prove the proposition itself. We will start with the following lemma.

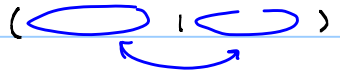
Lemma: Let $S = \langle g_1, \ldots, g_\ell \rangle$ be generated by ℓ independent generators and satisfies $-I \notin S$. Fix $j \in \{1, \ldots, \ell\}$ then $\exists\, g \in G_n$ such that

$$g g_j g^+ = -g_j$$
$$g g_k g^+ = g_k \text{ for all } k \neq j.$$

Pf of Lemma: Since the rows of C are lin indep., for each e_i (length ℓ vector – all 0's except for a 1 in location i),

$\exists\, x_i$ s.t. $C x_i = e_i$.

Let x_i' by x_i with the 1st n and 2nd n bits reversed:



We have that $\Lambda (x_i')^T = x_i^T$

So $C \Lambda (x_i')^T = e_i$.

Let h_i be the operator corresponding to x_i $(r(h_i) = x_i)$

We have that for $j \neq i$

$$g_j h_i = h_i g_j \Rightarrow g_j h_i g_j^\dagger = h_i$$
$$g_i h_i = -h_i g_i \qquad g_i h_i g_i^\dagger = -h_i.$$

operators either commute or anti-commute

Now for the proof of the proposition:

Let $S = \langle g_1, \ldots, g_{n-k} \rangle$ $-I \notin S$ g_i's are lin. indep. & commuting.

Let x be a vector of length $n-k$ $x = (x_1, x_2, \ldots, x_{n-k}) \in \mathbb{Z}_2^{n-k}$

$$P_S^x \equiv \frac{\prod_{j=1}^{n-k} (I + (-1)^{x_j} g_j)}{2^{n-k}}$$

$\frac{(I+g_i)}{2}$ projects onto the $+1$ eigenspace of g_i

P_i^+ ← projector to $+1$ eigenspace of g_i

P_i^- ← projector to -1 eigenspace of g_i

$$g_i = P_i^+ - P_i^-$$
$$(\underbrace{P_i^+ + P_i^-}_{I} + \underbrace{P_i^+ - P_i^-}_{g_i}) / 2 = P^+ \qquad (\text{and } \tfrac{I-g_i}{2} = P^-)$$

$P_S^{|0\ldots0\rangle}$ is the projector onto V_S.

By the lemma above $\forall x$ $\exists g_x \in G_n$ s.t.

$$g_x P_S^0 (g_x)^\dagger = P_S^x \qquad \left(g_x = \prod_{i: \text{ bit of } x \text{ is } 1} h_i\right)$$

Conjugation by h_i will convert g_i to $-g_i$. and leave everything else unchanged.

This tells us that P_S^x projects onto a space that has the same dimension as V_S.

If $|\phi_1\rangle \cdots |\phi_r\rangle$ is a basis of V_S then

$g_x|\phi_1\rangle \ldots g_x|\phi_r\rangle$ is a basis of the space onto which P_s^x projects (+ g_x^{-1} takes a basis for this space back to V_s).

If $x \neq x'$ then $P_s^x + P_s^{x'}$ project on to orthogonal subspaces. Suppose $x_k = 0$ + $x'_k = 1$. Since the g_i's commute

$P_s^x = P_k^+ (P_1^{+/-} \ldots P_\ell^{+/-})$ $P_s^{x'} = P_k^- (P_1^{+/-} \ldots P_\ell^{+/-})$ → the last projection projects onto orthogonal spaces.

(no k term) (no k term)

Finally: $$I = \sum_x P_s^x = \prod_{i=1}^{n-k} (P_i^+ + P_i^-)$$

I projects onto the entire 2^n-dimensional Hilbert space for n qubits. Each P_s^x projects onto a subspace that has the same dimension as V_s. There are 2^{n-k} P_s^x and they project onto mutually orthogonal subspaces.
⇒ dimension of V_s must be 2^k.