Universality of Quantum Gates

Markus Schmassmann

QSIT-Course
ETH Zürich

17. Oktober 2007

Outline

Basics and Definitions

Universality of CNOT and Single Qbit Unitaries

- Decompositon of Single Qbit Operation
- Controled Operations
- Universality of Two Level Gates

A Discrete Set of Universal Operations

Outline

Outline

Basics and Definitions

Universality of CNOT and Single Qbit Unitaries

- Decompositon of Single Qbit Operation
- Controled Operations
- Universality of Two Level Gates

A Discrete Set of Universal Operations

Basics and Definitions (I)

Definition

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

$$H = (X + Z)/\sqrt{2} \qquad S = T^2$$

Basics and Definitions (II)

$$R_X(\theta) = e^{-i\theta/2\cdot X} = \cos(\theta/2)\cdot I - i\sin(\theta/2)\cdot X$$
$$R_Y(\theta) = e^{-i\theta/2\cdot Y} = \cos(\theta/2)\cdot I - i\sin(\theta/2)\cdot Y$$
$$R_Z(\theta) = e^{-i\theta/2\cdot Z} = \cos(\theta/2)\cdot I - i\sin(\theta/2)\cdot Z$$

$$R_{\hat{n}}(\theta) = e^{-i\theta/2\cdot\hat{n}\cdot\vec{\sigma}} = \cos(\theta/2)\cdot I - i\sin(\theta/2)\cdot(n_X X + n_Y Y + n_Z Z)$$

$$XYX = -Y \qquad XR_Y(\theta)X = R_Y(-\theta)$$
$$XZX = -Z \qquad XR_Z(\theta)X = R_Z(-\theta)$$

X-Y decomposition of a single qbit gate

Theorem

X-Y decomposition of a single qbit gate
$\forall U \in \mathbb{C}^{2\times 2}$ *unitary* $\exists \alpha, \beta\, \gamma, \delta \in \mathbb{R}$:
$U = e^{i\alpha} R_Z(\beta) R_Y(\gamma) R_Z(\delta)$

Proof.

U can be written as

$$U = \begin{pmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos(\gamma/2) & e^{i(\alpha-\beta/2+\delta/2)}\sin(\gamma/2) \\ e^{i(\alpha+\beta/2-\delta/2)}\sin(\gamma/2) & e^{i(\alpha+\beta/2+\delta/2)}\cos(\gamma/2) \end{pmatrix}$$

□

also true for any two non-parallel rotation axis
$R_{\hat{n}}(\theta), R_{\hat{m}}(\theta) \quad \hat{n} \not\parallel \hat{m}$

X-Y decomposition of a single qbit gate

Theorem

X-Y decomposition of a single qbit gate
$\forall U \in \mathbb{C}^{2\times 2}$ *unitary* $\exists \alpha, \beta\, \gamma, \delta \in \mathbb{R}$:
$U = e^{i\alpha} R_Z(\beta) R_Y(\gamma) R_Z(\delta)$

Proof.

U can be written as

$$U = \begin{pmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos(\gamma/2) & e^{i(\alpha-\beta/2+\delta/2)}\sin(\gamma/2) \\ e^{i(\alpha+\beta/2-\delta/2)}\sin(\gamma/2) & e^{i(\alpha+\beta/2+\delta/2)}\cos(\gamma/2) \end{pmatrix}$$

□

also true for any two non-parallel rotation axis
$R_{\hat{n}}(\theta), R_{\hat{m}}(\theta) \quad \hat{n} \not\parallel \hat{m}$

Corrollary of decomposition

Corollary

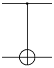
$\forall U \in \mathbb{C}^{2\times 2}$ *unitary* $\exists \alpha \in \mathbb{R} \exists A, B, C \in \mathbb{C}^{2\times 2}$ *unitary:*
$ABC = I, U = e^{i\alpha} AXBXC$

Proof.

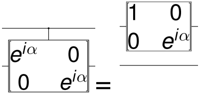
$A = R_Z(\beta) R_Y(\gamma/2)$, $B = R_Y(-\gamma/2) R_Z\left(-\frac{\delta+\beta}{2}\right)$,
$C = R_Z\left(\frac{\delta-\beta}{2}\right)$,
$XBX = XR_Y(-\gamma/2) XXR_Z\left(-\frac{\delta+\beta}{2}\right) X =$
$R_Y(\gamma/2) R_Z\left(\frac{\delta+\beta}{2}\right)$ □

Operations controled by one Qbit

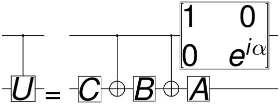
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} =$$



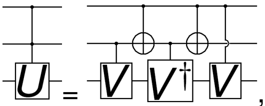
$$\text{Cphase} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha} & 0 \\ 0 & 0 & 0 & e^{i\alpha} \end{pmatrix} =$$



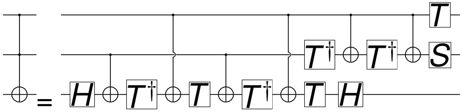
$$\text{controled } U = \begin{pmatrix} 1 & 0 \\ 0 & U \end{pmatrix} =$$



Operations controled by several Qbits



, where $V^2 = U$



,

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

Expansion to more control Qbits is tedious, but not difficult.

Universality of Two Level Gates

Theorem

Two level gates are universal.
$\forall U \in \mathbb{C}^{3\times 3}$ *unitary* $\exists U_i \in \mathbb{C}^{3\times 3} : U_i = U_i' \otimes 1, U_i' \in \mathbb{C}^{2\times 2}$
unitary $U = U_1^\dagger U_2^\dagger U_3^\dagger$

Proof.

$$U = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix},$$

$$b \neq 0: \quad U_1 = \begin{pmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$U_1 U = \begin{pmatrix} a' & b' & c' \\ 0 & 'e & f' \\ g' & h' & j' \end{pmatrix}$$

□

Proof contd.

Proof.

contd.

$$c' \neq 0 \; U_2 = \begin{pmatrix} \frac{a'^*}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{c'^*}{\sqrt{|a'|^2+|c'|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{-a'}{\sqrt{|a'|^2+|c'|^2}} \end{pmatrix}$$

$$U_2 U_1 U = \begin{pmatrix} 1 & b'' & c'' \\ 0 & e'' & f'' \\ 0 & h'' & j'' \end{pmatrix}, \text{ but } U_2 U_1 U \text{ are unitary}$$

$$\Rightarrow d'' = g'' = 0 \; U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{pmatrix}$$

$$\Rightarrow U_3 U_2 U_1 U = I \Rightarrow U = U_1^\dagger U_2^\dagger U_3^\dagger$$

□

for higher dimensions similar processes

Unitaries of Higher Dimensions

$U \in \mathbb{C}^{d\times d} \Rightarrow U = \prod_{j=1}^{N}(U'_j \otimes 1_{d-2}),\, U'_j \in \mathbb{C}^{2\times 2},\, N \leq \frac{d(d-1)}{2}$

$\exists U \in \mathbb{C}^{d\times d} : N \geq (d-1)$

ex: $U_{jk} = \delta_{jk} e^{\frac{2\pi i}{p_i}}$, where p_j is the j^{th} prime number.

With one single qbit gate and CNOTs an arbitrary two-level unitary operation on a state of n qbits can be implemented, where the CNOTs are used to shuffle.

Therefore CNOTs and unitary single Qbit operations form an universal set of quantum computing.
Unfortunately, for most single Qbit operations exists no straightforward method of error correction.

Approximation of Unitaries

Definition

$$\text{error } E(U, V) := \max_{|\psi\rangle} ||(U - V)|\psi\rangle||$$

$$E(U_m U_{m-1} \dots U_1, V_m V_{m-1} \dots V_1) \leq \sum_{j=1}^{m} E(U_j, V_j)$$

Proof.

$E(U_2 U_1, V_2 V_1) = ||(U_2 U_1 - V_2 V_1)|\psi\rangle||$
$= ||(U_2 U_1 - V_2 U_1)|\psi\rangle + (V_2 U_1 - V_2 V_1)|\psi\rangle||$
$\leq ||(U_2 U_1 - V_2 U_1)|\psi\rangle|| + ||(V_2 U_1 - V_2 V_1)|\psi\rangle||$
$\leq E(U_2, V_2) + E(U_1, V_1)$
further by induction □

Standard Set of universal Gates

Hadamard H, phase S, $CNOT$, $\pi/8 = T$, where $\pi/8$ could be replaced by Toffoli.
$T = R_Z(\pi/4)$, $HTH = R_X(\pi/4)$ up to a global phase.

$$\begin{aligned} &\exp(-i\pi/8 \cdot Z)\exp(-i\pi/8 \cdot X) \\ =&\left(\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}Z\right)\left(\cos\frac{\pi}{8}I - i\sin\frac{\pi}{8}X\right) \\ =&\cos^2\frac{\pi}{8}I - i\left(\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right)\sin\frac{\pi}{8} \\ =&R_{\hat{n}}(\theta), \end{aligned}$$

where $\hat{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$ and $\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$.

Multiples of irrational Angles

$\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8} = \frac{\sqrt{2}+2}{4} \Rightarrow \frac{\theta}{2\pi} \notin \mathbb{Q}$,
therefore any $R_{\hat{n}}(\alpha)$ can be arbitrary close approximated.
$HR_{\hat{n}}(\alpha)H = R_{\hat{m}}(\alpha)$, where $\hat{m} = \left(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8}\right)$.
$\forall U \in \mathbb{C}^{2\times 2}$ unitary $\exists \alpha, \beta\, \gamma, \delta \in \mathbb{R}$:
$U = e^{i\alpha} R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta)$
Finally, $\forall U \in \mathbb{C}^{2\times 2}$ unitary, $\forall \varepsilon > 0 \exists n_1, n_2, n_3 \in \mathbb{N}$:
$E\left(U, R_{\hat{n}}(\theta)^{n_1} HR_{\hat{n}}(\theta)^{n_2} HR_{\hat{n}}(\theta)^{n_3}\right) < \varepsilon$.

Universality of Generic qbit Gates

Definition

A "generic" qbit gate is a $U \in \mathbb{C}^{2^n \times 2^n}$ with eigenvalues $e^{i\theta_1}, e^{i\theta_2}, e^{i\theta_{2^n}}$: $\forall j, k \frac{\theta_j}{\pi} \notin \mathbb{Q} \frac{\theta_j}{\theta_k} \notin \mathbb{Q}$.

$\forall n \in \mathbb{N} U^n$ has eigenvalues $e^{in\theta_1}, e^{in\theta_2}, e^{in\theta_{2^n}}$,
each n defines therefore a point on a 2^k-torus.
If $U = e^{iA}\ \forall \lambda \in \mathbb{R} \forall \varepsilon \exists n : E\left(U^n, e^{i\lambda A}\right) < \varepsilon$.
By switching leads we can get another "generic" qbit gate $U^{=} PUP'$, where might be $P = SWAP$.
It can easily been shown, that $\left\{e^{i\lambda A}\right\}$ have a closed Lie Algebra.
$U' = e^{iB}, B = PAP^{-1}$;
by explicit computation can be shown, that the complete Lie-Algebra of $U(4)$ can be computed by successives commutation, starting by A and B.

Efficiency of Approximation

Theorem

Solovay-Kitaev theorem:
Any quantum circuit containing m CNOTs and single qbit gates can be approximatet to an accuracy ε using only $O\left(m \log^c(m/\varepsilon)\right)$ gates from a discrete set, where $c = \lim_{\substack{\delta \to 0 \\ \delta > 0}} 2 + \delta$.

On one hand $\forall U \in \mathbb{C}^{2^n \times 2^n} : O\left(n^2 4^n \log^c(n^2 4^n/\varepsilon)\right)$ operations are sufficient, on the other hand $\exists U \in \mathbb{C}^{2^n \times 2^n} : \Omega\left(2^n \log(1/\varepsilon)/\log(n)\right)$ operations are required for implementing a $V : E(U, V) \leq \varepsilon$.

Summary

- CNOTs and unitary single Qbit operations form an universal set for quantum computing.
- Unitary single Qbit operations can be approximated to an arbitrary precision by a finite set of gates.
- This approximation cannot always be done efficiently.

Literature

- Michael A. Nielsen, Isaac L. Chuang: *Quantum Computation and Quantum Information*, Chapter 4: *Quantum circuits*
- John Preskill: *Lecture Notes for Quantum Information and Computation*, Chapter 6.2.3: *Universal quantum gates*