Both Toffoli and CNOT need little help to do universal quantum computing

Yaoyun Shi

University of Michigan

Work done at Caltech

Question: What is the simplest gate needed to add to a classicaly universal gate set in order to do universal quantum computating?

Def: A basis (set of gates) is universal if it can approximate an arbitrary unitary (orthogonal) operator to an arbitrary precision, using ancillas.

Toffoli + ?

Thm:[Guttesman-Knill] A $\{CNOT, H\}$-circuit can be efficiently simulated classically.

Question: What if changing H to something else?

Known:[Barenco et al.] CNOT + all one-qubit gates is universal.

A generic gate: R_θ, θ irrational multiple of π, generates dense subgroup of $SO(2)$.

Universal: CNOT + any generic gate.

Question: How about adding $R_{\pi/3}$, etc.?

Answers

Def: A gate is basis-changing if it does not preserve the computational basis.

Def: The set of simple gates

$$\mathcal{S} = \{g : \text{single-qubit, real, basis-changing}\}.$$

Thm 1: For $\forall S$, $S \in \mathcal{S}$ and $S^2 \in \mathcal{S}$, $\{CNOT, S\}$ is universal.

Thm 2: For any $S \in \mathcal{S}$, $\{T, S\}$ is universal.

Proof of Theorem 1

Idea: prove $\{CNOT, S\}$ generates a dense subgroup of $SO(4)$.

Assume: $S \equiv R_\theta$, where $\theta \notin \frac{\pi}{4}\mathbb{Z}$.

Construct $U_1, U_2, \cdots, U_k$ s.t.

$$\langle U_1 \rangle \longrightarrow SO(H_1)$$

$$\langle U_1, U_2 \rangle \longrightarrow SO(H_2)$$

$\vdots$

$$\langle U_1, U_2, \cdots, U_i \rangle \longrightarrow SO(H_k) \equiv SO(4)$$

Thm:[Kitaev] $\mathcal{M}$: Hilbert space of dim ≥ 3;
$|\xi\rangle \in \mathcal{M}$, and $|\xi\rangle \neq 0$;
H: stabilizer of $\mathbb{R}|\xi\rangle$;
If $V \in O(\mathcal{M})$ does not preserve $\mathbb{R}[|\xi\rangle]$,
Then $H \bigcup V^{-1}HV$ generates a dense subgroup of $SO(\mathcal{M})$.

$U := [(S \otimes S) \cdot \Lambda(\sigma^x)\ [1,2]]^2 .$

Eigenvalues and eigenvectors:

1: $|\xi_1\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$

1: $|\xi_2\rangle = \frac{\sin\theta}{\sqrt{2}}(-|00\rangle + |01\rangle) + \frac{\cos\theta}{\sqrt{2}}(|10\rangle - |11\rangle)$

$\exp(\pm i\alpha)$: $|\xi_3\rangle$, $|\xi_4\rangle$, where $\cos\frac{\alpha}{2} = \cos^2\theta$.

Thm:[Wlodarski] If $\theta \notin \frac{\pi}{4}\mathbb{Z}$, and $\cos\frac{\alpha}{2} = \cos^2\theta$, then either θ or α is incommensurate with π.

Proof for Theorem 2

Given: $R_\theta \in \mathcal{S}$, R_α, ϵ
Output: Circuit C over $\{R_\theta, Toffoli\}$ approx. R_α. I.e. $\forall|\xi\rangle$, s.t. $\|\xi\| = 1$,

$$\|C\ |\xi\rangle|0^k\rangle - (R_\alpha|\xi\rangle)|0^k\rangle\| \leq \epsilon.$$

Step 1: Assume we have $W_{\alpha/2}$:

$$W_{\alpha/2}|0\rangle|0^k\rangle = |\phi_{\alpha/2}\rangle|0^k\rangle,$$

then done: if

$$W_\alpha := W_{\alpha/2} \cdot N \cdot W_{\alpha/2} \cdot \sigma^z[1],$$

then

$$W_\alpha|\xi\rangle|0^k\rangle = (R_\alpha|\xi\rangle)|0^k\rangle.$$

To do: approx. σ^z, $W_{\alpha/2}$.

Step 2: Approx. σ^z by $\{R_\theta, T\}$.

Example: Have H and $CNOT$.

$$\Lambda(\sigma^x)|b\rangle(|0\rangle - |1\rangle) = (-1)^b|b\rangle(|0\rangle - |1\rangle).$$

Generalize to biased quantum gate:

$$|\psi\rangle := R_\theta \otimes R_\theta|01\rangle =$$

$$\sin\theta\cos\theta(|11\rangle - |00\rangle) + \cos^2\theta|01\rangle - \sin^2\theta|10\rangle.$$

$$|b\rangle(|00\rangle - |11\rangle) \to (-1)^b|b\rangle(|00\rangle - |11\rangle).$$

Decrease error: Use $|\psi\rangle^{\otimes k}$.

Step 3: Creat $|\phi_{\alpha/2}\rangle$ from $|0\rangle$.

Idea: Creat logical $|\widehat{\phi}_{\alpha/2}\rangle = \cos\frac{\alpha}{2}|\widehat{0}\rangle + \sin\frac{\alpha}{2}|\widehat{1}\rangle$, then decode $|\widehat{0}\rangle \to |0\rangle|0^k\rangle$ and $|\widehat{1}\rangle \to |1\rangle|0^k\rangle$.

$T_\theta := U_{-\theta}[1] \cdot \Lambda(\sigma^x)[1,2] \cdot U_\theta$.

Conclusion

Universal quantum computing:

Toffoli + any single-qubit real gate that does not preserve compuational basis;

CNOT + any single qubit real gate that does not preserve computational basis *and* is not Hadamard or its alike.

Comparison of two proofs:

1. via Kitaev-Theorem: efficent approximation; not intuitive.

2. via Grover's algorithm: not efficient, but intuitively simple and uses some tricks!