A quantum system is a finite-dimensional complex inner-product space.

An n-qubit quantum computer is a quantum system with underlying space $\mathbb{C}^{2^n}$

Humans can interact with quantum computers/systems in 2 ways:

- We can give the computer instructions in the form of gates, or equiv. with unitary maps

  operators

- We can ask the computer a question about its state.

  this is called a measurement

Def: A linear operator on a vector space $V$ is a linear map $L: V \to V$

We showed that unitary operators on $\mathbb{C}^n$ form a group under composition $U(n)$

We also showed that

$$U(1) = \{ \lambda \in \mathbb{C} \mid |\lambda| = 1 \}$$
$$= \{ e^{i\theta} \mid \theta \in [0, 2\pi) \}$$
$$= S^1$$
$$= \mathbb{R} / 2\pi \mathbb{Z}$$

Def: We say that a linear operator $\Pi : V \to V$ is a projection operator if $\Pi$ is idempotent ($\Pi^2 = \Pi$)

Def: If $V = W \oplus W'$ is a direct sum decomposition, then we say that $W'$ is a complement of $W$

Problem - subspaces have infinitely many complements

Def: If $W \subseteq V$ is a subspace, the orthogonal complement of $W$ is

$$W^\perp = \{ |v\rangle \in V \mid \langle w | v \rangle = 0 \ \forall w \in W \}.$$

pronounced "W perp"

Def: We say that two subspaces $V_1, V_2 \subseteq V$ are orthogonal if

$$\langle V_1, V_2 \rangle \doteq \left\{ \langle v_1 | v_2 \rangle \;\middle|\; \begin{matrix} |v_1\rangle \in V_1 \\ |v_2\rangle \in V_2 \end{matrix} \right\}$$

$$= \{0\}.$$

We write $V_1 \perp V_2$

Def: If $\{V_i\}_{i \in I}$ is a collection of subspaces st

- $\sum_{i \in I} V_i = V$
- $\forall i \neq j, \quad V_i \perp V_j$

then we say $V = \bigoplus_{i \in I} V_i$ is an orthogonal decomposition

Exercise: why is this a direct sum decomposition?

Want $V_i \cap \sum_{j \in I \setminus \{i\}} V_j = 0$

is contained in $V_i^{\perp}$

Remark: Given an orthogonal decomposition

$$V = \bigoplus_{i \in I} V_i$$

if we have an orthonormal basis for each subspace $V_i$, then the union of all these bases (for all $i$) will be an orthonormal basis for $V$

## Ket-Bra notation

Idea: Linear operators can be written using bra-ket notation

So far: vectors $v \in V$ give kets $|v\rangle$ (or bras)

functionals $f: V \to \mathbb{C}$ give bras $\langle f|$

We can extend this to $L: V \to V$

**Example:** Let $V = \mathbb{C}^2$.

Consider the object $|e_2\rangle\langle e_1|$

Consider how it acts on a vector

$$a|e_1\rangle + b|e_2\rangle \in \mathbb{C}^2$$

$$|e_2\rangle\langle e_1| \left(a|e_1\rangle + b|e_2\rangle\right)$$

$$= \left(|e_2\rangle\langle e_1| a|e_1\rangle\right) + \left(|e_2\rangle\langle e_1| b|e_2\rangle\right)$$

$$= a|e_2\rangle\underbrace{\langle e_1|e_1\rangle}_{1} + b|e_2\rangle\cancel{\langle e_1|e_2\rangle}^{0}$$

$$= a|e_2\rangle$$

So $|e_2\rangle\langle e_1|$ is the linear operator on $\mathbb{C}^2$ which maps

$$a|e_1\rangle + b|e_2\rangle \mapsto a|e_2\rangle$$

Thus, ket-bras are operators on $V$.

Example:

$$|e_2\rangle\langle e_1| + |e_1\rangle\langle e_2|$$

is the linear operator such that

$$e_1 \mapsto e_2$$

$$e_2 \mapsto e_1$$

Example:

$$|v\rangle\langle e_1|$$

sends

$$e_1 \mapsto v$$

$$e_2 \mapsto 0$$

The set of linear operators on $V$ form a vector space, denoted

$$\mathrm{End}(V)$$

endomorphisms

If $V = \mathbb{C}^n$, then

$$\mathrm{End}(V) \cong \mathbb{C}^{n \times n}$$

$n \times n$ matrices

**Thm:** The following set is a basis for $\mathrm{End}(\mathbb{C}^n)$:

$$\{ |e_j\rangle\langle e_i| \mid 1 \leq i,j \leq n \}$$

The ket-bra $|e_j\rangle\langle e_i|$ is the operator sending

$$|e_k\rangle \mapsto 0 \text{ if } k \neq i$$

$$|e_i\rangle \mapsto |e_j\rangle$$

Solution to last problem:

If $L$ is a linear operator, then

$$L = \sum_{i=1}^{n} |L(e_i)\rangle\langle e_i|$$

Back to quantum!!

Def: A (pure) state of a quantum system is a one-dimensional subspace of the underlying vector space $V$.

(I'll usually denote this with an $\ell$, for line)

Def: A state vector of a state $\ell$

is a nonzero vector $|\psi\rangle$ in $\mathcal{C}$.

We say that $|\psi\rangle$ is normalized if $\langle\psi|\psi\rangle = 1$.

A quantum computer has, at any point in time, a "current state" (which is a state)

There are 2 interactions a human can have with a quantum computer.

- Given a unitary operator $U$ on $V$, we can
  Apply $U$ to the current state

- Given a subspace $W \subseteq V$, we can ask:

Is the current state contained in $W$?

The results of these operations:

- If we apply a unitary $\mathcal{U}$ to a system with current state $\ell$, then the current state becomes $\mathcal{U}\ell$

- If we ask whether the current state $\ell$ is contained in a subspace $W \subseteq V$, then there are two options, from which the system will choose randomly.

  Pick a statevector $|\psi\rangle$ for $\ell$

  Let $\Pi$ be the orthogonal projection onto $W$

  - With probability equal to
$$\frac{\langle \Pi\psi | \Pi\psi \rangle}{\langle \psi | \psi \rangle},$$

the computer will output yes
and then change the current
state to span$\{\Pi|\psi\rangle\}$

- With probability equal to

$$\frac{\langle \Pi^{\perp} \psi | \Pi^{\perp} \psi \rangle}{\langle \psi | \psi \rangle},$$

the computer will output no
and then change the current
state to span$\{\Pi^{\perp}|\psi\rangle\}$

These probabilities are computed
by Born's rule