作业1：证明量子门组合的完备性

定理1：n量子比特的一般逻辑门的矩阵表示构成一个$U(2^n)$群，它的维数是$(2^n)^2=4^n$.

证：为了证明该定理成立，我们先讨论$U(N)$群的维数，这是由于一般的量子门是幺正矩阵. 由于$U(N)$群是李群，考虑无穷小参数生成的群元$U(\vec{\theta})$，$\vec{\theta}$是无穷小量

$$U(\vec{\theta}) = \exp(i\theta^\alpha A_\alpha) \approx 1+i\theta^\alpha A_\alpha$$

幺正群满足：$U^\dagger(\vec{\theta})U(\vec{\theta})=1$. 故

$$U^\dagger(\vec{\theta})U(\vec{\theta}) \approx (I-i\theta^\alpha A_\alpha^\dagger)(I+i\theta^\beta A_\beta) \approx I+i\theta^\alpha A_\alpha - i\theta^\alpha A_\alpha^\dagger = I.$$

从上式得知：

$$i\theta^\alpha A_\alpha - i\theta^\alpha A_\alpha^\dagger = 0 \quad \Rightarrow \quad A_\alpha^\dagger = A_\alpha$$

故$U(N)$群的李代数A_α是厄米的$N\times N$复矩阵. 其一共由$N+\frac{N^2-N}{2}\times 2 = N^2$个实数决定. 故$U(N)$群的维数是$N^2$. 那么，对于$n$个量子比特的一般逻辑门，它是一个$2^n\times 2^n$幺正矩阵，构成$U(2^n)$群，根据上述结论，其维数为$(2^n)^2=2^{2n}=4^n$.

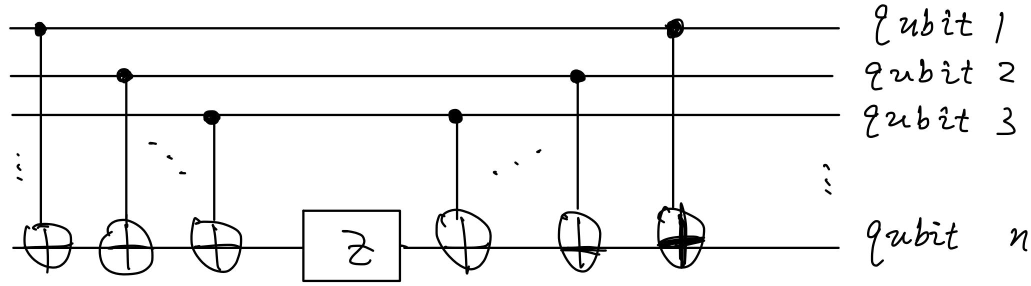
定理2：记$\sigma^\mu=(I,\sigma^1,\sigma^2,\sigma^3)$，那么$\{\sigma_1^{\mu_1}\otimes\sigma_2^{\mu_2}\otimes\cdots\otimes\sigma_n^{\mu_n}\}$可以成为$U(2^n)$李代数的一组基.

证：由于$I,\sigma^1,\sigma^2,\sigma^3$四个矩阵是线性独立的，故它们的直积也线性独立，故$\{\sigma_1^{\mu_1}\otimes\sigma_2^{\mu_2}\otimes\cdots\otimes\sigma_n^{\mu_n}\}$是一组相互独立的矩阵.

由于$\mu_1,\mu_2,\cdots,\mu_n=0,1,2,3$. 故这样相互独立的矩阵有$4^n$个. 故它们

构成 $U(2^n)$ 群的一组完备基矢.

定理3. 定理2中完备基的其中一种类型 $\sigma_1^z\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z$ 可以表示成以下量子线路:



证: $\sigma_1^z\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z$ 作用任何一个计算基矢上不改变基矢的构形

$$\sigma_1^z\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z|i_1 i_2,\cdots,i_n\rangle = (-1)^{i_1+i_2+\cdots+i_n}|i_1 i_2,\cdots,i_n\rangle,\quad i_1,\cdots,i_n=0,1$$

而 σ_n^z 作用到 $|i_1,i_2,\cdots,i_n\rangle$ 上得

$$\sigma_n^z|i_1,i_2,\cdots,i_n\rangle = (-1)^{i_n}|i_1,i_2,\cdots,i_n\rangle,\quad i_1,\cdots,i_n=0,1$$

σ_n^z 与 $\sigma_1^z\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z$ 之间只相差了 $(-1)^{i_1+i_2+\cdots+i_{n-1}}$. 我们只要用某算符来统计 $(-1)^{i_1+i_2+\cdots+i_{n-1}}$ 的值即可. 而CNOT可办到:

$$\mathrm{CNOT}(1,n)\,\mathrm{CNOT}(2,n)\cdots\mathrm{CNOT}(n-1,n)|i_1,i_2,\cdots,i_n\rangle$$

$$= X_n^{i_1}X_n^{i_2}\cdots X_n^{i_{n-1}}|i_1,i_2,\cdots,i_n\rangle$$

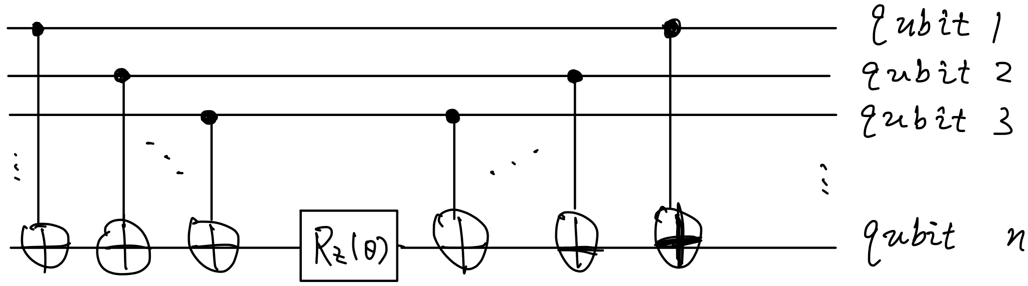
$$= X_n^{i_1+i_2+\cdots+i_{n-1}}|i_1,i_2,\cdots,i_n\rangle$$

而 $$\sigma_n^z X_n^{i_1+\cdots+i_{n-1}}|i_1,i_2,\cdots,i_n\rangle = \sigma_n^z|i_1,i_2,\cdots,(i_1+i_2+\cdots+i_n)\bmod 2\rangle$$

$$= (-1)^{i_1+i_2+\cdots+i_n}|i_1,i_2,\cdots,(i_1+i_2+\cdots+i_n)\bmod 2\rangle$$

σ_n^z 后面的CNOT是为了把 i_n 的状态恢复原状. 故 $\sigma_1^z\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z$ 的确可用以上量子线路表示, 定理成立.

定理4: $\exp\left(i\,\sigma_1^z\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z\,\frac{\theta}{2}\right)$ 可由以下量子线路表示



证：我们记 $U = CNOT(1,n)\,CNOT(2,n)\cdots CNOT(n-1,n)$

那么上述线路可表述为：$U R_z(\theta) U^\dagger$.

$$U R_z(\theta) U^\dagger = U \exp\left(i\,\sigma_n^z\,\frac{\theta}{2}\right) U^\dagger$$

$$= U\left(\cos\frac{\theta}{2} + i\sin\frac{\theta}{2}\,\sigma_n^z\right)U^\dagger$$

$$= \cos\frac{\theta}{2} + i\sin\frac{\theta}{2}\,U\sigma_n^z U^\dagger$$

根据定理3有 $$= \cos\frac{\theta}{2} + i\sin\frac{\theta}{2}\left(\sigma_1^z\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z\right)$$

$$= \exp\left(i\,\sigma_1^z\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z\cdot\frac{\theta}{2}\right).$$

故定理成立.

定理5: $\exp\left(i\,\sigma_1^x\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z\cdot\frac{\theta}{2}\right) = H_1\exp\left(i\,\sigma_1^z\otimes\sigma_2^z\otimes\cdots\sigma_n^z\cdot\frac{\theta}{2}\right)H_1$

$\exp\left(i\,\sigma_1^y\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z\cdot\frac{\theta}{2}\right) = R_{1x}\left(-\frac{\pi}{2}\right)\exp\left(i\,\sigma_1^z\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z\right)R_{1x}\left(\frac{\pi}{2}\right)$

$\exp\left(i\,I_1\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z\cdot\frac{\theta}{2}\right) = \sigma_1^z\exp\left(i\,\sigma_1^z\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z\right).$

证明: $H_1\exp\left(i\,\sigma_1^z\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z\cdot\frac{\theta}{2}\right)H_1$

$$= \cos\frac{\theta}{2} + i\left(H_1\sigma_1^z H_1\right)\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z\cdot\sin\frac{\theta}{2}$$

$$= \cos\frac{\theta}{2} + i\,\sigma_1^x\otimes\sigma_2^z\otimes\cdots\otimes\sigma_n^z\cdot\sin\frac{\theta}{2}$$

$= \exp(i\sigma_1^x \otimes \sigma_2^z \otimes \cdots \otimes \sigma_n^z \cdot \frac{\theta}{2})$

其它两式证明方法类似。定理5可知，若要将 $\exp(i\sigma_1^z \otimes \sigma_2^z \otimes \cdots \otimes \sigma_n^z \frac{\theta}{2})$ 中的哪个 σ^z 替换成 σ^x, σ^y, I，只要在定理4线路的首末分别作用上单比特量子门 $H, R_x(\frac{\pi}{2}), \sigma^z$.

定理6：CNOT 和单比特量子门是完备的.

由定理2可知，$\{\sigma_1^{\mu_1} \otimes \cdots \otimes \sigma_n^{\mu_n}\}$ 是 n 比特量子门的一组完备基. 故任意 n 比特量子门总可写成 $\exp(i\sigma_1^{\mu_1} \otimes \cdots \otimes \sigma_n^{\mu_n} \frac{\theta}{2})$ 的组合形式. 而由定理5，$\exp(i\sigma_1^{\mu_1} \otimes \cdots \otimes \sigma_n^{\mu_n} \frac{\theta}{2})$ 总可由 $\exp(i\sigma_1^z \otimes \cdots \otimes \sigma_n^z \frac{\theta}{2})$ 加上单比特量子门 $H, R_x(\frac{\pi}{2}), \sigma^z$ 组合而成. 由定理4. $\exp(i\sigma_1^z \otimes \cdots \otimes \sigma_n^z \frac{\theta}{2})$ 可由 $n-1$ 个 CNOT 以及 1 个 $R_z(\theta)$ 组合而成. 综上所述，任意 n 比特量子门可被分解为单比特门 $H, R_x(\frac{\pi}{2}), \sigma^z, R_z(\theta)$ 以及两比特门 CNOT. 故 CNOT 和单比特量子门是完备的.

(1) 量子门操作满足 $U^\dagger U = I$. n 比特…，$U(2^n)$ 群. 是李群，满足 $U(\vec{\theta}) = \exp(iT^\alpha \theta_\alpha)$.、维数是 N^2.

(2) 对于 $U(2)$（单比特量子门）可看作某种旋转，轴为 x, y, z, I.
$R_x(\alpha) = \exp(\frac{i}{2}\alpha\sigma_x)$，…，…. 任意 $U \in U(2)$ 有 $U(\alpha, \beta, \gamma, \delta) = R_x(\alpha) R_y(\beta) R_z(\gamma) \cdots$
推广到 $U(2^n)$ 也如此，不过要 4^n 个轴.

(3) 轴为 $\sigma_1^{\mu_1} \otimes \sigma_2^{\mu_2} \otimes \cdots \otimes \sigma_n^{\mu_n}$. 关键是如何构造 $\exp(i\frac{\theta}{2}\sigma_1^{\mu_1} \otimes \sigma_2^{\mu_2} \otimes \cdots \otimes \sigma_n^{\mu_n})$.
先从简单的 $\exp(i\frac{\theta}{2}\sigma_1^3 \otimes \sigma_2^3 \otimes \cdots \otimes \sigma_n^3)$ 开始. $\exp(\cdots) = \cos\frac{\theta}{2} + i\sin\frac{\theta}{2}(\cdots)$.
只要构造 $\sigma_1^3 \otimes \sigma_2^3 \otimes \cdots \otimes \sigma_n^3$.