Approximately universal gate sets (continued)

There are some obvious criteria that a gate set must meet to be universal, and some less obvious.

Obvious ones:

1) must create entanglement:

e.g. CNOT

but CNOT alone is not enough, also need superposition to generate entangled states

2) must create superposition:

e.g. H

H & CNOT only have real entries

3) also need complex phases:

→ what about $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$?

can generate $Z = SS$

$X = HZH = HSSH$

$Y = SHZ(SH)^\dagger = SHSSHS^\dagger$

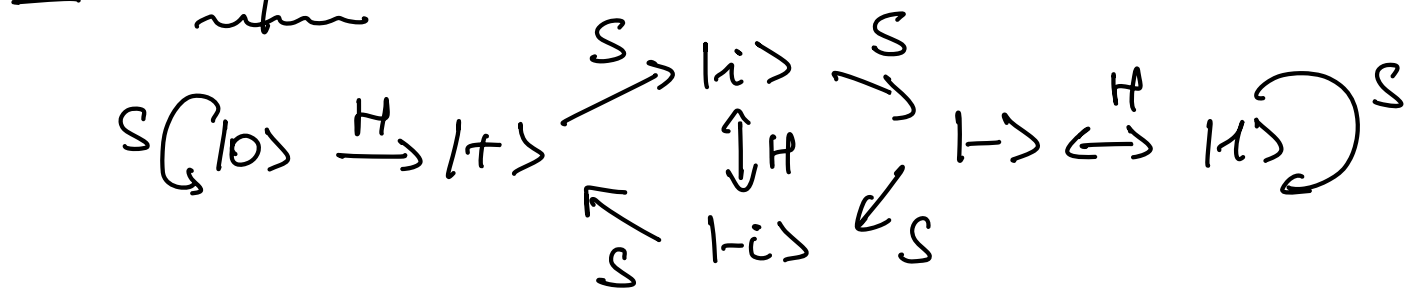
But in fact $\{H, S, CNOT\}$ is not universal.

If we combine these gates in all possible ≠ ways, we see that we can only generate particular states.

$\{H, S, CNOT\}$ are "stabilizer gates". This name comes from the stabilizer formalism developped initially for Quantum Error Correction.

They can only generate "stabilizer states"

ex: 1 qubit



Applying H & S in all possible ways only yields $|0\rangle, |1\rangle, |+\rangle, |-\rangle, |i\rangle$ or $|-i\rangle$

where $|\pm i\rangle = \frac{|0\rangle \pm i|1\rangle}{\sqrt{2}}$ eigenvectors of Y.

These are the 6 stabilizer states for 1-qubit systems.

ex: 2 qubits can generate 60 stabilizer states (36 tensor products of the 6 1-q stabilizer states + 24 entangled states incl. Bell states).

$\{H, S, CNOT\}$ are the generators of the Clifford group = group of unitaries that maps the n-qubit Pauli group $\mathbb{P}_n$ onto itself.

$$= \{ V \in U(2^n) \text{ such that } V P V^\dagger = P' \text{ with } P \& P \in \mathbb{P}_n \}.$$

Gottesman–Knill theorem:

Any circuit which can be built with only H, S, CNOT (ie involving only Clifford operators), applied to the computational-basis states $|0\rangle^{\otimes n}$, can be simulated efficiently with a classical computer.

D. Gottesman, "The Heisenberg representation of quantum computers" (1998) arXiv: 9807006 (quant-ph)

~> we need another gate for universal quantum computation, and this other gate is what brings quantum advantage
↳ potential

For example: the T gate

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

In fact $\{H, T, CNOT\}$ is approximately universal.

Quantum states which require T for their preparation are "non-stabilizer" states, also called "magic" states.

* Let us show that the set

$\{H, T, CNOT\}$ is approximately universal.

Since we know that the set of 1-qubit gates + CNOT is exactly universal, we only have to show that H & T can approximate any 1-qubit gate (to arbitrary precision).

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = e^{i\pi/8}\, U(\vec{e}_z, \pi/4)$$

↳ rotation of $\frac{\pi}{4}$ around z (up to a phase)

(Reminder: $\hat{U}(\vec{n}, \theta) = \hat{I}\cos\left(\frac{\theta}{2}\right) - i\sin\left(\frac{\theta}{2}\right)\vec{n}\cdot\vec{\hat{\sigma}}$

$\vec{\hat{\sigma}} = (\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z) = (\hat{X}, \hat{Y}, \hat{Z})$

$= \exp\left(-i\frac{\theta}{2}\hat{n}\cdot\vec{\sigma}\right)$)

$$HTH = e^{i\pi/8}\, U(\vec{e}_x, \pi/4)$$

↳ rotation of $\pi/4$ around x (up to a phase)

$$\Rightarrow T(HTH) \propto U(\vec{e}_z, \pi/4)\; U(\vec{e}_x, \pi/4)$$

$$= \left(\hat{1}\cos\frac{\pi}{8} - i\hat{Z}\sin\frac{\pi}{8}\right)\left(\hat{1}\cos\frac{\pi}{8} - i\hat{X}\sin\frac{\pi}{8}\right)$$

$$= \hat{1}\cos^2\left(\frac{\pi}{8}\right) - i(\hat{X}+\hat{Z})\cos\frac{\pi}{8}\sin\frac{\pi}{8} - \hat{Z}\hat{X}\sin^2\left(\frac{\pi}{8}\right)$$

$$+ i\hat{Y}\sin^2\left(\frac{\pi}{8}\right)$$

$$(\hat{J}\hat{K} = \delta_{jk}\hat{1} + i\varepsilon_{jkl}\hat{L})$$

$$\Rightarrow T(HTH) \propto$$

$$\hat{1}\cos^2\left(\frac{\pi}{8}\right) - i\left[\cos\left(\frac{\pi}{8}\right)(\hat{X}+\hat{Z}) - \sin\left(\frac{\pi}{8}\right)\hat{Y}\right]\sin\frac{\pi}{8}$$

$$= \hat{1}\cos^2\left(\frac{\pi}{8}\right) - i\sin\left(\frac{\pi}{8}\right)\vec{n}\cdot\vec{\sigma}$$

with $\vec{n} = \left(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8}\right)$.

Denote $\hat{n} = \vec{n}/\|\vec{n}\|$ the corresp. normalized vect.

$$\Rightarrow T\,HTH \propto \hat{1}\cos\left(\frac{\alpha}{2}\right) - i\sin\left(\frac{\alpha}{2}\right)\hat{n}\cdot\vec{\sigma} = U(\hat{n},\alpha)$$

which is a rotation about axis $\hat{n}$

of angle α with $\cos\left(\frac{\alpha}{2}\right) = \cos^2\left(\frac{\pi}{8}\right)$.

Such α can be shown to be an irrational multiple of 2π (i.e. $\alpha \neq \frac{p}{q} \cdot 2\pi$ with p, q integers)

- Now we show that repeated iterations of $U(\hat{n}, \alpha)$ can be used to approx to arbitrary accuracy any $U(\hat{n}, \theta)$:

$$\exists \text{ integer } m: \quad E\left(U(\hat{n},\theta), \left[U(\hat{n},\alpha)\right]^m\right) \leq \underbrace{\varepsilon}_{\text{desired accuracy}}.$$

$$U(\hat{n},\theta) = \cos\left(\frac{\theta}{2}\right)\hat{1} - i\sin\left(\frac{\theta}{2}\right)\hat{n}\cdot\vec{\sigma}$$

$$= \exp\left(-i\theta\,\hat{n}\cdot\vec{\sigma}/2\right)$$

$\Rightarrow$ will show: $e^{-i\frac{\theta}{2}\hat{n}\cdot\vec{\sigma}} = e^{-i\frac{\alpha m}{2}\hat{n}\cdot\vec{\sigma}} + O(\varepsilon)$

ie that $|\alpha m - \theta| < \varepsilon$.

(αm can come as close as we want to θ)

Consider the set of points

$$\{ \alpha_k = k\alpha \pmod{2\pi}, \; k = 1, 2, 3 \ldots \} \in [0, 2\pi)$$

- We note that all the points are distincts:

if $\exists\, k \neq k'$ with $\alpha_k = \alpha_{k'}$ $\Rightarrow$ $k\alpha$

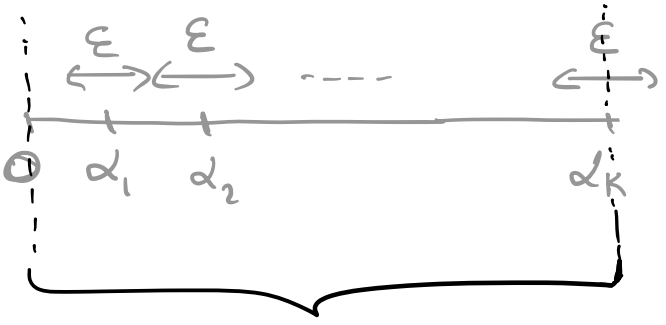
$\Rightarrow$ $k\alpha = k'\alpha + \text{integer} \times 2\pi$

$\Rightarrow$ $\alpha = \dfrac{\text{integer}}{k - k'} \times 2\pi$

$\Rightarrow$ α would be rational multiple of 2π.

- Now consider integer $K > \dfrac{2\pi}{\varepsilon}$

and consider (open) intervals of width ε centered on each of the K points α_k $(k = 1, 2 \ldots K)$.



if there was no overlap this segment would have length $\geq K\varepsilon > 2\pi$ which is not possible (because the length of the full interval is 2π).

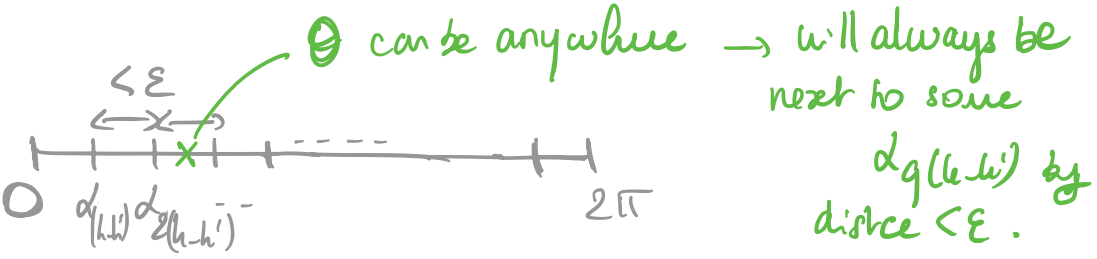
$\Rightarrow$ There must be overlap, i.e.

$\exists\ k, k' < K$ with $\underbrace{|\alpha_k - \alpha_{k'}|}_{|\alpha_{(k-k')}|} < \varepsilon$ (if $k > k'$)

$\rightarrow$ Define new set of points

$$\{ \alpha_{q(k-k')} \ , \ q = 1, 2, \ldots \}$$

These are now equally spaced points separated by distance $< \varepsilon$.



$\Rightarrow$ For given integer Q sufficiently large the sequence $\{ \alpha_{q(k-k')} \ , q = 1, 2 \ldots, Q \}$ will fill up the full $[0, 2\pi)$ interval.

$\Rightarrow$ $\forall\ \theta \in [0, 2\pi)$, there is ($m$ an integer) $m = q(k-k')$ such that $|\theta - m\alpha| < \varepsilon$.

It follows that

$$E\left(U(\hat{n},\theta), \left[U(\hat{n},\alpha)\right]^m\right) < \varepsilon/3$$

(exercise)

Now what if we want to apply a rotation around a $\neq$ axis than $\hat{n}$?

We have $H\,U(\hat{n},\theta)\,H = U(\hat{n}',\theta)$

where $\vec{n}' = (\cos\pi/8, -\sin\pi/8, \cos\pi/8)$

and $\hat{n}' = \frac{\vec{n}'}{\|\vec{n}'\|}$

$$\Rightarrow E\left(U(\hat{n}',\theta), \left[U(\hat{n}',\alpha)\right]^m\right) < \varepsilon/3$$

Now we can use the Euler decomposition (any single-qubit rotation can be written as prod of 3 separate rotations around 2 $\neq$ axes):

$$V = U(\hat{n},\beta)\,U(\hat{n}',\gamma)\,U(\hat{n},\delta)$$

approx by ↓ ↓ ↓

$$\left[U(\hat{n},\alpha)\right]^{m_1} \quad \left[U(\hat{n}',\alpha)\right]^{m_2} \quad \left[U(\hat{n}',\alpha)\right]^{m_3}$$

$\Rightarrow$ all in all there exists 3 integers m_1, m_2, m_3 such that

$$E\left(V_1 \left[U(\hat{n}_1,\alpha)\right]^{m_1} \left[H\, U(\hat{n}_1,\alpha) H\right]^{m_2} \left[U(\hat{n}_1,\alpha)\right]^{m_3} \right) < \varepsilon$$

$\Rightarrow$ It is possible to approximate any 1-qubit gate $U(\hat{n}, \theta)$ $(\theta \in [0, 2\pi))$ using H & T gates, up to arbitrary precision ε.

$\Rightarrow$ if we want an accuracy of ε_{tot} for the whole circuit, then this may be achieved by approx each single-qubit unitary using the above procedure to within ε_{tot}/m (m = number of gates).

$\varepsilon =$

So far we have focused on <u>reachability</u> (i.e. can we approx a certain unitary to accuracy ε)

but what about <u>complexity</u>?

→ how large of a circuit does it take to achieve such accuracy?

Solovay-Kitaev theorem says that we can do it in a quite efficient way:

> Any single-qubit gate can be approximated to accuracy ε using a number of gates (from an approximately-universal gate set) that is
>
> $$O(\text{poly}(\log 1/\varepsilon))$$
>
> i.e. polynomial in the log of $1/\varepsilon$.

(For a proof of this theorem
→ see Nielsen & Chuang
"Quantum Computation and Quantum Info"
appendix 3.)

⇒ to approximate m gates, each with accuracy ε/m → the overhead required is $O(\text{poly}(\log(m/\varepsilon)))$.

see example

Ross and Selinger

"Optimal ancilla-free Clifford-T approximation of z rotations"

arXiv: 1403.2975 (2016)

for a gate sequence exponentially close to $U(\vec{e}_3, \pi/128)$.

→ Quantum Complexity Classes

Because of universality ⇒ can define notions of complexity that are indep. of the univ. gate set.

⇒ Similarly to classical complexity classes there are quantum complexity classes that classify the pbs in terms of how much resources they require to be solved.

* **BQP** ("bounded-error quantum poly time")

→ analogous of the BPP classical complexity class. (randomized comput.)

= class of pbs that can be solved (with proba of error $\leq 1/3$) by quantum computers using (uniform) quantum circuits with polynomial size

* **QMA** ("Quantum Merlin-Arthur")

= pbs where the 'yes' instances can be verified efficiently (with poly-size quantum circuit) if someone provides a witness. ↳ with proba of error $\leq 1/3$.

(c) Equivalence classical / quantum :

* classical from quantum ?

A quantum computer can easily simulate a randomized classical computer

(can prepare $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and measure, i.e. project to $\{|0\rangle, |1\rangle\}$, to generate a random bit)

$\Rightarrow$ $BPP \subseteq BQP$

(and in turn we saw that randomized class. comp can efficiently simulate deterministic ones

$\Rightarrow$ $P \subseteq BPP \subseteq BQP$)

* quantum from classical

The Hilbert space of an n-qubit system has dim 2^n → grows exponentially.

ex $n = 100 \Rightarrow \sim 10^{30}$ → huge!

$\Rightarrow$ a priori no simple classical description of general quantum states

and naively one would expect that an exponential amount of memory is required to simulate a quantum syst on a classical computer.

However it turns out that despite the vastness of Hilbert space, a classical computer can simulate an n-qubit system with memory which is $O(\text{poly}(n))$

$\Rightarrow$ BQP $\subset$ PSPACE.

⚠ it may take an exponential amount of time.

Let us show this :

We want the classical computer to compute the proba $p(x)$ for each possible outcome $|x\rangle$ of the final measurement :

$$p(x) = |\langle x|\hat{U}|0\rangle|^2$$

($|0\rangle$: initial state of n-qubit syst.)

where $\hat{U}$ = circuit constructed from T gates

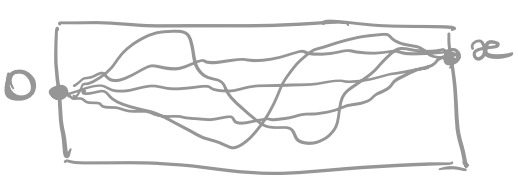
$$= \hat{U}_T \hat{U}_{T-1} \cdots \hat{U}_1$$

Inserting closure relations $\sum_x |x\rangle\langle x| = \mathbb{1}$

$$\Rightarrow \langle x|\hat{U}|0\rangle =$$

$$\sum_{\substack{x_{T-1} \\ x_{T-2} \\ \vdots \\ x_1}} \langle x|\hat{U}_T|x_{T-1}\rangle \times \langle x_{T-1}|\hat{U}_{T-1}|x_{T-2}\rangle \times \cdots \langle x_2|U_2|x_1\rangle \langle x_1|U_1|0\rangle$$

("sort of" a Feynman path integral)



(sum over all computational path taking state $|0\rangle$ to $|x\rangle$).

Each intermediate n-qubit state $|x_i\rangle$ can take 2^n values, and there are $T-1$ matrix elements

$\Rightarrow$ there are $(2^n)^{T-1}$ possible paths.

- Each matrix element $\langle x_i | U_i | x_{i-1} \rangle$ is easy to calculate (we only consider certain 1- & 2-qubit gates) -

In fact most of them are zero unless all other computational basis states match left and right.

ex: $\langle 11\ldots11 | H \otimes 1 \otimes \ldots \otimes 1 | 011\ldots0 \rangle$

$= \underbrace{\langle 1|H|0\rangle}_{\neq 0} \otimes \underbrace{\langle 1|1|1\rangle}_{1} \otimes \ldots \underbrace{\langle 1|1|0\rangle}_{0}$

- The multiplication of all $(T-1)$ ME for one path is also easy (in poly-time and memory).
- Adding all the $(2^n)^{T-1}$ paths is also polynomial in memory (reuse the space for each path & sum = sum + path)

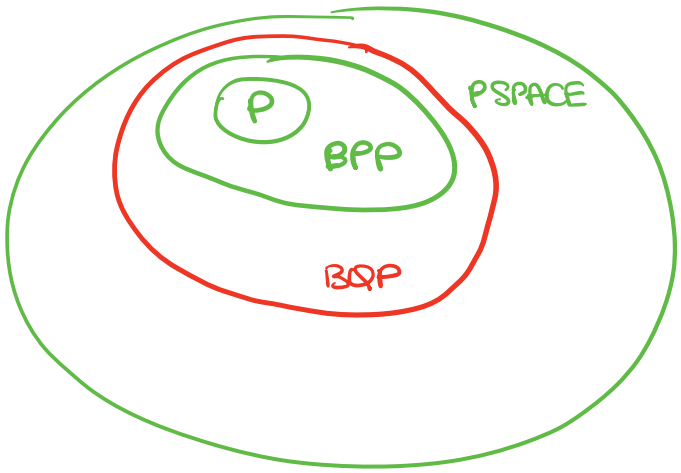
⇒ A quantum circuit with $T = \mathcal{O}(\text{poly}(n))$ gates acting on n-qubits can be simulated with classical computer with memory scaling polynomially.

→ BQP ⊆ PSPACE

⚠ it is clear that the simulation we have described takes exponential time because we need to evaluate the sum of all $(2^n)^{T-1}$ paths (sum of $(2^n)^{T-1}$ complex numbers).

→ quantum should still be superior to classical.

Overall: $P \subseteq BPP \subseteq BQP \subseteq PSPACE$



We hope that some pbs are in BQP but not in BPP, i.e. we hope that BQP is strictly larger than BPP.

We don't know how to prove that yet (from first pcples) but we believe it is true.