Elementary Quantum Gates and Identities

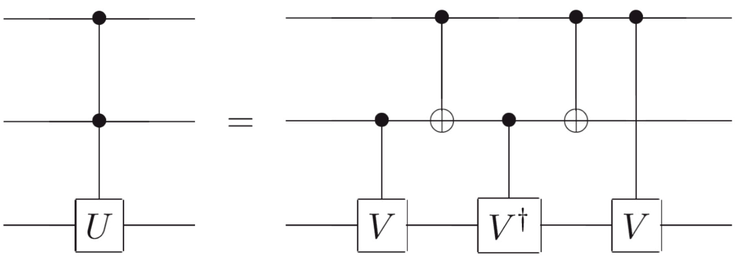
- Three other quantum gates
  - **Hadamard, phase, and $\pi/8$ gates:** $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ $S = \begin{bmatrix} 1 & \\ & i \end{bmatrix}$ $T = \begin{bmatrix} 1 & \\ & e^{i\pi/4} \end{bmatrix}$
    - $T^2 = S, S^2 = Z$, and $H = (X+Z)/\sqrt{2}$
  - $HXH = Z; \ HYH = -Y; \ HZH = X$
- Rotation operator: for $A \in \{X, Y, Z\}$: $R_A(\theta) \equiv e^{-i\theta A/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}A$
  - Corollary: $A \in \{X, Y, Z\} = R_A(\pi)$
  - Corresponds to counterclockwise θ rotation about axis A *on the Bloch sphere*
  - $T = e^{i\pi/8}R_z(\pi/4), \ S = e^{i\pi/4}R_z(\pi/2)$
- $XYX = -Y \implies XR_Y(\theta)X = R_Y(-\theta)$
  - Bloch sphere intuition: X maps $(Y, -Y) \mapsto (-Y, Y)$. Plug in formula for $R_Y(\theta)$
  - Similarly, $XZX = -Z, YZY = -Z, Z(-Y)Z = Y$
- $Z\!-\!Y$ decomposition of single-qubit operation: $\forall U, \exists \alpha, \beta, \gamma, \delta : U = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)$
  - Remark: do not neglect the global phase $e^{i\alpha}$
- $\forall U, \exists A, B, C : ABC = I, U \simeq AXBXC$
  - Let $B = R_z(b_1)R_y(b_2)R_z(b_3) = (b_1, b_2, b_3)$, note then $XBX = (-b_1, -b_2, -b_3)$
  - Then for $U = (\alpha, \beta, \gamma), A = (\alpha, \beta/2, 0), B = (0, -\beta/2, -(\gamma+\alpha)/2), C = ((\gamma-\alpha)/2, 0, 0)$

Controlled Quantum Gates

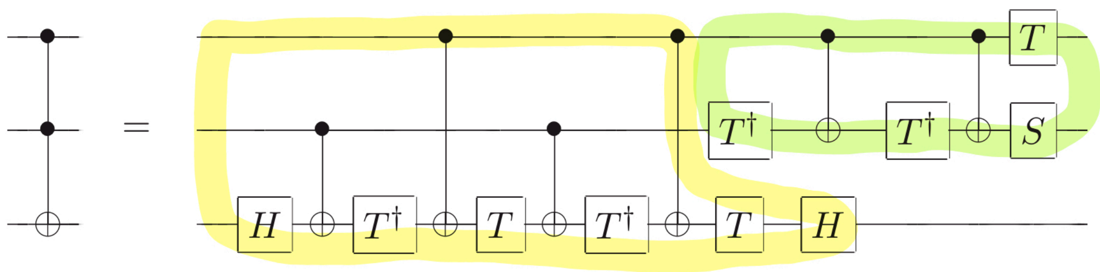
- Prototypical control-gates: $\mathrm{CNOT} = C^X \equiv \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{bmatrix}$ and $C^Z = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}$
  - $HXH = Z \implies C^X = (I \otimes H)C^Z(I \otimes H)$
    - Corollary: CNOT_{12} equals CNOT_{21} in Hadamard basis
      - Note that $C^Z_{12} = C^Z_{21}$, and change into Hadamard basis reverses the roles
- General controlled-operation notation: Given n control qubits and unitary U acting on $|\psi\rangle$,
  $C^n(U)|x_1 \ldots x_n\rangle|\psi\rangle \equiv |x_1 \ldots x_n\rangle U^{x_1 \cdots x_n}|\psi\rangle$
- Generating $C^1(U)$ using C^X and single-qubit gates:

- Nielson: Given $U = e^{i\alpha}AXBXC$ where $ABC = I$, then $C(U) = C^{e^{i\alpha}}AC^XBC^XC$
- Clever trick: $C^{e^{i\alpha}} = \begin{bmatrix} 1 & \\ & e^{i\alpha} \end{bmatrix} \otimes I$
  - *Remark: note how controlled "single-qubit global phase shift" is achieved by op on first qubit only! This phase shift is global, so it doesn't matter where we apply.*
- Shor's method: $C^{R_A(\theta)} = R_A(\theta/2)C^X R_A(-\theta/2)C^X$ for $A \in \{Y, Z\}$, and

  $U = e^{i\alpha}R_z(\alpha R_y(\beta)R_z(\gamma) \implies C(U) = C^{e^{i\alpha}}C^{R_z(\beta)}C^{R_y(\gamma)}C^{R_z(\delta)}$
- Constructing $C^2(U)$ — **Sleator-Weinfurter construction**



- For $V : V^2 = U$, then $C^2(U) = C_{23}(V)C_{12}^X C_{23}(V^\dagger)C_{12}^X C_{13}(V)$
  - $q_1 = 1 - q_2 = 0 : VV^\dagger = I; \quad q_2 = 1 - q_1 = 0 : V^\dagger V = I$
- Example: constructing Toffoli $C^2(X)$



- Consider yellow part: $C^2(-iX)$
  - Note that $XT^\dagger X = e^{-i\pi/4}T$ (this overall phase is not negligible in multi-qubits!)
  - $00 : H(T^\dagger T)^2 H = I; \;\; 01 : HXT^\dagger TXTT^\dagger H = I; \;\; 10 : HT^\dagger XTT^\dagger XTH = I$
  - $11 : HT^4H = HZH = e^{-i\pi/2}X = -iX$
  - Remark: Yellow part provides an alternative way to compute $C^2(U)$ based on $U^{1/4}$
    - It essentially utilizes the identity $T^4 = -iX$
- Green part computes C^S: $|11\rangle \mapsto i|11\rangle$, then $C_{12}^2(-iX)C^S = C^2(X)$
  - $|11x\rangle \mapsto -i|11\neg x\rangle \mapsto i(-i)|11\neg x\rangle = |11\neg x\rangle$
  - Remark: initial idea may be to introduce $C_{12\to 12}^2(-iI)$ into the whole system, we can do better by change the relative phase of the whole system—if both first two qubits are one—even just by operating on qubits 1 & 2

Universality of Quantum Gates

- Arbitrary unitary operator may be expressed *exactly* using single-qubit gates and C^X
- Single-qubit operation may be approximated to arbitrary accuracy via H, S, T
- **Two-level unitary operators** act non-trivially on less than three vector components
- Theorem: arbitrary unitary U on n qubits is the composition of at most $2^{n-1}(2^n - 1) = O(4^n)$ two-level unitary operators
  - Given $\alpha = U_{11} \neq 0,\ \beta = U_{j1} \neq 0$ and $U_{21} = \ldots = U_{(j-1)1} = 0$, consider unitary

$$V = \begin{bmatrix} v_{11} = \frac{\alpha^*}{\sqrt{|\alpha|^2 + |\beta|^2}} & \cdots_0 & v_{1j} = \frac{\beta^*}{\sqrt{|\alpha|^2 + |\beta|^2}} & 0 & \cdots & 0 \\ \vdots_0 & \ddots_1 & \vdots_0 & & & \\ v_{j1} = \frac{\beta}{\sqrt{|\alpha|^2 + |\beta|^2}} & \cdots_0 & v_{jj} = \frac{-\alpha}{\sqrt{|\alpha|^2 + |\beta|^2}} & \cdots & & 0 \\ \vdots & & \vdots & 1 & & \\ & & & & \ddots_1 & \\ 0 & & 0 & & & 1 \end{bmatrix}$$

    - Specified $v_{11}, v_{j1}, v_{1j}, v_{jj}$, and $\forall i, k \notin \{1,j\} : v_{ik} = \delta_{ik}$, and all other entries zero.
  - Then $U' = VU$ satisfies $U'_{21} = \ldots = U'_{j1} = 0,\ \ U'_{(j+1)1} \neq 0$: U_{j1} is newly zeroed out
  - Move on to next j until $U_{j1} = \delta_{j1}$, then by unitary we also have $U_{1j} = \delta_{1j}$
    - Move onto the next column / row — U now acts trivially on one more subspace!
  - For unitary operator on $\mathbb{C}^d$ we need at most $d(d-1)/2$
- Theorem: single-qubit and C^X gates can implement arbitrary two-level unitary operation
  - Given two binary strings $x, y \in \{0,1\}^n$, a **gray code** connecting s, t is a sequence $g_0, \ldots, g_m; (m \leq n)$ such that $g_0 = s, g_m = t$, and g_i, g_{i+1} differ in *exactly* one bit.
  - Given a two-level unitary operation U which applies $U' \in \mathscr{L}(\mathbb{C}^2)$ on span of $|x\rangle, |y\rangle$, let $g_0, \ldots, g_m$ be a gray code connecting x, y, then use CNOTs to effect the cyclic permutation $P = (|g_{m-1}\rangle, \ldots, |g_0\rangle) : |g_0 = x\rangle \mapsto |g_{m-1}\rangle, |g_{m-1}\rangle \mapsto |g_{m-2}\rangle, \ldots, |g_1\rangle \mapsto |g_0\rangle$.
  - We design P by only considering the sequence $|x\rangle \mapsto |g_1\rangle \mapsto |g_2\rangle \mapsto \ldots \mapsto |g_{m-1}\rangle$
    - Let g_i and g_{i+1} differ at k_i, then $P = C^X_{i \neq k_{m-2}} C^X_{i \neq k_{m-3}} \ldots C^X_{i \neq k_1} C^X_{i \neq k_0}$ (each C^X is conditional on all other bits being equal to non-differing bits of g_i, g_{i+1})

- Example: $x = 00001, y = 10111$ with gray code $(00001, 00011, 00111, 10111)$, then $P = C^X(x_{i\neq 0} = 0111)C^X(x_{i\neq 2} = 0011)C^X(x_{i\neq 3} = 0001)$ effects the sequence $|00001\rangle \mapsto |00011\rangle \mapsto |00111\rangle \mapsto |10111\rangle$
- $P(|x\rangle) = |g_{m-1}\rangle, P(|y\rangle) = |g_m\rangle$ differ by only one bit i_0: then $U = P^\dagger C^{n-1}_{i\neq i_0}(U')P$
  - $C(U')$ and each $C^X_{i\neq k_i}$ takes $O(n)$ gates, so P thus U takes $O(n^2)$ gates
- Corollary: At most $O(n^2)$ single qubit and C^X gates needed for arbitrary 2-level unitary op

Approximating Single-qubit Gates via Discrete set

- Motivating problem: it's hard to implement arbitrary single-qubit op fault-tolerantly
- Define the **error** when V is implemented instead of U by $E(U, V) = \max_{|\psi\rangle} \|(U - V)|\psi\rangle\|$
  - For arbitrary measurement M and $|\psi\rangle$, $|P_U - P_V| \leq 2E(U, V)$
    - $P_U \equiv \langle\psi|U^\dagger M U|\psi\rangle, P_V \equiv \langle\psi|V^\dagger M V|\psi\rangle$. Let $|\Delta\rangle = (U - V)|\psi\rangle$, then $|P_U - P_V| = \langle\psi|U^\dagger M|\Delta\rangle + \langle\Delta|MV|\psi\rangle = \langle\psi|U^\dagger M(U - V)|\psi\rangle + \langle\psi|(U - V)^\dagger MV|\psi\rangle$ thus $|P_U - P_V| \leq 2\||\Delta\rangle\|^2 = 2E(U, V)$
  - $E\left(\prod U_i, \prod V_i\right) \leq \sum E(U_i, V_i)$: $\|(U_2U_1 - V_2V_1)|\psi\rangle\| = \|(U_2 - V_2)U_1|\psi\rangle + V_2(U_1 - V_1)|\psi\rangle\|$
  - Corollary: $\forall j = 1, \ldots, m : E(U_i, V_i) \leq \Delta(2_m) \implies E(U_m \ldots U_1, V_m \ldots V_1) \leq \Delta$
- The **standard set** of universal gates: H, T, C^X. Alternative: $H, S, C^X, C^2(X)$
- **Theorem: H, T may approximate any single-qubit operation to arbitrarily small error**
  - $T \cong R_z(\pi/4)$ and $HTH \cong R_x(\pi/4)$ (recall that $H = R_{(x+z)/\sqrt{2}}(\pi)$), then

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

    corresponds to $R_n(\theta)$ where $n = \dfrac{1}{\sqrt{1 + \sin^2(\pi/8)}}\left(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8}\right)$ and

    $\theta = \arccos(2\cos^2(\pi/8))$
    - Note that $\sin(\theta/2) = \dfrac{\sin(\pi/8)}{\sqrt{1 + \cos^2(\pi/8)}}$
  - Now $2\pi/\theta$ is irrational, so $(\theta_n) = (n\theta \mod 2\pi)$ must be dense in $[0, 2\pi)$:
    - Given each $\alpha \in [0, 2\pi), \delta > 0$ for $N > 2\pi/\delta$ by pigeonhole principle there must be $\theta_i, \theta_j : 0 < \theta_i - \theta_j < 2\pi/N < \delta$, then for some n we must have $|\theta_{n(i-j)} - \alpha| < \delta$

- Lemma $\forall \epsilon > 0, \exists \delta : E(R_n(\theta), R_n(\theta + \delta)) < \epsilon$:

  $\|(R_n(\theta) - R_n(\theta+\delta))|\psi\rangle\| = \| \left(\left(\cos\frac{\theta}{2} - \cos\frac{\theta+\delta}{2} \right) I - i(n\cdot\sigma)\left(\sin\frac{\theta}{2} - \sin\frac{\theta+\delta}{2} \right) \right) |\psi\rangle\| \leq \delta$

- Now $\forall \alpha, HR_n(\alpha)H = R_m(\alpha)$ for $m = (\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$

- Lemma: $\forall \hat{n}, \hat{m}, \hat{v} \in \mathbb{R}^3, \theta : \hat{n} \neq \hat{m} \implies R_{\hat{v}}(\theta) = \left(\prod_{j=1}^{k} R_{\hat{n}}(\beta_j) R_{\hat{m}}(\gamma_j) \right) R_{\hat{n}}(\alpha)$

  - Suppose the angle between $\hat{n}, \hat{m}$ is $\langle \hat{n}, \hat{m} \rangle = \phi$: $R_{\hat{n}}(\alpha)$ rotates the axis itself, and first application of the product terms allows us to map $\hat{n} \mapsto \hat{n}'$ such that $\langle \hat{n}', \hat{n} \rangle \leq 2\phi$, second application $\langle \hat{n}, \hat{n}'' \rangle \leq 4\phi$ etc.., until $n(\phi) \geq \pi$ suffices to cover the whole hemisphere

- **Solovay-Kitaev Theorem**: Arbitrary single qubit gate may be approximated to accuracy $1 - \epsilon$ using $O(\log^c(1/\epsilon))$ H, T gates where $c \simeq 2$