# 5. Quantum circuits

(a) Quantum circuit model (KLM 4.1, NC 1.3.4) ✓

(b) Quantum gates (NC 4.2-4.3, KLM 4.2) ✓

(c) Continuous universal set of quantum gates (reading) (NC 4.5.1-4.5.2, KLM 4.3)

(d) Quantum gate approximations (NC Box 4.1, KLM 4.3)

(e) Finite universal set of q. gates (NC 4.5.3, KLM 4.3)

(f) Efficiency & Kitaev-Solovay thm (NC App 3, KLM 4.4)

(g) Quantum circuits for measurements (reading/defer) (KLM 4.5*)

(h) Hardness of approximating most unitaries (reading) (NC 4.5.6)

The unitaries acting on a Hilbert space form a continuous set. Is a continuous set of gates needed for universality (e.g., CNOT+all 1-qubit gates)?

Idea: approximating any unitary to arbitrary accuracy is good enough.

<u>How to measure the quality of approximate unitaries?</u>

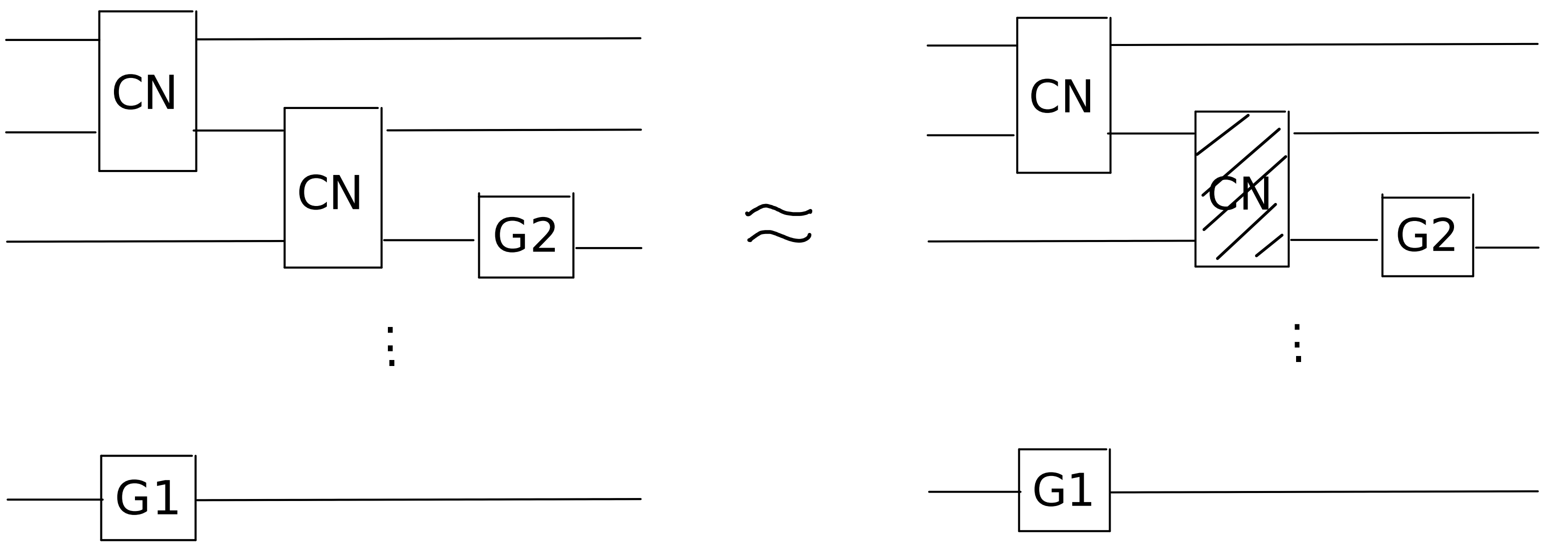
Depends on the goal !

Here: replace one gate (that we want) by another (that we can apply) in a circuit without affecting the correctness of the "computation."

# How to measure the quality of approximate unitaries?

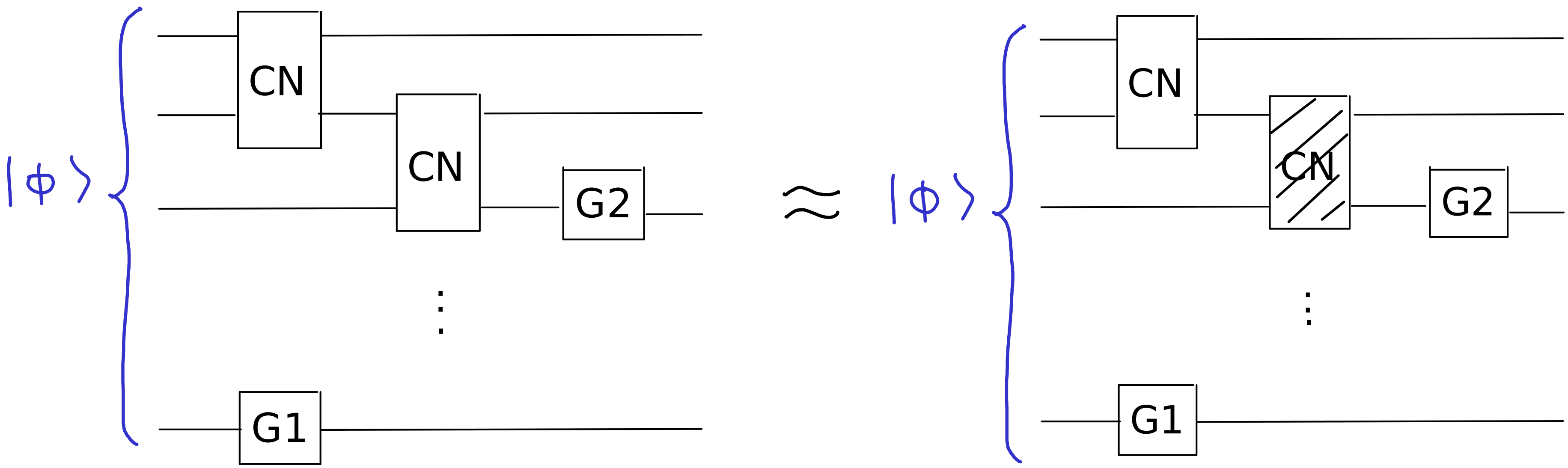
Depends on the goal !

Here: replace one gate (that we want) by another (that we can apply) in a circuit without affecting the correctness of the "computation."



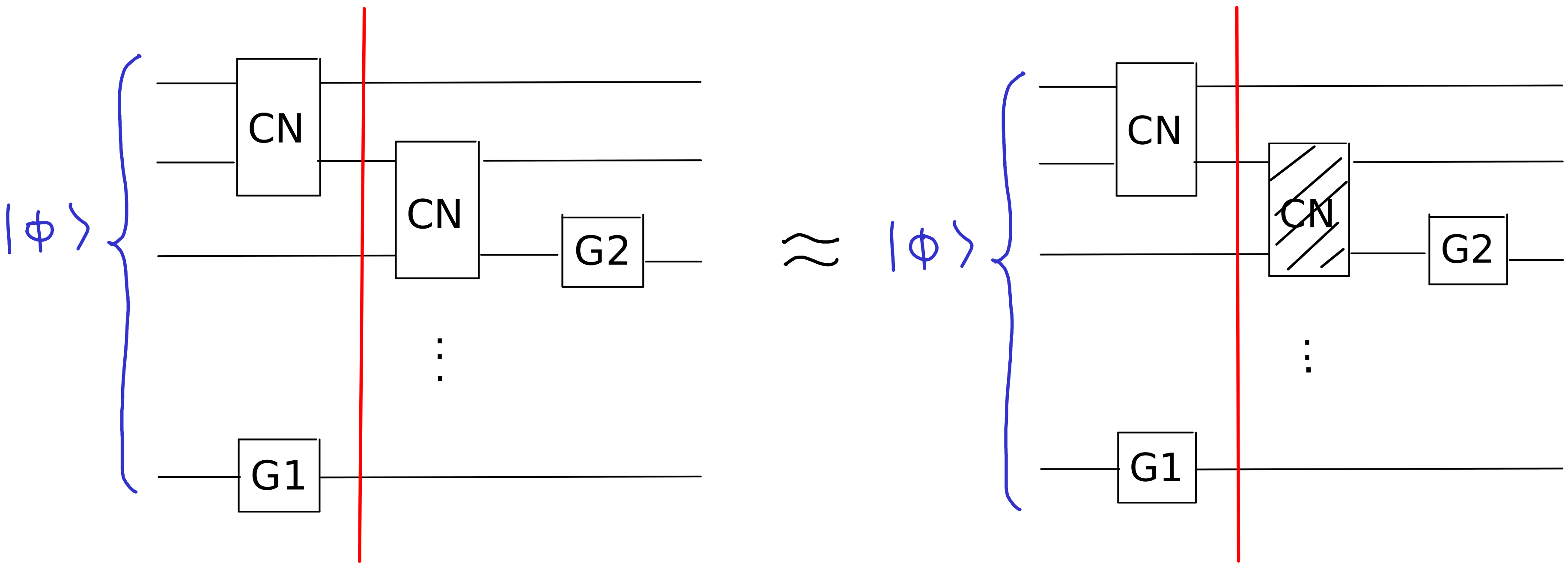
## How to measure the quality of approximate unitaries?

If, for all possible input $|\phi\rangle$ , the outputs from the two circuits are "similar", our computation is not too affected and the approximation is good.



## How to measure the quality of approximate unitaries?

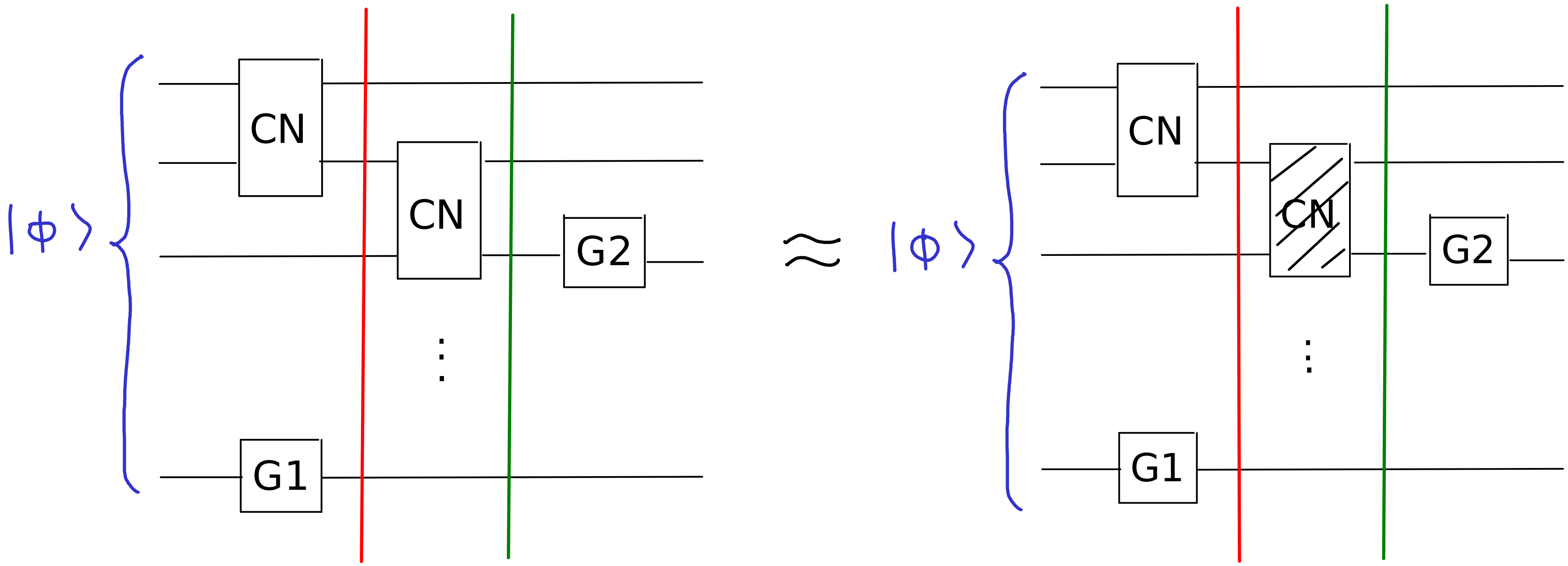
If, for all possible input $|\phi\rangle$, the outputs from the two circuits are "similar", our computation is not too affected and the approximation is good.




Up to red stage: identical states in both circuits

# How to measure the quality of approximate unitaries?

If, for all possible input $|\phi\rangle$ , the outputs from the two circuits are "similar", our computation is not too affected and the approximation is good.




Up to red stage: identical states in both circuits

Green stage onwards, identical computation

Suffices if the states at the green stage are similar.

# How to measure the quality of approximate unitaries?

Definition: the error of approximating U by V is

$$E^*(U,V) = \max_{|\psi\rangle_{RS}} \left\| (I \otimes U)|\psi\rangle - (I \otimes V)|\psi\rangle \right\|$$

where U, V act on system S, and system R is arbitrary.

($|\psi\rangle_{RS}$ unit vector.)

Euclidean norm

# How to measure the quality of approximate unitaries?

Definition: the error of approximating U by V is

$$E^*(U,V) = \max_{|\psi\rangle_{RS}} \| I \otimes U |\psi\rangle - I \otimes V |\psi\rangle \|$$

where U, V act on system S, and system R is arbitrary.

($|\psi\rangle_{RS}$ unit vector.)

For our circuit:
S = qubit(s) acted on by the gate to be approximate
R = all other qubits

$|\psi\rangle_{RS}$ the worst case state right before the gate.

## Indistinguisability:

Exercise: for two unit vectors $|a\rangle, |b\rangle$

$$\| |a\rangle - |b\rangle \| = \sqrt{2}\sqrt{1 - \mathrm{Re}\langle a|b\rangle}$$

## Indistinguisability:

Exercise: for two unit vectors $|a\rangle, |b\rangle$

$$\| |a\rangle - |b\rangle \| = \sqrt{2}\sqrt{1 - \mathrm{Re}\langle a|b\rangle}$$

Recall: Holevo-Helstrom theorem

If each of $|\psi_1\rangle, |\psi_2\rangle$ is chosen with probability 1/2,

then the max prob to distinguish the states is

$$\frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2}$$

## Indistinguisability:

Exercise: for two unit vectors $|a\rangle, |b\rangle$

$$\| |a\rangle - |b\rangle \| = \sqrt{2}\sqrt{1 - \mathrm{Re}\langle a|b\rangle}$$

Recall: Holevo-Helstrom theorem

If each of $|\psi_1\rangle, |\psi_2\rangle$ is chosen with probability 1/2,

then the max prob to distinguish the states is

$$\frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2} \leq \frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\psi_1|\psi_2\rangle|}\sqrt{1 + |\langle\psi_1|\psi_2\rangle|}$$

## Indistinguisability:

Exercise: for two unit vectors $|a\rangle, |b\rangle$

$$\| |a\rangle - |b\rangle \| = \sqrt{2}\sqrt{1 - \mathrm{Re}\langle a|b\rangle}$$

Recall: Holevo-Helstrom theorem

If each of $|\psi_1\rangle, |\psi_2\rangle$ is chosen with probability 1/2,

then the max prob to distinguish the states is

$$\frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2} \leq \frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\psi_1|\psi_2\rangle|}\sqrt{1 + |\langle\psi_1|\psi_2\rangle|}$$

$$\leq \frac{1}{2} + \frac{1}{2}\frac{1}{\sqrt{2}}\| |\psi_1\rangle - |\psi_2\rangle \|\sqrt{2}$$

# Indistinguisability:

Exercise: for two unit vectors $|a\rangle, |b\rangle$

$$\| |a\rangle - |b\rangle \| = \sqrt{2}\sqrt{1 - \mathrm{Re}\langle a|b\rangle}$$

Recall: Holevo-Helstrom theorem

If each of $|\psi_1\rangle, |\psi_2\rangle$ is chosen with probability 1/2,

then the max prob to distinguish the states is

$$\frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2} \leq \frac{1}{2} + \frac{1}{2}\sqrt{1 - |\langle\psi_1|\psi_2\rangle|}\sqrt{1 + |\langle\psi_1|\psi_2\rangle|}$$

$$\leq \frac{1}{2} + \frac{1}{2}\frac{1}{\sqrt{2}}\| |\psi_1\rangle - |\psi_2\rangle \|\sqrt{2}$$

So, $I\otimes U|\psi\rangle$, $I\otimes V|\psi\rangle$ can be distinguished with prob

$$\leq \frac{1}{2} + \frac{1}{2}E^*(U, V)$$

so no one can tell if U or V has been applied if E* small

# How to evaluate this error?

$$E^*(U,V) = \max_{|\psi\rangle_{RS}} \| I \otimes U |\psi\rangle - I \otimes V |\psi\rangle \|$$

R is arbitrary

i.e., We max over all possible R.
Non-trivial: we can limit dim(R) to dim(S) without affecting the value of the optimization (deferring the proof which needs more about the Schmidt decomposition).

Note the difference from NC etc.
R needed to compose approximations.

# How to evaluate this error?

$$E^*(U,V) = \max_{|\psi\rangle_{RS}} \| I \otimes U |\psi\rangle - I \otimes V |\psi\rangle \|$$

R is arbitrary

Definition:

$$E(U,V) = \max_{|\mu\rangle_S} \| U|\mu\rangle - V|\mu\rangle \|$$

## How to evaluate this error?

$$E^*(U,V) = \max_{|\psi\rangle_{RS}} \| I \otimes U|\psi\rangle - I \otimes V|\psi\rangle \|$$

R is arbitrary

Definition:

$$E(U,V) = \max_{|\mu\rangle_{S}} \| U|\mu\rangle - V|\mu\rangle \|$$

Theorem: E*(U,V) = E(U,V) !

**Theorem**: $E^*(U,V) = E(U,V)$

Proof:

(1) $E^*(U,V)$ is optimized over a larger range compared to $E(U,V)$ so $E^*(U,V) \geqslant E(U,V)$.

<u>Theorem</u>: $E^*(U,V) = E(U,V)$

Proof:

(1) $E^*(U,V)$ is optimized over a larger range compared to $E(U,V)$ so $E^*(U,V) \geq E(U,V)$.

(2) For any system R, let $|\psi\rangle_{RS}$ attain the max in $E^*(U,V)$.

NB. for fixed R, the optimization is compact so $|\psi\rangle$ exists.

Theorem: $E^*(U,V) = E(U,V)$

Proof:

(1) $E^*(U,V)$ is optimized over a larger range compared to $E(U,V)$ so $E^*(U,V) \geq E(U,V)$.

(2) For any system R, let $|\psi\rangle_{RS}$ attain the max in $E^*(U,V)$.

NB. for fixed R, the optimization is compact so $|\psi\rangle$ exists.

(3) Let $\{|e_i\rangle\}_{i=1}^{r}$ be a basis for R (dim r). Express

$$|\psi\rangle_{RS} = \sum_{i=1}^{r} \alpha_i |e_i\rangle \otimes |\eta_i\rangle$$

where $\alpha_i \geq 0$, $\sum_{i=1}^{r} \alpha_i^2 = 1$, $|\eta_i\rangle$ are unit vectors on S.

(4) $E^*(U,V)^2 = \| I \otimes U |\psi\rangle - I \otimes V |\psi\rangle \|^2$

$\because |\psi\rangle$ attains max

(4) $$E^*(U,V)^2 = \| I\otimes U|\psi\rangle - I\otimes V|\psi\rangle \|^2$$

$\because |\psi\rangle$ attains max

$$= \| I\otimes (U-V)|\psi\rangle \|^2$$

$$= \langle\psi| I\otimes (U-V)^\dagger \cdot I\otimes (U-V) |\psi\rangle$$

(4) $$E^*(U,V)^2 = \| I\otimes U|\psi\rangle - I\otimes V|\psi\rangle\|^2$$

$\because |\psi\rangle$ attains max

$$= \| I\otimes (U-V)|\psi\rangle\|^2$$

$$= \langle\psi| I\otimes(U-V)^\dagger \cdot I\otimes(U-V)|\psi\rangle$$

$$= \sum_{j=1}^{r} \alpha_j \langle e_j| \otimes \langle \eta_j| \; I\otimes(U-V)^\dagger \cdot I\otimes(U-V) \sum_{i=1}^{r} \alpha_i |e_i\rangle \otimes |\eta_i\rangle$$

(4) $E^*(U,V)^2 = \| I\otimes U|\psi\rangle - I\otimes V|\psi\rangle \|^2$

$\because |\psi\rangle$ attains max

$$= \| I\otimes (U-V)|\psi\rangle \|^2$$

$$= \langle\psi| I\otimes (U-V)^\dagger \cdot I\otimes (U-V) |\psi\rangle$$

$$= \sum_{j=1}^{r} \alpha_j \langle e_j| \otimes \langle \eta_j| \; I\otimes (U-V)^\dagger \cdot I\otimes (U-V) \sum_{i=1}^{r} \alpha_i |e_i\rangle \otimes |\eta_i\rangle$$

$$= \sum_{j=1}^{r} \alpha_j \langle e_j| \otimes \langle \eta_j| (U-V)^\dagger \; \sum_{i=1}^{r} \alpha_i |e_i\rangle \otimes (U-V)|\eta_i\rangle$$

(4) $E^*(U,V)^2 = \| I\otimes U|\psi\rangle - I\otimes V|\psi\rangle \|^2$

$\because |\psi\rangle$ attains max

$$= \| I\otimes (U-V)|\psi\rangle \|^2$$

$$= \langle\psi| I\otimes (U-V)^\dagger \cdot I\otimes (U-V) |\psi\rangle$$

$$= \sum_{j=1}^{r} \alpha_j \langle e_j| \otimes \langle \eta_j| \, I\otimes (U-V)^\dagger \cdot I\otimes (U-V) \sum_{i=1}^{r} \alpha_i |e_i\rangle \otimes |\eta_i\rangle$$

$$= \sum_{j=1}^{r} \alpha_j \langle e_j| \otimes \langle \eta_j| (U-V)^\dagger \sum_{i=1}^{r} \alpha_i |e_i\rangle \otimes (U-V)|\eta_i\rangle$$

$$= \sum_{i=1}^{r} \alpha_i^2 \langle \eta_i| (U-V)^\dagger (U-V) |\eta_i\rangle$$

$$(4)\quad E^*(U,V)^2 = \| I\otimes U|\psi\rangle - I\otimes V|\psi\rangle \|^2$$

$\because |\psi\rangle$ attains max

$$= \| I\otimes (U-V)|\psi\rangle \|^2$$

$$= \langle\psi| I\otimes(U-V)^\dagger \cdot I\otimes(U-V)|\psi\rangle$$

$$= \sum_{j=1}^{r} \alpha_j \langle e_j|\otimes\langle\eta_j|\, I\otimes(U-V)^\dagger \cdot I\otimes(U-V) \sum_{i=1}^{r}\alpha_i |e_i\rangle\otimes|\eta_i\rangle$$

$$= \sum_{j=1}^{r} \alpha_j \langle e_j|\otimes\langle\eta_j|(U-V)^\dagger \sum_{i=1}^{r}\alpha_i |e_i\rangle\otimes(U-V)|\eta_i\rangle$$

$$= \sum_{i=1}^{r} \alpha_i^2 \langle\eta_i|(U-V)^\dagger(U-V)|\eta_i\rangle$$

$$= \sum_{i=1}^{r} \alpha_i^2 \|(U-V)|\eta_i\rangle\|^2$$

$$(4)\quad E^*(U,V)^2 \overset{\because\ |\psi\rangle \text{ attains max}}{=} \| I\otimes U|\psi\rangle - I\otimes V|\psi\rangle \|^2$$

$$= \| I\otimes (U-V)|\psi\rangle \|^2$$

$$= \langle\psi| I\otimes (U-V)^\dagger \cdot I\otimes (U-V)|\psi\rangle$$

$$= \sum_{j=1}^{r} \alpha_j \langle e_j| \otimes \langle\eta_j|\ I\otimes (U-V)^\dagger \cdot I\otimes (U-V) \sum_{i=1}^{r} \alpha_i |e_i\rangle \otimes |\eta_i\rangle$$

$$= \sum_{j=1}^{r} \alpha_j \langle e_j| \otimes \langle\eta_j| (U-V)^\dagger \sum_{i=1}^{r} \alpha_i |e_i\rangle \otimes (U-V)|\eta_i\rangle$$

$$= \sum_{i=1}^{r} \alpha_i^2 \langle\eta_i| (U-V)^\dagger (U-V)|\eta_i\rangle$$

$$= \sum_{i=1}^{r} \alpha_i^2 \| (U-V)|\eta_i\rangle \|^2 \leq \underbrace{\sum_{i=1}^{r} \alpha_i^2}_{=1} E(U,V)^2 .$$

## Composition of approximations:

Suppose a gate U1 on S1 is approximated by V1, and then a gate U2 on S2 is approximate by V2.

What is the error of the two step approximation, in terms of the error of each step?

## Composition of approximations:

Suppose a gate U1 on S1 is approximated by V1, and then a gate U2 on S2 is approximate by V2.

What is the error of the two step approximation, in terms of the error of each step?

$$E\left( (U_{2\,S_2} \otimes I_{R_2})(U_{1\,S_1} \otimes I_{R_1}) \,,\, (V_{2\,S_2} \otimes I_{R_2})(V_{1\,S_1} \otimes I_{R_1}) \right)$$

E without * when R1, R2 explicitly included

## Composition of approximations:

Suppose a gate U1 on S1 is approximated by V1, and then a gate U2 on S2 is approximate by V2.

What is the error of the two step approximation, in terms of the error of each step?

$$E\left( (U_{2\,S_2} \otimes I_{R_2})(U_{1\,S_1} \otimes I_{R_1}),\ (V_{2\,S_2} \otimes I_{R_2})(V_{1\,S_1} \otimes I_{R_1}) \right)$$

E without * when R1, R2 explicitly included

$$\leqslant E\left( (U_{2\,S_2} \otimes I_{R_2}),\ (V_{2\,S_2} \otimes I_{R_2}) \right) + E\left( (U_{1\,S_1} \otimes I_{R_1}),\ (V_{1\,S_1} \otimes I_{R_1}) \right)$$

see NC for proof

## Composition of approximations:

Suppose a gate U1 on S1 is approximated by V1, and then a gate U2 on S2 is approximate by V2.

What is the error of the two step approximation, in terms of the error of each step?

$$E\left( (U_{2\,S_2} \otimes I_{R_2})(U_{1\,S_1} \otimes I_{R_1}),\ (V_{2\,S_2} \otimes I_{R_2})(V_{1\,S_1} \otimes I_{R_1}) \right)$$

E without * when R1, R2 explicitly included

$$\leq E\left( (U_{2\,S_2} \otimes I_{R_2}),\ (V_{2\,S_2} \otimes I_{R_2}) \right) + E\left( (U_{1\,S_1} \otimes I_{R_1}),\ (V_{1\,S_1} \otimes I_{R_1}) \right)$$

see NC for proof

$$= E(U_2, V_2) + E(U_1, V_1).$$

So, error of composition is subadditive, & without *.

Recursively, for a circuit with m gates each with error e', the overall circuit error is at most e'm.
To have overall error e, it suffices to implement each gate with error at most e/m.

Definition: A set of gates G is universal for quantum computation, if for any positive integer n, any n-qubit unitary U, and any e > 0, there are $V_1, V_2, \ldots, V_k$ in G

s.t. $E(U, V_k \ldots V_2 V_1) \leq e$ .

suppressing the $I \otimes$ parts

Definition: A set of gates G is universal for quantum computation, if for any positive integer n, any n-qubit unitary U, and any e > 0, there are $V_1, V_2, \ldots, V_k$ in G s.t. $E(U, V_k \ldots V_2 V_1) \leq e$ .

suppressing the $I \otimes$ parts

Theorem: {H, T, CNOT} is universal for QC, where

T is called the $\frac{\pi}{8}$-gate

$T = R_z\left(\frac{\pi}{4}\right)$ .

Theorem: {H, T, CNOT} is universal for QC.

Proof: see NC 4.5.2-4.5.3 or PMATH 343.

Theorem: {H, T, CNOT} is universal for QC.

Proof: see NC 4.5.2-4.5.3 or PMATH 343.

Ideas:

(1) HTH = $R_x\left(\frac{\pi}{4}\right)$

irrational multiple of $\pi$ !!

(2) T HTH = $R_z\left(\frac{\pi}{4}\right) R_x\left(\frac{\pi}{4}\right) = R_{\hat{n}}(\theta) = U$

Theorem: {H, T, CNOT} is universal for QC.

Proof: see NC 4.5.2-4.5.3 or PMATH 343.

Ideas:

(1) HTH = $R_x\left(\frac{\pi}{4}\right)$

irrational multiple of $\pi$ !!

(2) T HTH = $R_z\left(\frac{\pi}{4}\right) R_x\left(\frac{\pi}{4}\right) = R_{\hat{n}}(\theta) = U$

(3) $\forall \xi, \forall \varepsilon, \exists r$ s.t. $E(U^r, R_{\hat{n}}(\xi)) \leq \varepsilon$

Theorem: {H, T, CNOT} is universal for QC.

Proof: see NC 4.5.2-4.5.3 or PMATH 343.

Ideas:

(1) HTH = $R_x(\frac{\pi}{4})$

irrational multiple of $\pi$ !!

(2) T HTH = $R_z(\frac{\pi}{4})\, R_x(\frac{\pi}{4}) = R_{\hat{n}}(\theta) = U$

(3) $\forall \xi, \forall \varepsilon, \exists r$ s.t. $E(U^r, R_{\hat{n}}(\xi)) \leq \varepsilon$

(4) HTH T = $R_x(\frac{\pi}{4})\, R_z(\frac{\pi}{4}) = R_{\hat{m}}(\theta), \quad \hat{n} \neq \hat{m}$.

Theorem: {H, T, CNOT} is universal for QC.

Proof: see NC 4.5.2-4.5.3 or PMATH 343.

Ideas:

(1) HTH = $R_x(\frac{\pi}{4})$

irrational multiple of $\pi$ !!

(2) T HTH = $R_z(\frac{\pi}{4}) R_x(\frac{\pi}{4}) = R_{\hat{n}}(\theta) = U$

(3) $\forall \xi, \forall \varepsilon, \exists r$ s.t. $E(U^r, R_{\hat{n}}(\xi)) \leq \varepsilon$

(4) HTH T = $R_x(\frac{\pi}{4}) R_z(\frac{\pi}{4}) = R_{\hat{m}}(\theta), \quad \hat{n} \neq \hat{m}$.

Any single qubit gate is a composition of some sequence of $R_{\hat{n}}$ and $R_{\hat{m}}$.

It is CRUCIAL that the universal gate set is discrete !

Quantum computation is discrete, not analog.
This is how noise can be handled.

## 5. Quantum circuits

(a) Quantum circuit model (KLM 4.1, NC 1.3.4) ✓

(b) Quantum gates (NC 4.2-4.3, KLM 4.2) ✓

(c) Continuous universal set of quantum gates (reading) (NC 4.5.1-4.5.2, KLM 4.3)

✓ (d) Quantum gate approximations (NC Box 4.1, KLM 4.3)

✓ (e) Finite universal set of q. gates (NC 4.5.3, KLM 4.3)

(f) Efficiency & Kitaev-Solovay thm (NC App 3, KLM 4.4)

(g) Quantum circuits for measurements (reading/defer) (KLM 4.5*)

(h) Hardness of approximating most unitaries (reading) (NC 4.5.6)

# (f) Efficiency & Kitaev-Solovay thm (NC App 3, KLM 4.4)

Solovay-Kitaev Theorem

Given any universal set of 1-qubit gates G, whose inverses can be implemented exactly, any 1-qubit gate can be approximated with error $< \varepsilon$

using poly( log( $\frac{1}{\varepsilon}$ ) ) gates.

## (f) Efficiency & Kitaev-Solovay thm (NC App 3, KLM 4.4)

Solovay-Kitaev Theorem

Given any universal set of 1-qubit gates G, whose inverses can be implemented exactly, any 1-qubit gate can be approximated with error $< \varepsilon$

using poly( log( $\frac{1}{\varepsilon}$) ) gates.

Remark:
Most universal sets of gates are very efficient in approximating single qubit gates.

Proof idea: optional reading in NC Appendix 3,
or PMATH 343.

## Consequence of the Solovay-Kitaev Theorem

Suppose circuit C has m CNOT and 1-qubit gates.

There is a circuit C' with m' = m poly( log( m/e ) ) gates from {CNOT, H, T} approximating C with error at most e.

i.e., circuit complexity is largely preserved.

## Consequence of the Solovay-Kitaev Theorem

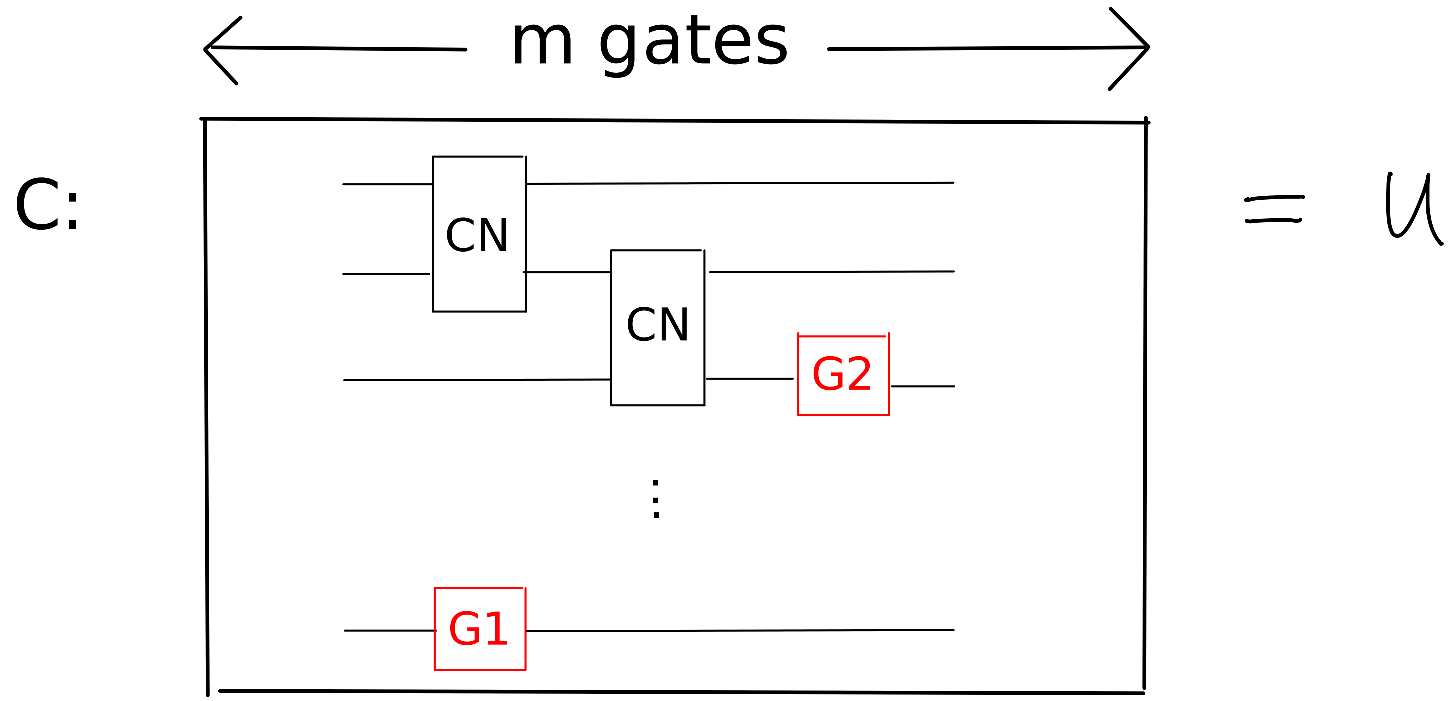
Suppose circuit C has m CNOT and 1-qubit gates.

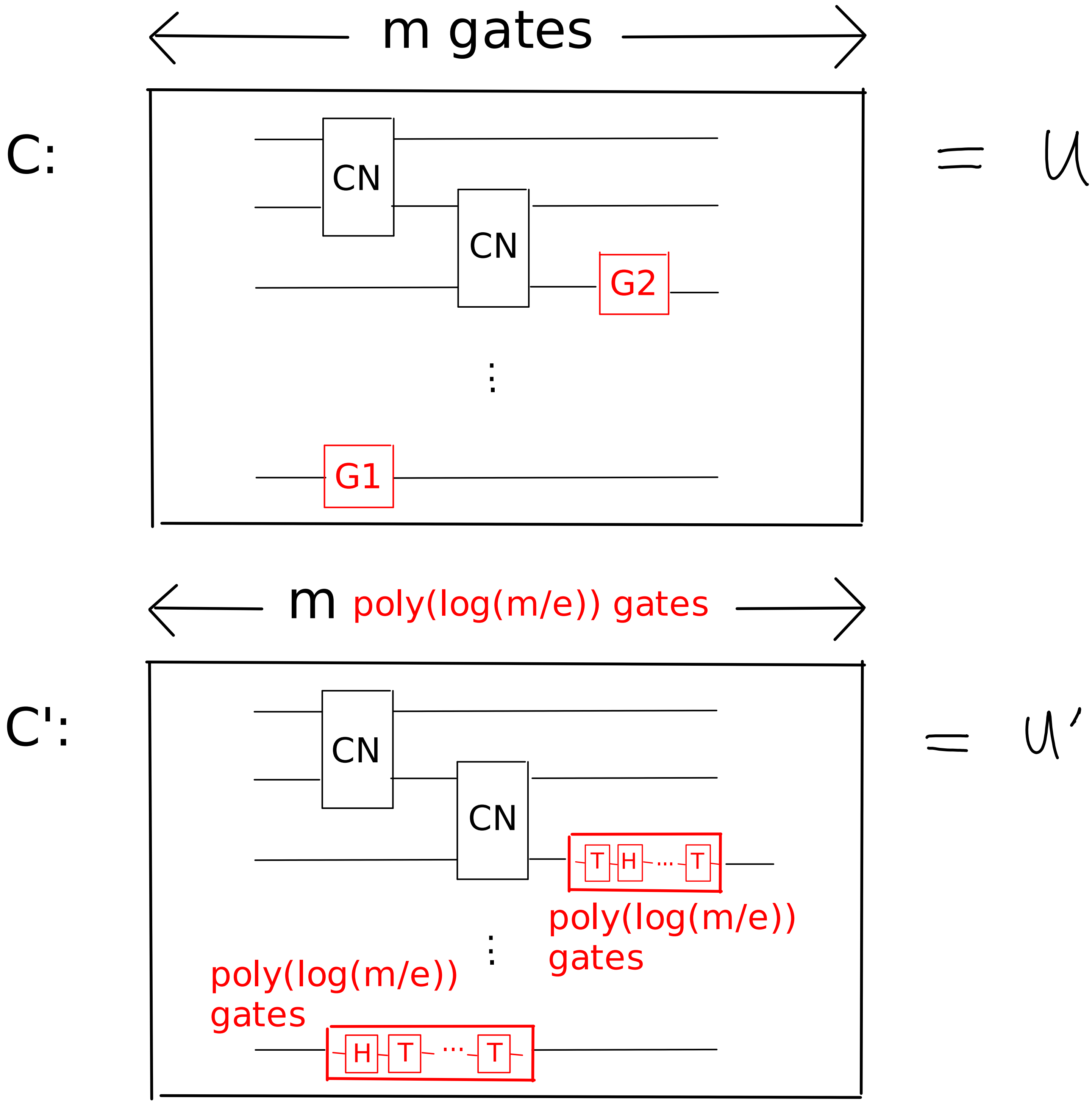
There is a circuit C' with m' = m poly( log( m/e ) ) gates from {CNOT, H, T} approximating C with error at most e.

i.e., circuit complexity is largely preserved.

Idea:

Suffices to approx each 1-qubit gate in C with error <= e/m, which takes poly(log( m/e )) H & T gates by SK-thm. So, total # gates m'


m gates
C:
CN
CN
G2
⋮
G1
= U


m gates
C:
CN
CN
G2
G1
= U
m poly(log(m/e)) gates
C':
CN
CN
T H ... T
poly(log(m/e)) gates
poly(log(m/e)) gates
H T ... T
= U'

## 5. Quantum circuits

(a) Quantum circuit model (KLM 4.1, NC 1.3.4)

(b) Quantum gates (NC 4.2-4.3, KLM 4.2)

(c) Continuous universal set of quantum gates (reading) (NC 4.5.1-4.5.2, KLM 4.3)

(d) Quantum gate approximations (NC Box 4.1, KLM 4.3)

(e) Finite universal set of q. gates (NC 4.5.3, KLM 4.3)

(f) Efficiency & Kitaev-Solovay thm (NC App 3, KLM 4.4)

(g) Quantum circuits for measurements (reading/defer) (KLM 4.5*)

(h) Hardness of approximating most unitaries (reading) (NC 4.5.6)

## (h) Hardness of approximating most unitaries (reading) (NC 4.5.6)

In short, most classical and quantum computations requires a circuit of exponentially many gates ...

There are too many different computations, but too few gates in the universal gate set.

Polynomial-sized circuits and computations are rare!