Topological Quantum Computation

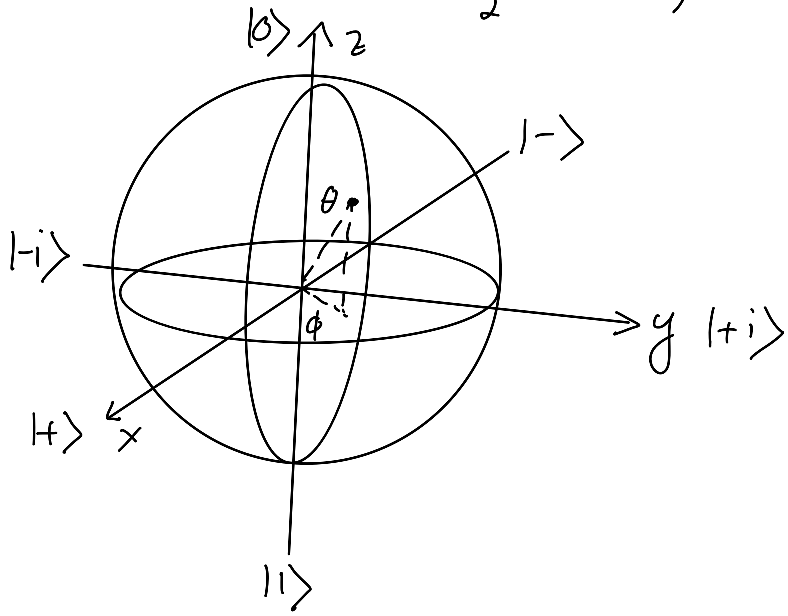
§1.1 Quantum Bit and Elementary Operations

The "qubit" is defined as a linear superposition of two orthogonal quantum states $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

with $\alpha, \beta \in \mathbb{C}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$

$$\longrightarrow \quad \alpha = \cos\frac{\theta}{2}, \quad \beta = e^{i\phi}\sin\frac{\theta}{2}$$



"Bloch sphere"

Time evolution is given in terms of unitary operators. Pauli operators:

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

Z-eigenstates: $|0\rangle$, $|1\rangle$

$$|1\rangle = X|0\rangle, \quad |0\rangle = X|1\rangle \qquad \text{"spin flip"}$$

X-eigenstates:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Y-eigenstates:

$$|+i\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \qquad |-i\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

Hadamard and phase S operators:

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

$$H: \{|0\rangle, |1\rangle\} \leftrightarrow \{|+\rangle, |-\rangle\}$$

$$S: \{|+\rangle, |-\rangle\} \leftrightarrow \{|+i\rangle, |-i\rangle\}$$

equivalently:

$$X = HZH, \quad Y = SXS^\dagger$$

$\rightarrow$ H and S are "Clifford gates"

Measurement of qubit $|\psi\rangle$ in Z-basis

$\rightarrow$ outcomes 0 and 1 have probabilities

$$p_0 = |\langle 0|\psi\rangle|^2 = \mathrm{Tr}\left[|0\rangle\langle 0|\psi\rangle\langle\psi|\right]$$

$$p_1 = |\langle 1|\psi\rangle|^2 = \mathrm{Tr}\left[|1\rangle\langle 1|\psi\rangle\langle\psi|\right]$$

Suppose we have quantum states $|\psi\rangle$ and $|\phi\rangle$ with probability p_ψ and p_ϕ,

$\rightarrow$ "density matrix":

$$\rho = p_\psi\, |\psi\rangle\langle\psi| + p_\phi\, |\phi\rangle\langle\phi|$$

more generaly:

$$\rho = \sum_k p_k |\psi\rangle\langle\psi|$$

ρ is positive self-adjoint operator with $\mathrm{Tr}[\rho] = 1$

Mixed state can be represented as a point inside the Bloch sphere

$$(r_x, r_y, r_z) = (\mathrm{Tr}[X\rho], \mathrm{Tr}[Y\rho], \mathrm{Tr}[Z\rho])$$

For a pure state $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$, the coordinates are

$$(r_x, r_y, r_z) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$$

§ 1.2 The Solovay-Kitaev algorithm

Let us define an "instruction set"

Definition 1:

An instruction set $\mathcal{G}$ for a d-dimensional qudit is a finite set of quantum gates satisfying:

1) All gates $g \in \mathcal{G}$ are in $SU(d)$
2) For $g \in \mathcal{G} \longrightarrow g^\dagger \in \mathcal{G}$ also
3) $\mathcal{G}$ is a "universal" set for $SU(d)$, i.e. the group generated by $\mathcal{G}$ is dense in $SU(d)$.

This means: given $U \in SU(d)$, $\varepsilon > 0$ $\exists$ $S \equiv g_1 \cdots g_m$ with $g_i \in \mathcal{G}$ such that $\|U - S\| < \varepsilon$

In the above, a sequence of instructions generating a unitary operation S is an "ε-approximation" to U if

$$d(U,S) \equiv \|U-S\| \equiv \sup_{\|\psi\|=1} \|(U-S)\psi\| < \varepsilon$$

Example 1:

Define the "$\frac{\pi}{8}$-gate" $T = e^{i\pi/8}\begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$

$\longrightarrow$ the set $\{H, T\}$, i.e. the Hadamard and $\frac{\pi}{8}$-gates, is an instruction set for $SU(2)$ (will show later).

Question:

Given an instruction set, $\mathcal{G}$, how may we approximate an arbitrary quantum gate with a sequence of instructions from $\mathcal{G}$ most efficiently?

$\longrightarrow$ "quantum compilation"

Theorem 1 (Solovay-Kitaev):

Let $\mathcal{G}$ be an instruction set for $SU(d)$, and let $\varepsilon > 0$ be given. Then $\exists$ $c > 0$ s.th. $\forall$ $U \in SU(d)$: $\exists$ finite sequence $S \subset \mathcal{G}$

of length $O(\log^c(1/\varepsilon))$ with $d(U,S) < \varepsilon$.

<u>Implementation:</u>

function Solovay-Kitaev(Gate U, depth n)
if $(n == 0)$
  Return Basic Approximation to U
else
  Set $U_{n-1} = $ Solovay-Kitaev$(U, n-1)$
  Set $V, W = $ GC-Decompose$(U U_{n-1}^\dagger)$
  Set $V_{n-1} = $ Solovay-Kitaev$(V, n-1)$
  Set $W_{n-1} = $ Solovay-Kitaev$(W, n-1)$
  Return $U_n = V_{n-1} W_{n-1} V_{n-1}^\dagger W_{n-1}^\dagger U_{n-1}$;

Let's examine each line in detail:

function Solovay-Kitaev(Gate U, depth n)

target   controls accuracy

returns sequence approximating U to accuracy ε_n with $\varepsilon_n \to 0$ as $n \to \infty$

The algorithm is recursive and terminates at

if $(n == 0)$ Return Basic Approximation to U

means finding a basic ε_0-appr. to U.

$\longrightarrow$ can be implemented by storing a large number of instruction sequences from $\mathcal{G}$.

At higher levels of recursion we have

else

Set $U_{n-1} = \text{Solovay-Kitaev}(U, n-1)$

returns ε_{n-1}-appr. U_{n-1} to U

Define $\Delta \equiv U U_{n-1}^{\dagger}$

$\longrightarrow \quad \| \Delta - I \| < \varepsilon_{n-1}$

then decompose

$$\Delta = \underbrace{V W V^{\dagger} W^{\dagger}}_{\text{"group commutator"}} \quad \text{(will show later how)}$$

with $d(I,V), d(I,W) < c_{gc} \sqrt{\varepsilon_{n-1}}$

Set $V, W = \text{GC-Decompose}(U U_{n-1}^{\dagger})$

In the next step approximate V and W to order ε_{n-1}:

Set $V_{n-1} = \text{Solovay-Kitaev}(V, n-1)$

Set $W_{n-1} = \text{Solovay-Kitaev}(W, n-1)$

It turns out $\| \Delta - V_{n-1} W_{n-1} V_{n-1}^{\dagger} W_{n-1}^{\dagger} \| < \varepsilon_n$

where $\varepsilon_n \equiv c_{appr} \, \varepsilon_{n-1}^{3/2}$

for $\varepsilon_{n-1} < \frac{1}{c_{appr}^2} \longrightarrow \varepsilon_n < \varepsilon_{n-1}$

$\longrightarrow \varepsilon_0 < \frac{1}{c_{appr.}^2}$ (will show $\varepsilon_0 < \frac{1}{32}$)

The algorithm concludes by returning

Return $U_n = V_{n-1} W_{n-1} V_{n-1}^{\dagger} W_{n-1}^{\dagger} U_{n-1}$;