CS419/CS939: Quantum computing

Seminar 1

- Admin stuff
- Linear algebra review
  - Vector spaces
  - Basis and dimension
  - Linear transforms and matrices
  - Inner products, norms and unitaries (maybe)
- Classical computation in ket notation

Vector space: Set V associated to a field ($\mathbb{R}$ or $\mathbb{C}$, or...)
Satisfies $\alpha|v\rangle + |w\rangle \in V$ for all $\alpha \in \mathbb{R}$, $|v\rangle, |w\rangle \in V$.

↑ Linear combination

Examples: $\mathbb{R}$, $\mathbb{C}$
$\mathbb{R}^n$, $\mathbb{C}^n$
$\mathcal{F} = \{f : \mathbb{R} \to \mathbb{R}\}$

Bra-ket notation: Column vector $|v\rangle = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$, row vector $\langle w| = \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}$. "Dagger" is conjugate transpose:
$|v\rangle^\dagger = [v_1^* \; v_2^* \; \cdots \; v_n^*]$.

Basis: Minimal set B of vectors s.t. any $|v\rangle \in V$ can be obtained by their linear combination, i.e., $\text{span}(B) = V$.

(Linearly independent)

Examples: $\{1\}$ is a basis for $\mathbb{R}$, $\left\{\begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}1\\-1\end{bmatrix}\right\}$ is a basis for $\mathbb{R}^2$

$\left\{\begin{bmatrix}1\\0\end{bmatrix}\right\}$ and $\left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1\\1\end{bmatrix}\right\}$ are <u>not</u> bases for $\mathbb{R}^2$

Canonical basis of $\mathbb{R}^n$ (or $\mathbb{C}^n$):

$$e_0 = \begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}, \quad e_1 = \begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix}, \quad \ldots \quad e_n = \begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix}$$

Exercise: Prove that $\text{span}(S)$ is a vector space for any $S \subseteq V$ and that $\text{span}(V) = V$.

Writing a vector in another basis: $T = \{|t\rangle, |t'\rangle, |t''\rangle\}$

$$|t\rangle = \begin{bmatrix}1\\1\\1\end{bmatrix}, \quad |t'\rangle = \begin{bmatrix}1\\0\\1\end{bmatrix}, \quad |t''\rangle = \begin{bmatrix}2\\0\\0\end{bmatrix}$$

$$|v\rangle = \begin{bmatrix}5\\3\\-1\end{bmatrix} = 5|0\rangle + 3|1\rangle + |2\rangle = ?|t\rangle + ?|t'\rangle + ?|t''\rangle$$

Dimension: Size of a(ny) basis of V.

A subspace is a set $W \subseteq V$ that is itself a vector space

Examples: $\dim(\mathbb{R}^n) = n$

$\dim(\mathbb{R}^{2^n}) = 2^n$

$\dim(\mathbb{C}) = ?$

$\dim(\mathcal{F}) = ?$

Exercise: Suppose $|B| = \dim V$. Then,
(useful!)

B is LI $\Rightarrow \text{span}(B) = V$,

and, conversely,

$\text{span}(B) = V \Rightarrow B$ is LI.

Linear transformation: Function $f: V \to W$ that satisfies

$$f(\alpha|v\rangle + \beta|w\rangle) = \alpha f(|v\rangle) + \beta f(|w\rangle)$$

Examples: $g(x) = 2x$ is linear, while

$h(x) = 2x+1$ is not.

Matrices $\leftrightarrow$ Linear transformations

Proof: Take $f: \mathbb{R}^3 \to \mathbb{R}^3$ given by $f\left(\begin{bmatrix} v_0 \\ v_1 \\ v_2 \end{bmatrix}\right) = \begin{bmatrix} v_0 + v_1 + 3v_2 \\ v_1 - 4v_2 \\ v_0 + 6v_1 \end{bmatrix}$.

Linearity means

$$f(v_0|0\rangle + v_1|1\rangle + v_2|2\rangle) = v_0 f(|0\rangle) + v_1 f(|1\rangle) + v_2 f(|2\rangle),$$

so we just need to calculate f on the basis.

$$f(|0\rangle) = \begin{bmatrix} ? \\ ? \\ ? \end{bmatrix} \quad f(|1\rangle) = \begin{bmatrix} ? \\ ? \\ ? \end{bmatrix} \quad f(|2\rangle) = \begin{bmatrix} ? \\ ? \\ ? \end{bmatrix}.$$

Then, with $A_f = \begin{bmatrix} | & | & | \\ f(|0\rangle) & f(|1\rangle) & f(|2\rangle) \\ | & | & | \end{bmatrix} = \begin{bmatrix} & & \\ & & \\ & & \end{bmatrix}$,

$f(|v\rangle) = \qquad\qquad = A_f \cdot |v\rangle$

Exercise: We showed LTs $\Rightarrow$ Matrices. Show that Matrices $\Rightarrow$ LTs.

Change of basis: Suppose we know $|v\rangle = x|s\rangle + y|s'\rangle + z|s''\rangle$ for some basis $S = \{|s\rangle, |s'\rangle, |s''\rangle\}$. If we're given another basis $T = \{|t\rangle, |t'\rangle, |t''\rangle\}$, how to find $\alpha, \beta, \gamma \in \mathbb{R}$ s.t. $|v\rangle = \alpha|t\rangle + \beta|t'\rangle + \gamma|t''\rangle$?

In other words, we want $f_{ST}: \mathbb{R}^3 \to \mathbb{R}^3$ taking $\begin{bmatrix} x \\ y \\ z \end{bmatrix} \mapsto \begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix}$.

Luckily, f_{ST} is linear! (Ex: prove it)

Example: $S = \{|0\rangle, |1\rangle, |2\rangle\}$, $T = \{|t\rangle, |t'\rangle, |t''\rangle\}$

$$\left(|t\rangle = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \quad |t'\rangle = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad |t''\rangle = \begin{bmatrix} 2 \\ 0 \\ 0 \end{bmatrix} \right)$$

$$f_{ST}(x|0\rangle + y|1\rangle + z|2\rangle)$$

$$= x f_{ST}(|0\rangle) + y f_{ST}(|1\rangle) + z f_{ST}(|2\rangle).$$

$$A_{ST} = ?$$

Inner product: Some vector spaces come with something extra — a way to "compare" vectors.

$$\langle v|w\rangle := \langle v| \cdot |w\rangle = \text{scalar}$$

(row vector · column vector)

Example: With $|v\rangle = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$, $|w\rangle = \begin{bmatrix} 0 \\ 2 \end{bmatrix}$, then $\langle v|w\rangle = -2$

$|v\rangle = \begin{bmatrix} i \\ 1 \end{bmatrix}$ $|w\rangle = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$, then $\langle v|w\rangle = ?$

Norm: Inner products give us a way of "measuring distance":

$$\||v\rangle\| := \sqrt{\langle v|v\rangle}$$

Exercise: Prove that $\langle v|v\rangle \geq 0$ and that $\langle v|v\rangle = 0 \Leftrightarrow |v\rangle = 0$.

If you're inclined, show $\||v\rangle + |w\rangle\| \leq \||v\rangle\| + \||w\rangle\|$ too.

If $\langle v|w\rangle = 0$, the vectors are orthogonal. If $\||v\rangle\| = 1$, then $|v\rangle$ is a unit vector.

A basis is orthonormal if it is composed of pairwise orthogonal unit vectors.

Exercise: Verify that $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, with

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

are orthonormal bases.

Unitary matrices: Linear transformations that preserve distance, i.e., $\|U|v\rangle\| = \||v\rangle\|$ (over $\mathbb{C}$).

Theorem 4. *Any of the following four conditions on a matrix U are equivalent:*

1. *U preserves distances, that is, $\|U|v\rangle\| = \||v\rangle\|$ for all $|v\rangle \in V$.*
2. *$U^\dagger = U^{-1}$, so $U^\dagger U = I$, the identity matrix*[23].
3. *The columns of U form an orthonormal basis.*
4. *U preserves inner products, that is, $\langle u|A^\dagger A|v\rangle = \langle u|v\rangle$ for all $|u\rangle, |v\rangle \in V$.*