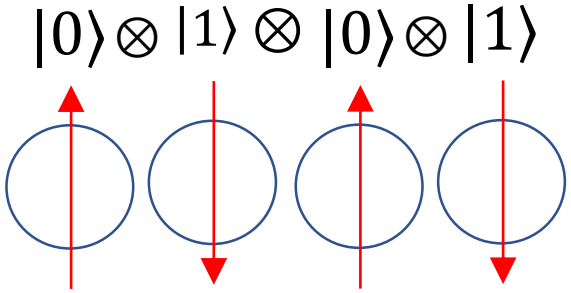
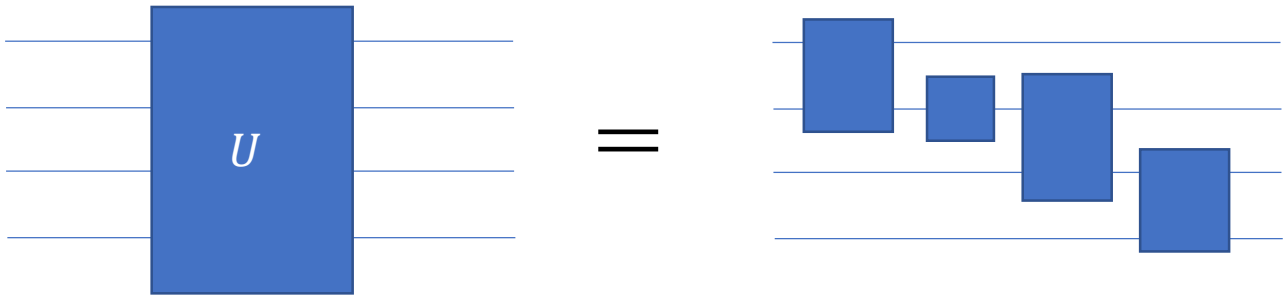
量子計算量理論入門

Vol. 2

Time evolution of n-qubit states

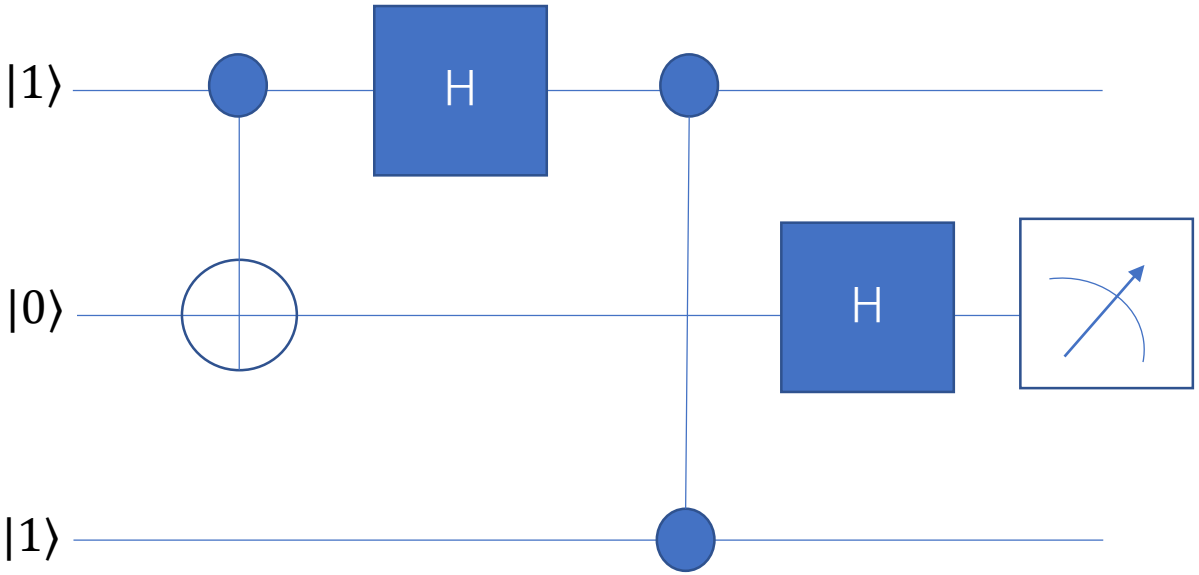
- 状態空間
  - $|0^n\rangle, |0^{n-1}1\rangle, \ldots, |1^n\rangle$で張られる$2^n$次元複素内積空間
- 状態
  - $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$
  - 計算基底で測定すると確率$|\alpha_x|^2$で測定値xを得る
- 時間発展
  - 2^n次ユニタリ行列（n個の量子ビットを変化させるような操作）←一発では無理
  - 1〜3量子ビットに作用するユニタリの列で表現（量子回路: quantum circuit）



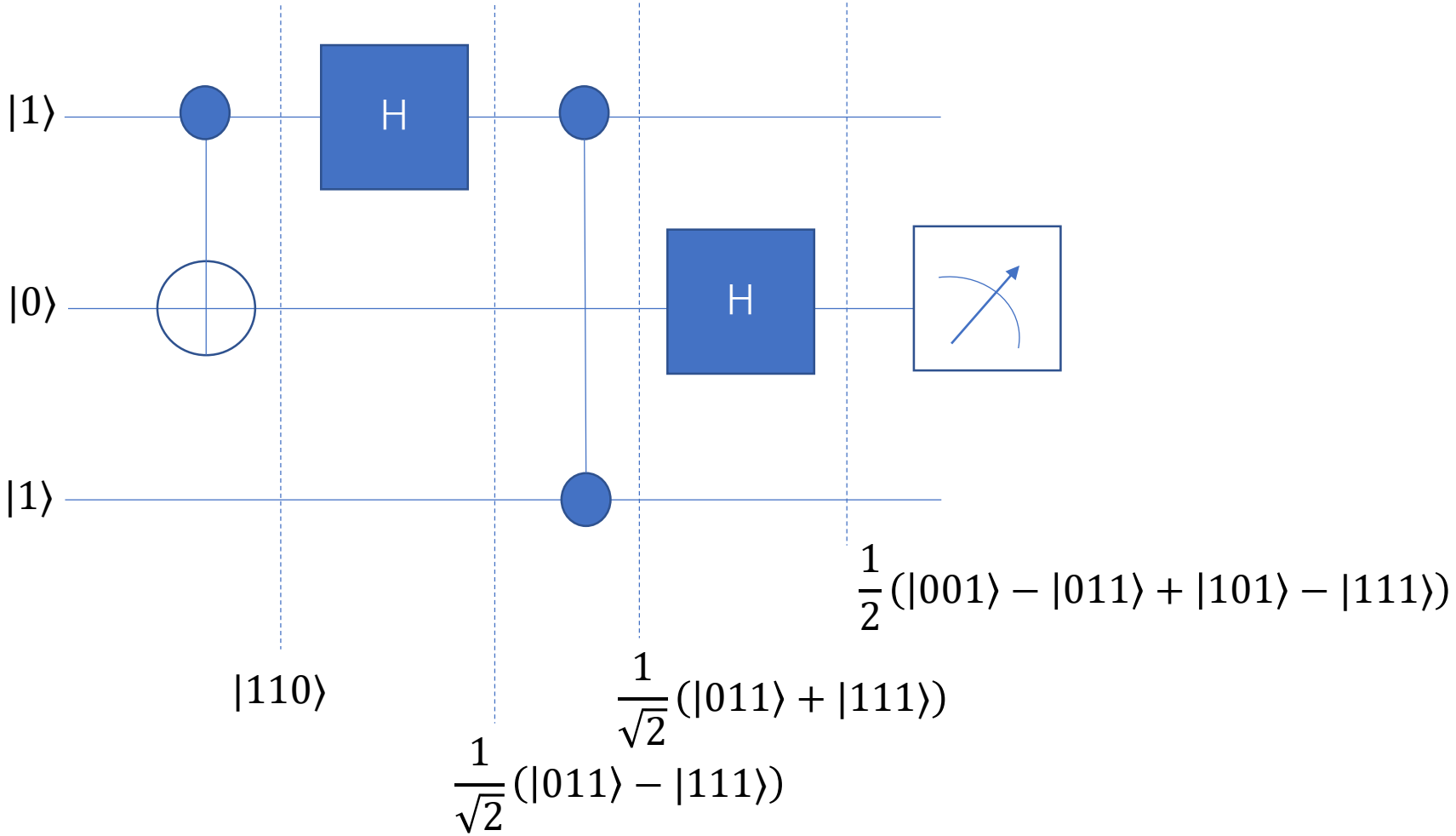


量子回路の例(Examples of quantum circuits)

量子回路(quantum circuit)の例

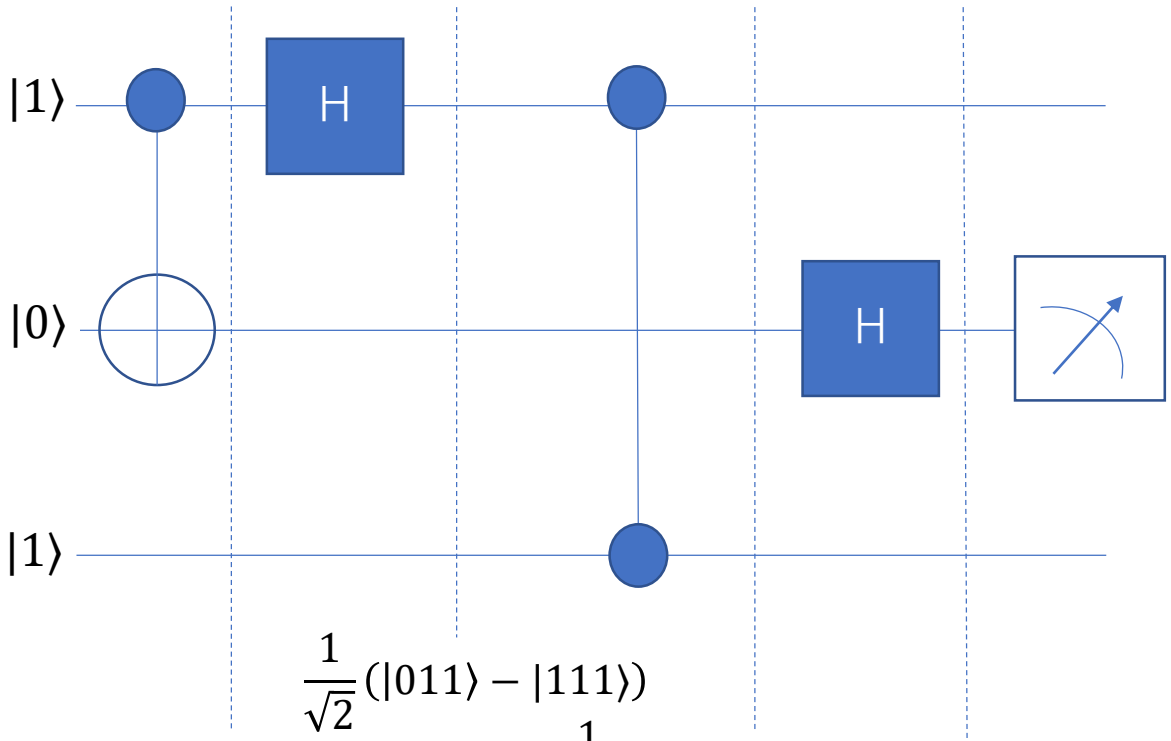


量子回路(quantum circuit)の例



Computation Trees of Quantum Computation

- 量子計算の時間発展は有向木（計算木: computation tree）で表現できる

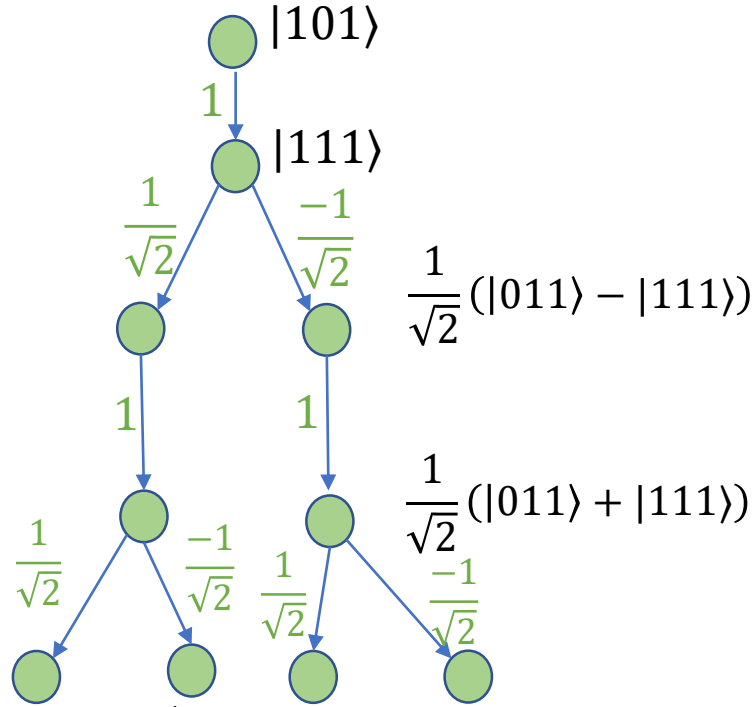


$|111\rangle$

$\frac{1}{\sqrt{2}}(|011\rangle - |111\rangle)$

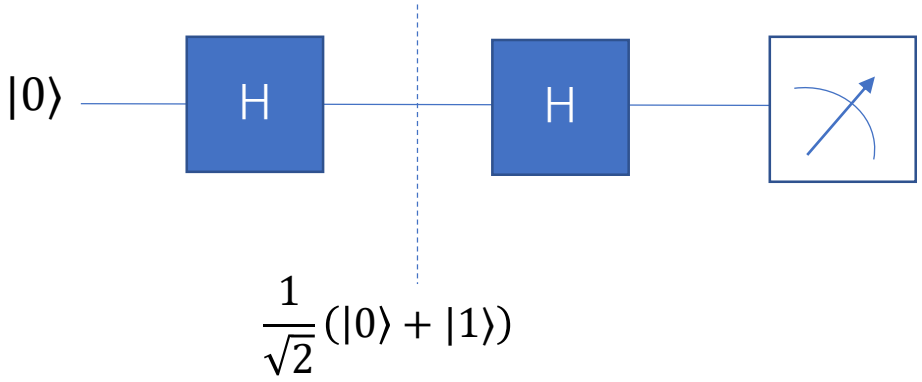
$\frac{1}{\sqrt{2}}(|011\rangle + |111\rangle)$

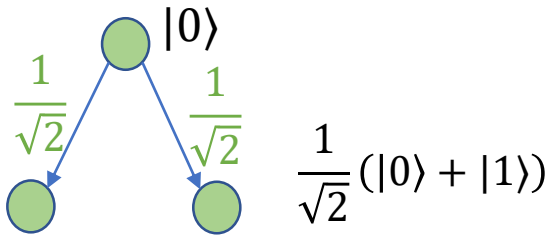
$\frac{1}{2}(|001\rangle - |011\rangle + |101\rangle - |111\rangle)$



Computation Trees of Quantum Computation

- 量子計算の時間発展は有向木（計算木: computation tree）で表現できる





古典計算 vs 量子計算

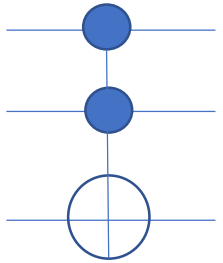
- 量子計算は古典計算で模倣できる
  - n量子ビットの量子回路＝$2^n \times 2^n$行列
  - 量子計算の計算木を追跡する（Feynman’s approach）

古典計算 vs 量子計算

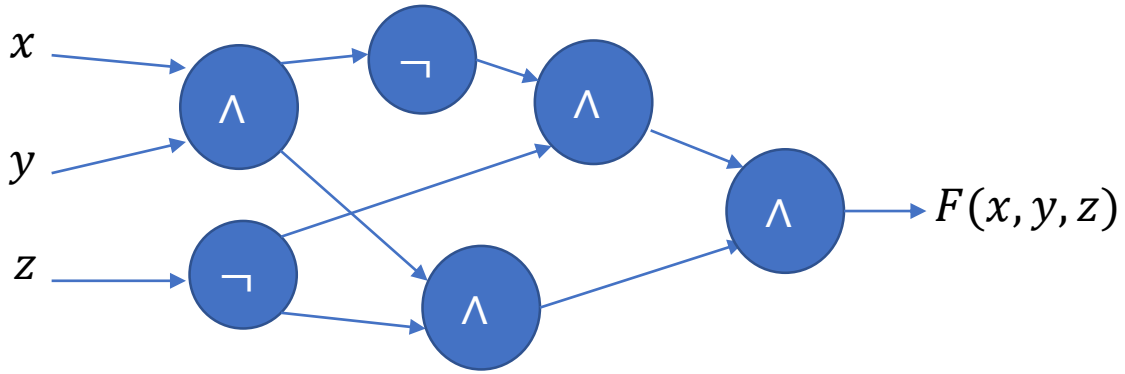
- 量子計算は古典計算で模倣できるが指数時間かかる
- 量子計算は古典計算を効率的に模倣できるのか？
  - 量子回路は可逆
  - ブール回路は非可逆

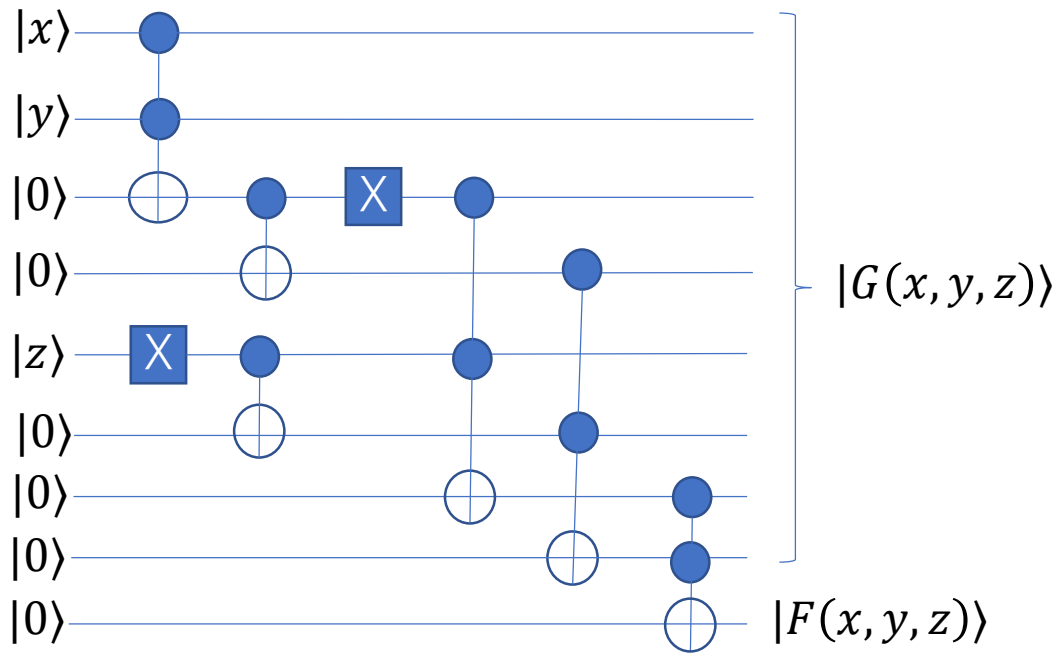
Classical computation can be implemented by Quantum circuits

- Toffoli gate CCX
  - $CC\text{-}X|x\rangle|y\rangle|z\rangle = |x\rangle|y\rangle|z \oplus (x \wedge y)\rangle$
  - NOTとANDを実行可能
- すべての古典計算はToffoli gate（及びCNOT, NOT）のみからなる量子回路で模倣可能(simulatable)



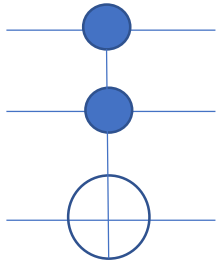
Boolean circuits ⇒ Quantum circuits





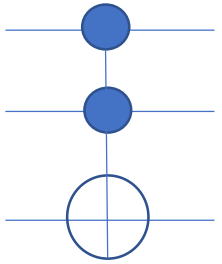
古典計算は量子回路で効率的に模倣可能

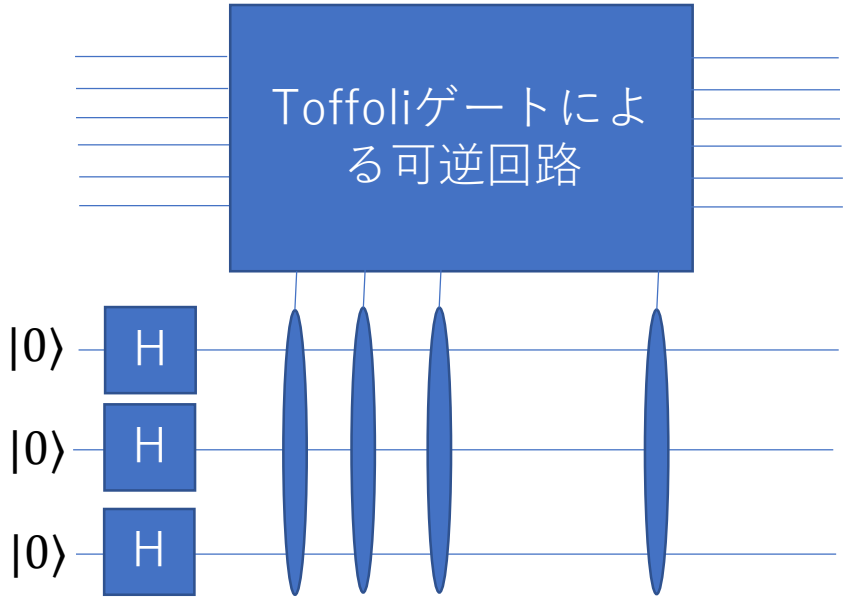
- Toffoliゲート CCX
  - $CC\text{-}X|x\rangle|y\rangle|z\rangle = |x\rangle|y\rangle|z \oplus (x \wedge y)\rangle$
  - NOTとANDを実行可能
- すべてのブール回路はToffoliゲートのみからなる量子回路で模倣可能
- 乱択計算＝ブール回路＋ランダムコイン



古典計算は量子回路で効率的に模倣可能

- Toffoliゲート CCX
  - $CC\text{-}X|x\rangle|y\rangle|z\rangle = |x\rangle|y\rangle|z \oplus (x \wedge y)\rangle$
  - NOTとANDを実行可能
- すべてのブール回路はToffoliゲートのみからなる量子回路で模倣可能
- 乱択計算＝ブール回路＋ランダムコイン
  - ランダムビットはアンシラを$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$に準備





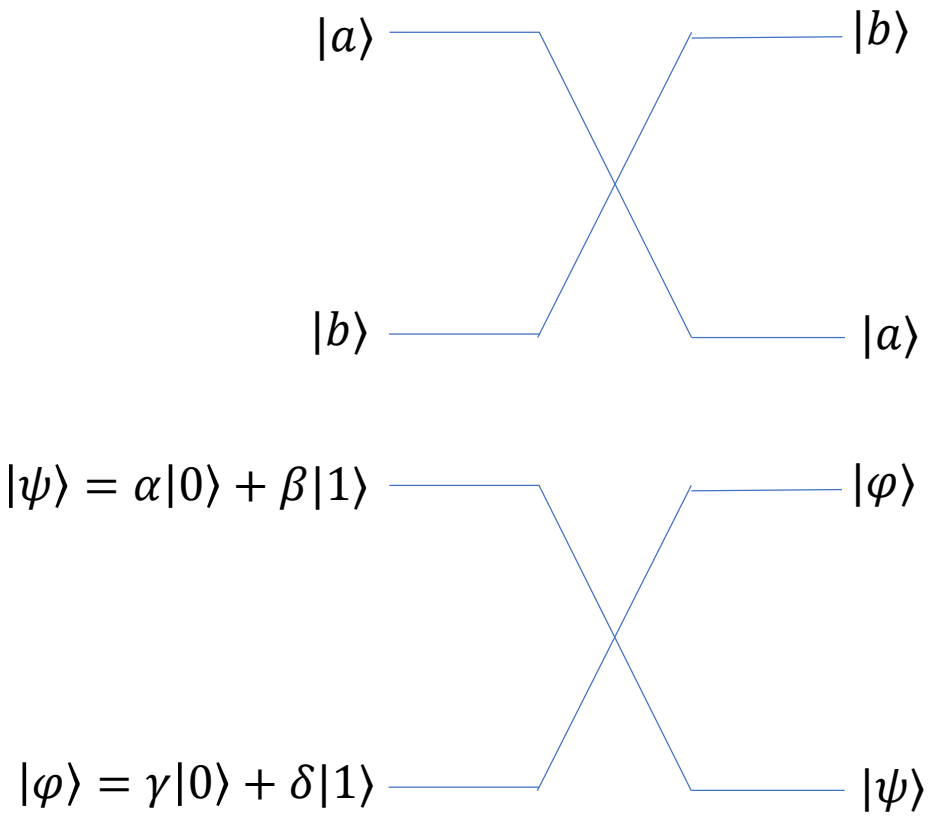
よく使用する量子回路

- 量子ワイヤの交換
- 一様重ね合わせ状態の生成
- 量子フーリエ変換
- 任意の量子状態の生成

量子ワイヤの交換(Swapping quantum wires)

- 2量子ビットゲートSWAP

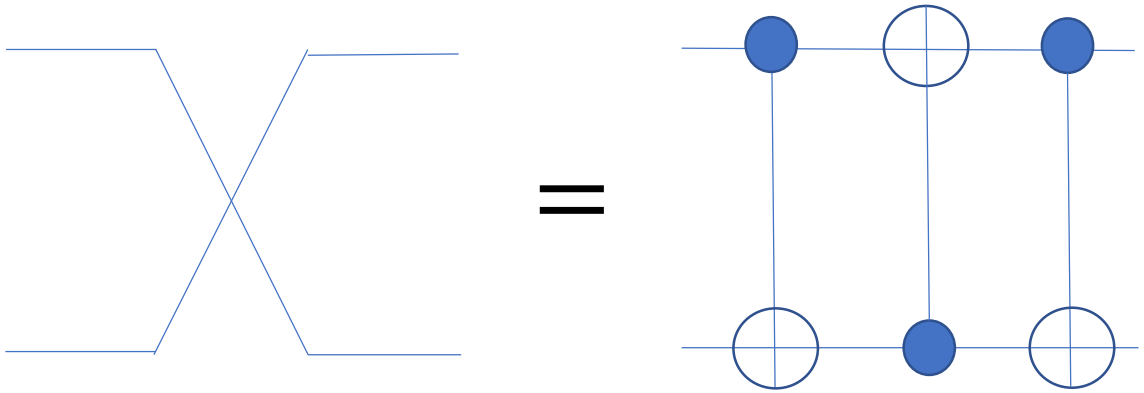
$|ab\rangle \mapsto |ba\rangle \ (a, b \in \{0,1\})$



量子ワイヤの交換(Swapping quantum wires)

- 2量子ビットゲートSWAP

$|ab\rangle \mapsto |ba\rangle \ (a, b \in \{0,1\})$



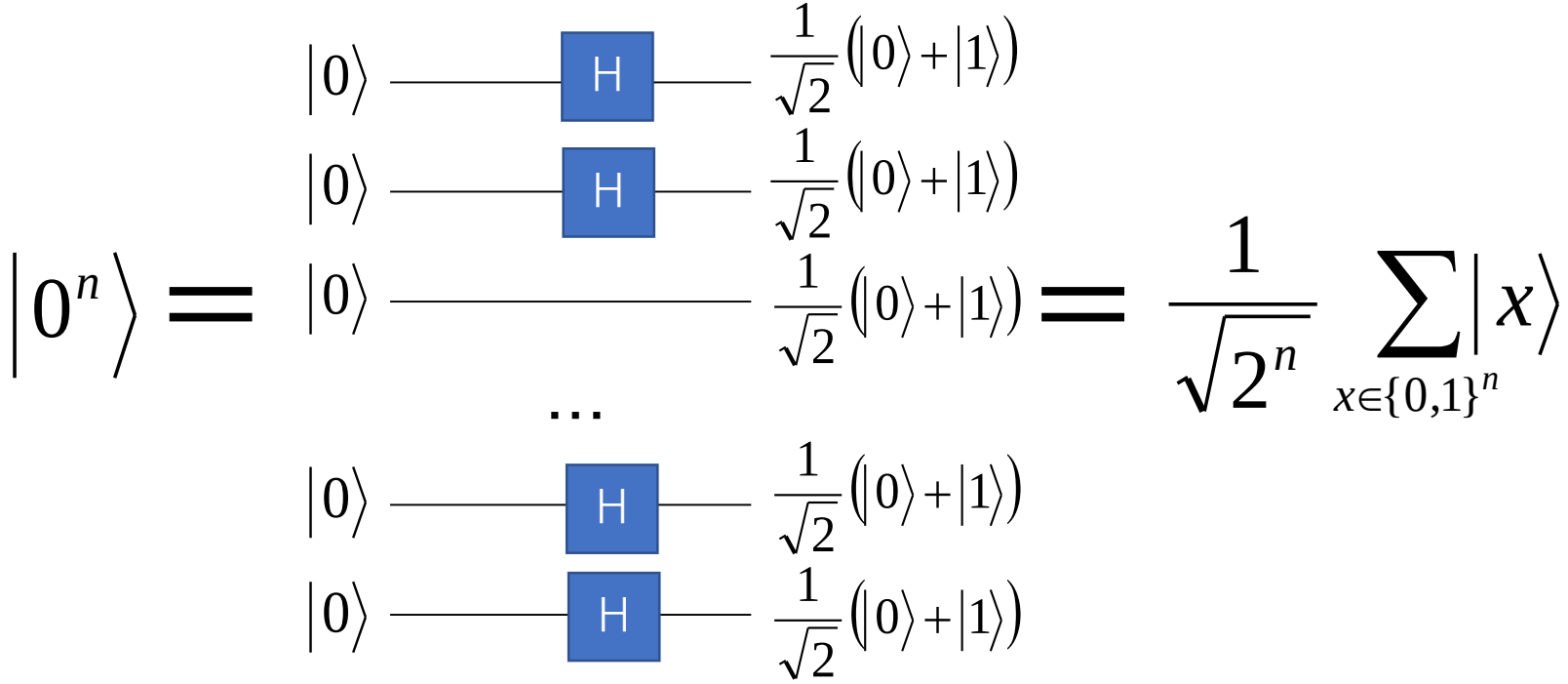
一様重ね合わせ状態(uniform superposition)

- nビット列の一様重ね合わせ状態(uniform superposition)

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

一様重ね合わせ状態(uniform superposition)

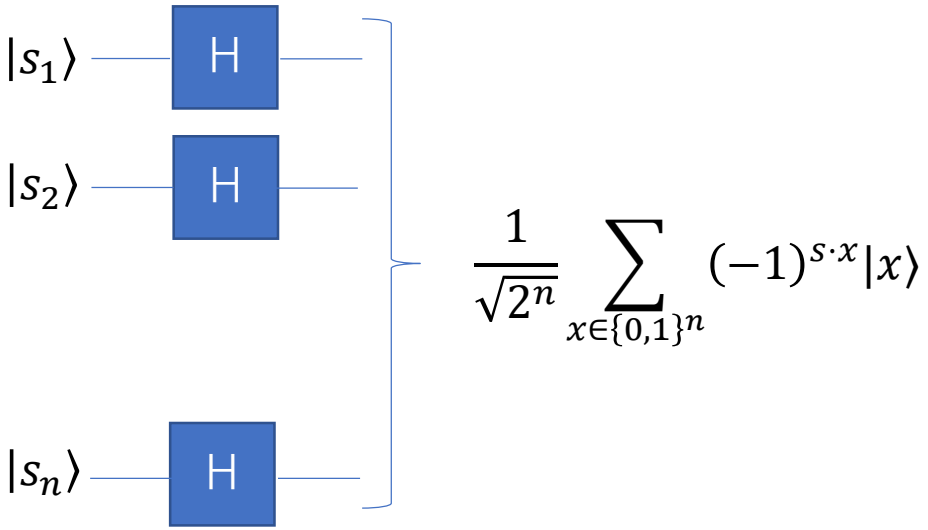
- nビット列の一様重ね合わせ状態の生成



量子アダマール変換(quantum Hadamard transform)

$$H^{\otimes n}|s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{s\cdot x}|x\rangle$$

ただし，$s \cdot x = s_1x_1 + s_2x_2 + \cdots + s_nx_n \pmod 2$



- $H|s_j\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{s_j}|1\rangle)$
- $H|s_1\rangle H|s_2\rangle \cdots H|s_n\rangle$
  $= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{s_1}|1\rangle) \cdots \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{s_n}|1\rangle)$
  $= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{s_1x_1+s_2x_2+\cdots+s_nx_n}|x\rangle$
  $= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{s\cdot x}|x\rangle$

量子フーリエ変換(quantum Fourier transform)

- 離散フーリエ変換

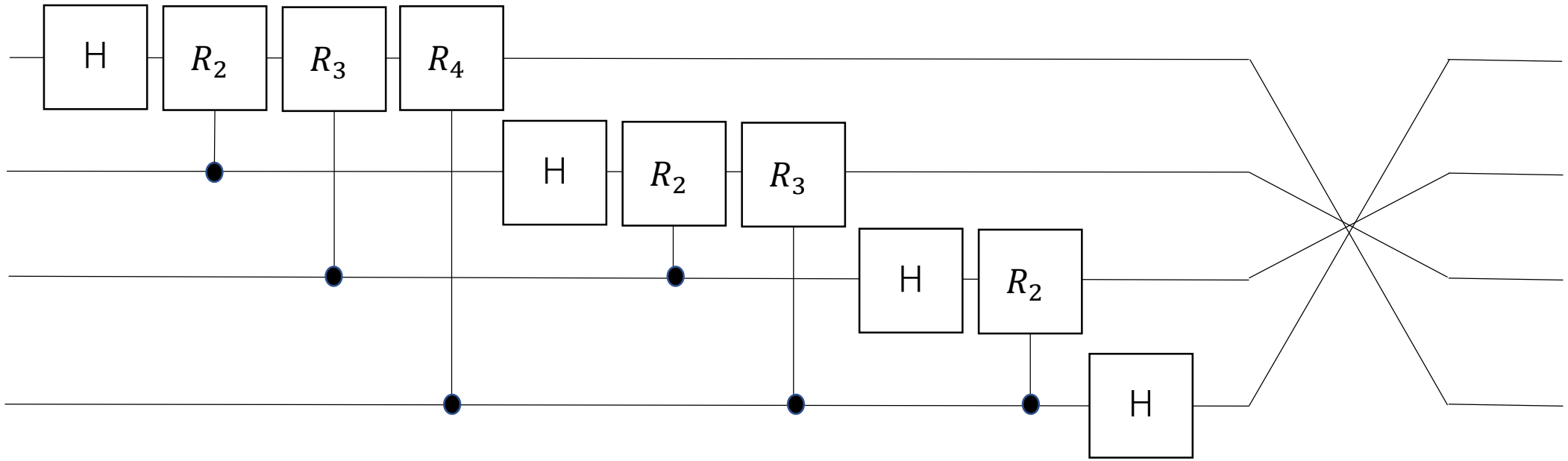
$$\begin{pmatrix} x_0 \\ \vdots \\ x_{m-1} \end{pmatrix} \mapsto \begin{pmatrix} e^{\frac{2\pi i}{m}0\cdot 0} & \cdots & e^{\frac{2\pi i}{m}(m-1)\cdot 0} \\ \vdots & \ddots & \vdots \\ e^{\frac{2\pi i}{m}0\cdot(m-1)} & \cdots & e^{\frac{2\pi i}{m}(m-1)(m-1)} \end{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{m-1} \end{pmatrix}$$

- 量子フーリエ変換

$$FT\colon |j\rangle \mapsto |\hat{j}\rangle := \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} e^{\frac{(2\pi i)jk}{m}} |k\rangle$$

量子Fourier変換

$$FT: |j\rangle \mapsto |\hat{j}\rangle := \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{(2\pi i)jk}{2^n}} |k\rangle$$



回路サイズ（基本ゲート使用数）$= O(n^2)$
離散フーリエ変換だと実行時間$= O(n2^n)$

ただし，$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$

よく使用する量子回路

- 量子ワイヤの交換
- 一様重ね合わせ状態の生成
- 量子フーリエ変換
- 任意の量子状態の生成

Grover-Rudolph

- 任意のn量子ビット状態の生成法
  - 1量子ビット目から順に振幅の重み（絶対値）の比に従って振り分け
  - 最後に各基底状態に対して位相シフト

Grover-Rudolph

- 任意のn量子ビット状態の生成法
  - $|0^n\rangle$からスタート
  - 1量子ビット目から順に振幅の重み（絶対値）の比に従って振り分け

$$|\psi\rangle = |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle$$

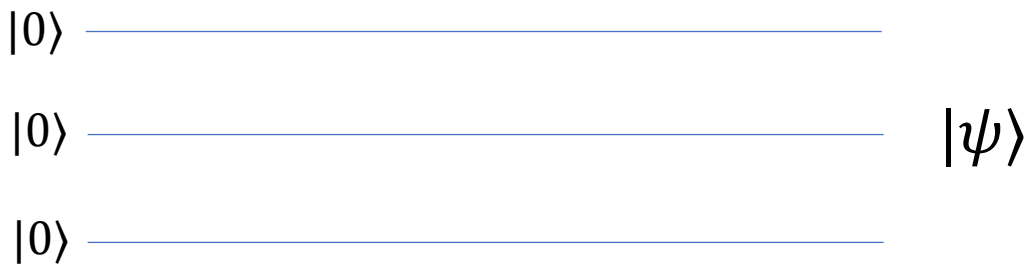
の場合，第1量子ビットを

$$(\||\psi_0\rangle\|)|0\rangle + (\||\psi_1\rangle\|)|1\rangle$$

にする（重みの振り分け）

  - $|\psi_0\rangle, |\psi_1\rangle$についても同様の振り分けを行う

Grover-Rudolph



- 任意のn量子ビット状態の生成法
  - 1量子ビット目から順に振幅の重み（絶対値）の比に従って振り分け
  - 最後に各基底状態に対して位相シフト

例：$|\psi\rangle = \frac{1}{2}|000\rangle - \frac{1}{2}|100\rangle + \frac{1}{2}|110\rangle + \frac{1}{2}|111\rangle$

1量子ビット目から順に振幅の重み（絶対値）の比に従って振り分け

$$|\psi\rangle = |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle$$

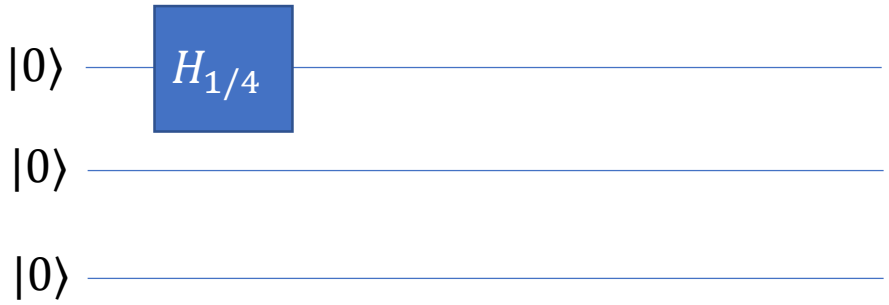
の場合，第1量子ビットを

$$(\||\psi_0\rangle\|)|0\rangle + (\||\psi_1\rangle\|)|1\rangle$$

にする（重みの振り分け）

$|\psi_0\rangle, |\psi_1\rangle$についても同様の振り分けを行う

Grover-Rudolph



- 任意のn量子ビット状態の生成法
  - 1量子ビット目から順に振幅の重み（絶対値）の比に従って振り分け
  - 最後に各基底状態に対して位相シフト

$$H_a = \begin{pmatrix} \sqrt{a} & \sqrt{1-a} \\ \sqrt{1-a} & -\sqrt{a} \end{pmatrix}$$

例：$|\psi\rangle = \frac{1}{2}|000\rangle - \frac{1}{2}|100\rangle + \frac{1}{2}|110\rangle + \frac{1}{2}|111\rangle$

$$(= |0\rangle\left(\frac{1}{2}|00\rangle\right) + |1\rangle\left(-\frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\right))$$

$$|000\rangle \mapsto \left(\sqrt{\frac{1}{4}}|0\rangle + \sqrt{\frac{3}{4}}|1\rangle\right)|00\rangle = \frac{1}{2}|000\rangle + \frac{\sqrt{3}}{2}|100\rangle$$

1量子ビット目から順に振幅の重み（絶対値）の比に従って振り分け

$$|\psi\rangle = |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle$$

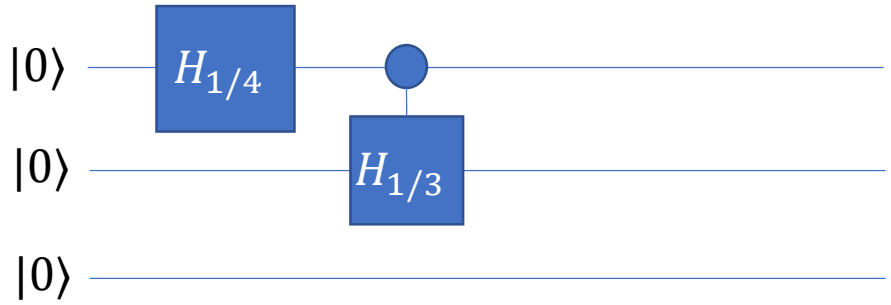
の場合，第1量子ビットを

$$(\||\psi_0\rangle\|)|0\rangle + (\||\psi_1\rangle\|)|1\rangle$$

にする（重みの振り分け）

$|\psi_0\rangle, |\psi_1\rangle$についても同様の振り分けを行う

Grover-Rudolph



- 任意のn量子ビット状態の生成法
  - 1量子ビット目から順に振幅の重み（絶対値）の比に従って振り分け
  - 最後に各基底状態に対して位相シフト

$$H_a = \begin{pmatrix} \sqrt{a} & \sqrt{1-a} \\ \sqrt{1-a} & -\sqrt{a} \end{pmatrix}$$

例：$|\psi\rangle = \frac{1}{2}|000\rangle - \frac{1}{2}|100\rangle + \frac{1}{2}|110\rangle + \frac{1}{2}|111\rangle$

$$(= |0\rangle\left(\frac{1}{2}|00\rangle\right) + |1\rangle\left(-\frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\right))$$

$$\left(-\frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\right)$$
$$= |0\rangle\left(-\frac{1}{2}|0\rangle\right) + |1\rangle\left(\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$

$$|000\rangle \mapsto \frac{1}{2}|000\rangle + \frac{\sqrt{3}}{2}|100\rangle$$
$$\mapsto \frac{1}{2}|000\rangle + \frac{\sqrt{3}}{2}|1\rangle\left(\sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{2}{3}}|10\rangle\right)$$

1量子ビット目から順に振幅の重み（絶対値）の比に従って振り分け

$$|\psi\rangle = |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle$$

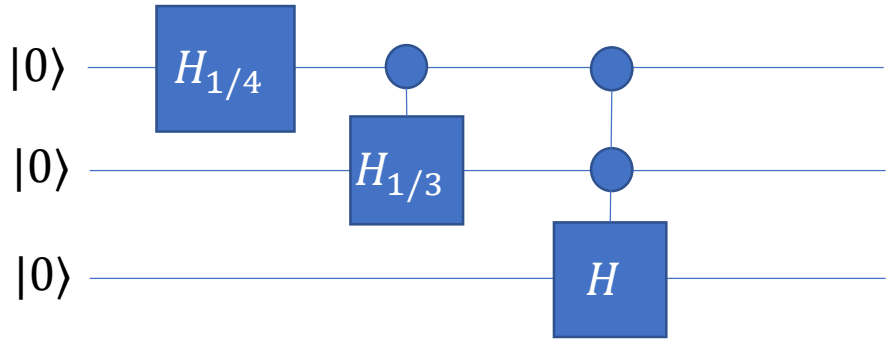
の場合，第1量子ビットを

$$(\||\psi_0\rangle\|)|0\rangle + (\||\psi_1\rangle\|)|1\rangle$$

にする（重みの振り分け）

$|\psi_0\rangle, |\psi_1\rangle$についても同様の振り分けを行う

Grover-Rudolph



- 任意のn量子ビット状態の生成法
  - 1量子ビット目から順に振幅の重み（絶対値）の比に従って振り分け
  - 最後に各基底状態に対して位相シフト

CC-$U|a\rangle|b\rangle|c\rangle = |a\rangle|b\rangle U^{ab}|c\rangle$

例：$|\psi\rangle = \frac{1}{2}|000\rangle - \frac{1}{2}|100\rangle + \frac{1}{2}|110\rangle + \frac{1}{2}|111\rangle$

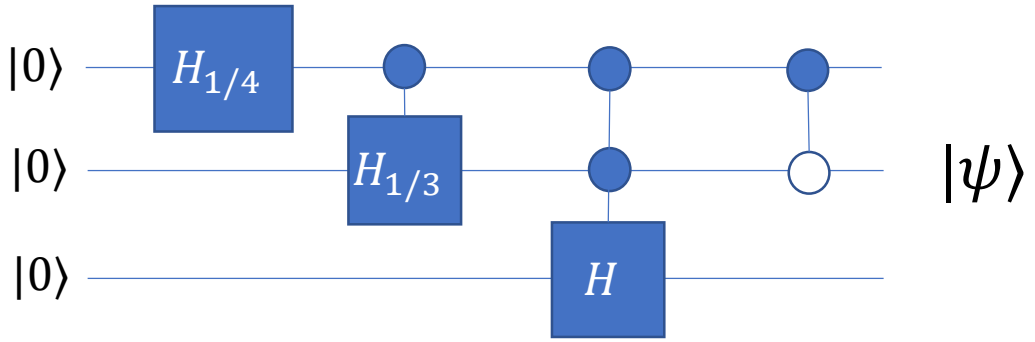
$(= |0\rangle\left(\frac{1}{2}|00\rangle\right) + |1\rangle\left(-\frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\right))$

$|000\rangle \mapsto \frac{1}{2}|000\rangle + \frac{\sqrt{3}}{2}|100\rangle$

$\mapsto \frac{1}{2}|000\rangle + \frac{\sqrt{3}}{2}|1\rangle\left(\sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{2}{3}}|10\rangle\right)$

$\mapsto \frac{1}{2}|000\rangle + \frac{\sqrt{3}}{2}|1\rangle\left(\sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{2}{3}}|1\rangle\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\right) = \frac{1}{2}|000\rangle + \frac{1}{2}|100\rangle + \frac{1}{2}|110\rangle + \frac{1}{2}|111\rangle$

Grover-Rudolph



- 任意のn量子ビット状態の生成法
  - 1量子ビット目から順に振幅の重み（絶対値）の比に従って振り分け
  - 最後に各基底状態に対して位相シフト

例：$|\psi\rangle = \frac{1}{2}|000\rangle - \frac{1}{2}|100\rangle + \frac{1}{2}|110\rangle + \frac{1}{2}|111\rangle$

$(= |0\rangle\left(\frac{1}{2}|00\rangle\right) + |1\rangle\left(-\frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\right))$

$$|000\rangle \mapsto \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right)|00\rangle = \frac{1}{2}|000\rangle + \frac{\sqrt{3}}{2}|100\rangle$$

$$\mapsto \frac{1}{2}|000\rangle + \frac{\sqrt{3}}{2}|1\rangle\left(\sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{2}{3}}|10\rangle\right)$$

$$\mapsto \frac{1}{2}|000\rangle + \frac{\sqrt{3}}{2}|1\rangle\left(\sqrt{\frac{1}{3}}|00\rangle + \sqrt{\frac{2}{3}}|1\rangle\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)\right) = \frac{1}{2}|000\rangle + \frac{1}{2}|100\rangle + \frac{1}{2}|110\rangle + \frac{1}{2}|111\rangle$$

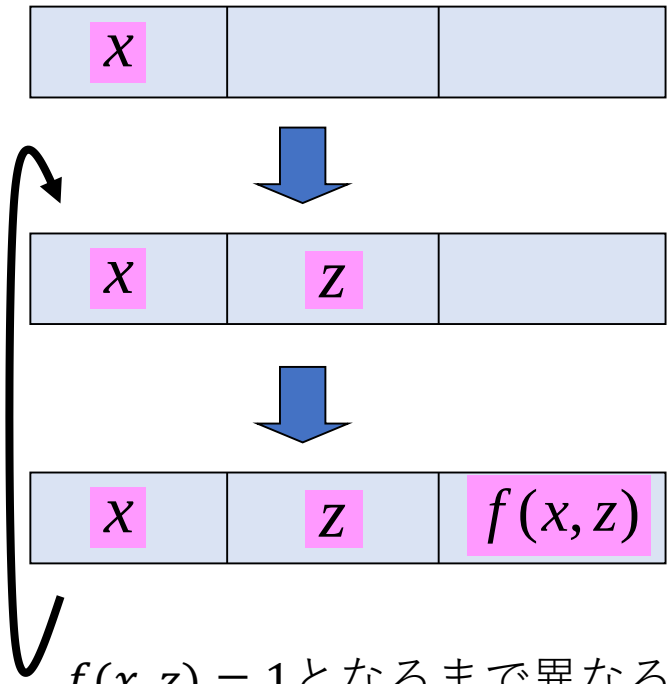
$$\mapsto \frac{1}{2}|000\rangle - \frac{1}{2}|100\rangle + \frac{1}{2}|110\rangle + \frac{1}{2}|111\rangle = |\psi\rangle$$

量子アルゴリズム

Power of Quantum Algorithms

問題(problem)：入力(input) x に対して，$f(x,z)=1$なる解(solution) $z \in \{0,1\}^m$ を見つけよ

従来の（素朴な）アルゴリズム



$f(x,z)=1$となるまで異なるzに対して繰り返し(repetition)

（素朴な）量子アルゴリズム(quantum algorithm)

$$|x\rangle|0\rangle|0\rangle$$

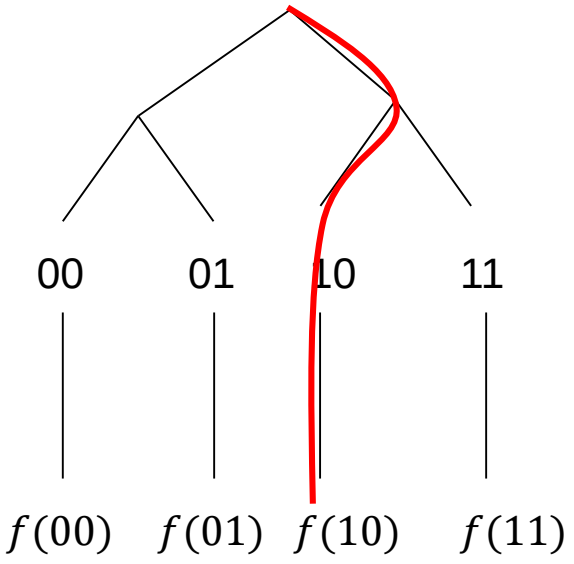
$$\frac{1}{\sqrt{2^m}}\sum_z |x\rangle|z\rangle|0\rangle$$

$$\frac{1}{\sqrt{2^m}}\sum_z |x\rangle|z\rangle|f(x,z)\rangle$$

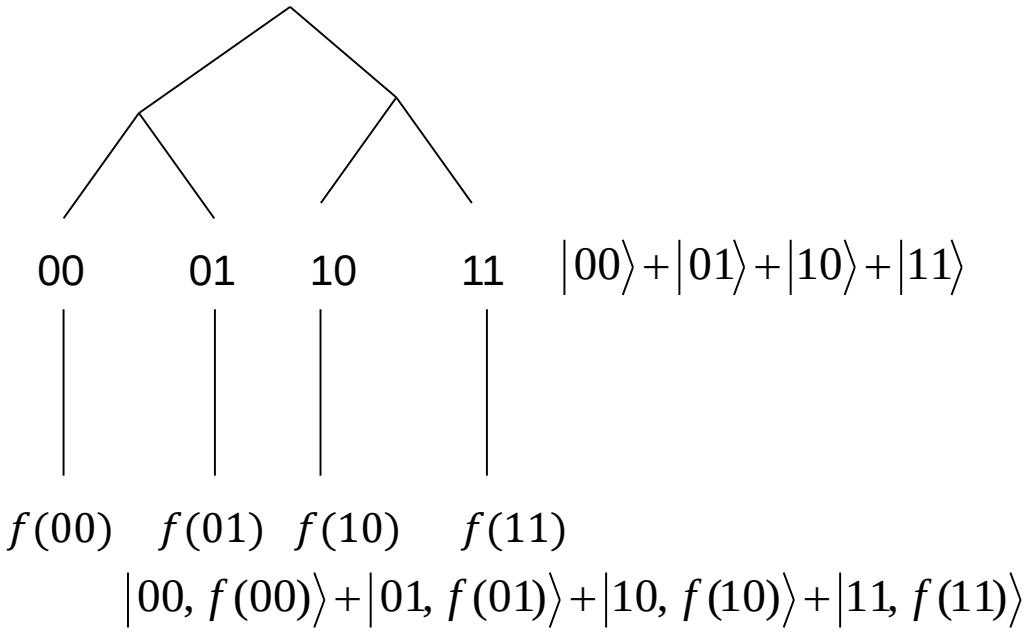
2^m個の$f(x,z)$が量子状態を利用すると並列的に計算可能（量子並列性: quantum parallelism）

Randomized Algorithm vs Quantum Algorithm

乱択アルゴリズム(randomized algorithm)



量子アルゴリズム(quantum algorithm)



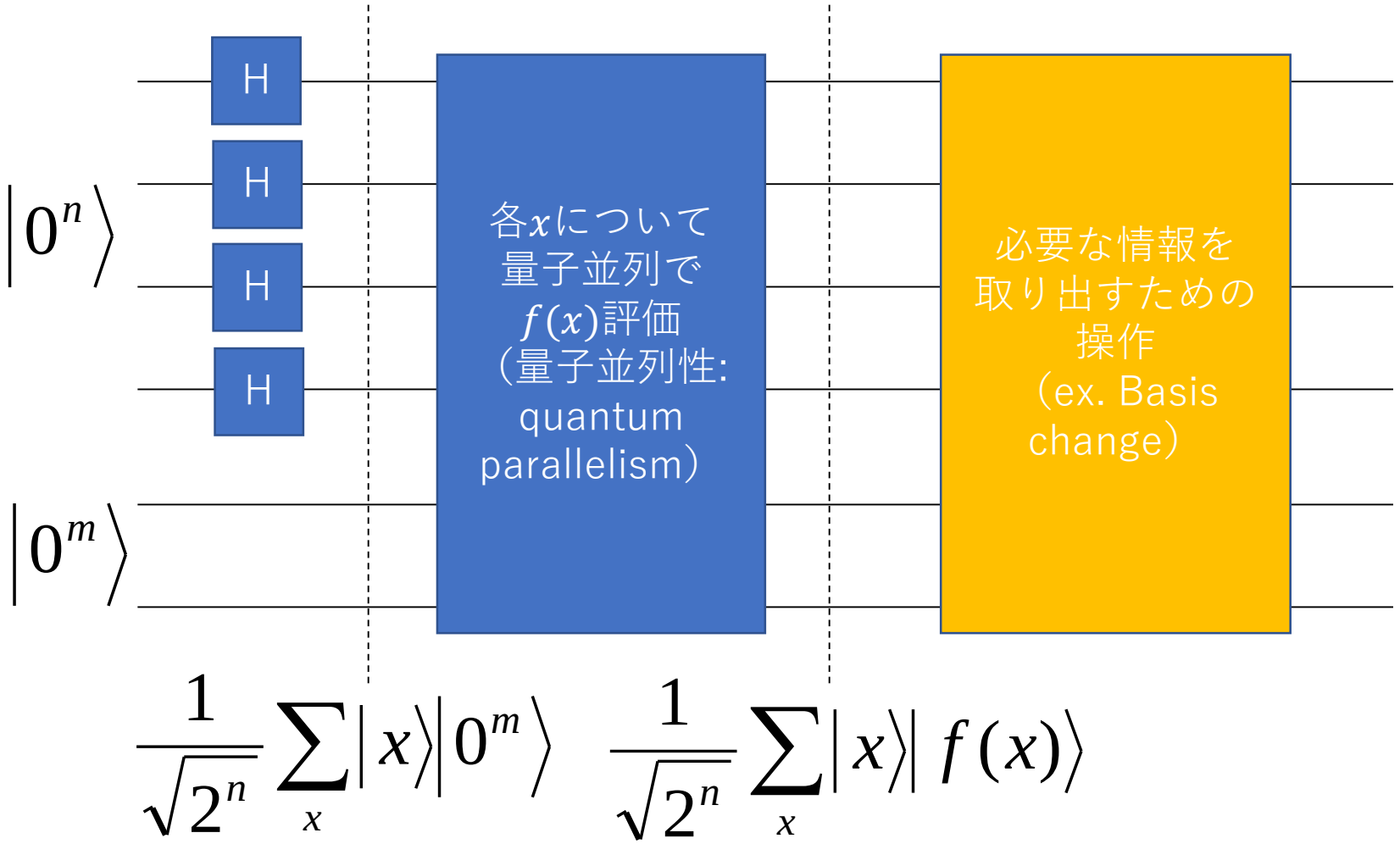
f が評価されるのは

4つの選択肢のうち1つだけ

4つすべてが量子重ね合わせで評価される

fの評価回数自体は1回

Standard Quantum Algorithm



礎となった量子アルゴリズム(Foundational Quantum Algorithms)

- Deutsch-Jozsaのアルゴリズム [Proc.Roy.Soc.Lon, 1992]
  - 量子計算が古典計算に優ることが示された最初のアルゴリズム
  - 決定性古典計算(deterministic classical computation)にのみ優っている
  - 人工的問題(artifitial)
- Bernstein-Vaziraniのアルゴリズム [STOC, 1993]
  - 量子計算が確率計算(randomized algorithm)に優ることが示された最初のアルゴリズム
- Simonのアルゴリズム [FOCS, 1994]
  - 量子計算が確率計算に指数的に優る(exponential speedup)ことが示された最初のアルゴリズム
- Shorのアルゴリズム [FOCS, 1994]
  - 整数の素因数分解問題（および離散対数問題）に対する高速な量子アルゴリズム
- Groverのアルゴリズム [STOC, 1996]
  - 探索問題に対する平方的高速化(quadratic speedup)を実現する量子アルゴリズム

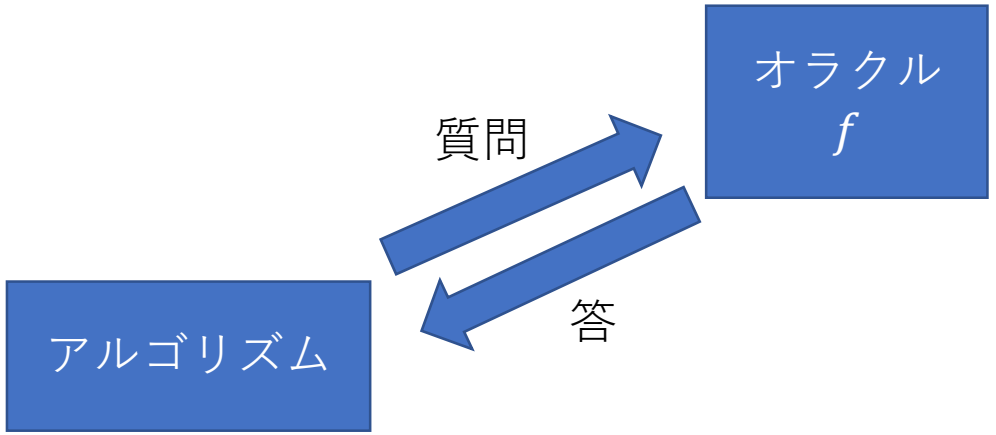
Basic Quantum Algorithms

- Bernstein-Vazirani
- Grover
- Simon (+Shor)
- Factoring by Phase estimation

Bernstein-Vaziraniのアルゴリズム

内積オラクル問題(IP problem)

- 入力（オラクル）：関数 $f:\{0,1\}^n \to \{0,1\}^n$
  - オラクルへのアクセスは質問形式
  - $x = x_1 \cdots x_n$をオラクルに質問すると答$f(x)$が返ってくる
- 約束：ある$s = s_1 \cdots s_n \in \{0,1\}^n$に対して$f(x) = s \cdot x$
  - ただし、$s \cdot x = s_1 x_1 + \cdots + s_n x_n \bmod 2$
- 出力：s



内積オラクル問題(IP problem)

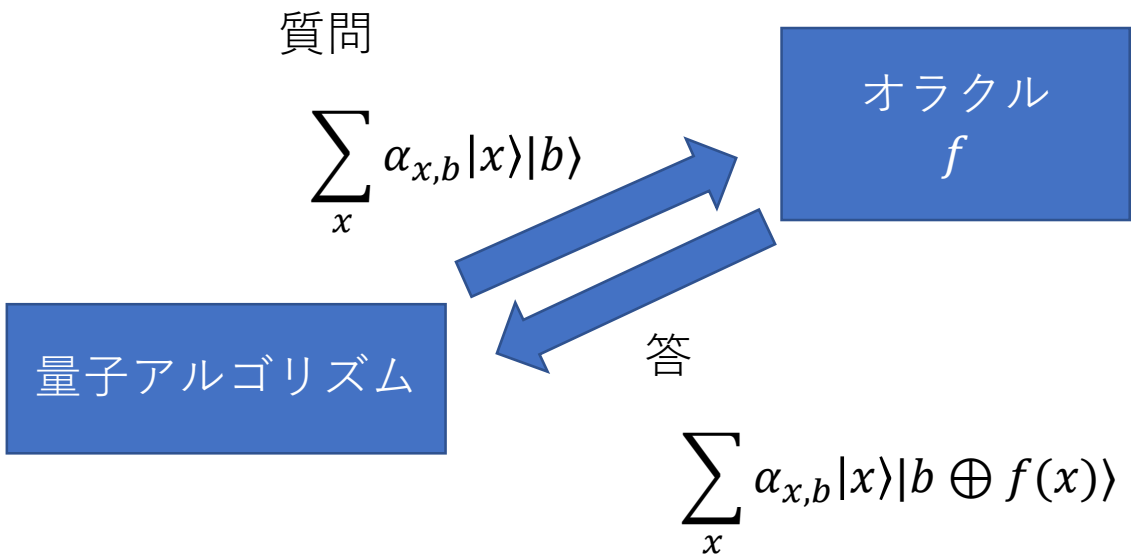
- 入力（オラクル）：関数 $f:\{0,1\}^n \to \{0,1\}^n$
  - オラクルへのアクセスは質問形式
  - $x = x_1 \cdots x_n$をオラクルに質問すると答$f(x)$が返ってくる
- 約束：ある$s = s_1 \cdots s_n \in \{0,1\}^n$に対して$f(x) = s \cdot x$
  - ただし、$s \cdot x = s_1 x_1 + \cdots + s_n x_n \bmod 2$
- 出力：s

古典のアルゴリズム（質問回数n回）

1. 各$j \in \{1, \ldots, n\}$について$e_j = 0^{j-1}10^{n-j}$をオラクルに質問し、答え$f(e_j)$を得る
2. $f(e_1) \cdots f(e_n)$を出力する

量子計算における質問(query)と答(answer)

- オラクルfへの質問(query)
  - 重ね合わせ状態$\sum_x \alpha_{x,b}|x\rangle|b\rangle$
- オラクルの答(answer)
  - ユニタリ行列$O_f: |x\rangle|b\rangle \mapsto |x\rangle|b \oplus f(x)\rangle$



Quantum algorithm for IP problem

1. $(n+1)$個の量子ビットを状態$|0^n\rangle_A|0\rangle_B$に準備
2. レジスタAの各量子ビットにHを施す

ステップ２の後の状態

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A\,|0\rangle_B$$

IP problem
入力（オラクル）：関数 $f:\{0,1\}^n\to\{0,1\}^n$
　　$x=x_1\cdots x_n$をオラクルに質問すると答$f(x)$が返ってくる
約束：ある$s=s_1\cdots s_n\in\{0,1\}^n$に対して$f(x)=s\cdot x$
　　ただし、$s\cdot x=s_1x_1+\cdots+s_nx_n \bmod 2$
出力：s

Quantum algorithm for IP problem

1. $(n+1)$個の量子ビットを状態$|0^n\rangle_A|0\rangle_B$に準備
2. レジスタAの量子ビットにHを施す
3. Aに格納された各xに対してオラクルfに質問して答をBに書き込む
   - ステップ3の操作に対応するユニタリ行列O_fは

$$O_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle$$

ステップ２の後の状態

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A |0\rangle_B$$

ステップ3の後の状態

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A |f(x)\rangle_B$$

IP problem
入力（オラクル）：関数 $f:\{0,1\}^n \to \{0,1\}^n$
　　$x = x_1 \cdots x_n$をオラクルに質問すると答$f(x)$が返ってくる
約束：ある$s = s_1 \cdots s_n \in \{0,1\}^n$に対して$f(x) = s \cdot x$
　　ただし、$s \cdot x = s_1x_1 + \cdots + s_nx_n \bmod 2$
出力：s

Quantum algorithm for IP problem

1. $(n+1)$個の量子ビットを状態$|0^n\rangle_A|0\rangle_B$に準備
2. レジスタAの量子ビットにHを施す
3. Aに格納された各xに対してオラクルfに質問して答をBに書き込む
   - ステップ3の操作に対応するユニタリ行列O_fは$O_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle$
4. レジスタBの量子ビットにZを施す: $Z|c\rangle = (-1)^c|c\rangle$

ステップ3の後の状態　$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A\,|f(x)\rangle_B$$

ステップ4の後の状態　$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A\,(-1)^{f(x)}|f(x)\rangle_B$$

Quantum algorithm for IP problem

1. $(n+1)$個の量子ビットを状態$|0^n\rangle_A|0\rangle_B$に準備
2. レジスタAの量子ビットにHを施す
3. Aに格納された各xに対してオラクルfに質問して答をBに書き込む
   - ステップ3の操作に対応するユニタリ行列O_fは$O_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle$
4. レジスタBの量子ビットにZを施す: $Z|c\rangle = (-1)^c|c\rangle$
5. Aに格納された各xに対してオラクルfに質問して答をBに書き込む

ステップ4の後の状態

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle_A\,|f(x)\rangle_B$$

ステップ5の後の状態

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle_A\,|f(x) \oplus f(x)\rangle_B$$

Quantum algorithm for IP problem

質問回数：2回

1. $(n+1)$個の量子ビットを状態$|0^n\rangle_A|0\rangle_B$に準備
2. レジスタAの量子ビットにHを施す
3. Aに格納された各xに対してオラクルfに質問して答をBに書き込む
   - ステップ3の操作に対応するユニタリ行列O_fは$O_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle$
4. レジスタBの量子ビットにZを施す: $Z|c\rangle = (-1)^c|c\rangle$
5. Aに格納された各xに対してオラクルfに質問して答をBに書き込む
6. レジスタAの量子ビットにHを施す

ステップ5の後の状態 $\dfrac{1}{\sqrt{2^n}}\displaystyle\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle_A|0\rangle_B$ ➡ ステップ6の後の状態 $|s\rangle_A|0\rangle_B$

IP problem
入力（オラクル）：関数 $f:\{0,1\}^n \to \{0,1\}^n$
　　$x = x_1 \cdots x_n$をオラクルに質問すると答$f(x)$が返ってくる
約束：ある$s = s_1 \cdots s_n \in \{0,1\}^n$に対して$f(x) = s \cdot x$
　　ただし、$s \cdot x = s_1x_1 + \cdots + s_nx_n \bmod 2$
出力：s

O_fの固有状態(eigenstate)と固有値(eigenvalue)

- $Z|c\rangle = (-1)^c|c\rangle$
- $O_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle$の固有状態は？
  - $O_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$
  - $O_f|x\rangle|1\rangle = |x\rangle|\neg f(x)\rangle$

  $\Rightarrow$

  $O_f|x\rangle(|0\rangle + |1\rangle) = |x\rangle(|f(x)\rangle + |\neg f(x)\rangle) = |x\rangle\ (|0\rangle + |1\rangle)$
  $O_f|x\rangle(|0\rangle - |1\rangle) = |x\rangle(|f(x)\rangle - |\neg f(x)\rangle) = (-1)^{f(x)}|x\rangle\ (|0\rangle - |1\rangle)$
- **O_fの固有状態**
  - $O_f|x\rangle|+\rangle = |x\rangle|+\rangle$
  - $O_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$

Improved quantum algorithm for IP problem

1. $(n+1)$個の量子ビットを状態$|0^n\rangle_A|-\rangle_B$に準備
2. レジスタAの各量子ビットにHを施す

ステップ２の後の状態

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$$

IP problem
入力（オラクル）：関数 $f:\{0,1\}^n\to\{0,1\}^n$
　　$x=x_1\cdots x_n$をオラクルに質問すると答$f(x)$が返ってくる
約束：ある$s=s_1\cdots s_n\in\{0,1\}^n$に対して$f(x)=s\cdot x$
　　ただし、$s\cdot x=s_1x_1+\cdots+s_nx_n \bmod 2$
出力：s

Improved quantum algorithm for IP problem

1. $(n+1)$個の量子ビットを状態$|0^n\rangle_A|0\rangle_B$に準備
2. レジスタAの量子ビットにHを施す
3. Aに格納された各xに対してオラクルfに質問して答をBに書き込む
   - ステップ3の操作に対応するユニタリ行列O_fは

$$O_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle$$

ステップ２の後の状態

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$$

$$O_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$

ステップ3の後の状態

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle_A|-\rangle_B$$

IP problem
入力（オラクル）：関数 $f:\{0,1\}^n \to \{0,1\}^n$
　　$x = x_1 \cdots x_n$をオラクルに質問すると答$f(x)$が返ってくる
約束：ある$s = s_1 \cdots s_n \in \{0,1\}^n$に対して$f(x) = s \cdot x$
　　ただし、$s \cdot x = s_1x_1 + \cdots + s_nx_n \bmod 2$
出力：s

Improved quantum algorithm for IP problem

1. $(n+1)$個の量子ビットを状態$|0^n\rangle_A|0\rangle_B$に準備
2. レジスタAの量子ビットにHを施す
3. Aに格納された各xに対してオラクルfに質問して答をBに書き込む
   - ステップ3の操作に対応するユニタリ行列O_fは$O_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle$
4. レジスタAの量子ビットにHを施す

ステップ3の後の状態　$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{s\cdot x}|x\rangle_A|-\rangle_B$$

ステップ4の後の状態　$$|s\rangle_A|-\rangle_B$$

IP problem
入力（オラクル）：関数 $f:\{0,1\}^n \to \{0,1\}^n$
　　$x = x_1 \cdots x_n$をオラクルに質問すると答$f(x)$が返ってくる
約束：ある$s = s_1 \cdots s_n \in \{0,1\}^n$に対して$f(x) = s \cdot x$
　　ただし、$s \cdot x = s_1x_1 + \cdots + s_nx_n \bmod 2$
出力：s

Gradient Decent Estimation [Jordan 2005]

入力：$f: \mathbb{R}^n \to \mathbb{R}$; 微分可能な連続関数

出力：原点での勾配$\nabla f(0) := \left(\frac{\partial f}{\partial x_1}(0), \cdots, \frac{\partial f}{\partial x_n}(0)\right)$の近似

- $f(x) \approx f(0) + \nabla f(0) \cdot x$と一次近似できる
- Bernstein-Vaziraniと同様の量子アルゴリズムで$\nabla f(0)$（の近似）を取り出せる

Groverのアルゴリズム(Grover's algorithm)

Unordered Search

入力：関数(オラクル; oracle) $f: \{1,2,\dots,N\} \to \{0,1\}$

出力：$f(j) = 1$なる解(solution) j (そのような解がないときは「解なし」)

以下，$f(j) = 1$となる解の個数(number of solutions)Kが既知(known)とする

定理(Grover) 質問回数 $O\left(\sqrt{\frac{N}{K}}\right)$ で高確率でUnordered Searchを解く量子アルゴリズムが存在
（実際にはKが未知(unknown)でも成立）

Grover's algorithm

以下，簡単のため$N = 2^n$として，$\{1,2,\dots,N\}$を$\{0,1\}^n$とみなす．

1. $n+1$個の量子ビットを$|0^n\rangle_A|-\rangle_B$の状態に準備
2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$

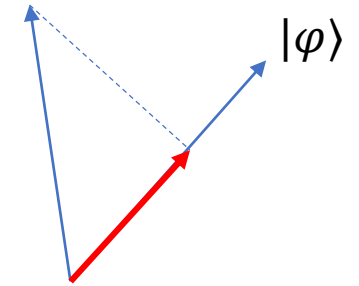
以下，$|\psi\rangle \coloneqq \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

3. 以下のサブルーチン(subroutine)を$m = O(\sqrt{\frac{N}{K}})$回繰り返す
    1. Aに格納されたxをオラクル(oracle) fに質問(query)して答をBに書く
    2. 「平均に関する折り返し(reflection around the mean)」$R(|\psi\rangle) \coloneqq 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

折り返し変換(Reflection) $R(|\psi\rangle) := 2|\psi\rangle\langle\psi| - I$

- 2^n次(縦)単位ベクトル$|\varphi\rangle$に対して，$\langle\varphi|$はその転置共役
- $|\varphi\rangle\langle\varphi|$は$2^n$次正方行列

  例：$|\varphi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$のとき，$|\varphi\rangle\langle\varphi| = \begin{pmatrix} a \\ b \end{pmatrix}(a^* \quad b^*) = \begin{pmatrix} aa^* & ab^* \\ ba^* & bb^* \end{pmatrix}$
- $|\varphi\rangle\langle\varphi|$は射影行列
  - 正方行列Mが射影$\Leftrightarrow M^2 = M$かつ$M^\dagger = M$ (エルミート: Hermite)

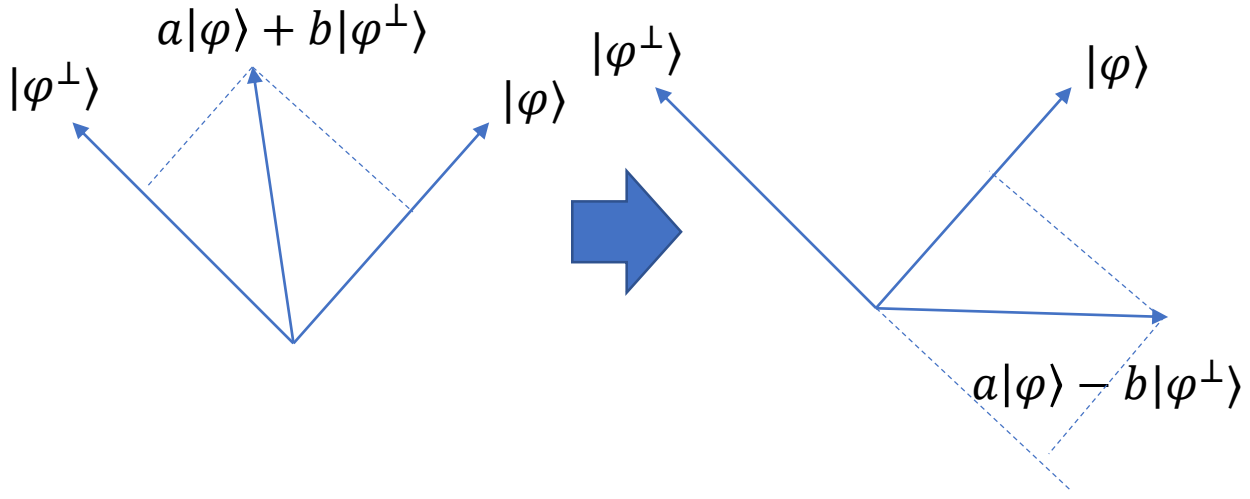


$$(|\varphi\rangle\langle\varphi|)|\varphi'\rangle = (|\varphi\rangle, |\varphi'\rangle)|\varphi\rangle$$

折り返し変換(Reflection) $R(|\psi\rangle) := 2|\psi\rangle\langle\psi| - I$

- 2^n次(縦)単位ベクトル$|\varphi\rangle$に対して，$\langle\varphi|$はその転置共役
- $|\varphi\rangle\langle\varphi|$は$2^n$次正方行列

  例：$|\varphi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$のとき，$|\varphi\rangle\langle\varphi| = \begin{pmatrix} a \\ b \end{pmatrix}\begin{pmatrix} a^* & b^* \end{pmatrix} = \begin{pmatrix} aa^* & ab^* \\ ba^* & bb^* \end{pmatrix}$
- $|\varphi\rangle\langle\varphi|$は射影行列
  - 正方行列Mが射影$\Leftrightarrow M^2 = M$かつ$M^\dagger = M$ (エルミート)
- $R(|\varphi\rangle)$はユニタリ行列
- $R(|\varphi\rangle)$は「$|\varphi\rangle$に関する折り返し」
  - $R(|\varphi\rangle)(a|\varphi\rangle + b|\varphi^\perp\rangle) = a|\varphi\rangle - b|\varphi^\perp\rangle$



Grover's algorithm

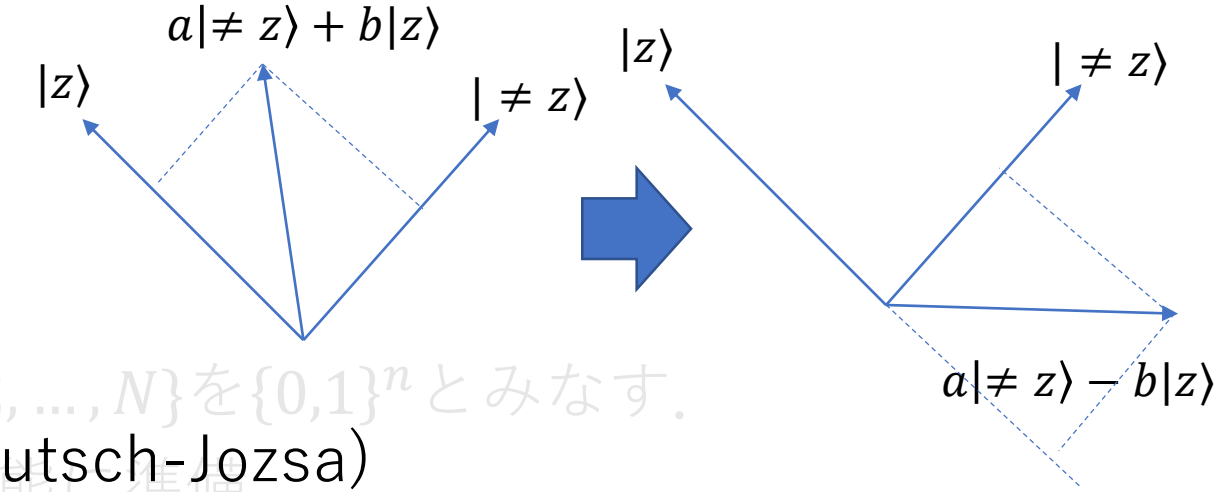
以下，簡単のため$N = 2^n$として，$\{1,2,\dots,N\}$を$\{0,1\}^n$とみなす．

1. $n+1$個の量子ビットを$|0^n\rangle_A|-\rangle_B$の状態に準備
2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$

以下，$|\psi\rangle \coloneqq \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

3. 以下のサブルーチンを$m = O(\sqrt{\frac{N}{K}})$回繰り返す
    1. Aに格納されたxをオラクルfに質問して答をBに書く：O_fも「非解に関する折り返し」
    2. 「平均に関する折り返し」$R(|\psi\rangle) \coloneqq 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

$K = 1$(解がzのみ)



- $O_f|x\rangle|b\rangle := |x\rangle|b \oplus f(x)\rangle$
- $O_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$ (cf. Deutsch-Jozsa)
- $O_f(a|\neq z\rangle + b|z\rangle)|-\rangle = (a|\neq z\rangle - b|z\rangle)|-\rangle$

3. 以下のサブルーチンを$m = O(\sqrt{N})$回繰り返す
   1. Aに格納されたxをオラクルfに質問して答をBに書く: $O_f = 2|\neq z\rangle\langle\neq z| - I$
   2. 「平均に関する折り返し」$R(|\psi\rangle) := 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

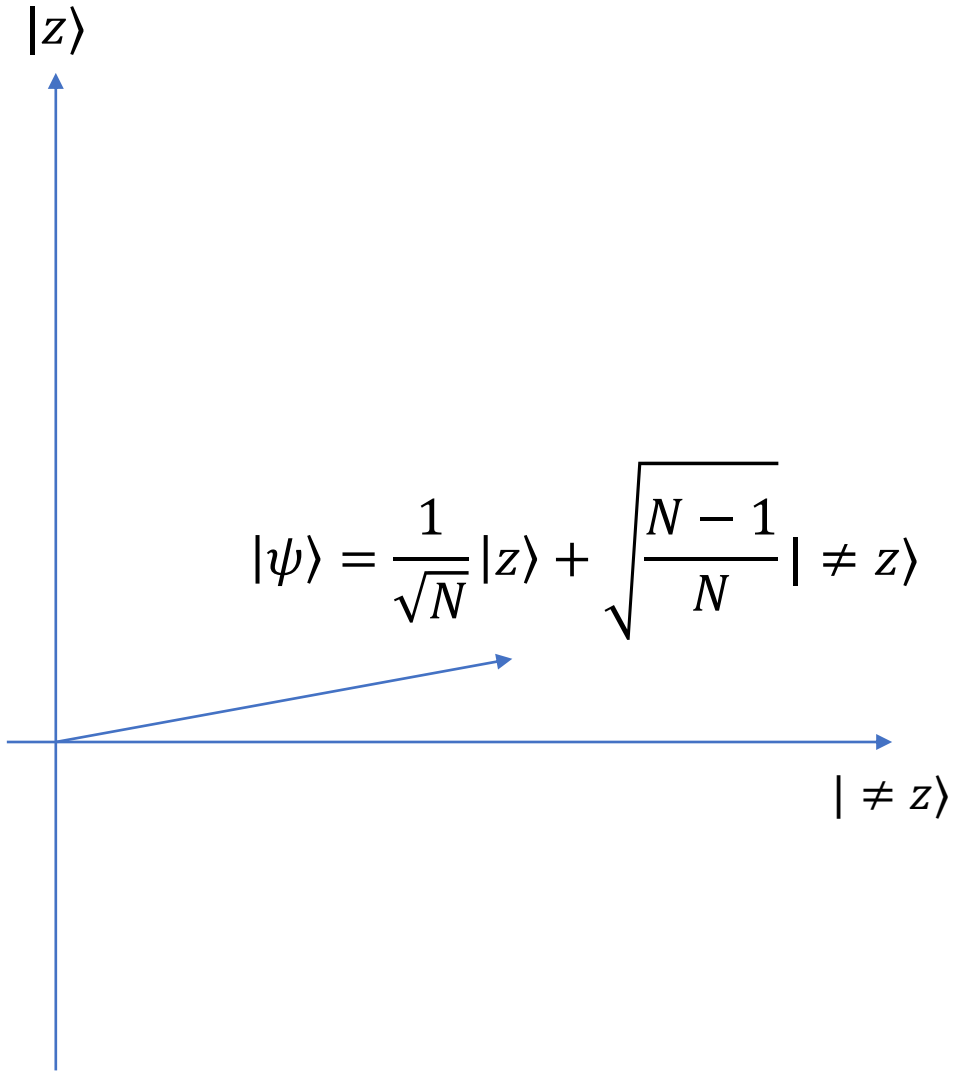
Geometric Picture $(K = 1)$: After Step 2

1. $n+1$個の量子ビットを$|0^n\rangle_A|-\rangle_B$の状態に準備
2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$

以下，$|\psi\rangle \coloneqq \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

3. 以下のサブルーチンを$m = O(\sqrt{N})$回繰り返す
   1. Aに格納されたxをオラクルfに質問して答をBに書く：$O_f = 2|\neq z\rangle\langle\neq z| - I$
   2. 「平均に関する折り返し」$R(|\psi\rangle) \coloneqq 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

ただし，$|\neq z\rangle := \frac{1}{\sqrt{N-1}}\sum_{x\neq z}|x\rangle$



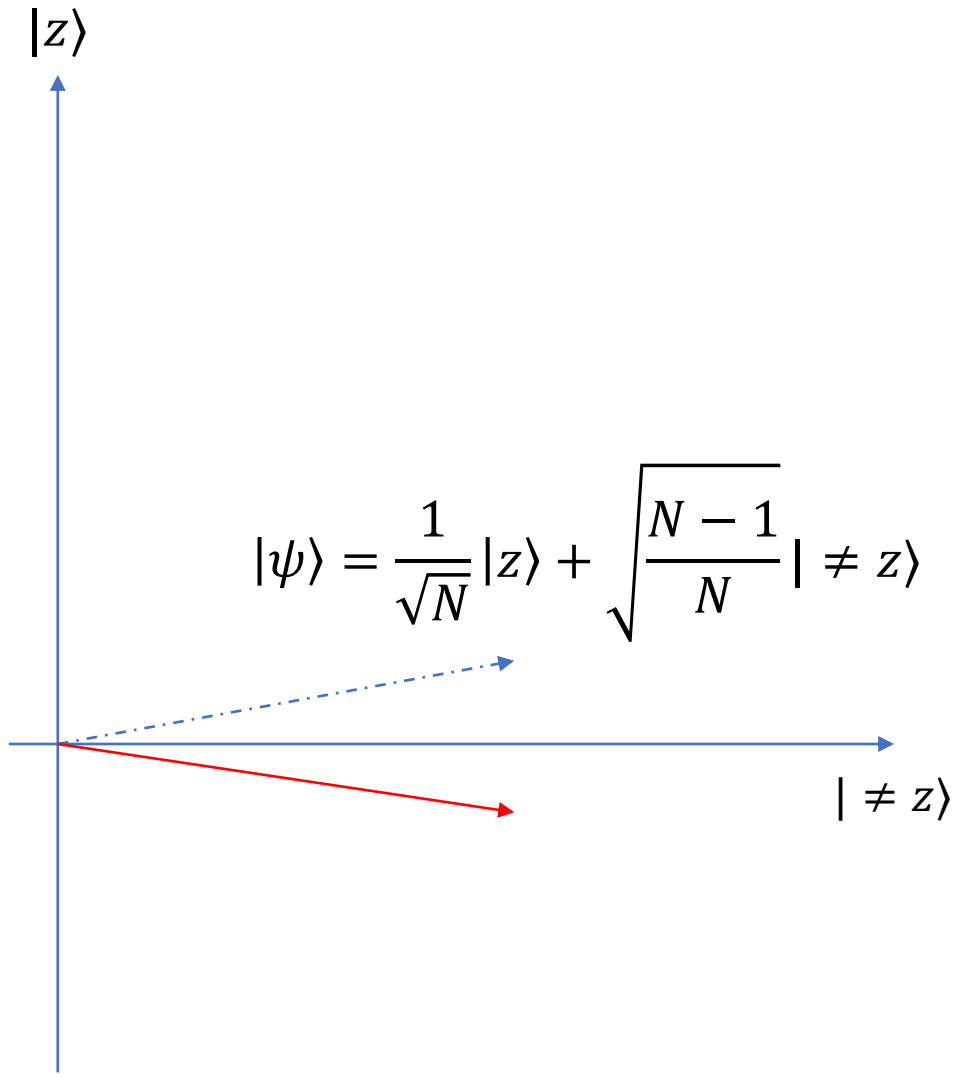
Geometric Picture $(K = 1)$: After Step 3.1

1. $n+1$個の量子ビットを$|0^n\rangle_A|-\rangle_B$の状態に準備
2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$

以下，$|\psi\rangle \coloneqq \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

3. 以下のサブルーチンを$m = O(\sqrt{N})$回繰り返す
   1. Aに格納されたxをオラクルfに質問して答をBに書く：$O_f = 2|\neq z\rangle\langle\neq z| - I$
   2. 「平均に関する折り返し」$R(|\psi\rangle) \coloneqq 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

ただし，$|\neq z\rangle := \frac{1}{\sqrt{N-1}}\sum_{x\neq z}|x\rangle$



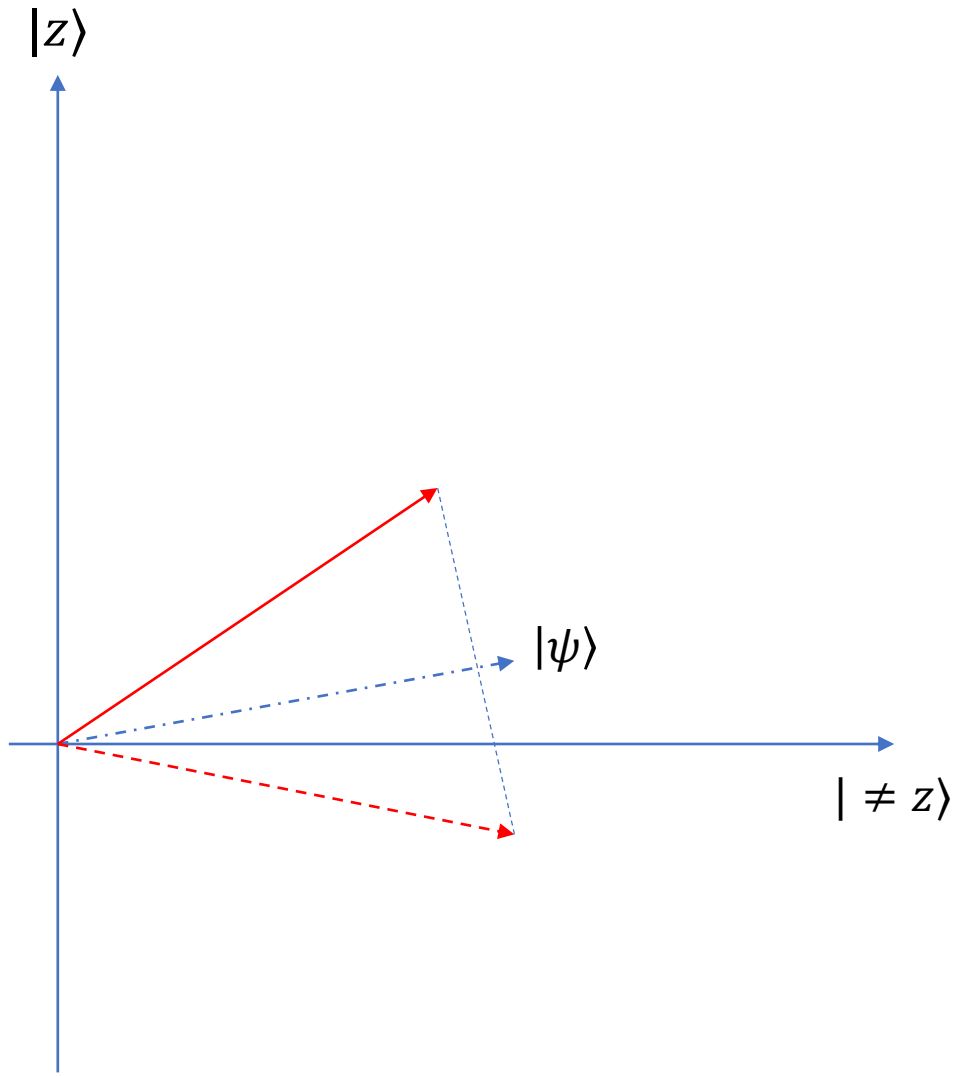
Geometric Picture $(K = 1)$: After Step 3.2

1. $n+1$個の量子ビットを$|0^n\rangle_A|-\rangle_B$の状態に準備
2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$

以下，$|\psi\rangle \coloneqq \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

3. 以下のサブルーチンを$m = O(\sqrt{N})$回繰り返す
   1. Aに格納されたxをオラクルfに質問して答をBに書く：$O_f = 2|\neq z\rangle\langle\neq z| - I$
   2. 「平均に関する折り返し」$R(|\psi\rangle) \coloneqq 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

ただし，$|\neq z\rangle := \frac{1}{\sqrt{N-1}}\sum_{x\neq z}|x\rangle$



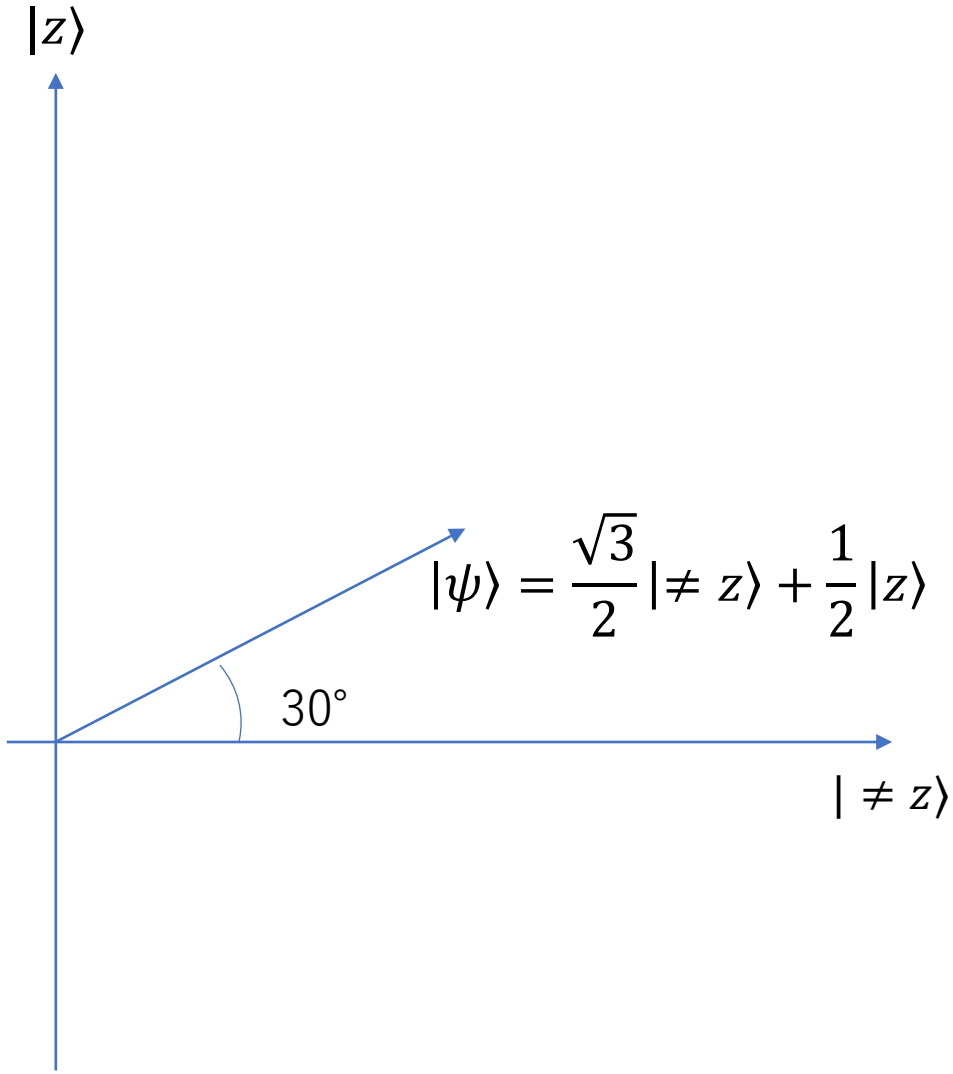
Geometric Picture $(K = 1, N = 4)$: After Step 2

1. $n+1$個の量子ビットを$|0^n\rangle_A|-\rangle_B$の状態に準備
2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$

以下，$|\psi\rangle \coloneqq \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

3. 以下のサブルーチンを$m = O(\sqrt{N})$回繰り返す
   1. Aに格納されたxをオラクルfに質問して答をBに書く：$O_f = 2|\neq z\rangle\langle\neq z| - I$
   2. 「平均に関する折り返し」$R(|\psi\rangle) \coloneqq 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

ただし，$|\neq z\rangle := \frac{1}{\sqrt{3}}\sum_{x\neq z}|x\rangle$



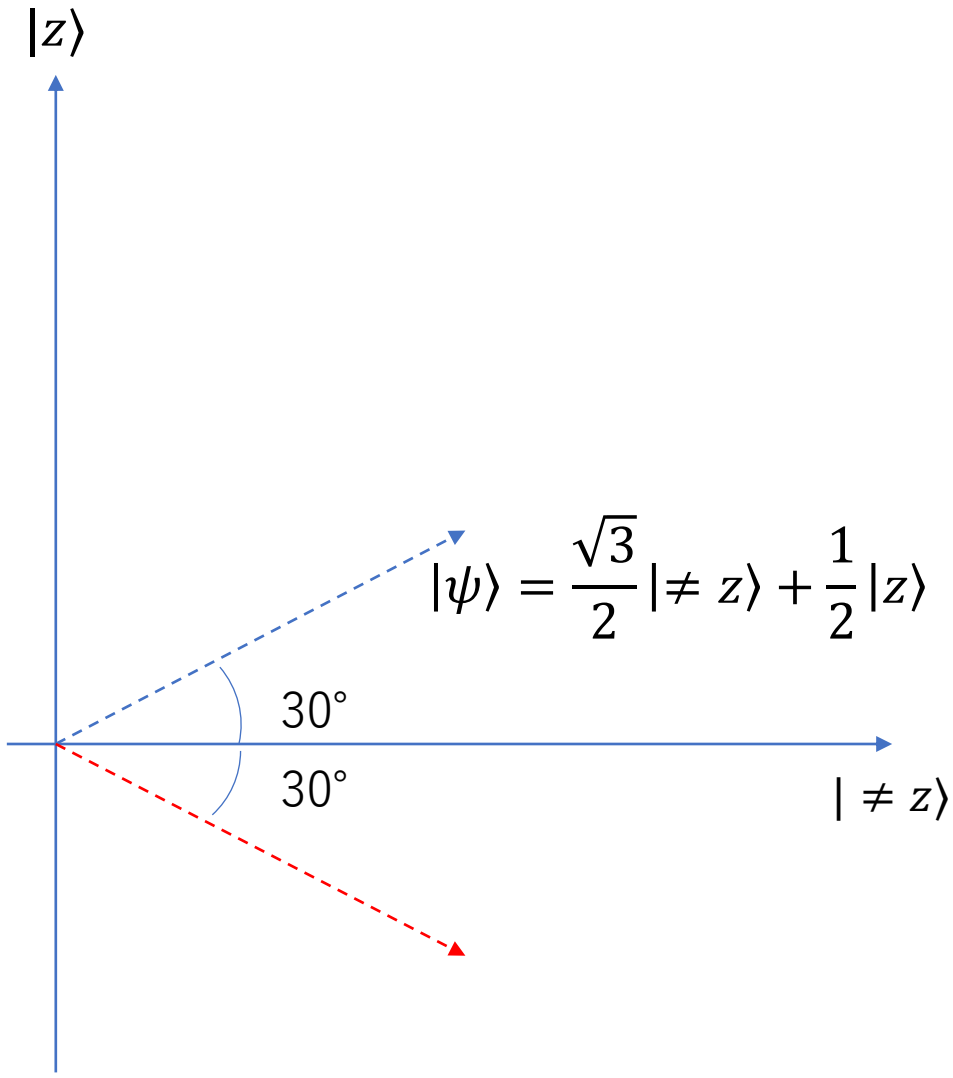
Geometric Picture $(K = 1, N = 4)$: After Step 3.1

1. $n+1$個の量子ビットを$|0^n\rangle_A|-\rangle_B$の状態に準備
2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$

以下，$|\psi\rangle \coloneqq \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

3. 以下のサブルーチンを$m = O(\sqrt{N})$回繰り返す
   1. Aに格納されたxをオラクルfに質問して答をBに書く：$O_f = 2|\neq z\rangle\langle\neq z| - I$
   2. 「平均に関する折り返し」$R(|\psi\rangle) \coloneqq 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

ただし，$|\neq z\rangle := \frac{1}{\sqrt{3}}\sum_{x\neq z}|x\rangle$



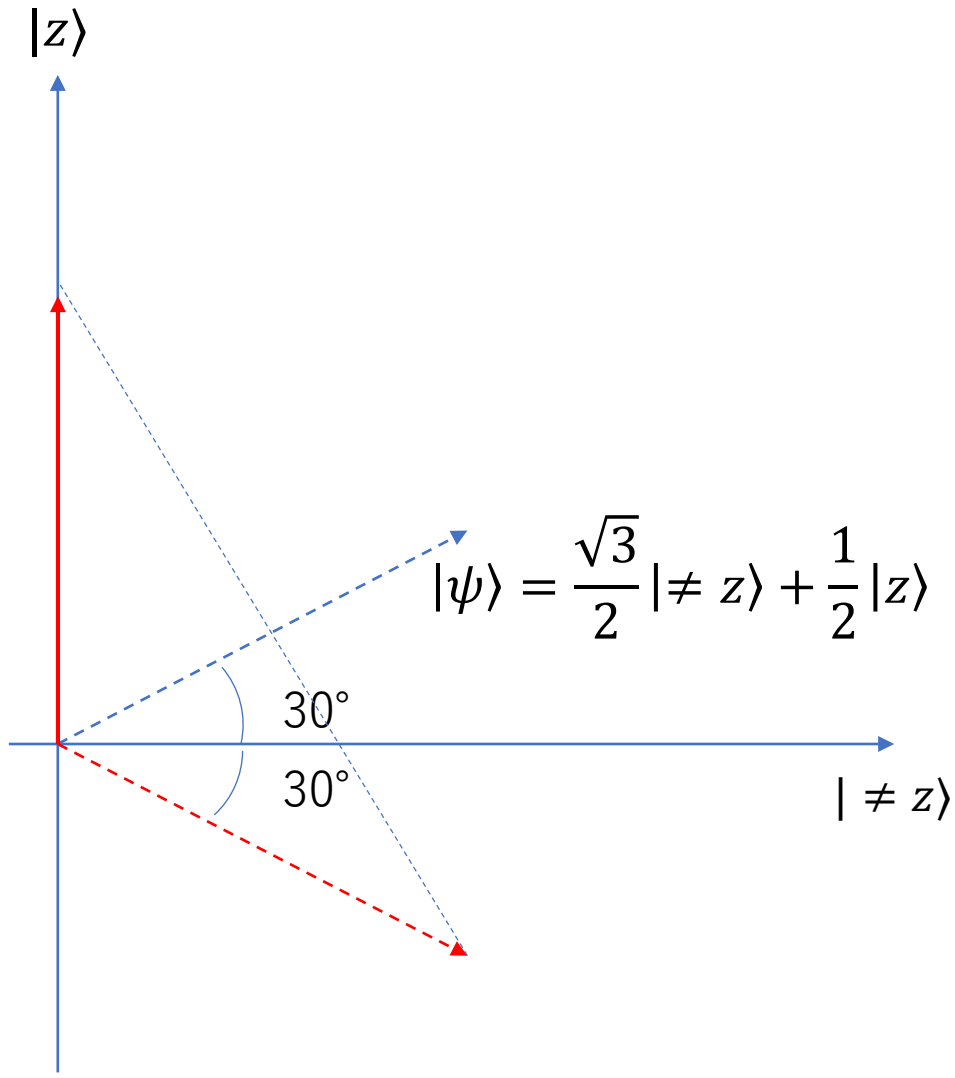
Geometric Picture $(K = 1, N = 4)$: After Step 3.2

1. $n+1$個の量子ビットを$|0^n\rangle_A|-\rangle_B$の状態に準備
2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$

以下，$|\psi\rangle \coloneqq \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

3. 以下のサブルーチンを$m = O(\sqrt{N})$回繰り返す
   1. Aに格納されたxをオラクルfに質問して答をBに書く：$O_f = 2|\neq z\rangle\langle\neq z| - I$
   2. 「平均に関する折り返し」$R(|\psi\rangle) \coloneqq 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

ただし，$|\neq z\rangle := \frac{1}{\sqrt{3}}\sum_{x\neq z}|x\rangle$



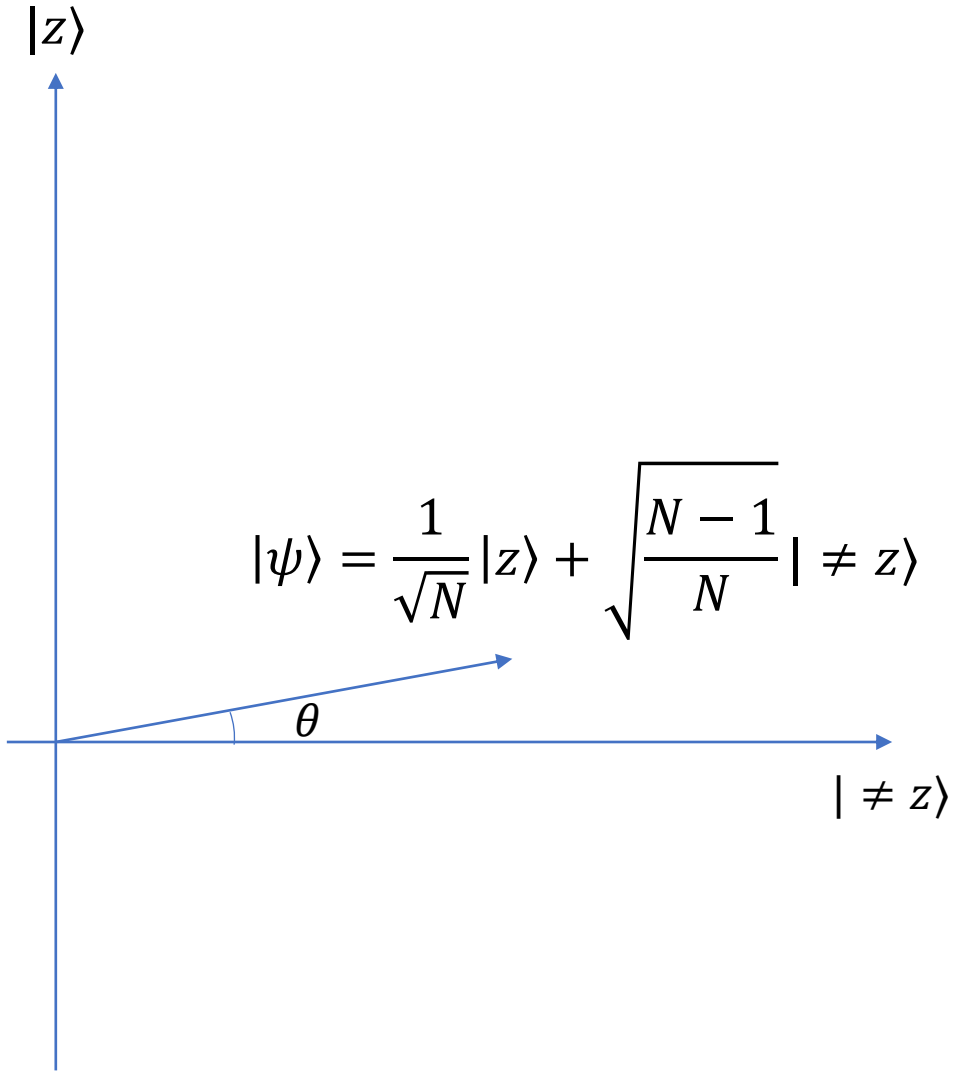
Geometric Picture $(K = 1)$: After Step 2

1. $n+1$個の量子ビットを$|0^n\rangle_A|-\rangle_B$の状態に準備
2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$

以下，$|\psi\rangle \coloneqq \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

3. 以下のサブルーチンを$m = O(\sqrt{N})$回繰り返す
   1. Aに格納されたxをオラクルfに質問して答をBに書く：$O_f = 2|\neq z\rangle\langle\neq z| - I$
   2. 「平均に関する折り返し」$R(|\psi\rangle) \coloneqq 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

ただし，$|\neq z\rangle := \frac{1}{\sqrt{N-1}}\sum_{x\neq z}|x\rangle$



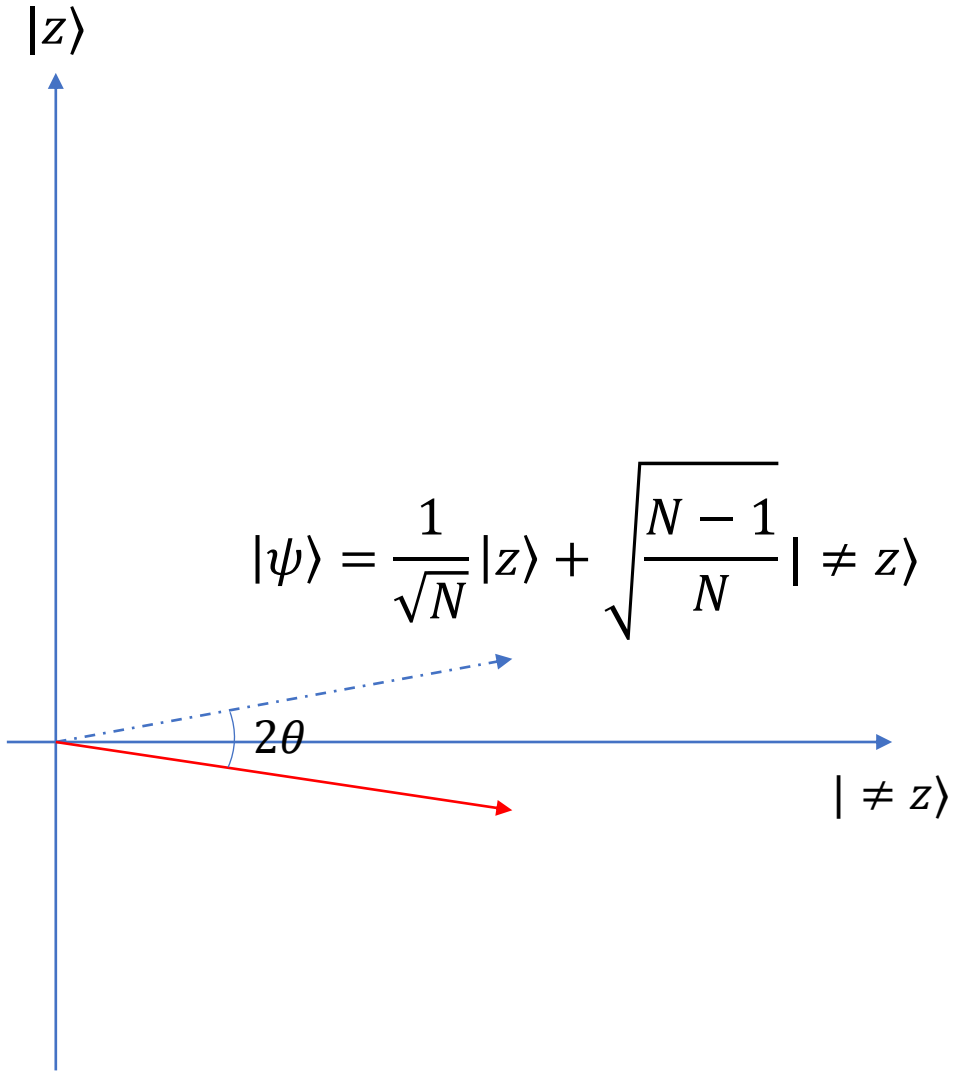
Geometric Picture $(K = 1)$: After Step 3.1

1. $n+1$個の量子ビットを$|0^n\rangle_A|-\rangle_B$の状態に準備
2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$

以下，$|\psi\rangle \coloneqq \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

3. 以下のサブルーチンを$m = O(\sqrt{N})$回繰り返す
   1. Aに格納されたxをオラクルfに質問して答をBに書く：$O_f = 2|\neq z\rangle\langle\neq z| - I$
   2. 「平均に関する折り返し」$R(|\psi\rangle) \coloneqq 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

ただし，$|\neq z\rangle := \frac{1}{\sqrt{N-1}}\sum_{x\neq z}|x\rangle$



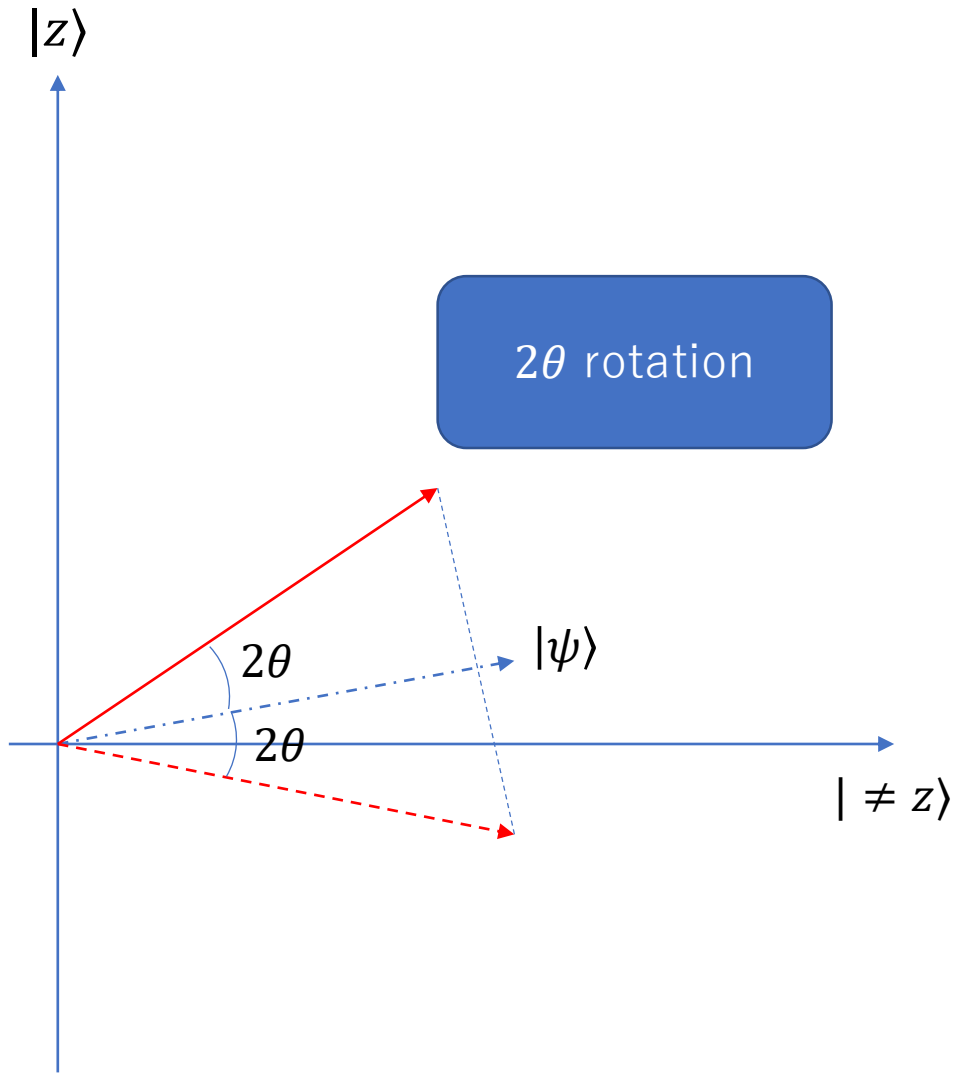
Geometric Picture $(K = 1)$: After Step 3.2

1. $n+1$個の量子ビットを$|0^n\rangle_A|-\rangle_B$の状態に準備
2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$

以下，$|\psi\rangle \coloneqq \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

3. 以下のサブルーチンを$m = O(\sqrt{N})$回繰り返す
   1. Aに格納されたxをオラクルfに質問して答をBに書く：$O_f = 2|\neq z\rangle\langle\neq z| - I$
   2. 「平均に関する折り返し」$R(|\psi\rangle) \coloneqq 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

ただし，$|\neq z\rangle := \frac{1}{\sqrt{N-1}}\sum_{x\neq z}|x\rangle$



解析(Analysis)

- $K = 1$のとき
  - Step 2の後の状態 $|\psi\rangle = \sqrt{\frac{N-1}{N}}|\neq z\rangle + \frac{1}{\sqrt{N}}|z\rangle = \cos\theta|\neq z\rangle + \sin\theta|z\rangle$
  - Step 3で状態は2θ回転
    - m回反復後の状態 $\cos\big((2m+1)\theta\big)|\neq z\rangle + \sin\big((2m+1)\theta\big)|z\rangle$
  - $\theta \approx \sin\theta = \frac{1}{\sqrt{N}}$ より$m = O(\sqrt{N})$で高確率でzが得られる
- 一般のK
  - $|S\rangle := \frac{1}{\sqrt{K}}\sum_{x:f(x)=1}|x\rangle$, $|\bar{S}\rangle := \frac{1}{\sqrt{N-K}}\sum_{x:f(x)=0}|x\rangle$
  - $|\psi\rangle = \sqrt{\frac{N-K}{N}}\,|\bar{S}\rangle + \sqrt{\frac{K}{N}}\,|S\rangle$

Number of Repetitions = Number of Queries

以下，簡単のため$N = 2^n$として，$\{1,2,\dots,N\}$を$\{0,1\}^n$とみなす．

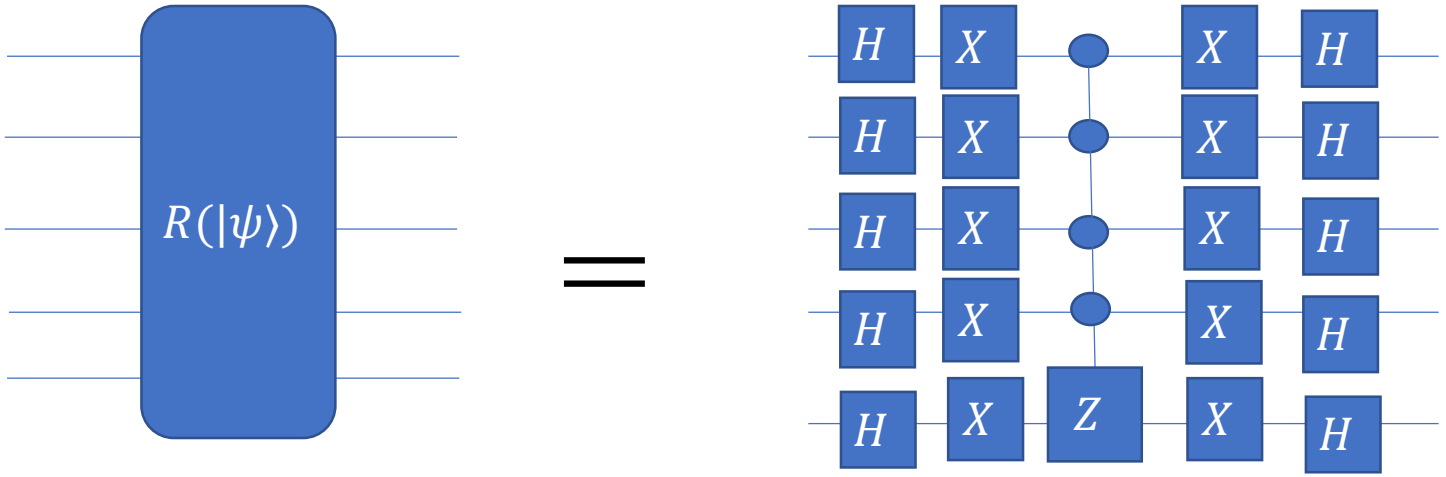
1. n個の量子ビットを$|0^n\rangle_A|-\rangle_B$の状態に準備
2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|-\rangle_B$

以下，$|\psi\rangle \coloneqq \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle$

3. 以下のサブルーチンを$m = O(\sqrt{\frac{N}{K}})$回繰り返す
    1. Aに格納されたxをオラクルfに質問して答をBに書く：O_fも「非解に関する折り返し」
    2. 「平均に関する折り返し」$R(|\psi\rangle) \coloneqq 2|\psi\rangle\langle\psi| - I$をA上で行う
4. Aを計算基底で測定してその値がzなら$f(z) = 1$（解）か否かをオラクルに確認．解ならzを出力，そうでないなら「解なし」と出力

Quantum Circuit for $R(|\psi\rangle)$

- $H^{\otimes n}|0^n\rangle = |\psi\rangle$
- $2|\psi\rangle\langle\psi| - I = -H^{\otimes n}(I - 2|0^n\rangle\langle 0^n|)H^{\otimes n}$



Applications of Grover's Algorithm

Applications of Grover's Algorithm

- 探索(Search)問題に適用可能
  - NP困難問題の解探索
  - 暗号の鍵探索
- **オラクル関数と違って「解か否かの情報」は1回の質問で得られない⇒古典計算を行う必要あり**

  例: 充足可能性問題SAT

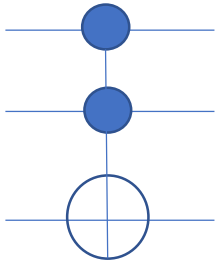
  入力：ブール論理式(Boolean formula) $F(x_1, x_2, \dots, x_n)$

  出力：$F(x_1, x_2, \dots, x_n) = 1$ (真: true)となる解$x = x_1 x_2 \cdots x_n \in \{0,1\}^n$

  ➢解の候補xが$F(x) = 1$か否かは古典の多項式時間アルゴリズムでチェック

古典計算は量子回路で実行可能

- Toffoli gate CCX
  - $CC\text{-}X|x\rangle|y\rangle|z\rangle = |x\rangle|y\rangle|z \oplus (x \wedge y)\rangle$
  - NOTとANDを実行可能
- すべての古典計算はToffoli gateのみからなる量子回路で模倣可能
- 問題点
  - 古典計算は一般に途中でいろいろ計算過程を残す
  - 古典計算ではそのような計算過程で出たゴミ(garbage)は消せる
  - 量子計算は可逆（ユニタリ）なのでそのようなゴミは消せない



理想(ideal)

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|F(x)\rangle$$

現実(real)

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|F(x)\rangle|G(x)\rangle$$

ゴミの消去: Garbage Elimination (by Bennett)

- $U|x\rangle|0\rangle|0\rangle \coloneqq |x\rangle|F(x)\rangle|G(x)\rangle$

目標： $U'|x\rangle|0\rangle = |x\rangle|F(x)\rangle$ の構築

1. $|x\rangle_A|0\rangle_B|0\rangle_C|0\rangle_D$を用意
2. A,B,C上でUを実行：
   $|x\rangle_A|F(x)\rangle_B|G(x)\rangle_C|0\rangle_D$
3. Bの各量子ビットを条件として対応するDの各量子ビットにCNOTを実行：
   $|x\rangle_A|F(x)\rangle_B|G(x)\rangle_C|F(x)\rangle_D$
4. A,B,C上でU^{-1}を実行：$|x\rangle_A|0\rangle_B|0\rangle_C|F(x)\rangle_D$

理想

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|F(x)\rangle$$

現実

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|0\rangle|0\rangle|F(x)\rangle$$

Applications of Grover's Algorithm

- 探索(Search)問題に適用可能
  - NP困難問題の解探索
  - 暗号の鍵探索
- オラクル関数と違って「解か否かの情報」は1回の質問で得られない⇒古典計算を行う必要あり

  例: 充足可能性問題SAT

  入力：ブール論理式 $F(x_1, x_2, \dots, x_n)$

  出力：$F(x_1, x_2, \dots, x_n) = 1$ (真)となる解$x = x_1 x_2 \cdots x_n \in \{0,1\}^n$

  ➢解の候補xが$F(x) = 1$か否かは古典の多項式時間アルゴリズムでチェック

  ➢Groverにより$O(\sqrt{2^n}\mathrm{poly}(n))$時間で解ける

振幅増幅アルゴリズム: Amplitude Amplification

- Groverのアルゴリズムは，古典の乱択アルゴリズムと組み合わせることが可能である！

振幅増幅(Amplitude Amplification)アルゴリズム

古典の乱択アルゴリズムが計算量T，成功率 p である要素を見つけるならば，

（古典の場合，繰り返しにより計算量 T/p，成功率 0.99でその要素を見つけるところを）

ある量子アルゴリズムが存在して，そのアルゴリズムは計算量 $T/\sqrt{p}$，成功率0.99で

その要素を見つけることができる

探索問題に対するGroverのアルゴリズムは，振幅増幅アルゴリズムの特殊ケース

fの評価を行う x をランダムに選べば $T = 1$ 回の評価で $p = 1/N$ の成功率で

$f(x) = 1$なる x が見つかる.

➡ 量子アルゴリズムは $T/\sqrt{p} = O(\sqrt{N})$回の評価で成功率0.99でそのような x を得る

Application to 3SAT

3SAT

入力　各節のリテラル(literal)（変数(variable)ないしその否定(negation)）

が3個の和積形論理式(CNF formula)　$f(x_1, x_2, \ldots, x_n)$

出力　$f(x) = 1$となる割当(assignment) $x = x_1 x_2 \cdots x_n$が存在すればYES，存在しなければNO

- 古典の全探索は2^n（×poly(n)）の時間計算量を要する
- Groverのアルゴリズムを使えば $2^{n/2} = (1.414)^n$
- しかし，問題の構造を考慮すれば3SATは古典でもっと速く解ける
- Schoningのランダムウォーク(random walk)を用いた乱択アルゴリズム:$\left(\frac{4}{3}\right)^n$の計算量
  - poly(n)の計算量，成功率$\left(\frac{3}{4}\right)^n$で割り当てを見つける

Application to 3SAT

3SAT

入力　各節のリテラル(literal)（変数(variable)ないしその否定(negation)）

が3個の和積形論理式(CNF formula)　$f(x_1, x_2, \dots, x_n)$

出力　$f(x) = 1$となる割当(assignment) $x = x_1 x_2 \cdots x_n$が存在すればYES，存在しなければNO

振幅増幅(Amplitude Amplification)アルゴリズム

古典の乱択アルゴリズムが**計算量T，成功率 p** である要素を見つけるならば，

量子アルゴリズムは**計算量 $\frac{T}{\sqrt{p}}$，成功率0.99**でその要素を見つける

- Schoningのランダムウォーク(random walk)を用いた乱択アルゴリズム:$\left(\frac{4}{3}\right)^n$の計算量
  - poly(n)の計算量，成功率$\left(\frac{3}{4}\right)^n$で割り当てを見つける

振幅増幅により量子だと計算量 poly(n)$\left(\frac{4}{3}\right)^{n/2}$=O((1.155)^n)で3SATが解ける

Other Applications

以下，fの定義域(domain)は$\{1,2,\dots,N\}$

- 解の全列挙(Enumeration of solutions)
  - $f(x)=1$なるすべての$x_1,x_2,\dots,x_k$を$O(\sqrt{kN})$回の質問で列挙可能
- 最大・最小(Max, Min) [Durr-Hoyer 1996]
  - $\max_x\{f(x)\}$を$O(\sqrt{N})$回の質問で求められる
- 解の個数(quantum counting) [Brassard-Hoyer-Tapp 1998]
  - $k:=\#\{x|f(x)=1\}$を$O(\sqrt{N})$回の質問で誤差$O(\sqrt{k})$で近似する
- 平均値の推定(Estimation of mean) [Brassard-Dupuis-Gambs-Tapp 2011他]
  - $f(j)\in[0,1]$のとき，$O(1/\varepsilon)$回の質問で$\mu=\frac{1}{N}\sum_{j=1}^{N}f(j)$を精度$\varepsilon$で推定する

Summary

- Groverのアルゴリズム
  - 非解空間から解空間への回転による移動を２つの折り返し変換で実現
  - 同様のアイデアは他の量子アルゴリズム（量子ウォークアルゴリズム）でも使用
- 応用
  - 乱択アルゴリズムの成功確率の増幅（振幅増幅アルゴリズム）
  - NP困難問題や暗号における鍵探索などの探索問題に適用可能
  - 最大・最小や解の数え上げにも適用可能

Simon’s Algorithm

Simon's Problem

入力(Input)：オラクル関数 $f: \{0,1\}^n \to \{0,1\}^n$

約束(promise)：fは2-1関数ですべての$x \in \{0,1\}^n$について,

$f(x \oplus s) = f(x)$なる$s \neq 0^n$（F_2^n上の周期(period)）が存在

出力(Output)：s

Simon's Problem

入力：オラクル関数 $f: \{0,1\}^n \to \{0,1\}^n$

約束：fは2-1関数ですべての$x \in \{0,1\}^n$について$f(x \oplus s) = f(x)$なる$s \neq 0^n$（F_2^n上の周期）

出力：s

例：

入力

$$f(000) = 101, f(001) = 110, f(010) = 000, f(011) = 011$$
$$f(100) = 000, f(101) = 011, f(110) = 101, f(111) = 110$$

出力 $s = 110$

Simon's Problem

入力：オラクル関数 $f:\{0,1\}^n \to \{0,1\}^n$

約束：fは2-1関数ですべての$x \in \{0,1\}^n$について$f(x \oplus s) = f(x)$なる$s \neq 0^n$（F_2^n上の周期）

出力：s

例：

入力

$$f(000) = 101, f(001) = 110, f(010) = 000, f(011) = 011$$
$$f(100) = 000, f(101) = 011, f(110) = 101, f(111) = 110$$

出力 $s = 110$

方法１：$f(0^n)$と同じ値$f(x)$を取るxを探索⇒$\Omega(2^n)$回の質問が必要

Simon's Problem

入力：オラクル関数 $f:\{0,1\}^n \to \{0,1\}^n$

約束：fは2-1関数ですべての$x \in \{0,1\}^n$について$f(x \oplus s) = f(x)$なる$s \neq 0^n$（F_2^n上の周期）

出力：s

例：

入力

$$f(000) = 101, f(001) = 110, f(010) = 000, f(011) = 011$$
$$f(100) = 000, f(101) = 011, f(110) = 101, f(111) = 110$$

出力 $s = 110$

方法2：$f(x) = f(y)$となるペア(x, y)を探索⇒$O(\sqrt{2^n})$回の質問でOK

Simon's Problem

入力：オラクル関数 $f:\{0,1\}^n \to \{0,1\}^n$

約束：fは2-1関数ですべての$x \in \{0,1\}^n$について$f(x \oplus s) = f(x)$なる$s \neq 0^n$
（F_2^n上の周期）

出力：s

方法2：$f(x) = f(y)$となるペア(x, y)を探索⇒$O(\sqrt{2^n})$回の質問でOK

←実は古典アルゴリズムのベストな方法

定理(Simon) $O(n)$回の質問で高確率でsを発見する量子アルゴリズムが存在

Simon's algorithm

1. 以下のサブルーチン(subroutine)を$m = O(n)$回繰り返す
    1. $2n$個の量子ビットを状態 $|0^n\rangle_A|0^n\rangle_B$ に準備
    2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|0^n\rangle_B$
    3. Aに格納されたxをオラクルに質問して答をBに書き込む：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|f(x)\rangle_B$

Simon's algorithm

1. 以下のサブルーチンを$m = O(n)$回繰り返す
   1. $2n$個の量子ビットを状態 $|0^n\rangle_A|0^n\rangle_B$ に準備
   2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|0^n\rangle_B$
   3. Aに格納されたxをオラクルに質問して答をBに書き込む：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|f(x)\rangle_B$
   4. Bを計算基底で測定する（←部分的に測定）：

Recap: Partial measurements

[部分測定の公理] $|\psi\rangle = \sum_x |\psi_x\rangle_A |x\rangle_B$ と書けるときにBを計算基底で測定すると確率 $\||\psi_x\rangle\|^2$ で測定値 x を得て，測定後の状態は $\frac{1}{\||\psi_x\rangle\|}|\psi_x\rangle|x\rangle$ になる

Simon's algorithm

[部分測定の公理] $|\psi\rangle = \sum_x |\psi_x\rangle_A |x\rangle_B$と書けるときにBを計算基底で測定すると確率 $\||\psi_x\rangle\|^2$ で測定値xを得て，測定後の状態は$\frac{1}{\||\psi_x\rangle\|}|\psi_x\rangle|x\rangle_B$になる

2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|0^n\rangle_B$
3. Aに格納されたxをオラクルに質問して答をBに書き込む：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|f(x)\rangle_B$
4. Bを計算基底で測定する：

- $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|f(x)\rangle_B = \frac{1}{\sqrt{2^n}}\sum_z(|x_z\rangle + |x_z \oplus s\rangle)_A|z\rangle_B$

$f(000)=101, f(001)=110, f(010)=000, f(011)=011$
$f(100)=000, f(101)=011, f(110)=101, f(111)=110$
の場合$(s=110)$

$$\frac{1}{\sqrt{8}}(|000\rangle+|110\rangle)_A|101\rangle_B + \frac{1}{\sqrt{8}}(|001\rangle+|111\rangle)_A|110\rangle_B + \frac{1}{\sqrt{8}}(|010\rangle+|100\rangle)_A|000\rangle_B + \frac{1}{\sqrt{8}}(|011\rangle+|101\rangle)_A|011\rangle_B$$

Simon's algorithm

[部分測定の公理] $|\psi\rangle = \sum_x |\psi_x\rangle_A |x\rangle_B$ と書けるときにBを計算基底で測定すると確率 $\||\psi_x\rangle\|^2$ で測定値xを得て，測定後の状態は $\frac{1}{\||\psi_x\rangle\|}|\psi_x\rangle|x\rangle_B$ になる

2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|0^n\rangle_B$
3. Aに格納されたxをオラクルに質問して答をBに書き込む：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|f(x)\rangle_B$
4. Bを計算基底で測定する：

- $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|f(x)\rangle_B = \frac{1}{\sqrt{2^n}}\sum_z(|x_z\rangle + |x_z \oplus s\rangle)_A|z\rangle_B$
- 確率 $\left\|\frac{1}{\sqrt{2^n}}(|x_z\rangle + |x_z \oplus s\rangle)\right\|^2 = \frac{1}{2^{n-1}}$ で測定値zが得られて測定後の状態は $\frac{1}{\sqrt{2}}(|x_z\rangle + |x_z \oplus s\rangle)_A|z\rangle_B$

Simon's algorithm

1. 以下のサブルーチンを$m = O(n)$回繰り返す
   1. $2n$個の量子ビットを状態 $|0^n\rangle_A|0^n\rangle_B$ に準備
   2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|0^n\rangle_B$
   3. Aに格納されたxをオラクルに質問して答をBに書き込む：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|f(x)\rangle_B$
   4. Bを計算基底で測定する：確率$\frac{1}{2^{n-1}}$で測定値zが得られて測定後の状態は
      $\frac{1}{\sqrt{2}}(|x_z\rangle + |x_z \oplus s\rangle)_A|z\rangle_B$

Simon's algorithm

1. 以下のサブルーチンを$m = O(n)$回繰り返す
   1. $2n$個の量子ビットを状態 $|0^n\rangle_A|0^n\rangle_B$ に準備
   2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|0^n\rangle_B$
   3. Aに格納されたxをオラクルに質問して答をBに書き込む：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|f(x)\rangle_B$
   4. Bを計算基底で測定する：確率$\frac{1}{2^{n-1}}$で測定値zが得られて測定後の状態は
      $\frac{1}{\sqrt{2}}(|x_z\rangle + |x_z \oplus s\rangle)_A|z\rangle_B$
   5. Aの各量子ビットにHを施す：
      $$\frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x_z\cdot y}|y\rangle + \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{(x_z\oplus s)\cdot y}|y\rangle\right)_A|z\rangle_B$$
      $$= \frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}\left\{(-1)^{x_z\cdot y} + (-1)^{(x_z\oplus s)\cdot y}\right\}|y\rangle_A|z\rangle_B$$
      $$= \frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}\left\{(-1)^{x_z\cdot y} + (-1)^{x_z\cdot y+s\cdot y}\right\}|y\rangle_A|z\rangle_B$$
      $$= \frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}(-1)^{x_z\cdot y}\left\{1 + (-1)^{s\cdot y}\right\}|y\rangle_A|z\rangle_B$$

Simon's algorithm

1. 以下のサブルーチンを$m = O(n)$回繰り返す
   1. $2n$個の量子ビットを状態 $|0^n\rangle_A|0^n\rangle_B$ に準備
   2. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|0^n\rangle_B$
   3. Aに格納されたxをオラクルに質問して答をBに書き込む：$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|f(x)\rangle_B$
   4. Bを計算基底で測定する：確率$\frac{1}{2^{n-1}}$で測定値zが得られて測定後の状態は $\frac{1}{\sqrt{2}}(|x_z\rangle + |x_z \oplus s\rangle)_A|z\rangle_B$
   5. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}(-1)^{x_z\cdot y}\{1+(-1)^{s\cdot y}\}|y\rangle_A|z\rangle_B$
   6. Aを測定する：測定値yはsについての方程式$y\cdot s = 0$をみたす
2. i回目の出力を$y(i)$とするとき，連立方程式(linear equations)

   $y(1)\cdot w = 0, \dots, y(m)\cdot w = 0$

   を解く：0^n以外の非自明解が一意に得られたらその値を出力とする.

Simon's algorithm

1. 以下のサブルーチンを$m = O(n)$回繰り返す
   1. $2n$個の量子ビットを状態 $|0^n\rangle_A|0^n\rangle_B$ に準備
   2. Aの各量子ビットにHを施す：$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}|x\rangle_A|0^n\rangle_B$
   3. Aに格納されたオラクルに質問して答をBに書き込む：$\frac{1}{2^n}\sum_{x\in\{0,1\}^n}|x\rangle_A|f(x)\rangle_B$
   4. Bを計算基底で測定する．確率$\frac{1}{2^{n-1}}$で測定値zが得られて測定後の状態は $\frac{1}{\sqrt{2}}(|x_z\rangle + |x_z \oplus s\rangle)_A|z\rangle_B$
   5. Aの各量子ビットにHを施す：$\frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}(-1)^{x_z\cdot y}\{1+(-1)^{s\cdot y}\}|y\rangle_A|z\rangle_B$
   6. Aを測定する：測定値yはsについての方程式$y\cdot s = 0$をみたす
2. i回目の出力を$y(i)$とするとき，連立方程式 $y(1)\cdot w = 0, \dots, y(m)\cdot w = 0$ を解く：0^n以外の非自明解が一意に得られたらその値を出力とする．

例：$n = 4, y(1) = 1110, y(2) = 1101, y(3) = 1001$のとき

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow \begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \end{pmatrix} = w_1\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \text{より} s = 1011$$

$m = O(n)$回の繰り返しでsが高確率で得られる

Simon & Shor

- Shorのアルゴリズムが解いた問題

整数の因数分解問題: Integer Factoring

入力　自然数 N;　出力　N の非自明な因数

- 量子計算で実際に解く問題はある種の周期発見問題(period finding)

位数発見問題: Order Finding

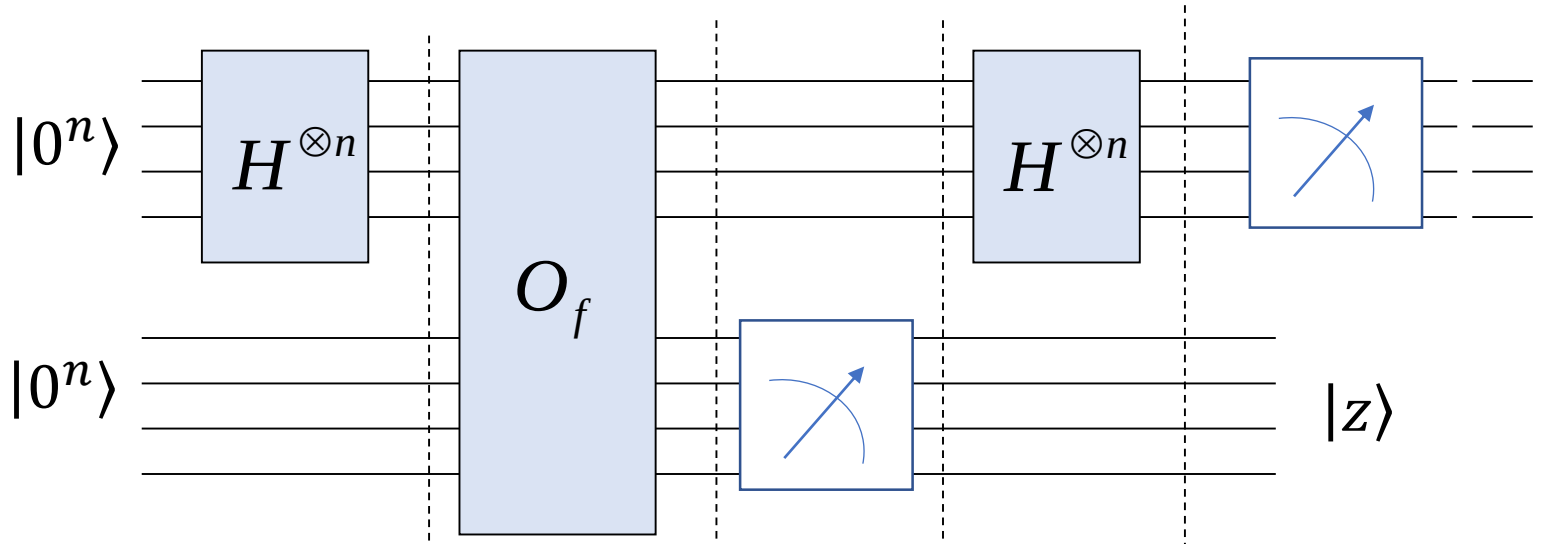
（整数の素因数分解問題は古典アルゴリズムによりこの問題に帰着可能）

入力　自然数 N および x ($<N$ で，かつ N と互いに素)

出力　$x^r = 1 \pmod N$ なる最小の自然数 r (x の位数)

- Simonの問題も周期発見問題の１つ
  - Simonのアルゴリズムにヒントを得てShorのアルゴリズムが誕生

Simon's Algorithm: for finding period s



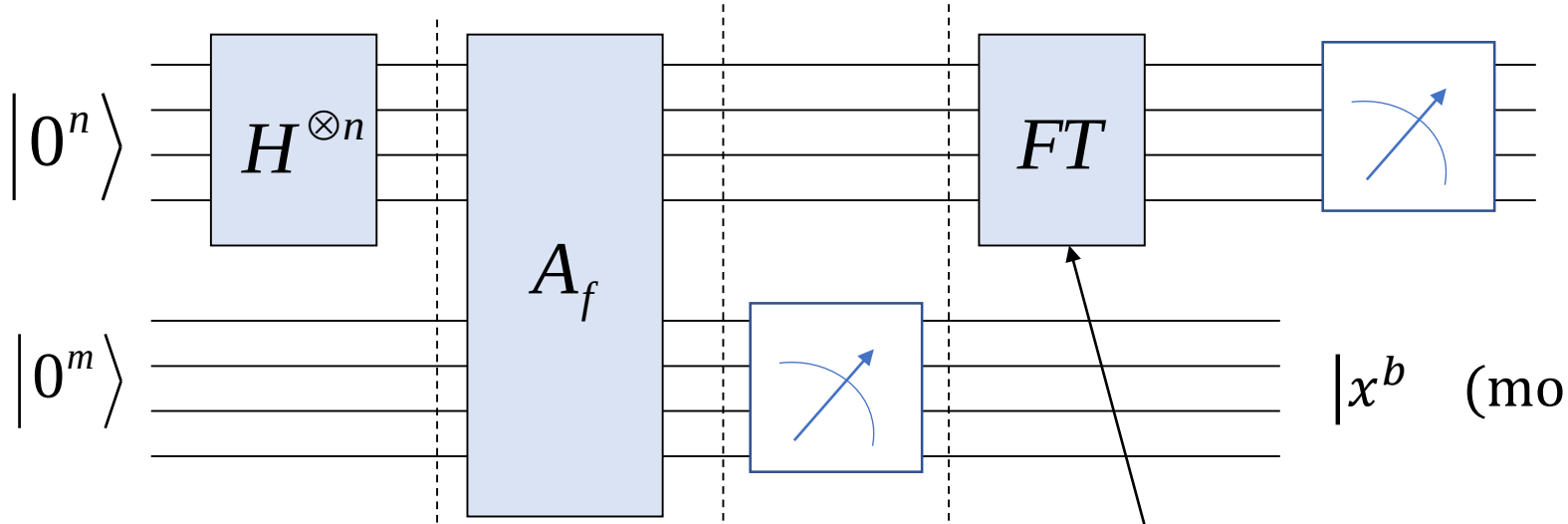
$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|0^n\rangle$$

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle$$

$$\frac{1}{\sqrt{2}}(|x_z\rangle + |x_z \oplus s\rangle)|z\rangle$$

$$\frac{1}{\sqrt{2^{n+1}}}(-1)^{y \bullet x_z}(1 + (-1)^{y \bullet s})|y\rangle|z\rangle$$

Quantum Algorithm for Order Finding



$$FT: |j\rangle \mapsto |\hat{j}\rangle := \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{(2\pi i)jk}{2^n}} |k\rangle$$

$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle|0^m\rangle$$

$$\frac{1}{\sqrt{2^n}} \sum_{z} |zr+b\rangle \left|x^b \pmod N\right\rangle$$

$$\frac{1}{\sqrt{2^n}} \sum_{k} |k\rangle|f(k)\rangle \quad \text{ただし，} \quad f(k) = x^k \pmod N$$

位相推定による素因数分解アルゴリズム

素因数分解問題（と同値な問題）

- 入力：奇数の合成数 $N > 1$
- 出力：Nの非自明な因数

Shorのアルゴリズム

1. 入力Nがある数aのべきで書けるかを調べて，もしそうならaを出力
2. ランダムな整数$x \in [2, N-1]$を選んで$\gcd(x, N) > 1$なら$\gcd(x, N)$を出力
3. 入力(N, x)のもとで位数発見問題を解き出力rを得る
4. 出力rが奇数あるいは$x^{r/2} = -1 \pmod N$なら「やり直し」．そうでなければ$\gcd(x^{\frac{r}{2}} - 1, N)$および$\gcd(x^{\frac{r}{2}} + 1, N)$を計算し，非自明な因数を得ればそれを出力．得られなければ「やり直し」

位数発見問題

- 入力：正整数Nおよびx ($x < N$はNと互いに素)
- 出力：$x^r = 1 \pmod N$なる最小の正整数（位数）r

定理(Shor)

位数発見問題を多項式時間（$O((\log N)^3)$時間）で高確率で解く量子アルゴリズムが存在

(Kitaev)

位相推定問題を解く量子アルゴリズムを利用した位数発見問題に対する量子アルゴリズム

位相推定

- 入力：ユニタリ行列UおよびUの固有状態$|\psi\rangle$（および近似精度ε）
- 出力：Uの固有状態$|\psi\rangle$に対する固有値$e^{2\pi i\theta}$の位相パラメータθ（の精度εでの近似値）

$\theta = \frac{m}{2^n}$と書ける場合の量子アルゴリズム

レジスタBに$|\psi\rangle$を入力として受け取るとする

1. レジスタAに$\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle$を準備
2. 制御U^kの実行：レジスタAがkのときレジスタBにU^kを施す

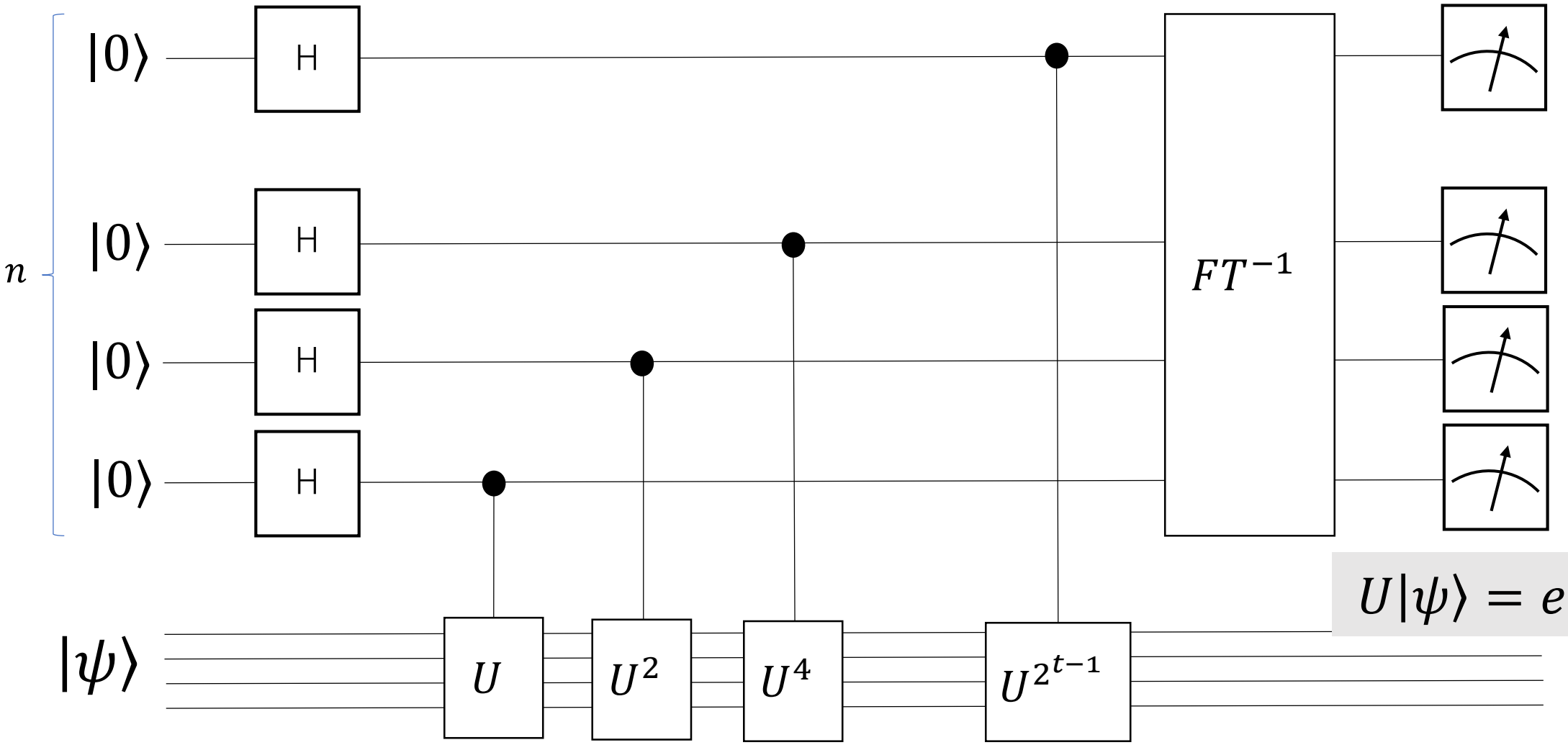
$$\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle_A \otimes U^k|\psi\rangle_B = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{\frac{(2\pi i)mk}{2^n}}|k\rangle_A \otimes |\psi\rangle_B$$

3. 量子フーリエ変換の逆変換をAに施す

$$FT^{-1}\colon |\hat{j}\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{\frac{(2\pi i)jk}{2^n}}|k\rangle \mapsto |j\rangle$$

位相推定の量子回路

$$FT^{-1}: |\hat{j}\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{(2\pi i) jk}{2^n}} |k\rangle \mapsto |j\rangle$$



$$U|\psi\rangle = e^{(2\pi i)\theta} |\psi\rangle$$

位相推定

- 入力：ユニタリ行列UおよびUの固有状態$|\psi\rangle$（および近似精度ε）
- 出力：Uの固有状態$|\psi\rangle$に対する固有値$e^{2\pi i\theta}$の位相パラメータθ（の精度εでの近似値）

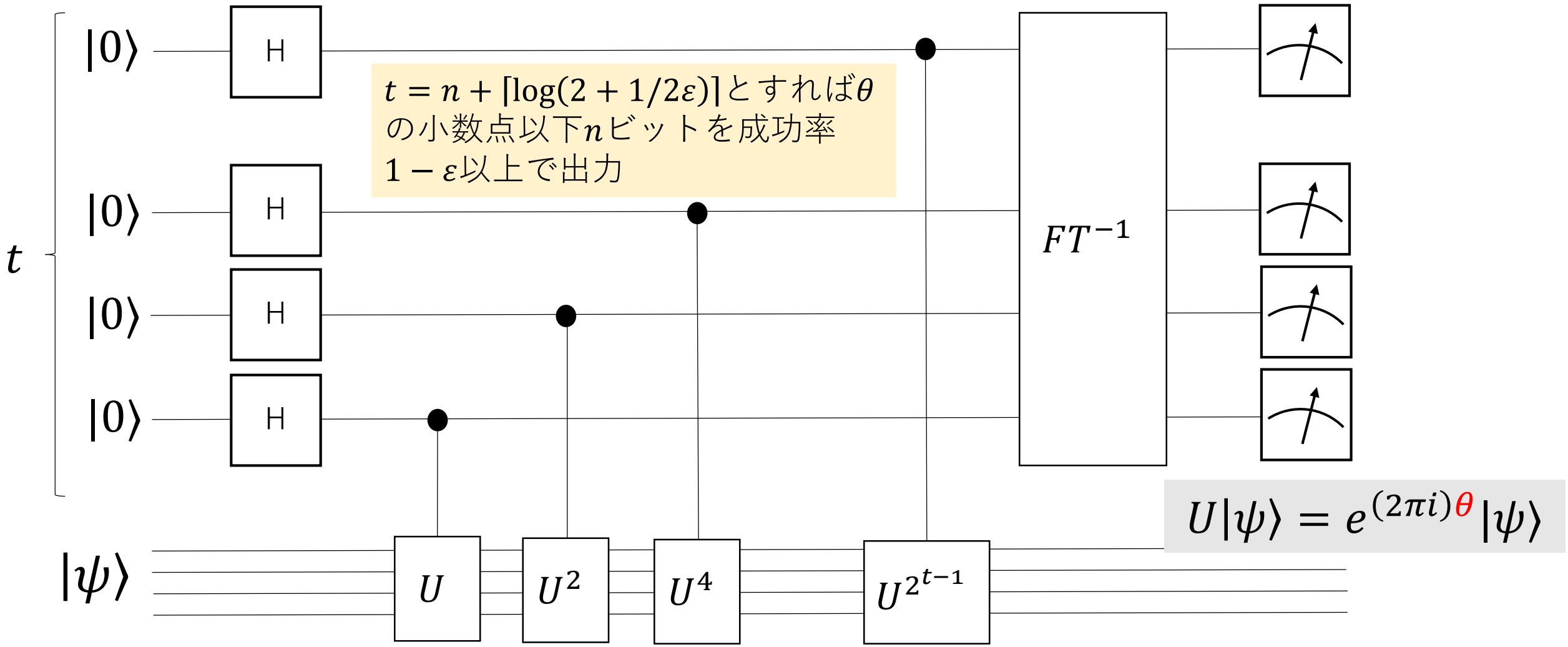
定理(Kitaev95, Cleve et al.96)

θの小数点以下nビットを成功率$1-\varepsilon$以上で出力する量子回路$C_{n,\varepsilon}$が存在して:

- $C_{n,\varepsilon}$のアンシラ量子ビット数$=O(n+\log\frac{1}{\varepsilon})$
- 制御U^j: $|j\rangle|x\rangle \mapsto |j\rangle(U^j|x\rangle)$を1回使用

位相推定の量子回路

$$FT^{-1}: |\hat{j}\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{(2\pi i) jk}{2^n}} |k\rangle \mapsto |j\rangle$$



$$U|\psi\rangle = e^{(2\pi i)\theta} |\psi\rangle$$

位数発見問題 vs 位相推定

- 位数発見問題
  - 入力：正整数Nおよびx ($x < N$はNと互いに素)
  - 出力：$x^r = 1 \pmod N$なる最小の正整数（位数）r
- 位相推定
  - 入力：ユニタリ行列UおよびUの固有状態$|\psi\rangle$（および近似精度ε）
  - 出力：Uの固有状態$|\psi\rangle$に対する固有値$e^{2\pi i\theta}$の位相パラメータθ（の精度εでの近似値）
- $U|y\rangle \coloneqq |xy \pmod N\rangle$で定義されるユニタリ行列$U$
  - $|u_s\rangle \coloneqq \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-\frac{2\pi isk}{r}} |x^k \bmod N\rangle$を固有ベクトルに持つ
  - 対応する固有値は$e^{\frac{2\pi is}{r}}$

位数発見に対する位相推定

- 位数発見問題
  - 入力：正整数Nおよびx ($x < N$はNと互いに素)
  - 出力：$x^r = 1 \pmod N$なる最小の正整数（位数）r
- 位相推定
  - 入力：ユニタリ行列UおよびUの固有状態$|\psi\rangle$（および近似精度ε）
  - 出力：Uの固有状態$|\psi\rangle$に対する固有値$e^{2\pi i\theta}$の位相パラメータθ（の精度εでの近似値）
- $U|y\rangle \coloneqq |xy \pmod N\rangle$で定義されるユニタリ行列$U$
  - $|u_s\rangle \coloneqq \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-\frac{2\pi isk}{r}} |x^k \bmod N\rangle$を固有ベクトルに持つ
  - 対応する固有値は$e^{\frac{2\pi is}{r}}$
- 位相推定によって$\frac{s}{r}$が近似できる⇒ rと互いに素なsに対しては位数rが計算できる（**連分数展開**）
- **問題点**：rと互いに素なsに対する$|u_s\rangle$をどうやって準備するか？

位数発見に対する位相推定

位数発見問題
入力：正整数Nおよび$x(x < N$はNと互いに素$)$
出力：$x^r = 1 \pmod N$なる最小の正整数（位数）r

- 位相推定
  - 入力：ユニタリ行列UおよびUの固有状態$|\psi\rangle$（および近似精度ε）
  - 出力：Uの固有状態$|\psi\rangle$に対する固有値$e^{2\pi i\theta}$の位相パラメータθ（の精度εでの近似値）
- $U|y\rangle \coloneqq |xy \pmod N\rangle$で定義されるユニタリ行列$U$
  - $|u_s\rangle \coloneqq \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-\frac{2\pi isk}{r}} |x^k \bmod N\rangle$を固有ベクトルに持つ
  - 対応する固有値は$e^{\frac{2\pi is}{r}}$
- 位相推定によって$\frac{s}{r}$が近似できる⇒rと互いに素なsに対しては位数rが計算できる（連分数展開）
- **問題点**： rと互いに素なsに対する$|u_s\rangle$をどうやって準備するか？
- **解決策**：一様重ね合わせ

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle$$

$\Omega\left(\frac{1}{\log\log r}\right)$の確率で$s$は$r$と互いに素

位数発見に対する位相推定

1. レジスタAに$|0^t\rangle$, レジスタBに$|1\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r}|u_s\rangle$を準備
2. レジスタAをアンシラとしてBの位相を推定

$$\approx \frac{1}{\sqrt{r}}\sum_{s=0}^{r}\left|\frac{s}{r}\right\rangle_A \otimes |u_s\rangle_B$$

3. レジスタAを測定して連分数展開
   - rと互いに素なsに対して出力としてrを得る

他の量子アルゴリズム

Other Quantum Algorithms

- 量子ウォーク(Quantum Walk)
  - 人工的だが，古典に対する指数的な優位性 [Childs et al 2003]
  - Groverの発展形ともいえる量子アルゴリズム [Ambainis 2003, Szegedy 2004]
  - AND-OR木に対する量子アルゴリズム [Ambainis et al 2007]
- 量子シミュレーション(Quantum Simulation)
  - ハミルトニアンHで定まる時間発展e^{iHt}の量子コンピュータによるシミュレーション [Lloyd 1996, Ahanorov & Ta-Shma 2003ほか]
  - 量子化学への応用
- Quantum Algorithm for Linear Equations [Harrow-Hassidim-Lloyd 2008]
  - 線形方程式 $Ax = b$ を指数的に速く解く
  - ただし，出力は$\sum_i |b_i\rangle$の形でしか受け取れない
  - 機械学習への応用 [Lloyd et al 2014]
  - 量子アルゴリズムをヒントにした古典アルゴリズム [Tang 2019]

Quantum Subroutines

- Block encoding
  - 任意の行列Mをユニタリ行列の一部に
$$U = \begin{pmatrix} M & \cdot \\ \cdot & \cdot \end{pmatrix}$$
のように埋め込んで確率的に実行
- Phase estimation
  - ユニタリ行列Uにおいて固有ベクトル$|\psi\rangle$の固有値$e^{2\pi i\theta}$の位相パラメータθを推定
- Quantum singular value transformation (QSVT)
  - 行列Aの特異値分解$A = \sum_j \sigma_j |w_j\rangle\langle v_j|$の特異値を変換した行列$f(A) = \sum_j f(\sigma_j) |w_j\rangle\langle v_j|$を実行する量子アルゴリズム
  - Groverや位相推定など様々な量子アルゴリズムがQSVTの枠組みで実行可能

Quantum Algorithm Sources

- Quantum Algorithm Zoo
  - quantumalgorithmzoo.org
  - Webpage by S. Jordan
  - 邦訳ページあり
- Quantum algorithms: A survey of applications and end-to-end complexities
  - arXiv:2310.03011
  - Survey document with wiki-like modular structure