Universal Gate set

A [finite] set of quantum gates

$$S = \{U_1, \dots, U_m\}$$

U_j acts on k_j qubits where $k_j \leq k$

and k is independent of n

- Any k_j qubits in the register.
- Architecture: nearest neighbour + SWAP $\begin{bmatrix} 1 & & & \\ & 0 & 1 & \\ & 1 & 0 & \\ & & & 1 \end{bmatrix}$

$\Rightarrow$ bring any two qubits together in linear time.

for $\forall\, U(2^n) \simeq \prod_i^{T} U_i \qquad U_i \in S$ (How large is T ?) n-dependent.

Exact universality:

If the set is described by a continous parameter

$\Rightarrow$ possible to get exact universality

i.e. for any $U(2^n) = \prod_i^{T} U_i$

Example: CNOT $\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{bmatrix}$

(~~any~~ other entangling operation)

single qubit rotations $R(\theta, \varphi)$

continous

Exactly universal

We will prove the universality of this set today

Relaxing exactness. for a <u>finite</u> set, we require that for any $U(2^n)$ there is a $\tilde{U}$

$$\tilde{U} = \prod_i^T U_i \qquad U_i \in S$$

and that
$$\| \tilde{U} - e^{i\phi} U \|_{\sup} \leq \delta$$

largest eigenvalue.

(over ϕ)

for <u>any</u> $\delta > 0$ (in particular n independent)

$\Rightarrow$ Operators constructed from this gate set are <u>dense</u> in the unitary group $U(2^n)$

How large is T? $\Leftrightarrow$ efficiency

How many gates can be constructed from T applications of gates from a set of S gates $\{U_1, \dots U_S\}$

- every gates can be applied on diff. $k \in n$ qubits
  $\binom{n}{k}$ choices

$\Rightarrow$ # of gates $\left[S \cdot \binom{n}{k} \right]^T = \left(S \cdot \text{poly}(n) \right)^T$

$$\frac{n!}{(n-k)!\,k!} < \frac{n^k}{k!} \sim \text{poly}(n)$$

How many Unitaries are enough to be δ-dense in $U(2^n)$?

$2^n \times 2^n = 2^{2n}$ free parameters.

~ Volume of $C=O(1)$ radius sphere in $D=2^{2n}$ space /

Volume of δ-radius sphere -"-

$$\# = \left(\frac{C}{\delta}\right)^{2^{2n}}$$

to be dense:

$$\left(S\,\mathrm{poly}(n)\right)^{T} > \left(\frac{C}{\delta}\right)^{2^{2n}}$$

$$\Rightarrow T \log\left(S\,\mathrm{poly}(n)\right) > 2^{2n} \log\left(\frac{C}{\delta}\right)$$

$$\Rightarrow T > 2^{2n} \frac{\log\left(\frac{C}{\delta}\right)}{\log\left(S\,\mathrm{poly}(n)\right)}$$

- Very inefficient (exact doesn't help.) ($\log \frac{1}{\delta}$
- with $T \sim \mathrm{poly}(n)$ can only approach a very small subset
- expected $\Rightarrow$ otherwise BQP can poly realize any binary function

A proof that CNOT + $R(\theta, \varphi)$ are exactly universal.

Two steps:

1. 2×2 unitaries are universal.
2. Any 2×2 unitary can be composed of CNOT's and single qubit rotations.

1. 2×2 unitaries: given an orthonormal basis

$$\{ |0\rangle \dots , |N-1\rangle \} \qquad N = 2^n$$

$U^{(2)}$ is a unitary acting only on the sub-space spanned by $|i\rangle$ and $|j\rangle$

- Not a 2-qubit operation, can be single qubit rotation.
- can be entangling e.g.

$$\{ |00\rangle, |11\rangle ; \tfrac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \}$$

2×2 unitary acting on $|00\rangle \leftrightarrow \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle]$

Express $U(2^n)$ in terms of 2x2 unitaries.

choose a basis $\{|0\rangle \dots |N-1\rangle\}$ $N=2^n$

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

look at the 2x2 Unitaries: freedom.

$$\hat{X}_0 |0\rangle \to a_0|0\rangle + b_1^{S}|1\rangle$$

$$\hat{X}_1 b_1|1\rangle \Rightarrow a_1|1\rangle + b_2|2\rangle$$

$$\hat{X}_2 b_2|2\rangle \to a_2|2\rangle + b_3|3\rangle$$

$$W_0 = \hat{X}_{N-1} \dots \hat{X}_2 \hat{X}_1 \hat{X}_0$$

un-∂_3

$$W_0|0\rangle = U|0\rangle$$

- The operator $W_0^{-1} U|0\rangle = |0\rangle$

stabilizes $|0\rangle$, acts only in the subspace spanned by $|1\rangle \dots |N-1\rangle$

Define $U_1 = W_0^{-1} U$

repeat for $U_1|1\rangle = \sum_{i=1}^{N-1} a_i |i\rangle$

$W_1|1\rangle = U_1|1\rangle$

$U_2|0\rangle = |0\rangle$

$U_2|1\rangle = |1\rangle$ $\quad U_2 = W_1^{-1} W_0^{-1} U$ etc.

$$\Rightarrow U_N = W_{N-1}^{-1} W_{N-2}^{-1} \cdots W_0^{-1} U = \hat{\mathbb{I}}$$

$$\Rightarrow \quad U = \prod_{i=0}^{N-1} W_i \qquad \leftarrow \text{inefficient } N = 2^n \text{ operations}$$

- work for ~~any~~ choice of orthonormal basis, e.g. logical basis

2. How do we construct any 2×2 unitary from 2 qubit CNOT's + single qubit $R(\theta,\varphi)$?

2×2 unitary. $V_{(i,j)}$ acting in the subspace spaned by $|i\rangle$; $|j\rangle \in$ logical basis

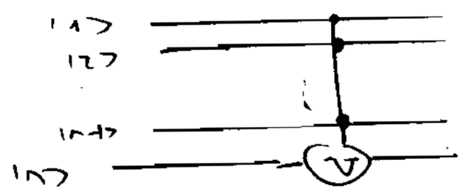
$i, j \Rightarrow$ Binary

1st step: $\Sigma_{(i,j)}$ is the unitary

$$|i\rangle \rightarrow |111\ldots10\rangle$$
$$|j\rangle \rightarrow |111\ldots11\rangle$$

mapping any binary word into $''$

$\Lambda^{n-1}(V)$ is a V rotation on target qubit n, iff all $n-1$ control qubit are in 1.

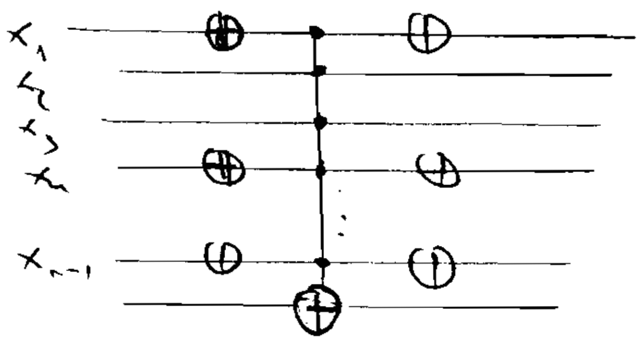


then:
$$V(i,j) = \Sigma^{-1}_{(i,j)} \Lambda^{n-1}(V) \Sigma_{(i,j)}$$

How can we construct a circuit that realizes $\Sigma_{(i,j)}$?

start with an operator that transposes any $|i\rangle$ $|k\rangle$ where i, k are binary words that differ by one bit x_n

a_n



$\oplus = \otimes$

$\leftarrow \Lambda^{n-1}(X)$

if the correct basis state is input $\rightarrow$ x_n is flipped

otherwise $\Rightarrow \hat{\mathbb{I}}$

if the two words differ by $k \leq n$ bits.

$\Rightarrow$ transpose bit-by-bit

$a_k \; a_{156} \; a_4 \; a_3$

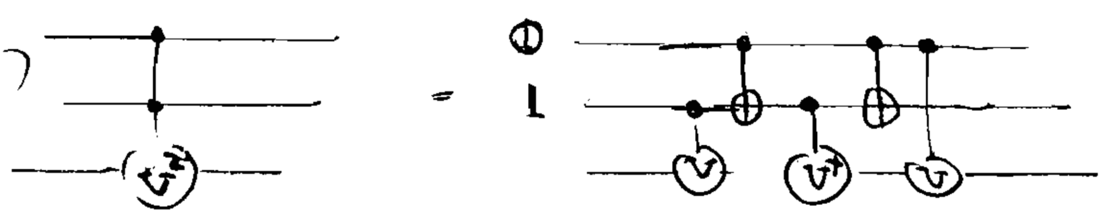
almost done ...

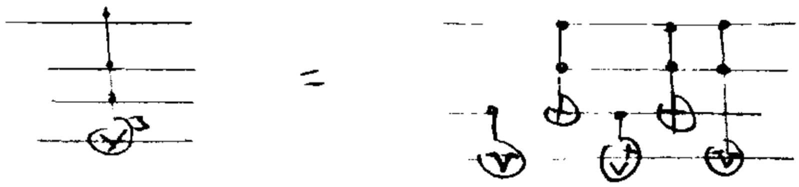
we are left with $\Lambda^n(U)$'s and X (not's)

to be decomposed in terms of CNOT's and $R(\theta,\varphi)$'s

easy!

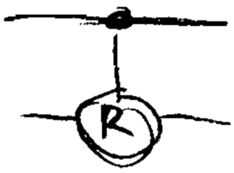
start with

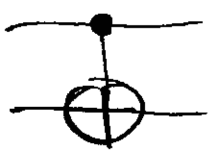
$\Lambda^2(V^2)$ 

$\Lambda^3(V^3)$ 

and so on.

$U = V^N$

<u>last thing:</u> construct 

from  +  's

<u>exercise.</u>

CNOT + $R(\theta, \varphi)$ is a uncountable set.

- Finite Universal gate sets:

How can $R(\theta,\varphi)$ be de-composed approximately into a product of rotations from a finite set?

1. lets initialy look at rotations around $\hat{z}$

$$U(\theta) = e^{i\frac{\theta}{2}\hat{\sigma}_z} = \cos\left(\frac{\theta}{2}\right)\hat{\mathbb{I}} + i\sin\left(\frac{\theta}{2}\right)\hat{\sigma}_z$$

$$0 < \theta < 2\pi$$

$\{U(2\pi\alpha)^n\}$ $n \in$ integer, are dense in $U(1)$
α - irrational #

$\Rightarrow$ the points $n\alpha \pmod 1$ are dense on the unit interval

proof. - all points $n\alpha \pmod 1$ are distinct:

otherwise $m\alpha = n\alpha + k$ where $n \neq m, k$ integers

$\Rightarrow \alpha = \frac{k}{m-n}$ $\leftarrow$ rational.

- consider $N > \frac{1}{\varepsilon}$ points $\{n\alpha_{\bmod (1)}, n=1 \dots N\}$

- look at ε intervals around points.

$\Rightarrow$ at least two intersect. $\Leftarrow$ their length $N\varepsilon$ is more that $[0,1]$'s length.

$\Rightarrow$ there exist ~~[illegible]~~ $n, m < \frac{1}{\varepsilon}$ such that

$$\underset{(\text{mod } 1)}{|n-m|\alpha} \equiv \underset{(\text{mod } 1)}{r\alpha} < \varepsilon$$

the points $\{ k r \alpha \ (\text{mod } 1), \ k = 1 \dots m \}$

are equally spaced by $< \varepsilon$ and cover the unity interval

$\boxed{\text{Fin}}$

- we can approach all $\hat{z}$ rotations with $e^{i \frac{\theta}{2} \hat{z}} \equiv e^{i \frac{\theta}{2} \hat{z}}$
- we can approach all $\hat{y}$ rotations with $e^{i \frac{\theta}{2} \hat{y}} \equiv e^{i \frac{\theta}{2} \hat{y}}$

- $$\lim_{n \to \infty} \left(e^{i \frac{\alpha \hat{y}}{n}} e^{i \frac{\beta \hat{z}}{n}} \right)^n = \lim_{n \to \infty} \left(1 + \frac{i}{n} (\alpha \hat{y} + \beta \hat{z}) + O\left(\frac{1}{n^2}\right) \right)^n$$

$$= e^{i(\alpha \hat{y} + \beta \hat{z})}$$ $\leftarrow$ rotation around any direction in the $\hat{y}$-$\hat{z}$ plane.

- $$\lim_{n \to \infty} \left(e^{i \frac{\cancel{A}}{\sqrt{n}}} e^{i \frac{\cancel{B}}{\sqrt{n}}} e^{-i \frac{\cancel{A}}{\sqrt{n}}} e^{-i \frac{\cancel{B}}{\sqrt{n}}} \right)^n$$

$$= \lim_{n \to \infty} \left(1 - \frac{1}{n} (\cancel{AB} - \cancel{BA}) + O\left(\frac{1}{n^{3/2}}\right) \right) = e^{-[Y, Z]} = e^{+\hat{X}}$$

$\Rightarrow$ universal!

Remarks:

- Due to non-commutativity, a product of rational fractions of 2π can give a rotation by an irrational angle.

Example: sometimes referred to as "standard":

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} ; \quad T = \begin{bmatrix} e^{-i\pi/8} & \\ & e^{i\pi/8} \end{bmatrix}$$

CNOT i.e. $\Lambda(X)$

- efficiency?

Solovay-Kitaev theorem
(by algorithmic construction)

$$\#\text{ of operators} \propto \left[\log\left(\frac{1}{\varepsilon}\right)\right]^{\beta}$$

$$\beta \simeq 4.$$

- Two qubits are starting out in an entangled state.

$$\frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle \right)$$

qubit 1 is coupled to the environment such that