* Pauli gates.

$ZX = iY$, X, Y, Z are pairwise 'anti-commute'.

e.g. $XY = -YX$.

* Pauli group : $G(n)$ is a set of n-qubit unitaries that are generated from $\{i, X, Y, Z\}$ by tensor product and composition.

e.g. $G(1) = \{\pm I, \pm iI, \pm X, \pm iX, \pm Z, \pm iZ, \pm iY, \pm Y\}$. (So $|G(n)| = 4^{n+1}$)

$G(2) = \{ aP_1 \otimes P_2 \mid a \in \{\pm 1, \pm i\}, P_1, P_2 \in G(1)\}$.

side note: G is a group if G is a set that is equiped with $e \in G$, $* : G \times G \to G$.

$inv : G \to G$ s.t.

$$e * g = g, \forall g \in G$$

$$inv(g) * g = g * inv(g) = e, \forall g \in G,$$

$$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3).$$

We write $S \trianglelefteq G$ iff S is a subgroup of G.

* Stabilizer states and stabilizers.

Let $S \trianglelefteq G(n)$. the stabilizer states of S, denoted by V_S, is the set

$$V_S = \{ \phi \mid \phi \in Q^n \ \forall P \in S,\ P(\phi) = \phi \}.$$

Q^n ← complex vector space of dim 2^n.

Thm: V_S is a vector space.

e.g. if $a, b \in V_S$, $a+b \in V_S$. ($P(a+b) = P(a)+P(b) = a+b$)

$\forall c \in \mathbb{C}$, $a \in V_S$, $ca \in V_S$. etc. $P(ca) = cP(a)$

S is call "stabilizer" of V_S.

* Example: ① $S = \{ I, ZZI, IZZ, ZIZ \}$. $= \langle ZZI, IZZ \rangle$.

We write ZZI for $Z \otimes Z \otimes I$.

$$V_{ZZI} = \langle |000\rangle, |001\rangle, |110\rangle, |111\rangle \rangle$$

$\langle \ \rangle$ ← vector space 'spanned' by ...

$$V_{IZZ} = \langle |000\rangle, |011\rangle, |100\rangle, |111\rangle \rangle$$

So $V_S = V_{ZZI} \cap V_{IZZ} = \langle |000\rangle, |111\rangle \rangle$.

② $S = \langle XX, ZZ \rangle$

$V_{XX} = \langle |+\rangle|+\rangle, |-\rangle|-\rangle \rangle$

$V_{ZZ} = \langle |00\rangle, |11\rangle \rangle$

$V_S = V_{XX} \cap V_{ZZ} = \langle \frac{|00\rangle + |11\rangle}{\sqrt{2}} \rangle = \frac{|++\rangle + |--\rangle}{\sqrt{2}}$

* we write

$S = \langle P_1, \cdots P_l \rangle$

to mean S is generated from $P_1 \cdots P_l \in G(n)$

and P_i, P_j are independent.

We assume P_i P_j comutes

and $P_i \neq -I$ $\forall i$.

Thm: Let $S = \langle P_1, \cdots P_l \rangle$ satisfying the assumption. Then we have

$\dim(V_S) = 2^{n-l}$

* Modeling Clifford Computation.

rather than working with state explicitly, we work with the stabilizer instead.

so $\langle Z \rangle$ instead of $|0\rangle$.

$\langle ZI, IZ \rangle$ instead of $|00\rangle$.

then: Applying a Clifford gate $\{H, S, CNOT\}$ on to a state can be described as 'group action', i.e. conjugation.

e.g.

$$\begin{array}{ccc} \langle Z \rangle & \xmapsto{H} & \langle HZH \rangle = \langle X \rangle \\ \text{Stablizes} \Big\} & & \text{Stablizes} \Big\} \\ |0\rangle & \xmapsto{H} & |+\rangle \end{array}$$

e.g.

$$\begin{array}{ccc} \langle ZI, IZ \rangle & \xmapsto{H \otimes I} & \langle XI, IZ \rangle \\ \Big\} & & \Big\} \\ |00\rangle & \longmapsto & |+\rangle|0\rangle \end{array}$$

This is because $\forall g \in S,\ \phi \in V_S,$

$$(U|\phi\rangle) = Ug|\phi\rangle = \underline{UgU^\dagger}(U|\phi\rangle)$$

So if g stabilizes $|\phi\rangle$,

$UgU^\dagger$ stabizes $U|\phi\rangle$.

* Side note. this is an example of a group G 'acting' on a set X.

$$e \bullet x = x$$
$$g_1 \bullet (g_2 \bullet x) = (g_1 * g_2) \bullet x.$$

So for $g \in S$,

$$U \bullet g = UgU^\dagger.$$

* Since $g \in G(n)$, it would be nice if $UgU^\dagger \in G(n)$. Unfortunately, this is not true in general. Only the so-call "Clifford gates" have this property.

*Some useful identities.

$H \bullet X = Z$ | $S \bullet X = Y$ | $CX \bullet (X \otimes I) = X \otimes X$

$H \bullet Z = X$ | $S \bullet Z = Z$ | $CX \bullet (I \otimes X) = I \otimes X$

$(S \bullet X = SXS^\dagger)$ | $CX \bullet (Z \otimes I) = Z \otimes I$

$CX \bullet (I \otimes Z) = Z \otimes Z$

Thm: Let $C = \langle H, S, CX \rangle$.

$\forall D \in C$, $P \in G(n)$, we have $D \bullet P \in G(n)$

Thm: More surprisingly, for any group K,

if $\forall D \in K$, $P \in G(n)$, $D \bullet P \in G(n)$,

then $K = \langle H, S, CX \rangle$.

* Measurement

Projective measurement.

Let M be hermitian.

If $M = \sum_i m_i P_i$, where $M(P_i(\phi)) = m_i P_i(\phi)$

$P_i P_j = 0$ if $i \neq j$. (m is an eigenvalue of M)

then

"measure ϕ in M-basis," means

applying one of the P_i to ϕ.

the probability of getting the result

m_i is $p(m_i) = \langle \phi | P_i | \phi \rangle$.

The average value of the measurement is:

$$E(M) = \sum_i p(m_i) \cdot m_i$$

$$= \sum_i \langle \phi | P_i | \phi \rangle \cdot m_i$$

$$= \langle \phi | \sum_i m_i P_i | \phi \rangle$$

$$= \langle \phi | M | \phi \rangle.$$

* So when people say "measure of $g \in G(a)$".
they mean g is hermitian and they do
projective measurement of g.

* Fun fact.

① if $g \in G(n)$ is a product of Paulis without -1 or $\pm i$. then g has only 2 eigenvalues, they are ± 1.

and. $g = \left(\frac{I+g}{2}\right) - \left(\frac{I-g}{2}\right)$

$$g\left(\frac{I+g}{2}|\varphi\rangle\right) = \frac{I+g}{2}|\varphi\rangle$$

$$g\left(\frac{I-g}{2}|\varphi\rangle\right) = -\frac{I-g}{2}|\varphi\rangle$$

Note that $\left(\frac{I+g}{2}\right)\cdot\left(\frac{I-g}{2}\right)$

$$= \frac{I-g+g-g\cdot g}{4} = \frac{I-g+g-I}{4} = 0.$$

so. $\frac{I+g}{2}$ and $\frac{I-g}{2}$ are orthogonal.

* If the stabilizer S of $|\varphi\rangle$'s $\langle g_1, \cdots g_n \rangle$, and g is hermitian, then measure on g basis will result in the following two cases.

① Suppose g commute with $g_1 \cdots g_n$.

In this case either g or $-g \in S$

because $\forall |\varphi\rangle \in V_s = \langle |\varphi\rangle \rangle$

$$g_i(g|\varphi\rangle) = (g_i g)|\varphi\rangle = (g g_i)|\varphi\rangle$$

$$= g(g_i|\varphi\rangle) = g|\varphi\rangle \quad \forall g_i$$

So $g|\varphi\rangle \in V_s$.

$$\Rightarrow \quad g|\varphi\rangle = a|\varphi\rangle \quad a \in \mathbb{C}.$$

$$|\varphi\rangle = gg|\varphi\rangle = g(a|\varphi\rangle) = a\,g|\varphi\rangle = a^2|\varphi\rangle$$

$$\Rightarrow a^2 = 1 \quad \Rightarrow \quad a = \pm 1.$$

So either g or $-g \in S$.

If $g \in S$, i.e. $g|\varphi\rangle = |\varphi\rangle$.

then $\frac{I+g}{2}|\varphi\rangle = |\varphi\rangle$.

$$\frac{I-g}{2}|\varphi\rangle = 0.$$

so g-measurement always return $+1$ result. and the state $|\varphi\rangle$ is unchanged after the measurement!

If $-g \in S$. i.e. $g|\varphi\rangle = -|\varphi\rangle$.

then $\frac{I+g}{2}|\varphi\rangle = 0$

$$\frac{I-g}{2}|\varphi\rangle = |\varphi\rangle.$$

so g-measurement alway return -1 and $|\varphi\rangle$ is unchanged.

② if g anti-commutes with g_1. Note that if g also anti-commutes with g_2, we can set

$$S = \langle g_1, g_1 g_2, g_3, \cdots g_k \rangle = \langle g_1, g_2, \cdots g_k \rangle$$

and $g_1 g_2$ commutes with g

So Without loss of generality, we can assume g only anti-commutes with g_1.

$$p(+1) = \langle \varphi | \frac{I+g}{2} | \varphi \rangle$$

$$= \frac{1 + \langle \varphi | g | \varphi \rangle}{2}$$

$$p(-1) = \langle \varphi | \frac{1-g}{2} | \varphi \rangle = \frac{1 - \langle \varphi | g | \varphi \rangle}{2}$$

$$\langle \varphi | g | \varphi \rangle = \langle \varphi | g g_1 | \varphi \rangle$$

$$= -(\langle \varphi | g_1) g | \varphi \rangle$$

$(g_1 = g_1^\dagger)$

$$= -\langle \varphi | g | \varphi \rangle$$

$$\Rightarrow \langle \varphi | g | \varphi \rangle = 0.$$

So with $\frac{1}{2}$, we get $+1$

and the resulting state $\frac{I+g}{2}|\varphi\rangle$

$$\forall i \neq 1 \quad g_i\left(\frac{I+g}{2}\right)|\varphi\rangle = \frac{g_i + g_i g}{2}|\varphi\rangle$$

$$= \frac{g_i + g g_i}{2}|\varphi\rangle$$

$$= \frac{I+g}{2} g_i |\varphi\rangle$$

$$= \frac{I+g}{2}|\varphi\rangle$$

and $g\left(\frac{I+g}{2}|\varphi\rangle\right) = \frac{I+g}{2}|\varphi\rangle$.

So $\frac{I+g}{2}|\varphi\rangle$ is stabilised by

$$\langle g, g_2, \cdots g_k\rangle.$$

Similarly, with $\frac{1}{2}$, the resulting state is stabilised by $\langle -g, g_2, \cdots g_k\rangle$.