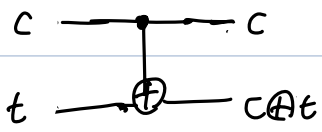
4.4. Controlled operators ~ 4.9. Implementation of controlled operators.

1 4.4.1 – Controlled not gate. (Lee chaeiow)

So far, we have discussed single-qubit operators,

From now, we will concern the multi-qubit operation.

In particular, Controlled operator.

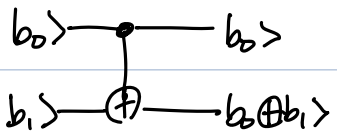


Recall the definition of classical controlled-not gate:

$(a \oplus b = XOR(a,b))$

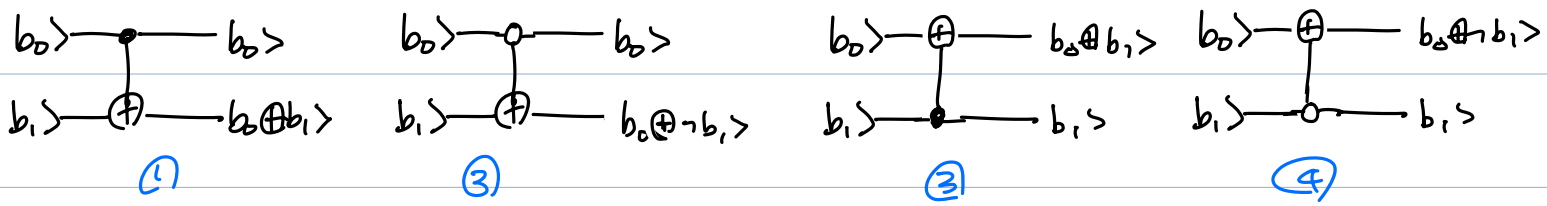
It applies not gate onto target bit t if and only if the control bit is 1.

From this, we may introduce the quantum Not gate as follows:



It applies Pauli X gate to a target qubit based on the control qubit.

There are three more variants of standard CNOT gate.



With respect to the standard basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, CNOT gate has matrix representation $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

By changing the basis, we can prove the equivalence between standard CNOT and its variant.

Recall the $|x_+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} = H|0\rangle$, $|x_-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} = H|1\rangle$

Then $\{|x_+x_+\rangle, |x_+x_-\rangle, |x_-x_+\rangle, |x_-x_-\rangle\}$ is an orthonormal basis of H_2.

and $CNOT|x_+x_+\rangle = \frac{1}{2}(CNOT|00\rangle + CNOT|01\rangle + CNOT|10\rangle + CNOT|11\rangle)$

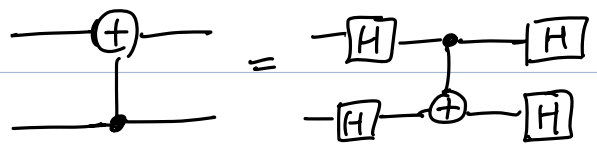
$= \frac{1}{2}(|00\rangle + |01\rangle + |11\rangle + |10\rangle) = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |x_+x_+\rangle$

$CNOT|x_+x_-\rangle = \frac{1}{2}(CNOT|00\rangle - CNOT|01\rangle + CNOT|10\rangle - CNOT|11\rangle)$

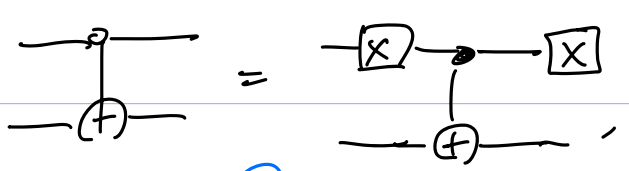
$= \frac{1}{2}(|00\rangle - |01\rangle + |11\rangle - |10\rangle) = |x_-x_-\rangle$

$CNOT|x_-x_+\rangle = |x_-x_+\rangle$, $CNOT|x_-x_-\rangle = |x_+x_-\rangle$

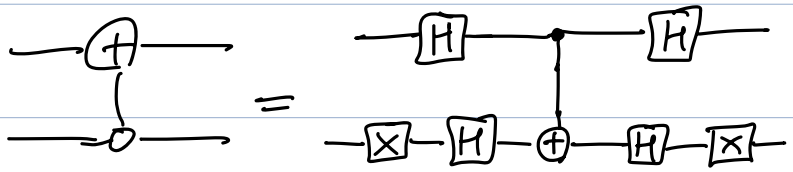
Hence, CNOT operator exchanges the first qubit if and only if the second qubit is $|x_-\rangle$, This implements ③



Similary, ② and ④ can be implemented as follows,



②



④

[2] Controlled U-operators.

We may generalized the Controlled not gate into controlled U-gate.

→ Apply U to the target qubit depending on the control qubit being $|0\rangle$ or $|1\rangle$

→ How can we implement such mechanism?

we can only do ① apply unitary operator to single qubit

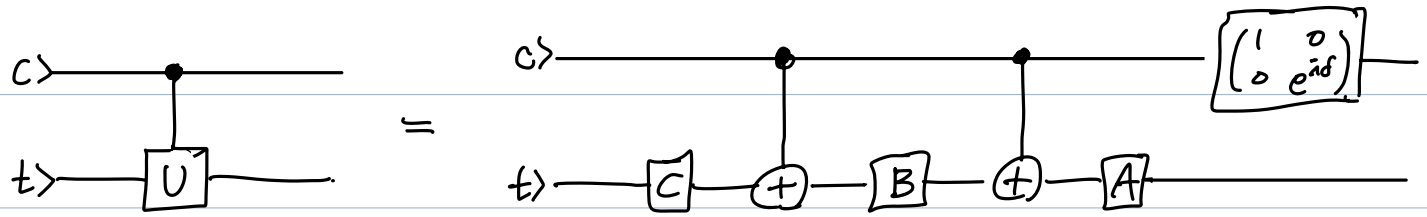
② CNOT gate.

→ That's where decomposition thm kicks in.

By thm 4.3.3, By given Unitary operator U, $\exists \delta \in \mathbb{R}$, A, B, C: unitary single-qubit operator

such that $U = e^{i\delta} AXBXC$ and $ABC = I$.

From this decomposition thm, we can implement controlled-U gate as follows:



In this implementation, ① If control qubit is $|0\rangle$, the circuit applies $ABC = I$ to target qubit

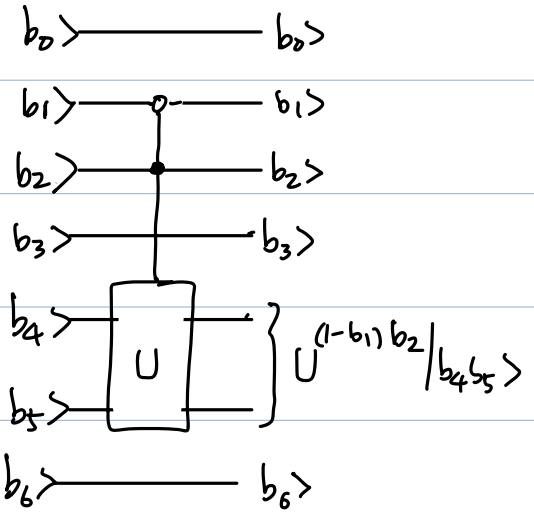
② If control qubit is $|1\rangle$, the circuit applies $e^{i\delta} AXBXC = U$ to target qubit.

Using this thm, One can implement controlled-Y, Z, S, T operators.

3 Generalized control operators,

Now we present the most general controlled operators.

Let's begin with an example.



This operator acts each qubits as: $|b_0\rangle, |b_3\rangle, |b_6\rangle$: not changed

$|b_1\rangle, |b_2\rangle$: not changed, control qubits

$|b_4b_5\rangle$: $\begin{cases} |b_4b_5\rangle & \text{if } b_1\rangle \neq 1 \text{ or } b_2\rangle \neq 0 \\ U^{(1-b_1)b_2}|b_4b_5\rangle & \text{if } b_1\rangle = 1 \text{ and } b_2\rangle = 0. \end{cases}$

Formally, we describe general controlled operators on H_n as follows.

Def 4.4.7 Let C_0, C_1, T be pairwise disjoint subsets of the index set Z_n.

Let $m = |T| > 0$, and let $T = \{t, t+1, \cdots, t+m-1\}$ with $t \in Z_n$.

Let U be unitary operator on H_m.

Then, the linear operator $C^{C_0, C_1, T}(U)$ is defined by its action on computational basis of H_n as follows: $C^{C_0, C_1, T}(U)|b_0 b_1 \cdots b_n\rangle$

$$= |b_0 \cdots b_{t-1}\rangle U^c |b_t \cdots b_{t+m-1}\rangle b_{t+m} \cdots b_n\rangle$$

Where $c = \prod_{i \in C_0} (1 - b_i) \prod_{j \in C_1} b_j$.

Two natural question arises

① Why do we restrict T to be consequtive integers?

A) For simplicity. Using SWAP gates. (Chapter 4.5), we may drop this assumption.

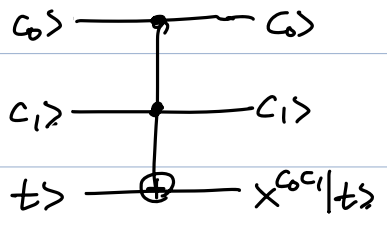
② How can we implement this? Now U is not a single qubit unitary operator.

A) We deal it at chapter 4.9.

With this notation, the example above can be written as $C^{1,2,\{4,5\}}(U)$

we illust several important instances of generalized controlled operators.

① Quantum toffoli gate (CCNOT) gate



$: C^{\emptyset, \{0,1\}, 2}(X)$

② $C^k(U)$ operators

let $m = n-k$, for any computational basis $|c_0 \cdots c_{k-1} t_0 \cdots t_{m-1}\rangle$,

$$C^k(U)\,|c_0 \cdots c_{k-1} t_0 \cdots t_{m-1}\rangle = |c_0 \cdots c_{k-1}\rangle\, U^{\prod c_i}\, |t_0 \cdots t_{m-1}\rangle .$$

or equivalently, $C^{\phi, \{0,\cdots k-1\}, \{k,\cdots k+m-1\}}(U)$

With this concept, we may write CCNOT gate $= C^2(X)$ on H_3.

③ Transposition operators.

let $\vec{c}: c_0 c_1 \cdots c_{t-1} * c_{t+1} \cdots c_{n-1}$ with $c_i \in \{0,1\}$ for each $i \in \mathbb{Z}_n$, $i \neq t$.

Then, we define $\text{TRANS}^{\vec{c}}$ as follows:

$\text{TRANS}^{\vec{c}}$ exchanges $|c_0 \cdots c_{t-1} 0 c_{t+1} \cdots c_{n-1}\rangle$ and $|c_0 \cdots c_{t-1} 1 c_{t+1} \cdots c_{n-1}\rangle$

and leaves any other basis unchanged.

for example, $\text{TRANS}^{(01*0)}$ switches $|0100\rangle$ and $|0110\rangle$,

and leaves other basis unchanged.

③ Swap and permutation operators.

There is another important multi-qubit operator which is not a controlled-type.

① SWAP gate: $\text{SWAP}|b_0 b_1\rangle = |b_1 b_0\rangle$.

SWAP gate can be implemented with three CNOT gate. $|b_0\rangle \times |b_1\rangle = |b_1\rangle \times |b_0\rangle$ =

proof) $|b_0\rangle$ — $|b_0\rangle$ — $|(b_0 \oplus b_1) \oplus b_0\rangle$ — $|(b_0 \oplus b_1) \oplus b_0\rangle$

$|b_1\rangle$ — $|b_0 \oplus b_1\rangle$ — $|b_0 \oplus b_1\rangle$ — $|((b_0 \oplus b_1) \oplus b_0) \oplus (b_0 \oplus b_1)\rangle$

Now, note that the XOR gate is commutative and associative

$\Rightarrow |b_0 \oplus b_1 \oplus b_0\rangle = |b_1 \oplus b_0 \oplus b_0\rangle = |b_1\rangle, \; |((b_0 \oplus b_1) \oplus b_0) \oplus (b_0 \oplus b_1)\rangle = |b_0 \oplus (b_0 \oplus b_1) \oplus (b_0 \oplus b_1)\rangle = |b_0\rangle.$ ■

② permutation gate.

Let $\pi \in S_n$ be given permutation on $\{0, \cdots, n-1\}$

The quantum permutation operator U_π is defined by

$$U_\pi |b_0 \cdots b_{n-1}\rangle = |b_{\pi(0)} b_{\pi(1)} \cdots b_{\pi(n-1)}\rangle.$$

From the abstract algebra class, we obtain the following:

Prop 4.5.2 U_π can be implemented by a quantum circuit that uses

$n-1$ SWAP gates or $3n-3$ CNOT gates, respectively.

④ Ancillary and erasure gates.

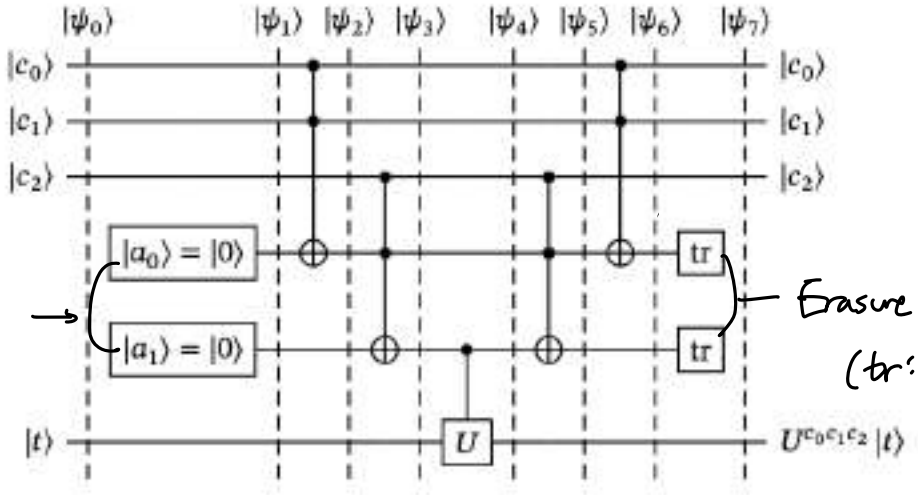
So far, we have introduced various unitary gates which can be used as building blocks of more complex quantum circuits.

However, in construction of many other quantum gates, we need two types of quantum gates that do not implement unitary operators.

: ① Ancillary operators ② Erasure operators.

You can understand these gates that ① inserts dummy qubit ② traces out dummy qubit.

Let's jump in with example: Implementation of $C^3(U)$



Ancillary gate →

← Erasure gate.
(tr: trace out)

The ancilla $a_0\rangle$, $a_1\rangle$ plays a role to determine all c_0, c_1, c_2 is 1 or not.

Through $\psi_0\rangle \sim \psi_2\rangle$, $a_0\rangle$ moves to $c_0 \cdot c_1\rangle$ and $a_1\rangle$ moves to $c_0 \cdot c_1 \cdot c_2\rangle$

Through $\psi_3\rangle$, The controlled U-gate acts on $a_1\rangle$ and $t\rangle$

and apply $U^{a_1\rangle} = U^{c_0c_1c_2}$ to the target qubit $t\rangle$

Through $\psi_4\rangle \sim \psi_7\rangle$, Two toffli gate takes back $a_0\rangle, a_1\rangle$ to their original state $0\rangle$.

and traces out them.

By thm 3.7.12, tracing out the ancilla does not change other qubit.

Hence we have nice implementation of $C^3[U]$

5 Quantum circuits (Revisited) & Purification.

Def A quantum circuit Q is specified by two positive integer n and k, and a finite sequence $(q_{f_0}, \dots q_{f_{k-1}})$, n: # of input qubit

for each $i \in \mathbb{Z}_k$, q_{f_i} contains the following

(1) a tuple of quantum gates that are either { all ancillary gates; all unitary gates; all erasure gate }

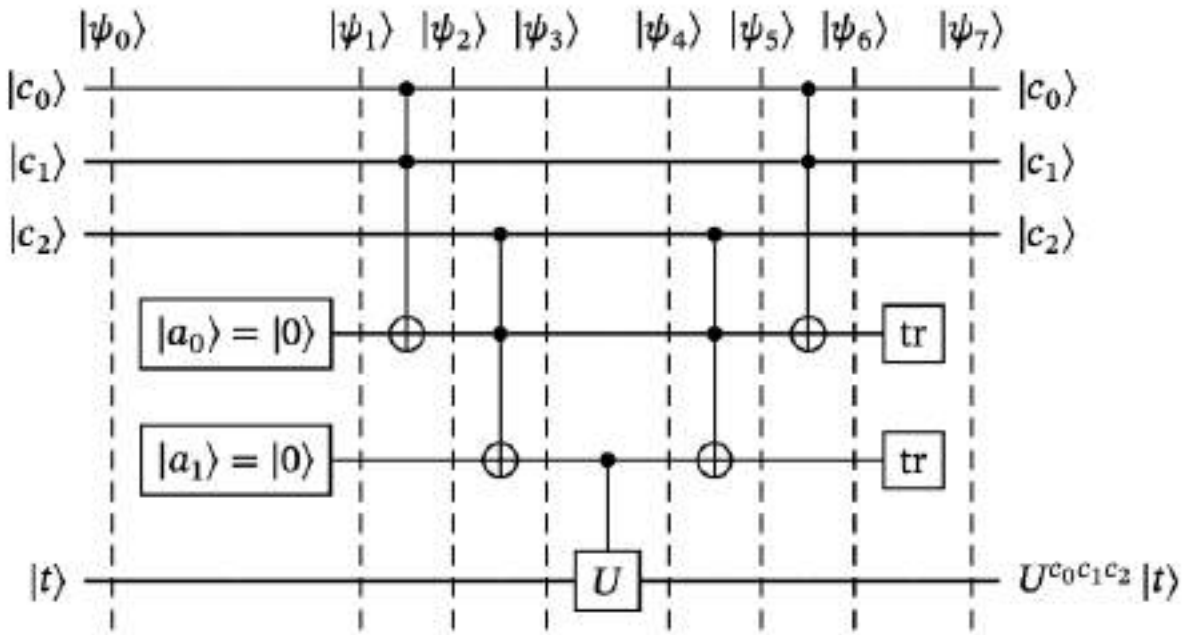
(2) the information about • How the ancilla qubits are initialized

• where they are inserted

or

Which qubits the unitary or erasure gates are applied

(At most one gate is applied to each qubit)



... (*)

In this example, we have $n=4$, $k=7$

q_{f_0}: Two ancillary gate, initialize them to $|0\rangle$, insert them behind the control qubit.

q_1, q_2: CCNOT gate, applied to $|a_0\rangle, |a_1\rangle$, respectively.

q_3: C(U) gate, applied to $|t\rangle$

q_4, q_5: CCNOT gate, applied to $|a_1\rangle, |a_0\rangle$, respectively.

q_6: Two erasure gate, traces out $|a_0\rangle$ and $|a_1\rangle$.

Def The size of a quantum circuit: $n + k$.

Remark ① "Tracing out" can produce mixed state result,

But if the state of a composite system AB is separable,

by Corollary 3.9.12, tracing out system B means omitting

the corresponding quantum bits.

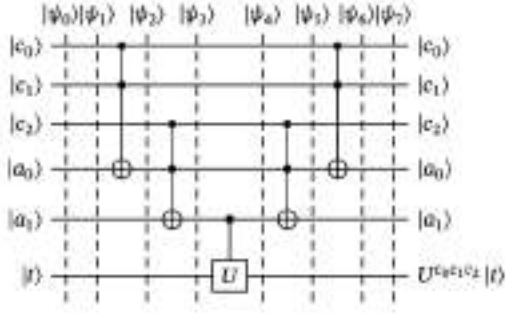
② The quantum circuit, as a operator, does not need to be unitary

but, every quantum circuit can be transformed into a unitary q.c.

1) Remove all ancillary gate and add corresponding qubits as input

2) Remove all erasure gate and add corresponding qubits as output.

The result is called "Purification" of Q.



$\in$ Purification of $(*)$

Recall the classical universality theorem.

Thm 1.9.12 For all boolean function $f: \{0,1\}^n \to \{0,1\}^m$,

$\exists p \in \mathbb{N}_0$, $p \le 2(|f|_F$, a reversible circuit D_r with $|D_r| = O(|f|_F)$

that uses only Toffoli, NOT, CNOT gates s.t D_r implements

$$h: \{0,1\}^n \times \{0,1\}^{n+p} \times \{0,1\}^m \to \{0,1\}^n \times \{0,1\}^{n+p} \times \{0,1\}^m$$

with $h(x,0,y) = (x, 0, y \oplus f(x)) \quad \forall x \in \{0,1\}^n, y \in \{0,1\}^m$

As an analogy, we can deduce the following result.

Thm 4.1.1 let $f: \{0,1\}^n \to \{0,1\}^m$, then there exists a quantum circuit Q

of size $O(|f|_F)$ that only uses Toffoli, ancillary, erasure gates

and implements the quantum operator

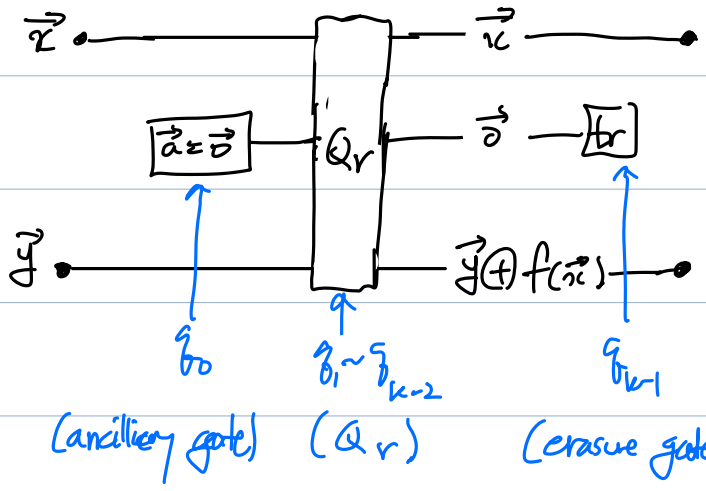
$$U: H_{n+m} \to H_{n+m}, \quad |\vec{x}\rangle|\vec{y}\rangle \mapsto |\vec{x}\rangle|\vec{y} \oplus f(\vec{x})\rangle$$

pf) By thm 1.9.12, $\exists$ q.c. Q_r which implements

$$U_r: H_n \otimes H_{n+p} \otimes H_m \to H_n \otimes H_{n+p} \otimes H_m, \quad U_r|\vec{x}\rangle|\vec{0}\rangle|\vec{y}\rangle = |\vec{x}\rangle|\vec{0}\rangle|\vec{y} \oplus f(\vec{x})\rangle$$

Then, construct Q from Q_r by the following method of 'reverse-purification'

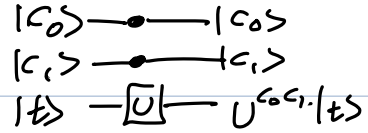
$Q =$



6 Implementation of controlled operators.

This section, we discuss the implementation of general controlled operators.

First, we present the implementation of $C^2(U)$:



(1) Proposition 4.9.1 Every unitary operator $U \in U_n$ has a square root.

(i.e. $\exists V \in U_n$ s.t. $V^2 = U$)

pf) Do a spectral decomposition of U: $\sum \lambda P_\lambda$

→ let $V = \sum \sqrt{\lambda} P_\lambda$, where $\sqrt{\lambda}$ is a square root of $\mathbb{C}$

$$\Rightarrow V^2 = \sum_{\lambda,\eta} \sqrt{\lambda}\sqrt{\eta} P_\lambda P_\eta = \sum_\lambda \lambda P_\lambda \quad \& \quad V \text{ is unitary.} \quad \square$$

For example, $V^2 = X$ for $V = (1+i)(I - iX)/2$.

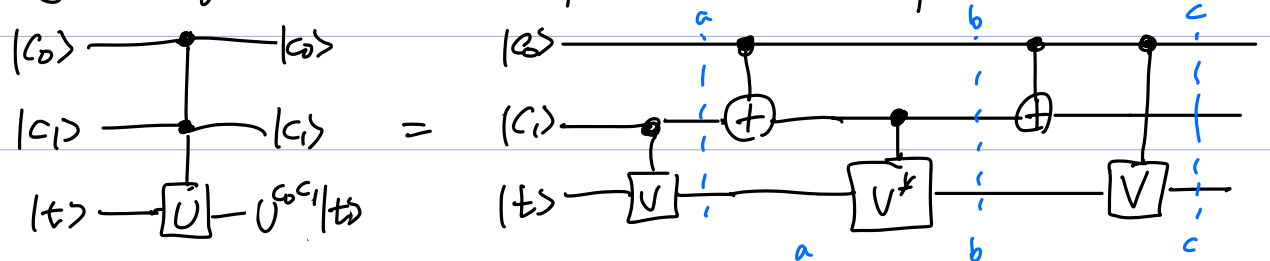
pf) $X = |x_+\rangle\langle x_+| - |x_-\rangle\langle x_-|$

$\Rightarrow V = |x_+\rangle\langle x_+| + i|x_-\rangle\langle x_-|$. Then $V|x^+\rangle = |x^+\rangle$, $V|x^-\rangle = i|x_-\rangle$

Then, If we set $V = \alpha I + \beta X$ for $\alpha, \beta \in \mathbb{C}$, we have $\alpha+\beta = 1$, $\alpha - \beta = i$

$\therefore V = \frac{1+i}{2} I - \frac{1-i}{2} X = \frac{1+i}{2}(I - iX)$ $\square$

Using the square root of the operator, we can implement the $C^2(U)$ gate as follows:



Description:

$(c_0, c_1) = (0,0) \Rightarrow |t\rangle \to |t\rangle \to |t\rangle \to |t\rangle$

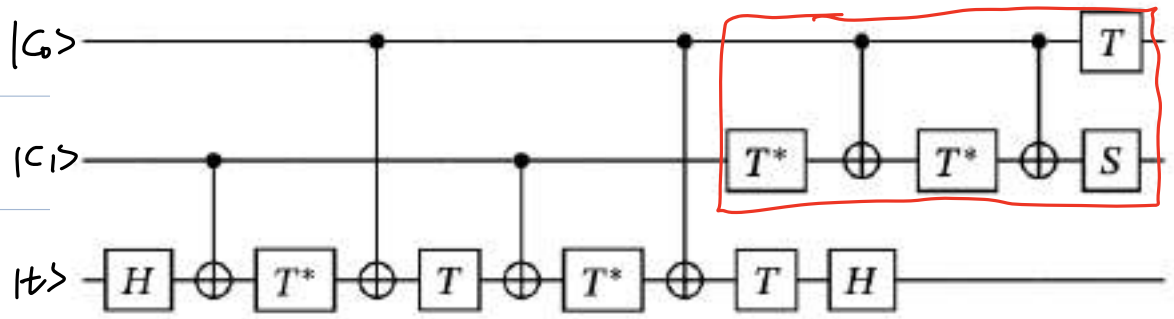
$(c_0, c_1) = (0,1) \Rightarrow |t\rangle \to V|t\rangle \to V^*V|t\rangle \to V^*V|t\rangle = |t\rangle$

$(c_0, c_1) = (1,0) \Rightarrow |t\rangle \to |t\rangle \to V^*|t\rangle \to VV^*|t\rangle = |t\rangle$

$(c_0, c_1) = (1,1) \Rightarrow |t\rangle \to V|t\rangle \to V|t\rangle \to V^2|t\rangle = U|t\rangle$

Using this, we can construct Toffoli $= C^2(X)$ gate.

Or, there exists another Implementation



Note that $T = e^{i\frac{\pi}{8}} \cdot \underbrace{\begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix}}_{=:D}$, $T^* = e^{-i\frac{\pi}{8}} \begin{pmatrix} e^{i\frac{\pi}{8}} & 0 \\ 0 & e^{-i\frac{\pi}{8}} \end{pmatrix}$

and the red part acts as

$\Rightarrow$
- $|00\rangle \to |00\rangle$
- $|01\rangle \to |01\rangle$
- $|10\rangle \hookrightarrow |10\rangle$
- $|11\rangle \to |1\rangle S|1\rangle = i|11\rangle$

Where $U = e^{i\frac{\pi}{4}} S \times T^* \times T^* = S \times \underbrace{D^* \times D^*}_{|0\rangle \to e^{i\frac{\pi}{8}}|1\rangle \to |0\rangle,\ |1\rangle \to e^{i\frac{\pi}{8}}|0\rangle \to |1\rangle} = S\begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} = S$

i) both $|c_0\rangle, |c_1\rangle = |1\rangle$: $|t\rangle$ moves to $HTXT^*XTXT^*XH|t\rangle$

$= HDXD^*XDXD^*XH|t\rangle = H\begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix} H|t\rangle = -iX$

$|11\rangle|t\rangle \longrightarrow (|1\rangle S|1\rangle)(-iX|t\rangle) = (|1\rangle \cdot i|1\rangle)(-iX|t\rangle) = |11\rangle X|t\rangle.$

ii) $(c_0, c_1) = (0,1)$: $|t\rangle$ moves to $HTT^*XTT^*XH|t\rangle = HXXH|t\rangle = |t\rangle,$

$\Rightarrow \quad |01\rangle|t\rangle \longrightarrow |01\rangle|t\rangle$

iii) $(c_0, c_1) = (1,0)$: $|t\rangle$ moves to $HTXT^*TXT^*H|t\rangle = |t\rangle \Rightarrow |10\rangle|t\rangle \longrightarrow |10\rangle|t\rangle$

iv) $(c_0, c_1) = (0,0)$: $|t\rangle$ moves to $HTT^*TT^*H|t\rangle = |t\rangle \Rightarrow |00\rangle|t\rangle \longrightarrow |00\rangle|t\rangle$ ∎

② by ①, we can use toffoli gate as our building block.

We claim the following

Proposition 4.9.10. Let U be unitary operator on $\mathbb{H}_m$ and let $k \in \mathbb{N}$,

Then we may implement $C^k(U)$ using $2k-2$ CCNOT (Toffoli) gate,

one $C^1(U)$ gate, $k-1$ ancillary & erasure gate.

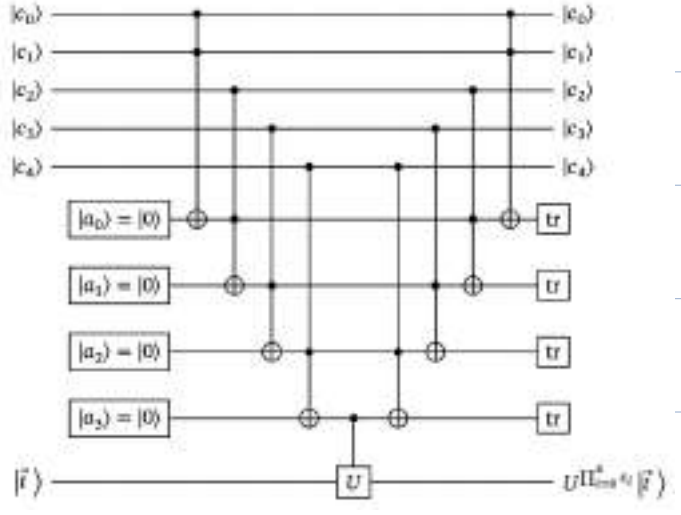
pf) The idea is, using toffoli gate, make the j-th ancillica qubits to $\prod_{i=0}^{j+1} C_i$. $(0 \le j \le k-2)$

and apply $C^1(U)$ gate with control qubit $|a_{k-2}\rangle = \left|\prod_{i=0}^{k-1} C_i\right\rangle$

and target qubit $|t\rangle$.

then, make the ancilla back to their initial qubit $|0\rangle$ by applying toffoli gate again.

This idea is illustrated as follow:



Read the algorithm 4.9.9.

□

Using this proposition and some X gate, we can implement the generalized controlled gate.

Theorem 4.9.13 Let C_0, C_1, T be pairwise disjoint subsets of $\mathbb{Z}_n$, let $m = |T| > 0$,

and assume that $T = \{i_1, i_2, \cdots i_m\}$. Let U be unitary operator on $\mathbb{H}_m$

set $k_0 = |C_0|$, $k_1 = |C_1|$, $k = k_0 + k_1$

Then the unitary operator $C^{C_0 C_1, T}(U)$ can be implemented by a q.c.

that uses $2k_0$ Pauli X gates, $2k-2$ Toffoli gates, one $C^k(U)$ gate,
and $k-1$ ancillary & erasure gates.

Then, how can we implement $C^k(U)$ gate for $U \in End(H_k)$ with $k \geq 2$?
A. Unknown, pass to chap 4.12.

7 Universal sets of quantum gates.

Recall that, $\{NAND\}$, or $\{AND, OR, NOT\}$ are universal. it means, $\forall f: \{0,1\}^n \to \{0,1\}^m$,
there exists an implementation of f that uses only the gate from S.
However, in quantum gates, the things are little bit different.

Theorem 4.8.1 Let S be a set of quantum gates such that $\forall n \in \mathbb{N}$ and
every unitary operator U on H_n $\exists$ q.c. that implements U and uses only gates from S.
Then, S is uncountable.

pf) Consider the rotation gates (such as $R_x(\theta)$) ∎

Then what can we do? $\Rightarrow$ Approximation.

First we define the distance between the operators.

Def U, V : unitary operator on H_n, $E(U,V) := \sup\{\|(U-V)|e\rangle\| : |e\rangle \in H_n, \langle e|e\rangle = 1\}$

$\Rightarrow$ same with operator norm in functional analysis.

The following proposition gives actual meaning to a $E(U,V)$

Proposition 4.8.3 U,V: unitary operators on H_n,

O: Observable with spectral decomposition $\sum \lambda P_\lambda$

Then, $\forall \lambda \in \Lambda$ and quantum state $|\psi\rangle \in H_n$, we have

$$\left| \langle U|\psi\rangle | P_\lambda | U|\psi\rangle \rangle - \langle V|\psi\rangle | P_\lambda | V|\psi\rangle \rangle \right| \leq E(U,V)$$

pf) Use Cauchy–Schwarz and Exercise 2.4.38: $\|P|\psi\rangle\| \leq \|\psi\|$. ☐

Now we can define universal sets of quantum gates

Def 4.8.4 (1) We say S is universal for a set T of unitary quantum operators if

$\forall \varepsilon > 0$, $U \in T$, $\exists$ unitary V which can be implemented (up to global fac)

by a q.c. that uses only gates from S, ancilla, erasure and $E(U-V) < \varepsilon$.

(2) We say that S is universal for quantum computation

if S is universal for the set of all unitary quantum operators.