Clifford circuits, magic, and mana:

Discussion closely follows:

[1] D. Gottesman, "The Heisenberg representation of quantum computers," arXiv: quant-ph/9807006v1 (1998);

[2] C. D. White, C.-J. Cao, and B. Swingle, "Conformal field theories are magical," PRB 103, 075145 (2021).

Outline:

1. Heisenberg representation; Clifford group; stabilisers.
2. Error-correcting codes; measurements.
3. Magic and mana.
4. Case study: $\mathbb{Z}_3$ Potts model.

1. a) Heisenberg representation and Pauli group.

Schrödinger: $|\psi\rangle \to U|\psi\rangle$

$$\therefore N|\psi\rangle \to UN|\psi\rangle = \underbrace{UNU^\dagger}_{\equiv \tilde{N}} U|\psi\rangle$$

$\Rightarrow$ Heisenberg: $N \to UNU^\dagger$.

Linear, so restrict N to a spanning basis:

B

$$N \in P \equiv \underbrace{\{\overbrace{\alpha O_1 O_2 \dots O_n}^{\text{outer product (one operator per qubit)}}\}}_{\text{"Pauli group"}}, \quad \text{where } \alpha \in \{1, -1, i, -i\}, \quad O_j \in \{I, X, Y, Z\}.$$

"Pauli group": elements are (phased) Pauli strings.

Multiplicative, i.e. $\widetilde{(MN)} = \tilde{M}\tilde{N}$, so only need a generating set, e.g. $\{X_1, X_2, \dots, X_n, Z_1, Z_2, \dots, Z_n\}$.

b) Clifford group: set of operators that map P to itself. $C \subset U(2^n)$. It includes:

i) Single-qubit Hadamard gate: $R|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$R|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

ii) Phase gate: $P|0\rangle = |0\rangle$, $P|1\rangle = i|1\rangle$.

iii) CNOT gate: $\text{CNOT}|0\sigma\rangle = |0\sigma\rangle$
$\text{CNOT}|1\sigma\rangle = |1\bar{\sigma}\rangle$.

These gates generate the Clifford group.

Induced transformations on the Pauli matrices:

$$RXR^\dagger = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
$$= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z.$$

One derives similarly (exercise) that:

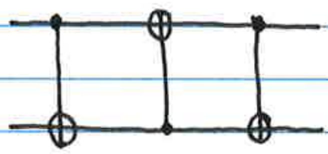
R: $X \to Z$, $Z \to X$.

P: $X \to Y$, $Z \to Z$.

CNOT: $XI \to XX$ $\quad ZI \to ZI$

$IX \to IX$ $\quad IZ \to ZZ$.

Example: what does this circuit do?



Consider its action on XI:

$$XI \to XX = (XI)(IX)$$
$$\to (XI)(XX) = IX$$
$$\to IX.$$

Can show similarly that:

$IX \to XI$, $ZI \to IZ$, $IZ \to ZI$,

i.e. the circuit swaps the two qubits.

c) Stabilisers. Specify to a subset of inputs, $|\psi\rangle$ (e.g. fix first qubit to $|0\rangle$). Stabiliser S defined by:

$$S = \{ M \in P \text{ s.t. } M|\psi\rangle = |\psi\rangle \text{ for all allowed } |\psi\rangle \}.$$

Always Abelian; proof:

D

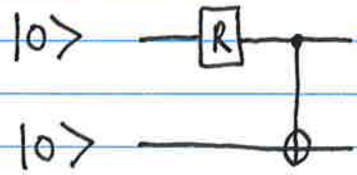
If $M, N \in S$ then: $MN|\psi\rangle = M|\psi\rangle = |\psi\rangle$

$$NM|\psi\rangle = N|\psi\rangle = |\psi\rangle$$

$$\therefore [M,N]|\psi\rangle = 0.$$

But since any two elements of P either commute or anticommute, $[M,N] = 0$.

Example:



Stabiliser of input state includes IZ and ZI.

$$IZ \to IZ \to ZZ$$

$$ZI \to XI \to XX.$$

So stabiliser of final state is $\{XX, ZZ, \underbrace{II, -YY}_{\text{generated from } XX,\, ZZ.}\}$

The only state stabilised by this is

$$|\psi\rangle = \left(\sum_{M\in S} M\right)|00\rangle = 2|00\rangle + 2|11\rangle,$$

a Bell state. It is a <u>stabiliser state</u>: one that can be completely described by specifying its stabiliser.

Another important two-qubit stabiliser state is the singlet; its stabiliser is $\{II, -XX, -YY, -ZZ\}$, so the state is:

$$|\psi\rangle = \left(\sum_{M\in S} M\right)|10\rangle = 2|10\rangle - 2|01\rangle.$$

Note that we can't use $|00\rangle$ as the input here. (Exercise: why not?)

2. a) Error-correcting codes.

i) Error detection.

Suppose I have a string of qubits, 1 to M, and I wish to detect whether one has been altered. Take each pair, e.g. 1 & 2, and add two auxiliary qubits, 1' and 2'. To this set of four, apply the stabiliser generated by $\{XXXX, ZZZZ\}$. These anticommute with any single-qubit Pauli (or at least one of them does); thus any single-qubit error flips the sign of the stabiliser eigenvalues (or at least one of them). This stabiliser code is an analogue of parity checking in classical computing.

F

ii) Error correction.

α) 3 physical qubits; corrects X errors.

Stabiliser: $\{ZZI, IZZ\} \equiv \{g_1, g_2\}$.

Start with a state where g_1, g_2 both have eigenvalues $+1$ (the 'codespace').

XII flips g_1; IXI flips both; IIX flips g_2.

So if we measure g_1 and g_2:

Result	Action
1, 1	No action needed.
-1, 1	Apply XII.
1, -1	Apply IIX.
-1, -1	Apply IXI.

Actual actions on the logical qubit are performed by $\{XXX, ZZZ\}$, which commute with the stabiliser but are not generated by it.

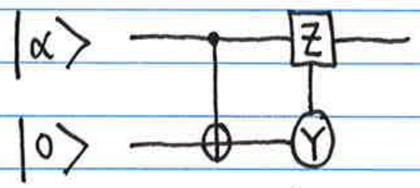
β) 5 physical qubits; corrects all single-qubit errors: stabiliser $\{XZZXI, IXZZX, XIXZZ, ZXIXZ\}$. Key properties:

single-qubit Pauli, e.g. IIIXI or IZIII

G

- $\forall P, \exists g \in S$ s.t. $\{P, g\} = 0$.
- Pattern of stabiliser flips uniquely identifies error, e.g. IIIXI gives $+--+$. (Exercise: why does this imply that S must have at least four entries?)
- Some non-trivial operators still exist that commute with all members of S, here {XXXXX, ZZZZZ}: these are the logical qubit operators.

b) Measurements. Basic idea: describe states / subspaces using stabilisers. Example: show that the following circuit implements a phase gate ($|0\rangle \to |0\rangle$, $|1\rangle \to i|1\rangle$).



Initially: stabiliser IZ; flip XI; meas. ZI.

After CNOT (see rule): stabiliser ZZ; flip XX; meas. ZI.

After Y-measurement: stabiliser IY; flip −YI; meas. ZI.

<u>or</u> stabiliser −IY; flip YI; meas. ZI.

H

The two outcomes are related by ZZ, the stabiliser before the measurement was made; hence we act ZZ if the measurement result is 'down'. That gives: stabiliser IY; flip $-YI$; measure ZI. This now does $X \to -Y$ and $Z \to Z$, which is $P^\dagger$ (see rules).

General rules: To evolve operators after a measurement of A:

1. Identify $M \in S$ satisfying $\{M, A\} = 0$.
2. Remove M from the stabiliser.
3. Add A to the stabiliser.
4. For all other $g \in S$, and for $\bar{X}$ and $\bar{Z}$ (the 'flip' and 'measure' operators), left-multiply by M if they anticommute with A.

For this example, $A = IY$, so $M = ZZ$.
$\bar{X}$ was XX; this anticommutes with A, so $\bar{X} \to -YY$.
$\bar{Z}$ was ZI; this commutes with A, so is left alone.