A-II

## 3 b) Universal quantum gates and quantum complexity classes

→ The first notion that we will discuss is universality -

Are there universal sets of quantum gates? i.e. are there sets of quantum gates from which we can build any unitary transformation in the state (Hilbert) space of n qubits ?

→ Yes .

However there are ≠ versions of the notion of universality in the quantum case

→ Exact universality : the universal gate set can implement any n-qubit unitary exactly.

For instance :

* The (infinite) set of 2-qubit gates. (shown below)
* The (infinite) set of 1-qubit gates + one entangling 2-qubit gate (ex : CNOT)

The pb with this notion of universality is that in practice these quantum gates cannot be implemented with perfect precision and only a few of them can be implemented in a way which is resistant to errors (see part B of the course).

However it turns out that there are particular finite sets of gates which can approximate any unitary operation.

→ "Approximate" universality

Examples :

$\{H, T, CNOT\}$ , $\{H, CS\}$ , $\{H, S, CCNOT\}$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{+i\pi/4} \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & e^{+i\pi/2} \end{pmatrix}$$

↓

"phase gate"

CS = Controlled-S

CCNOT = Toffoli

These sets of gates are "approx." universal in the sense that any unitary can be arbitrarily well approximated using circuits with only gates from one of these sets.

(In fact $\{H, \text{CCNOT}\}$ is approx universal for all unitaries with <u>real</u> entries).

## * Exact universality of 2-qubit gates *

We will now show that any unitary op. acting on n-qubit states ( $\in U(2^n)$ ) can be achieved by circuits of 2-qubit gates -

There will 2 steps :

i) will show that any $2^n \times 2^n$ unitary can be expressed as product of 2-level unitaries.

ii) will show how to obtain any 2-level unitary from a circuit of 2-qubit unitaries.

Note: what we call 2-level unitary is actually a unitary transfo acting in the $2^n$-dim. space but acting non-trivially only on 2 basis states.

$\Rightarrow$ it has only 2 non zero off diago entries.

(acting "trivially" means acting like the identity operator, i.e. $\hat{O}$ acts trivially on $|\psi\rangle$ means $\hat{O}|\psi\rangle = |\psi\rangle$ )

$\Rightarrow$ a 2-level unitary $\hat{U}$ can be written as a direct sum

$$\hat{U} = \hat{U}_{(2)} \oplus \mathbb{1}_{(2^n-2)}$$

$\hookrightarrow$ acts on the span of $|i\rangle$ & $|j\rangle$ (n-qubit states)

Note a 2-qubit unitary acting on $2^n$-dim space is a tensor product:

$$\hat{U} = \hat{U}^{(4)} \otimes \mathbb{1}^{(2^{n-2})}$$

In the following, we denote $N \equiv 2^n$.
There are $N$ n-qubit basis states:

$$\begin{cases} |00\ldots00\rangle \equiv |0\rangle \\ |00\ldots01\rangle \equiv |1\rangle \\ \vdots \\ |11\ldots11\rangle \equiv |2^n-1\rangle = |N-1\rangle \end{cases}$$

i). Consider the action of $\hat{u} \in U(N)$ on basis state $|0\rangle$:

$$\hat{u}|0\rangle = \sum_{i=0}^{N-1} a_i |i\rangle$$

We can see that $\hat{u}|0\rangle = \hat{v}_{(0)}|0\rangle$ where $\hat{v}_{(0)} = W_{N-2} \cdots W_0$ is a product of $(N-1)$ 2-level unitaries acting as follows:

$$W_0|0\rangle = a_0|0\rangle + b_0|1\rangle$$

$$W_1\left(a_0|0\rangle + b_0|1\rangle\right) = a_0|0\rangle + a_1|1\rangle + b_1|2\rangle$$

$$W_2\left(a_0|0\rangle + a_1|1\rangle + b_1|2\rangle\right)$$

$$= a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + b_2|3\rangle$$

$$\vdots$$

$$W_{N-2}\left(\cdots + b_{N-3}|N-2\rangle\right) = \cdots + a_{N-2}|N-2\rangle + a_{N-1}|N-1\rangle$$

it is clear that the $W_i$'s are 2-level unitaries:

they take $b_{i-1}|i\rangle \longmapsto a_i|i\rangle + b_i|i+1\rangle$

ie only act non-trivially on 2 basis states.

Now define $U_1 = V_{(0)}^{-1} U$

$$\Rightarrow U_1 |0\rangle = V_{(0)}^{-1} U |0\rangle$$
$$= V_{(0)}^{-1} V_{(0)} |0\rangle$$
$$= |0\rangle$$

$\Rightarrow U_1$ only acts non trivially on the $(N-1)$-dim span of $\{|1\rangle \ldots |N-1\rangle\}$ -

- Now we can repeat the same procedure above and construct $V_{(1)}$ as product of $(N-2)$ 2-level unitaries such that

$$\begin{cases} V_{(1)} |0\rangle = U_1 |0\rangle = |0\rangle \\ V_{(1)} |1\rangle = U_1 |1\rangle \end{cases}$$

$\Rightarrow$ then define $U_2 = V_{(1)}^{-1} U_1$

$$\Rightarrow \begin{cases} U_2 |0\rangle = V_{(1)}^{-1} U_1 |0\rangle = V_{(1)}^{-1} V_{(1)} |0\rangle = |0\rangle \\ U_2 |1\rangle = V_{(1)}^{-1} U_1 |1\rangle = V_{(1)}^{-1} V_{(1)} |1\rangle = |1\rangle \end{cases}$$

$\Rightarrow U_2$ preserves $|0\rangle$ and $|1\rangle$, and thus acts non-trivially (a priori) on the span of $\{|2\rangle, |3\rangle \ldots |N-1\rangle\}$.

- We can proceed in this way and construct

$V_{(2)}$ → product of $(N-3)$ $2\times 2$ unitaries which acts on $|0\rangle, |1\rangle, |2\rangle$ as $U_2$

$\Rightarrow U_3 = V_{(2)}^{-1} U_2$ acts non trivially on span of $\{|3\rangle \dots |N-1\rangle\}$

$V_{(3)}$ → prod of $(N-4)$ $2\times 2$ unitaries.
---

⋮

$V_{(N-2)}$ → $N-(N-2)-1 = 1$ $2\times 2$ unitary which acts on $|0\rangle, |1\rangle \dots |N-2\rangle$ as $U_{N-2}$

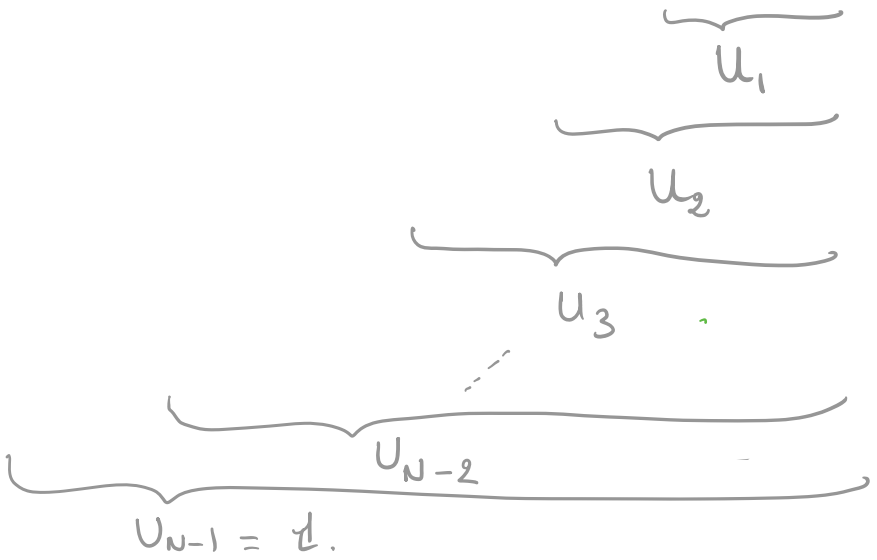
$\Rightarrow U_{N-1} = V_{(N-2)}^{-1} U_{N-2}$ acts trivially on $|0\rangle, |1\rangle, \dots |N-2\rangle$ → only $|N-1\rangle$ remains

$\Rightarrow U_{N-1}$ actually acts trivially on the whole span of $\{|0\rangle, \dots, |N-1\rangle\}$.

$\Rightarrow U_{N-1} = \mathbb{1}$.

$\Rightarrow$ In the end:

$$V_{(N-2)}^{-1} V_{(N-3)}^{-1} \cdots V_{(2)}^{-1} V_{(1)}^{-1} V_{(0)}^{-1} U = \mathbb{1}.$$




$\Rightarrow$ $U = V_{(0)} V_{(1)} V_{(2)} \cdots V_{(N-3)} V_{(N-2)}$

$\Rightarrow$ $U$ is a product of

$$(N-1) + (N-2) + (N-3) \cdots + 2 + 1$$

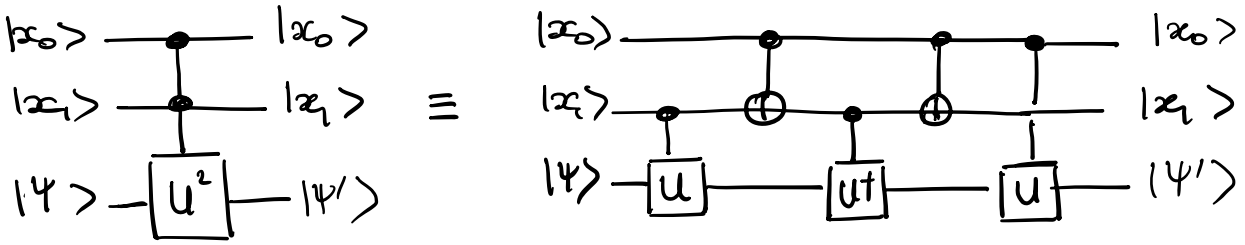
$$= \sum_{k=1}^{N-1} k = \frac{N(N-1)}{2} \text{ 2-level unitaries.}$$

$\Rightarrow$ we have shown step i), i.e. that any unitary can be expressed as product of 2-level unitary.

Now will show: (⚠ in what follows, will use U, V to denote 1-qubit gates)

ii) how to obtain any 2-level unitary from a circuit of 2-qubit unitaries.

It will be useful to use the following circuit identity: $(x_i = 0, 1)$




⇒ CC($U^2$) can be expressed in terms of C(U), C($U^\dagger$), CNOT (= C(X)) gates.

(Controlled-Controlled-$U^2$)

left circuit

$$|\psi'\rangle = U^2 |\psi\rangle \text{ if } |x_1 x_0\rangle = |11\rangle$$

right circuit

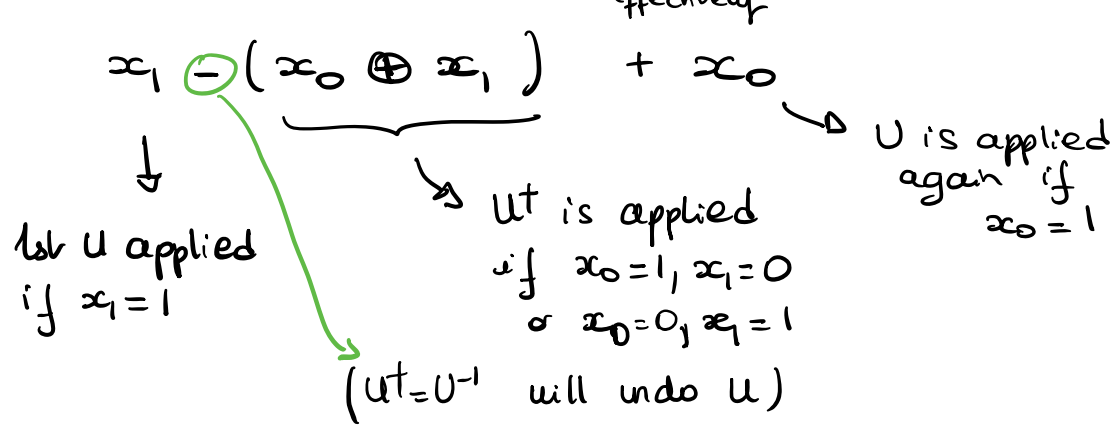
case $|x_1 x_0\rangle = |00\rangle \Rightarrow |\psi'\rangle = |\psi\rangle$

case $|x_1 x_0\rangle = |01\rangle \Rightarrow |\psi'\rangle = U U^\dagger |\psi\rangle = |\psi\rangle$

case $|x_1 x_0\rangle = |10\rangle \Rightarrow |\psi'\rangle = U^\dagger U |\psi\rangle = |\psi\rangle$

case $|x_1 x_0\rangle = |11\rangle \Rightarrow |\psi'\rangle = U U |\psi\rangle = U^2 |\psi\rangle$

Another way to see this is to count the number of times that $U$ is applied, this is:




$$= x_1 - (x_0 + x_1 - 2x_1x_0) + x_0$$

$$= 2x_1x_0 .$$

$\Rightarrow$ $U$ is applied twice if $x_0 = x_1 = 1$ and is not applied otherwise.

(Reminder $x \oplus y$ is the addition modulo 2)
$$x \oplus y = x + y - 2xy$$

Every unitary $V$ has a square root $U$ such that $V = U^2$.

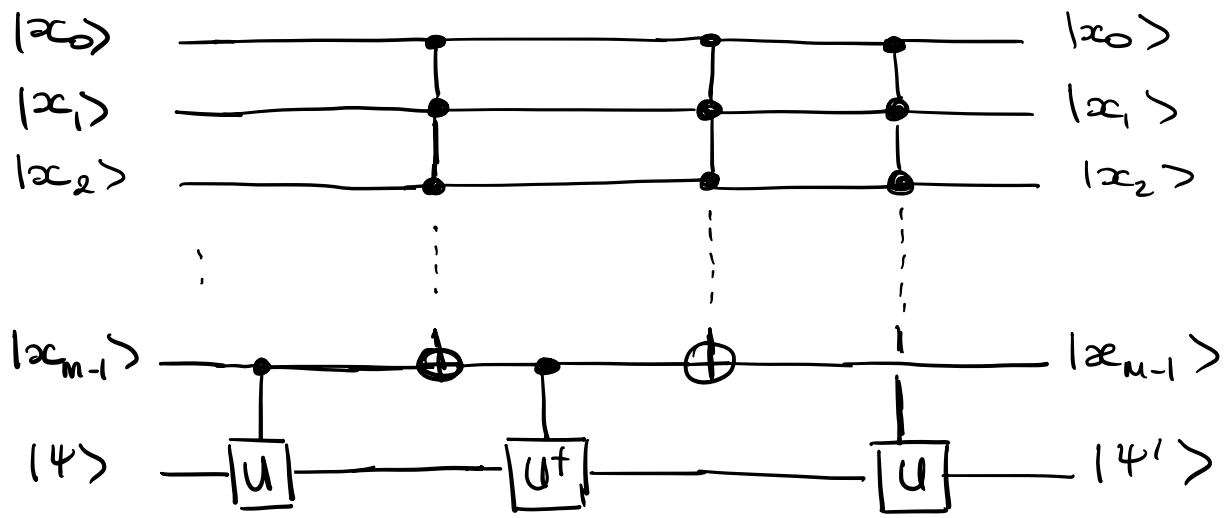
$\Rightarrow$ the construction shows that, using 2-qubit gates, we can achieve $CC(V)$ (Controlled-Controlled-$V$) (for any 1-qubit gate $V$).

⇒ This can be generalized to find a circuit that constructs $\underbrace{CC\ldots C}_{m \text{ times}}(U^2) = C^m(U^2)$

using $C^{m-1}(U)$, $C^{m-1}(X)$ ($\equiv C^{m-1}(\text{NOT})$), $C(U)$, $C(U^\dagger)$ gates.

In particular, replace

- all $C(X)$ by $C^{m-1}(X)$
- the last $C(U)$ by $C^{m-1}(U)$



$\Rightarrow$ the power of $U$ that is applied is :

$$x_{m-1} - (x_{m-1} \oplus x_0 x_1 x_2 \dots x_{m-2}) + x_0 x_1 \dots x_{m-2}$$

$x_{m-1}$ $\downarrow$ $U$ — $x_0 x_1 \dots x_{m-2}$ $\downarrow$ $U^\dagger$ — $x_0 x_1 \dots x_{m-2}$ $\downarrow$ last $U$

( if $x_{m-1} = 1$ & not all $x_0 \dots x_{m-2} = 1$
or
if $x_{m-1} = 0$ & all $x_0 \dots x_{m-2} = 1$

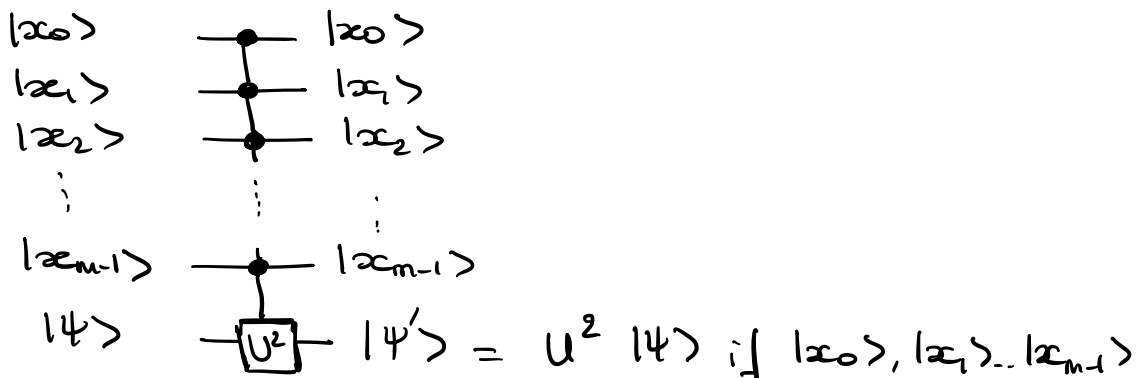
$\Rightarrow$ This is equal to :

$$x_{m-1} - (x_{m-1} + x_0 x_1 \dots x_{m-2} - 2 x_0 x_1 \dots x_{m-2} x_{m-1})$$
$$+ x_0 x_1 \dots x_{m-2}$$
$$= 2 x_0 x_1 \dots x_{m-2} x_{m-1}$$

$\Rightarrow$ $U$ is effectively applied
$(2 x_0 x_1 \dots x_{m-2} x_{m-1})$ times

i.e. ( is applied twice if all qubits states $|x_0\rangle, |x_1\rangle, \dots, |x_{m-1}\rangle = |1\rangle$
is not applied otherwise.

and this is exactly what the $C^m(U^2)$ gate does:




Using the construction recursively

- with 2-qubit gates $\longrightarrow$ can construct $C^2(U^2)$
  $C(U)$, $C(U^\dagger)$, $\underbrace{C(X)}_{CNOT}$ $= C^2(V)$

- with $C^2(U^2)$, $\underbrace{C^2(X)}_{CCNOT}$, $C(U)$, $C(U^\dagger)$ $\longrightarrow$ $C^3(U^2)$
  $= C^3(V)$

- with $C^3(U^2)$, $C^3(X)$, $C(U)$, $C(U^\dagger)$ $\longrightarrow$ $C^4(U^2)$
  $= C^4(V)$

  ⋮

  etc until $\longrightarrow$ $C^{n-1}(V)$

⇒ We have shown how to construct

$n$-qubit gates $C^{n-1}(V)$ for any $V$

using a circuit of 2-qubit gates.

(in fact $C(V)$, $C(V^\dagger)$, $C(X)$)

We have also shown i) any $2^n \times 2^n$ unitary can be expressed as product of 2-level unitaries.

Now we just need to show that any 2-level unitary can be constructed from $C^{n-1}(V)$ gates, and possibly other 2-qubit gates.

We note that $C^{n-1}(V)$ is in fact a $2 \times 2$ unitary : it applies $V$ in the 2-dim space spanned by

$$\{|11\ldots110\rangle, |11\ldots111\rangle\}$$

(control qubits. → target. ; ctrl → target)

($C^{n-1}(V)$ acts non-trivially only on the span of these two states → this is the def of a 2-level unitary)

If we want to apply $V$ in the space spanned by other computational basis states ↑ n_qubit

say $\{|i\rangle, |j\rangle\}$, we can use a permutation $\Sigma$ of the computational basis states with the action

$$\Sigma : |i\rangle \longmapsto |11\ldots110\rangle$$
$$|j\rangle \longmapsto |11\ldots111\rangle$$

constructing $\Sigma^{-1}\ C^{n-1}(V)\ \Sigma$ → any 2 level unitary can be written like this since $V$ can be any 1-qubit gate.

which is $V$ acting on span of $\{|i\rangle, |j\rangle\}$

And we saw before (when discussing reversible computations) that permutations can be obtained from Toffoli (CCNOT = $C^2(X)$) which is itself of the type $C^m(V)$

⇒ That completes the proof.

To summarize we have shown:

i) any $2^n \times 2^n$ unitary can be expressed as product of 2-level unitaries.

ii) . that any 2-level unitary can be constructed from $C^m(V)$ gates $(m \leq n-1)$

. and that any $C^m(V)$ can be constructed from 2-qubit gates
$(C(U), C(U^\dagger), C(X))$ $(V = U^2)$

$\Rightarrow$ any 2-level unitary can be constructed from 2 qubit gates

$\Rightarrow$ Any $2^n \times 2^n$ unitary (i.e. any unitary transforming on n-qubit states) can be constructed from 2-qubit gates.

$\Rightarrow$ The (infinite) set of 2-qubit gates is exactly universal.

* In fact we proven a stronger result: that the $(\infty)$ set of 2-qubit gates $C(U)$ (where $U$ can be any 1-qubit gate) is exactly universal.

* It can also be shown that the infinite set of single-qubit gates together with the CNOT $= C(X)$ gate (or any other entangling 2-qubit gate) constitute an exactly universal set.

## * Approximate universality *

In practice, only a few gates can be applied in a way where the error spreads in a controllable way (see part B of the course).

A finite (discrete) set of gates cannot implement any unitary operation exactly (since the set of unitary op is infinite (continuous)), however a finite set can approximate any unitary operation.

→ What does it mean to approx a unitary op?

Suppose $U$ is the "target" unitary operator we wish to implement, and $\tilde{U}$ is the actual operator implemented in practice

Then the actual state $|\tilde{\psi}\rangle = \tilde{U}|\psi_0\rangle$ (initial state) at the end of the computation will differ from the ideal state $|\psi\rangle = U|\psi_0\rangle$.

We define the **error**

$$E(U,\tilde{U}) = \max_{|\psi_0\rangle} \| (U-\tilde{U})|\psi_0\rangle \|$$

where the maximum is over all normalized quantum states $|\psi_0\rangle$ in the Hilbert space.

It can be shown (→ see below) that if $E(U,\tilde{U})$ is small, then any measurement performed on $\tilde{U}|\psi_0\rangle$ will give approximately the same measurement statistics as if the measurement was performed on $U|\psi_0\rangle$ $(\forall |\psi_0\rangle)$

---

Proof:

Still consider here that we have an isolated system (but can be generalized for open)

$\hat{P}_n$ = projector onto eigenvalue $a_n$ of observable $\hat{A}$

$p_n^{(U)} / p_n^{(\tilde{U})}$ = probability of obtaining an as outcome of the measurem$^t$ if $U/\tilde{U}$ was performed before.

$$\begin{cases} p_n^{(U)} = \langle\psi_0| U^\dagger \hat{P}_n U |\psi_0\rangle \\ p_n^{(\tilde{U})} = \langle\psi_0| \tilde{U}^\dagger \hat{P}_n \tilde{U} |\psi_0\rangle \end{cases}$$

$$\Rightarrow \left| p_n^{(u)} - p_n^{(\tilde{u})} \right| =$$

$$= \left| \langle \psi_0 | u^\dagger \hat{P}_n u | \psi_0 \rangle - \langle \psi_0 | \tilde{u}^\dagger \hat{P}_n \tilde{u} | \psi_0 \rangle \right|$$

$$= \Big| \langle \psi_0 | u^\dagger \hat{P}_n (u - \tilde{u}) | \psi_0 \rangle + \underline{\langle \psi_0 | u^\dagger \hat{P}_n \tilde{u} | \psi_0 \rangle}$$

$$+ \langle \psi_0 | (u - \tilde{u})^\dagger \hat{P}_n \tilde{u} | \psi_0 \rangle - \underline{\langle \psi_0 | u^\dagger \hat{P}_n \tilde{u} | \psi_0 \rangle} \Big|$$

$$= \left| \langle \psi_0 | u^\dagger \hat{P}_n | \Delta \rangle + \langle \Delta | \hat{P}_n \tilde{u} | \psi_0 \rangle \right|$$

where $|\Delta\rangle \equiv (u - \tilde{u}) |\psi_0\rangle$

$$\leq \underbrace{\left| \langle \psi_0 | u^\dagger \hat{P}_n | \Delta \rangle \right|}_{\leq \| |\Delta\rangle \|} + \underbrace{\left| \langle \Delta | \hat{P}_n \tilde{u} | \psi_0 \rangle \right|}_{\leq \| |\Delta\rangle \|}$$

↑ Cauchy Schwarz inequality

$\| |\Delta\rangle \| = \sqrt{\langle \Delta | \Delta \rangle}$

$$\leq 2 \| |\Delta\rangle \|$$

$$\leq 2 \max_{|\psi_0\rangle} \| |\Delta\rangle \| = 2 E(u, \tilde{u})$$

$$\Rightarrow \quad |p_n^{(U)} - p_n^{(\tilde{U})}| \leq 2\, E(U,\tilde{U})$$

$\Rightarrow$ we see that if the error $E(U,\tilde{U})$ is small then $|p_n^{(U)} - p_n^{(\tilde{U})}|$ is also small, meaning that the $\neq$ce in proba outcomes is small.

---

It can also be shown that if we perform a sequence of gates $\tilde{U}_1, \dots, \tilde{U}_m$ intended to approx $U_1, \dots U_m$ then the error adds at most linearly:

$$E(U_m U_{m-1} \cdots U_1 \,,\, \tilde{U}_m \tilde{U}_{m-1} \cdots \tilde{U}_1) \leq \sum_{j=1}^{m} E(U_j, \tilde{U}_j)$$

---

ex $\underline{m=2}$ $\quad E(U_2 U_1 \,,\, \tilde{U}_2 \tilde{U}_1) = \max \| (U_2 U_1 - \tilde{U}_2 \tilde{U}_1) |\psi_0\rangle \|$

$$= \max \Big( \| (U_2 U_1 - \tilde{U}_2 U_1) |\psi_0\rangle + (\tilde{U}_2 U_1 - \tilde{U}_2 \tilde{U}_1) |\psi_0\rangle \| \Big)$$

$$\leq \max \Big( \| (U_2 - \tilde{U}_2) U_1 |\psi_0\rangle \| + \| \tilde{U}_2 (U_1 - \tilde{U}_1) |\psi_0\rangle \| \Big)$$

$$\leq E(U_2, \tilde{U}_2) + E(U_1, \tilde{U}_1)$$

—— the result for any m follows.

→ Combine the 2 results:

⇒ The proba of ≠ measurement outcomes obtained from the approx. circuit will be within a "fault tolerance" $\Delta > 0$ of the correct proba if

$$E(U_j, \tilde{U}_j) \leq \frac{\Delta}{2m}$$

⇒ need to improve the accuracy of the gates linearly with the circuit size

⇒ not too bad, but also not too good - still need better & better gates for larger and larger computations

Note:

In fact, the theory of quantum error correction and fault tolerant QC (see part B of the course) will tell us that it suffices for the error per gate to be less than a sufficiently small cst (indep of $m$), at the cost of an increase in the circuit size that is $O(\text{poly}(\log m))$.