§1.3 Multi-Qubit Gates

An n-qubit state is given by a superposition of tensor product states

$$|\psi\rangle = \sum_{i_1, i_2, \cdots, i_n} c_{i_1 i_2 \cdots i_n} |i_1 i_2 \cdots i_n\rangle$$

where $i_k = 0, 1$ and $|i_1 i_2 \cdots i_n\rangle = |i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle$

A single qubit gate A acting on the kth qubit is denoted by

$$A_k = \underbrace{I \otimes \cdots \otimes I}_{k-1} \otimes A \otimes \underbrace{I \otimes \cdots I}_{n-k-1}$$

An important two-qubit gate is the controlled-NOT (CNOT) gate:

$$\Lambda_{c,t}(X) = |0\rangle\langle 0|_c I_t + |1\rangle\langle 1|_c X_t$$

It acts as

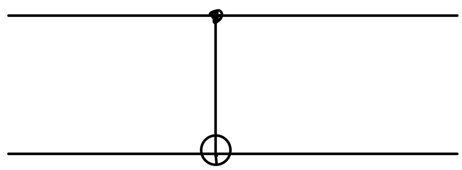
$$\Lambda_{c,t}(X) |i\rangle_c |j\rangle_t = |i \oplus j\rangle$$

$$\left[\begin{aligned} & \left(|0\rangle\langle 0|_c I_t + |1\rangle\langle 1|_c X_t \right) |i\rangle_c |j\rangle_t \\ = \; & \langle 0|i\rangle |0\rangle_c |j\rangle_t + \langle 1|i\rangle |1\rangle_c X_t |j\rangle_t \\ \overset{i=0}{=} \; & |0\rangle_c |j\rangle_t \\ \overset{i=1}{=} \; & |1\rangle_c |j+1\rangle_t \end{aligned}\right.$$

If the input state is $|+\rangle_c |0\rangle_t$, the output is the maximally entangled state:

$$\Lambda_{c,t}(X)\,|+\rangle_c |0\rangle_t = \left(|00\rangle + |11\rangle\right)/\sqrt{2}$$

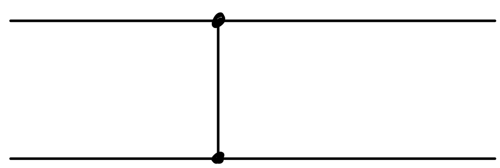
symbol:



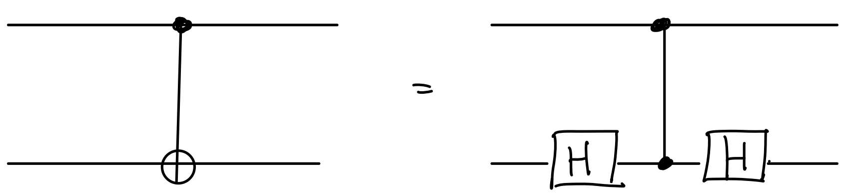
Define controlled-Z (CZ) gate:

$$\Lambda_{c,t}(Z) = |0\rangle\langle 0|_c\, I_t + |1\rangle\langle 1|_c\, Z_t$$

symbol:



Moreover,



Both Clifford-gates:

$$\Lambda(X)_{c,t}\, X_c \otimes I_t\, \Lambda(X)^\dagger_{c,t} = X_c \otimes X_t,$$

$$\Lambda(X)_{c,t}\, I_c \otimes Z_t\, \Lambda(X)^\dagger_{c,t} = Z_c \otimes Z_t,$$

$$\Lambda(Z)_{c,t}\, X_c \otimes I_t\, \Lambda(Z)^\dagger_{c,t} = X_c \otimes Z_t, \quad \text{etc.}$$

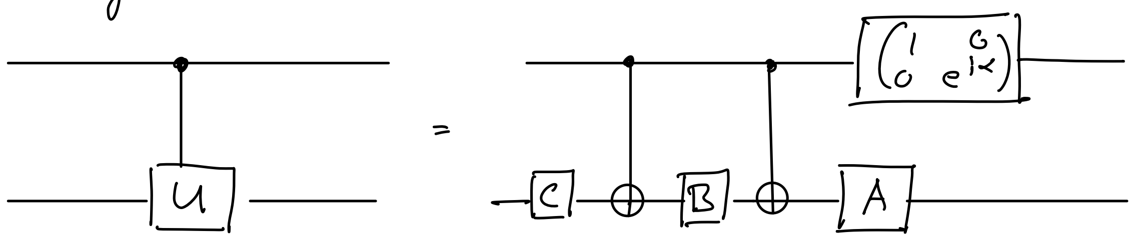
For arbitrary unitary operator U, the controlled-U gate is denoted by

$$\Lambda_{c,t}(U) = |0\rangle\langle 0|_c I_t + |1\rangle\langle 1|_c U_t ,$$

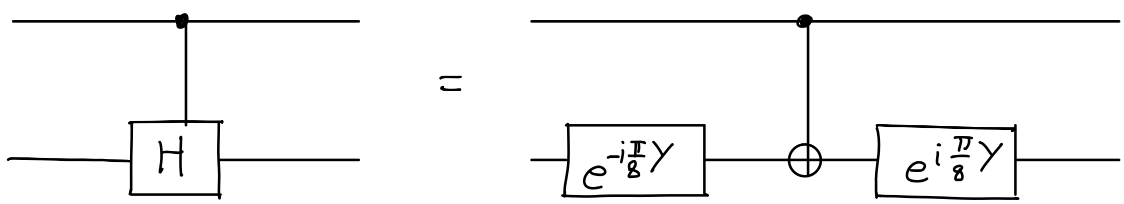
control qubit   target qubit

Decomposing $U = e^{i\alpha} A X B X C$, $ABC = I$,
(always possible, exercise)

we get :



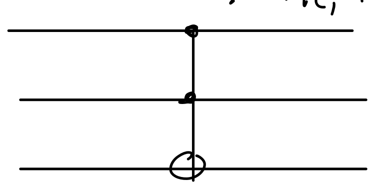
For example,



Next, we introduce the "Toffoli gate":

$$\Lambda^2_{c_1,c_2,t}(X) = \left(I_{c_1} I_{c_2} - |1\rangle\langle 1|_{c_1} |1\rangle\langle 1|_{c_2} \right) I_t$$
$$+ |1\rangle\langle 1|_{c_1} |1\rangle\langle 1|_{c_2} X_t ,$$

symbolically:



acts as:

$$\Lambda^2_{c_1, c_2, t}(X)\, |i_1\rangle_{c_1} |i_2\rangle_{c_2} |j\rangle_t = |i_1\rangle_{c_1} |i_2\rangle_{c_2} |j \oplus (i_1 \cdot i_2)\rangle_t$$

$\longrightarrow$ quantum extension of NAND operation

Quantum computation can simulate classical computation in a reversible manner:

compute a boolean function $f(x)$:

$$U_f |x\rangle_{input} |0\ldots0\rangle_{ancilla} |0\rangle_{answer}$$

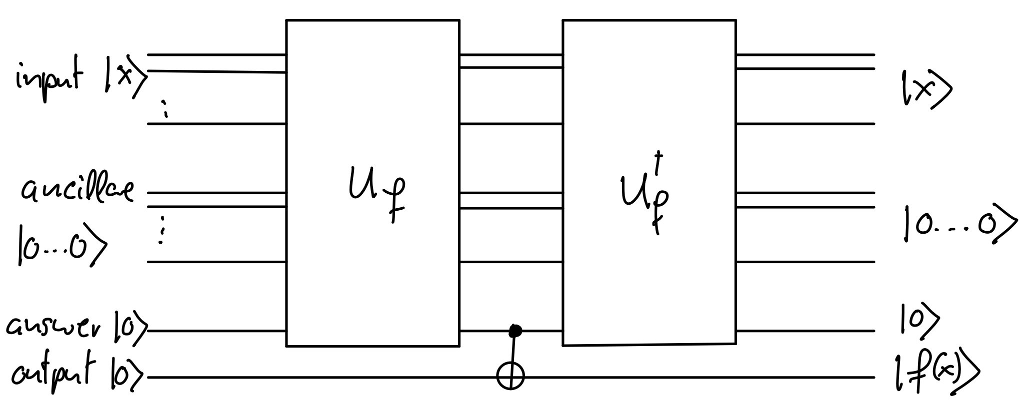
$$= |x\rangle_{input} \underbrace{|g(x)\rangle_{ancilla}}_{\text{redundant output}} |f(x)\rangle_{answer}$$

Set back red. output by:

$$U_f^\dagger \Lambda_{answer,out}(X)\, U_f\, |x\rangle_{input} |0\ldots0\rangle_{ancilla} |0\rangle_{answer} |0\rangle_{out}$$

$$= U_f^\dagger |x\rangle_{input} |g(x)\rangle_{ancilla} |f(x)\rangle_{answer} |f(x)\rangle_{out}$$

$$= |x\rangle_{input} |0\ldots0\rangle_{ancilla} |0\rangle_{answer} |f(x)\rangle_{out}$$

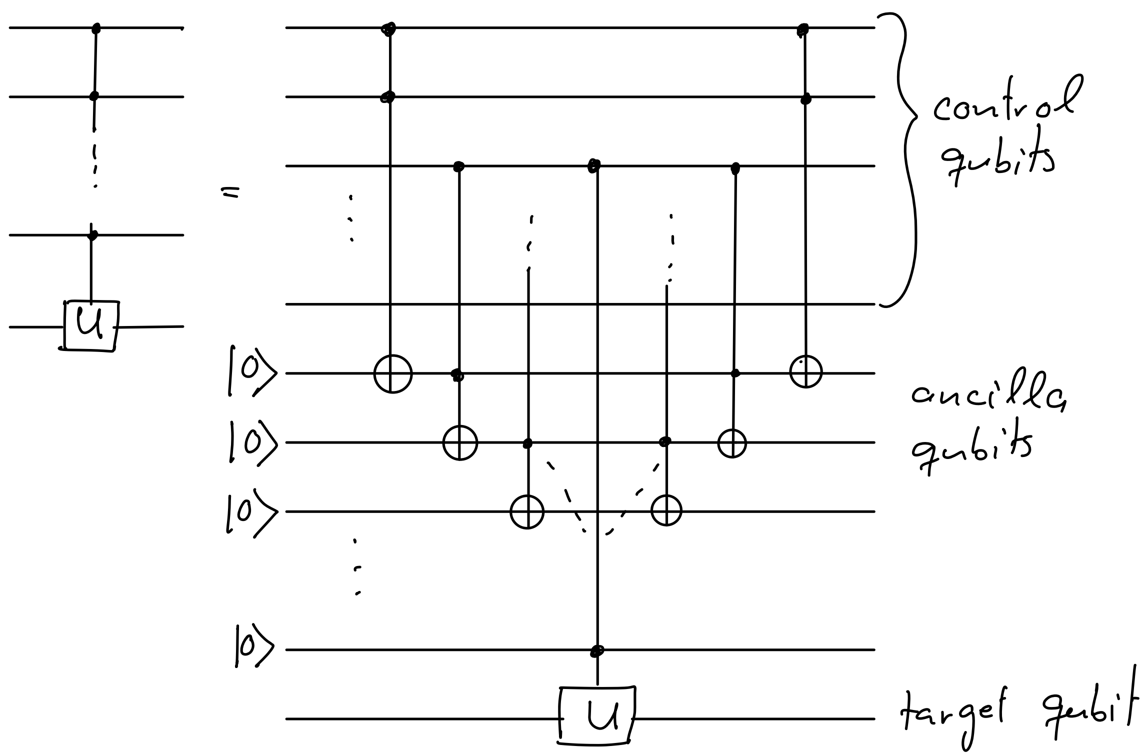


$\rightarrow$ reversible

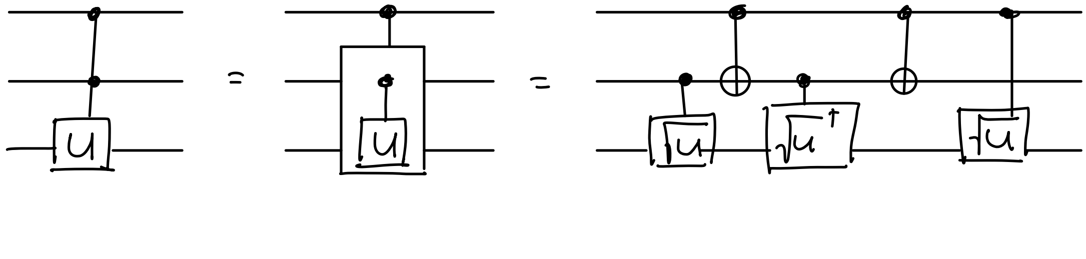
Finally, we introduce the multi-controlled unitary gate

$$\Lambda^k(U) = (I^{\otimes k} - |1\rangle\langle 1|^{\otimes k}) \otimes I + |1\rangle\langle 1|^{\otimes k} \otimes U$$

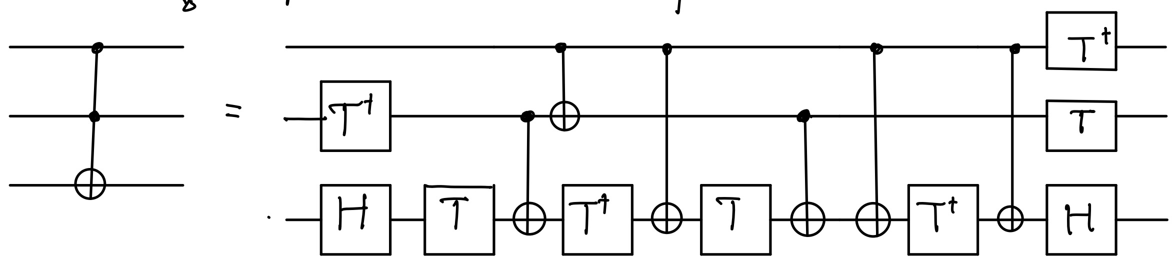
implemented as follows:



The $\Lambda^2(U)$ gate can be decomposed into CNOT and single-qubit gates by using an idea similar to the decomposition of the $\Lambda(U)$ gate:

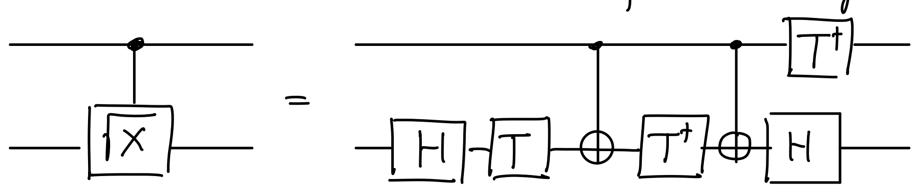


For example, the Toffoli gate can be constructed from the CNOT, Hadamard, and $\frac{\pi}{8}$ operations as follows:



$$T = e^{-(\pi/8)\, i Z}$$

where we used the following decomposition



§1.4 Universal Quantum Computation

Let U be an arbitrary n-qubit unitary operator, represented by an $m \times m$ unitary matrix with $m \equiv 2^n$. Let T_{ij} be a unitary operator such that $(T_{ij})_{kl} = \delta_{kl}$ if $k,l \neq i,j$,

$\rightarrow$ denote by "two-level unitary gate"

Can choose T_{mm-1} such that

$$U T_{mm-1} = \begin{pmatrix} u_{11} & \cdots & u_{1\,m-1} & u_{1m} \\ \vdots & \ddots & \vdots & \vdots \\ u_{m-1\,1} & & u'_{m-1\,m-1} & u'_{m-1\,m} \\ u_{m1} & & 0 & u'_{mm} \end{pmatrix}$$

where $(U_{ke}) = u_{ke}$. Repetition gives

$$U T_{m\,m-1} T_{m\,m-2} \cdots T_{m1} = \begin{pmatrix} u''_{11} & \cdots & u''_{1\,m-1} & u''_{1m} \\ \vdots & \ddots & \vdots & \vdots \\ u''_{m-1\,1} & & u''_{m-1\,m-1} & u''_{m-1\,m} \\ 0 & \cdots & 0 & u''_{mm} \end{pmatrix}$$

Unitarity $\longrightarrow$ $u''_{1m} = \cdots = u''_{m-1\,m} = 0$

and $|u''_{mm}| = 1$

Define $R_m \equiv T_{m\,m-1} T_{m\,m-2} \cdots T_{m1}$

$$\longrightarrow U = D\,(R_m \cdots R_1)^{\dagger}$$

where D is diagonal

$\longrightarrow$ an arbitrary unitary U can be decomposed into two-level unitary gates.

Next: show that any two level unitary T_{ij} can be implemented by CNOT and single-qubit gates.

Suppose T acts non-trivially on the computational basis states $|s\rangle$ and $|t\rangle$, where $s = s_1 \cdots s_n$ and $t = t_1 \cdots t_n$ (binary exp.)

Let $\tilde{T}$ be the non-trivial 2×2 submatrix of T

$\rightarrow$ unitary operator on single qubit

Suppose $s = 101001$, $t = 110011$

$\rightarrow$ consider matrix

$$\begin{array}{l} |g_1\rangle \rightarrow \\ \vdots \\ |g_i\rangle \rightarrow \\ |g_m\rangle \rightarrow \end{array} \begin{array}{cccccc} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{array} \xrightarrow{\text{bit flips}} \begin{array}{l} |g_1\rangle \rightarrow |g_{m-1}\rangle \\ |g_2\rangle \rightarrow |g_1\rangle \\ |g_3\rangle \rightarrow |g_2\rangle \\ \cdots \\ |g_{m-1}\rangle \rightarrow |g_{m-2}\rangle \end{array}$$

Suppose g_{m-1} and g_m differ in jth bit

$\rightarrow$ apply controlled-$\tilde{T}$ operation with the jth qubit as target

$\rightarrow$ complete T operation by undoing the swap