Lecture notes on Quantum Computing

Chapter 1 Mathematical Background

Basic notation: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

§1.1 Vector spaces

- $\mathbb{C}^n$ is the set of complex $n \times 1$ column vectors.
- $\mathbb{C}^n$ is a vector space under scalar multiplication and addition.
- We use the Dirac notation, bra-vector $\langle x|$ and ket-vector $|x\rangle$.

$$\mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : \ x_i \in \mathbb{R} \right\}$$

$$\mathbb{C}^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : \ x_i \in \mathbb{C} \right\}.$$

Terminology zero vector, (additive) inverse of a vector, complex and real vector spaces.

Example: $|u\rangle = \begin{bmatrix} 1+i \\ 1-i \end{bmatrix} \in \mathbb{C}^2$ $\quad |v\rangle = \begin{bmatrix} 3+4i \\ -5-i \end{bmatrix} \in \mathbb{C}^2$

rangle ↑ $\langle | \rangle$ ↓ ket

bra

$$|u\rangle + |v\rangle = \begin{bmatrix} 1+i+3+4i \\ 1-i-5-i \end{bmatrix} = \begin{bmatrix} 4+5i \\ -4-2i \end{bmatrix}$$

$\alpha = 2i$ $\quad \alpha|u\rangle = 2i \begin{bmatrix} 1+i \\ 1-i \end{bmatrix} = \begin{bmatrix} 2i(1+i) \\ 2i(1-i) \end{bmatrix} = \begin{bmatrix} 2i-2 \\ 2i+2 \end{bmatrix} = \begin{bmatrix} -2+2i \\ 2+2i \end{bmatrix}$

$\beta = (1+i)$ $\quad \beta|v\rangle = \begin{bmatrix} (1+i)(3+4i) \\ (1+i)(-5-i) \end{bmatrix} = \begin{bmatrix} (3-4)+3i+4i \\ (-5+1)+i(-5-1) \end{bmatrix} = \begin{bmatrix} -1+7i \\ -4-6i \end{bmatrix}$

Let $|0\rangle = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ be the zero vector in $\mathbb{C}^2$. Then $|u\rangle + |0\rangle = |u\rangle$.

For $|u\rangle = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} \in \mathbb{C}^2$, we can take $-|u\rangle = \begin{bmatrix} -u_1 \\ -u_2 \end{bmatrix}$ so that

$$|u\rangle + (-|u\rangle) = |0\rangle$$

$|u\rangle + |v\rangle$ $\qquad |v\rangle \equiv -|u\rangle$

§1.2 Linear independent vectors and basis.

- A set of vectors $\{|u_1\rangle, \ldots, |u_m\rangle\} \subseteq \mathbb{C}^n$ is linearly dependent if there are $a_1, \ldots, a_m \in \mathbb{C}$ not all zero such that $a_1|u_1\rangle + \cdots + a_m|u_m\rangle = |0\rangle$. Else, the set is linear independent. (How to check?)
- A set of vectors A set of vectors $\{|u_1\rangle, \ldots, |u_m\rangle\} \subseteq \mathbb{C}^n$ is generating if for every $|v\rangle \in \mathbb{C}^n$ there are $a_1, \ldots, a_m \in \mathbb{C}$ not all zero such that $|v\rangle = a_1|u_1\rangle + \cdots + a_m|u_m\rangle$. (How to check?)
- A linearly independent generating set for $\mathbb{C}^n$ is a basis. The number of vectors in it must be n, known as the dimension of $\mathbb{C}^n$.

Idea: one vector "depends" on the other. $|0\rangle = |u_1\rangle - a_2|u_2\rangle \cdots - a_m|u_m\rangle$

e.g. $|u_1\rangle = a_2|u_2\rangle + \cdots + a_m|u_m\rangle$ →

$|u_2\rangle = b_1|u_1\rangle + \cancel{b_2|u_2\rangle + \cdots + b_m} + b_3|u_3\rangle + \cdots + b_m|u_m\rangle$.

$|0\rangle = b_1|u_1\rangle - |u_2\rangle + b_3|u_3\rangle + \cdots + b_m|u_m\rangle$

Example: $|u\rangle = \begin{bmatrix} 1+i \\ 1-i \end{bmatrix}$, $|v\rangle = \begin{bmatrix} 3+4i \\ -5-i \end{bmatrix} \in \mathbb{C}^2$

Check: $\exists$? (not both zero) $a_1, a_2 \in \mathbb{C}$ s.t.

$a_1|u\rangle$ $\quad a_1|u_1\rangle + a_2|u_2\rangle = |0\rangle$.

$$\begin{bmatrix} 1+i & 3+4i \\ 1-i & -5-i \end{bmatrix}\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} a_1(1+i) + a_2(3+4i) \\ a_1(1-i) + a_2(-5-i) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\left[\begin{array}{cc|c} 1+i & 3+4i & 0 \\ 1-i & -5-i & 0 \end{array}\right] \to \left[\begin{array}{cc|c} 1+i & 3+4i & 0 \\ 1 & \frac{-5-i}{1-i} & 0 \end{array}\right]$$

$$\to \left[\begin{array}{cc|c} 1 & \frac{3+4i}{1+i} & 0 \\ 1 & \frac{-5-i}{1-i} & 0 \end{array}\right] \to \left[\begin{array}{cc|c} 1 & \frac{7+i}{2} & 0 \\ 1 & \frac{-4+6i}{2} & 0 \end{array}\right]$$

$$\to \left[\begin{array}{cc|c} 1 & \frac{7+i}{2} & 0 \\ 0 & \frac{1}{2}[-11-7i] & 0 \end{array}\right] \quad \therefore \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

$\therefore \{|u\rangle, |v\rangle\}$ is lin. indep.

In General.

Solve:

$$\begin{bmatrix} |u_1\rangle & \cdots & |u_m\rangle \end{bmatrix}\begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

If there is non-trivial solution $\begin{bmatrix} a_1 \\ \vdots \\ a_m \end{bmatrix}$ then $\{|u_1\rangle \cdots |u_m\rangle\}$ is lin dep.

Else, lin independent

Generating set: $|e_1\rangle$ $|e_2\rangle$

In $\mathbb{C}^2$, $\left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right\}$ is a generating set.

for example, $|u\rangle = \begin{bmatrix}1+i\\1-i\end{bmatrix} = (1+i)\begin{bmatrix}1\\0\end{bmatrix} + (1-i)\begin{bmatrix}0\\1\end{bmatrix}$.

Exaple: $\left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}, \begin{bmatrix}1+i\\1-i\end{bmatrix}\right\}$ is also generating

---

Exaple: $\left\{\begin{bmatrix}1\\1\end{bmatrix}, \begin{bmatrix}i\\-i\end{bmatrix}\right\}$ is a generating set.

Check: For any $\begin{bmatrix}b_1\\b_2\end{bmatrix} \in \mathbb{C}^2$, consider

$$\begin{bmatrix}1 & i\\1 & -i\end{bmatrix}\begin{bmatrix}a_1\\a_2\end{bmatrix} = \begin{bmatrix}b_1\\b_2\end{bmatrix}$$

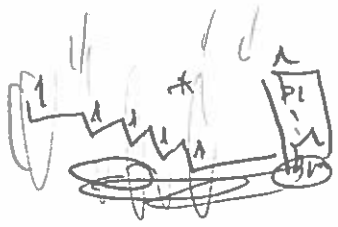
$$\left[\begin{array}{cc|c}1 & i & b_1\\1 & -i & b_2\end{array}\right] \to \left[\begin{array}{cc|c}1 & i & b_1\\0 & -2i & b_2-b_1\end{array}\right]$$

$\therefore$ $a_2 = \dfrac{b_2-b_1}{-2i}$, $a_1 = b_1 - ia_2 = b_1 - i\left(\dfrac{b_2-b_1}{-2i}\right)$

$= b_1 + \left(\dfrac{b_2-b_1}{2}\right)$.

In general: Reduce

$$n\left\{\overbrace{\left[\begin{array}{c|c}A & \begin{matrix}b_1\\\vdots\\b_n\end{matrix}\end{array}\right]}^{m} \to\right.$$



Side-track: In quantum mechanics $\left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right.$ may represent $|\uparrow\rangle$ $|\rightarrow\rangle$ polarization of photon

$\left\{\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\right\}$ is another measuring basis for photon

§1.3 Linear functions and dual vector spaces.

- A function $f : \mathbb{C}^n \to \mathbb{C}$ is a linear functional if $f(|u\rangle + |v\rangle) = f(|u\rangle) + f(|v\rangle)$ and $f(a|u\rangle) = af(|u\rangle)$ for all $a \in \mathbb{C}, |u\rangle, |v\rangle \in \mathbb{C}^n$.
- The set of functional on $\mathbb{C}^n$ form a vector space $\mathbb{C}^{n*}$, known as the dual space of $\mathbb{C}^n$.
- Each linear functional can be defined by $f(|u\rangle) = \langle v|u\rangle$ for some $|v\rangle \in \mathbb{C}^n$. Thus, $\mathbb{C}^{n*}$ can be viewed as the space of complex row vectors.

$f : \mathbb{C}^n \to \mathbb{C}$

$g : \mathbb{C}^n \to \mathbb{C}$

$h = f + g : \mathbb{C}^n \to \mathbb{C}$

$h(|u\rangle) = f(|u\rangle) + g(|u\rangle) \in \mathbb{C}$.

$\alpha \in \mathbb{C}$, $\alpha f : \mathbb{C}^n \to \mathbb{C}$, $(\alpha f)(|u\rangle) = \alpha f(|u\rangle) \in \mathbb{C}$

Suppose $f : \mathbb{C}^n \to \mathbb{C}$ is a linear functional

Then there $\langle v| = (\bar{v}_1, \cdots, \bar{v}_n)$ with $|v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$

$= (v_1^*, \cdots, v_n^*)$

s.t. $f(|u\rangle) = \bar{v}_1 u_1 + \cdots + \bar{v}_n u_n = \langle v|u\rangle$

$= \langle v|\,|u\rangle = \langle v|u\rangle$

$(\bar{v}_1 \cdots \bar{v}_n) \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$

Example. On $\mathbb{C}^2$, let

$f(|u\rangle) = (1+i)u_1 + (1-i)u_2$.

Then f is a linear function

$f(|u\rangle) = (1+\bar{i}, 1-\bar{i}) \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$

$= \langle v|u\rangle$ $\quad |v\rangle = \begin{pmatrix} 1-i \\ 1+\bar{i} \end{pmatrix}$