Universality

1. 我们称一组 gates 是"功能完备的 (universal)"，若可以通过其生成任意的计算。

e.g. 在布尔代数中，NAND 可以生成所有逻辑门.

但是在 Quantum Operations 中，这是不严格存在的！

一个 Quantum Gate $U \in SU(2)$，其无法由任何有限集的整数个元素生成！

但我们可以考虑，在一定精度下，近似地用有限 gate set 实现 universality.

2. State distance

① Fidelity 保真度

对于两 qubit $|\psi\rangle$，$|\phi\rangle$，我们定义：

$$F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|^2$$ 为其"保真度 (Fidelity)"

不难联想到 Born's rule，$F = P(|\phi\rangle)$ i.e. 测量 $|\psi\rangle = |\phi\rangle$ 的概率

② Bures Distance

global phase (全局相位)

$$d(|\psi\rangle, |\phi\rangle) = \min_r \| |\psi\rangle - e^{ir}|\phi\rangle \|$$

$$= \min_r \sqrt{(\langle\psi| - e^{-ir}\langle\phi|)(|\psi\rangle - e^{ir}|\phi\rangle)}$$

$$= \min_r \sqrt{\langle\psi|\psi\rangle + \langle\phi|\phi\rangle - e^{ir}\langle\psi|\phi\rangle - e^{-ir}\langle\phi|\psi\rangle}$$

$$= \min_r \sqrt{2 - e^{ir}\langle\psi|\phi\rangle - \overline{e^{ir}\langle\psi|\phi\rangle}}$$

$$= \min_r \sqrt{2 - Re(e^{ir}\langle\psi|\phi\rangle)}$$

$$= \sqrt{2(1-\sqrt{F})}$$

对于 e^{ir} 的解释：由于对一个量子态乘一个全局相位，在物理上是等价的，故我们讨论"相似程度"时，带上全局相位.

3. gate distance

Distance:

$$d(U,V) = \max_{|\psi\rangle} d\left(V|\psi\rangle, U|\psi\rangle\right) = \max_{|\psi\rangle}\min_{r} \left\|\left(V - e^{ir}U\right)|\psi\rangle\right\|$$

我们称 $d(U,V)$ 是最大的"由 U,V 制约的量子态距离"

我们称 U 与 U' 是 ε-close 的，若：

$$d(U',U) \leq \varepsilon$$

4. Universal Gate Set

我们的目的：找到一个有限的 gate set，使得通过有限个其中元素，可以以任意精度逼近任意量子门。

4.1 我们先考虑单qubit情况。

注意到，在 Bloch Sphere 上，任意量子门都等价于一个旋转，我们有：

$$U = R_{\vec{n}}(\varphi) = R_x(\varphi_x) R_y(\varphi_y) R_z(\varphi_z) = e^{\frac{i}{2}(n_x X + n_y Y + n_z Z)\varphi}$$

H 与 T，可组成一个符合要求的 gate set：$\{H, T\}$

绕轴 $(\hat{x}+\hat{z})$ 转 π　　绕z轴转 $\frac{\pi}{4}$

Proof:

※重要事实1：对任意两不平行向量 $\vec{v_1}, \vec{v_2}$，任何旋转可由绕 $\vec{v_1}, \vec{v_2}$ 的旋转的组合以任意精度有限步内逼近

推论：任何旋转都可以通过有限的如下操作得到：

$$R_z(\gamma) R_y(\beta) R_z(\alpha)$$　(α,β,γ) 也被称作"欧拉角"

这个将 $U \to (\alpha,\beta,\gamma)$ 的过程也被称作"Z-Y-Z 欧拉角参数化"

※重要事实2：对于一个非 π 有理数倍的旋转角，其倍数可以逼近任意旋转角。

我们令：$\Big\{ U = THTH \Rightarrow$ 绕 $\left(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8}\right)$ 旋转 $2\arccos\left(\cos^2\frac{\pi}{8}\right)$

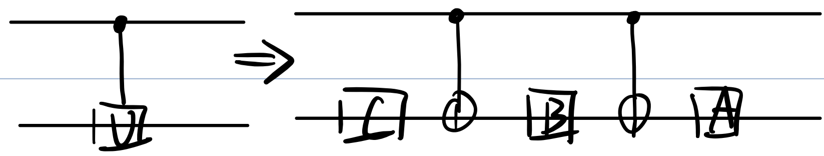
$V = HTHT \Rightarrow$ 绕 $(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$ 旋转 $2\arccos((\cos\frac{\pi}{8})^2)$

USV 的组合显然满足题意.

综上所述，我们不难证明 $\{H, T\}$ 是 Universality Set for 1-qubit
↳并非

4.2. 考虑二比特情况.

我们希望构建 $C(U)$，Lec 我们提到如下装置:



也即:
$$\begin{cases} e^{i\gamma}AXBXC = U & \rightarrow \text{control bit} = |0\rangle \\ ABC = I & \rightarrow \text{control bit} = |1\rangle \end{cases}$$

若 $U \longrightarrow (\alpha, \beta, \gamma)$, $= e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)$

我们只需:
$$\begin{cases} A = R_z(\beta)R_y(\frac{\gamma}{2}) \\ B = R_y(-\frac{\gamma}{2})R_z(-\frac{\delta+\beta}{2}) \\ C = R_z(\frac{\delta-\beta}{2}) \end{cases}$$

此时
$$\begin{cases} ABC = R_z(\beta)R_y(\frac{\gamma}{2})R_y(-\frac{\gamma}{2})R_z(-\frac{\delta+\beta}{2})R_z(\frac{\delta-\beta}{2}) = I \\ e^{i\alpha}AXBXC = \end{cases}$$

$X R_y(\theta) X = R_y(-\theta)$

$$e^{i\alpha}R_z(\beta)R_y(\frac{\gamma}{2})\left(-iR_x(\pi)R_y(-\frac{\gamma}{2})R_z(-\frac{\delta+\beta}{2})-iR_x(\pi)\right)R_z(\frac{\delta-\beta}{2})$$
$$= e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)$$

因此，任意 2-qubit 控制门可以被分解成 2 个 CNOT 门与 3 个单比特门.

而对任意 - 2-qubit gate，有如下算法:

Vatan & Williams: 任意 2-qubit gate 可被分解为 3CNOT + 单比特门.

5. 量子算法复杂度

5.1 Solovay-Kitaev Algorithm

对于任意 gate U，以精度 ε 实现 U 的量子门个数不少于：

$$\sim \left(\log\left(\frac{1}{\varepsilon}\right)\right)^{3.97}$$

理论上最优的下限不低于：$\log\left(\frac{1}{\varepsilon}\right)$

4. 为什么 $\log(1/\epsilon)$ 是极限?

- 想象你要存储一个实数（如 π）到精度 ϵ。
- 需要的比特数是 $\log_2(1/\epsilon)$。
- 在量子编程中，"程序"就像一段编码，告诉硬件如何实现一个门。
- 如果你想区分 $\sim 1/\epsilon^d$ 个不同的门（体积估计），你需要至少 $\log(1/\epsilon)$ 的程序长度。

这与李群的维度有关：$\mathrm{SU}(2)$ 是 3 维，所以覆盖它需要 $\sim (1/\epsilon)^3$ 个球，每个球对应一个程序，程序长度 $L \sim \log(1/\epsilon)$。

但是不存在完美编程 (perfect programming), s.t. $\varepsilon = 0$