Universal Quantum Gates

Subscriber: Y. Hua

October 17, 2019

1 General Purposes

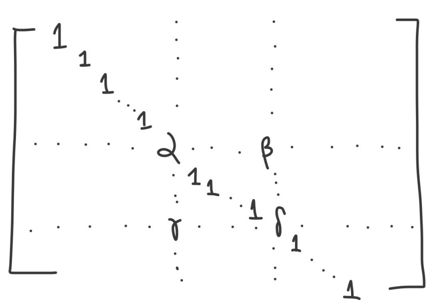
Any unitary operator can be built with universal 1-quit gates and CNOT gates. To show this, we divide the proof into two steps:

1. Show that any d by d unitary matrix can be written as the product of d(d-1)/2 2-level unitary matrices.

2. Show that any 2-level unitary matrix can be implemented using 1-qubit gates and CNOT gates.

2 Writing an arbitrary d-by-d matrix into 2-level matrices

Consider an arbitrary 2-level unitary matrix $T^{JK} =$



$$where\ \widetilde{T} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \text{ is unitary, and } \alpha,\ \beta,\ \gamma,\ \delta \in \mathbb{C}$$

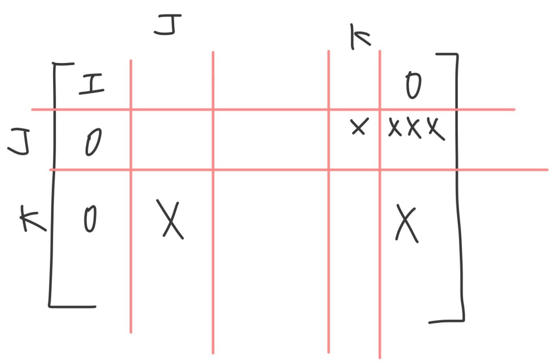
To have a clearer view, take d = 2, then ${T^{JK}}_{d=2} = \begin{bmatrix} 1 & 0 \\ 0 & \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \end{bmatrix}$

Now let $U' = UT^{JK}$, which has the same elements as U, except for those on the J^{th} and K^{th} column. We have

$$U'_{jJ} = U_{jJ}T^{JK}_{JJ} + U_{jK}T^{JK}_{KJ} = U_{jJ}\alpha + U_{jK}\gamma$$

$$U'_{kK} = U_{kJ}T^{JK}_{JK} + U_{kK}T^{JK}_{KK} = U_{kJ}\beta + U_{kK}\delta$$

Suppose U is in the form of



Then $\exists T^{JK}$ such that U', which $= UT^{JK}$, has the same structure as U, except that $U'_{JK} = 0$.

If $U'_{JK} = U_{JJ}\beta + U_{JK}\delta = 0$, and $U'_{JJ} = U_{JJ}\alpha + U_{JK}\gamma = 0$, $\widetilde{T}$ can be arbitrary. If not, then

$$\beta = \frac{U_{JK}}{\sqrt{|U_{JJ}|^2|U_{JK}|^2}} = \gamma^*$$

$$\sigma = -\alpha^* = -\frac{U_{JJ}}{\sqrt{|U_{JJ}|^2 |U_{JK}|^2}}$$

For a U^J in the form of

$$\begin{array}{cc} & \begin{array}{cc} & J \end{array} \\ J & \left[\begin{array}{c|c} I & 0 \\ \hline 0 & X \end{array}\right] \end{array},$$

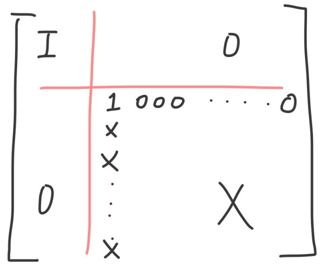
Since $T^{J,J+1}$ replaces $U_{J,J+1}$ with 0 in the matrix, with $T^{J,J+1}T^{J,J+2}T^{J,J+3}...$, we can transform the matrix into V =

$$\begin{array}{cc} & \begin{array}{cc} & J \end{array} \\ J & \left[\begin{array}{c|c} I & 0 \\ \hline 0 & \begin{array}{ccccc} x & 0\,0\,0 & \cdots & 0 \\ x & & & \\ x & & X & \\ \vdots & & & \\ x & & & \end{array} \end{array}\right] \end{array}$$

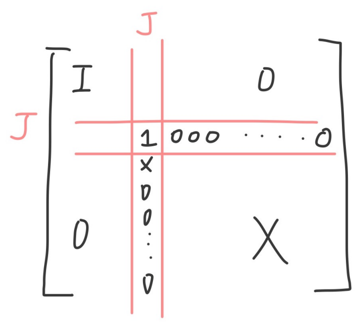
Let A demote the upper left element that is not in the unitary sub-matrix:

$$\left[\begin{array}{c|c} I & 0 \\ \hline 0 & \begin{array}{ccccc} A & 0\,0\,0 & \cdots & 0 \\ x & & & \\ x & & X & \\ \vdots & & & \\ x & & & \end{array} \end{array}\right]$$

With the property of unitary matrices such that rows of which form an orthornomal basis, A has to be 1 if it is some real, non-negative number. The matrix thus can be transformed into



Similarly, since the columns of a unitary matrix also form orthonormal basis, all elements on the J^{th} column except for V_{JJ} has to be 0. The matrix can thus be rewritten into



$$
\begin{aligned}
I &= U^{d-1}T^{d-1,d} \\
&= U^{d-2}T^{d-2,d-1}T^{d-2,d}T^{d-1,d} \\
&= U^{d-3}(T^{1,2}T^{1,3}...T^{1,d})(T^{2,3}T^{2,4}...T^{2,d})(T^{3,4}T^{3,5}...T^{3,d})....(T^{d-1,d}
\end{aligned}
$$

$$
U = (T^{d-1,d\dagger})(T^{d-2,d\dagger}T^{d-2,d-1\dagger})(T^{d-3,d\dagger}T^{d-3,d-2\dagger}T^{d-3,d-1\dagger})...(T^{1,d\dagger}T^{1,d-1\dagger}...T^{1,2\dagger})
$$

$$
\sum_{i=1}^{d} i = \frac{d(d-1)}{2}
$$

3 Writing an arbitrary 2-level matrix into 1-qubit gates and CNOT gates

3.1 General Idea

Shuffle until two important levels are $\begin{cases} |1\rangle^{\otimes n-1}|0\rangle \\ |1\rangle^{\otimes n-1}|1\rangle \end{cases}$. Then we apply $C^{n-1}\widetilde{T}$ and then shuffle back.

$$T^{JK} \longrightarrow C^{n-1}\widetilde{T} \longrightarrow \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & \widetilde{T} \end{bmatrix}$$

3.2 Demonstration

Let T^{JK}, where

$$\begin{cases} |J\rangle = |j_1, j_2, ..., j_n\rangle = |g_0\rangle & where |j_1, j_2, ..., j_n\rangle \text{ is the binary representation of } |J\rangle \\ |K\rangle = |k_1, k_2, ..., k_n\rangle = |g_m\rangle & where m \text{ is \# of bits differ} \end{cases}$$

J = $g_0, g_1, g_2, ..., g_m$ = k, where two consecutive binary numbers just differ in one bit.
From g_{i-1} to g_i, just need to switch the last bit in g_{i-1}

E.g. For $\begin{cases} |J\rangle = |000\rangle \\ |K\rangle = |111\rangle \end{cases}$ Gray Code will be

$$g_0 = 000 \to g_1 = 001 \to g_2 = 011 \to g_3 = 111 \tag{1}$$

. Then,

$$|g_0\rangle = |000\rangle \to |g_1\rangle = |001\rangle \to |g_2\rangle = |011\rangle \xrightarrow{C^{(n-1)}(\widetilde{T})} |g_2\rangle = |011\rangle \to |g_1\rangle = |001\rangle \to |g_0\rangle = |000\rangle$$

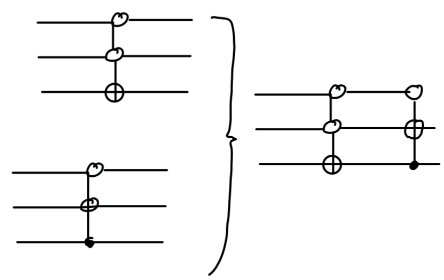
Then, applying the $C^{(n-1)}(\widetilde{T})$,

$$\begin{aligned} |g_2\rangle &\to |g_2\rangle\alpha + |g_3\rangle\gamma \\ |g_3\rangle &\to |g_2\rangle\beta + |g_3\rangle\delta \end{aligned}$$

For example, ... Circuits

After applying controlled state $C^{(n-1)}(\widetilde{T})$, we reverse the shuffling, for example

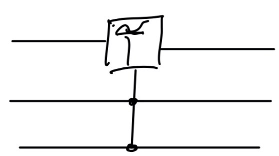
$$|011\rangle \rightarrow |001\rangle \rightarrow |111\rangle$$

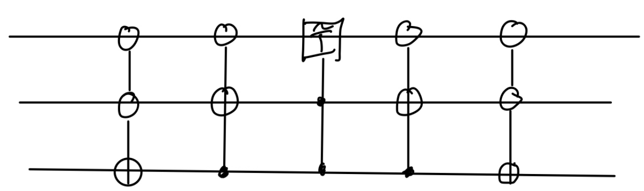


and its circuit is following

The operations above are equivalent to

$$|J\rangle = |g_0\rangle \rightarrow \alpha|g_0\rangle + \gamma|g_m\rangle \rightarrow \alpha|T\rangle + \gamma|K\rangle$$
$$|K\rangle = |g_m\rangle \rightarrow \beta|g_m\rangle + \delta|g_m\rangle \rightarrow \beta|T\rangle + \delta|K\rangle$$





Complexity:

Gate count: $2m - 1 = O(n)$ which is shuffle for each T^{JK} gate. And, we totally have $O(n)$ controlled $C^{(n-1)}$. So, we have $O(n^2)$ gates. Also, we have $N^2 = n^{2n}$ qubits. Thus, total complexity is $O(n2^n \log(n))$