量子計算機と暗号解読

光成滋生

last update: 2025/12/11

概要

古典計算機

- 現在（古典）計算機はビット (0 or 1) を基本単位として計算
- 論理ゲート: AND, OR, NOTなどのビット演算の組合せ

量子計算機 QC (Quantum Computer)

- 量子力学で記述される量子状態を利用した計算機
  - 攻撃: 量子計算機を利用して暗号技術を破る量子アルゴリズム
  - 対策: 耐量子計算機暗号（量子計算機が登場しても安全な現在の計算機で実行できる暗号）
  - 量子鍵配送（量子暗号）: 量子の性質を利用した秘密鍵を共有する技術

粒子と波

- 粒子は1個, 2個と数えられ, 同じ場所に複数個存在できない
- 波は数えられない広がりを持った状態
- 複数の波が重なり合って干渉する

量子

粒子と波の両方の性質をもった状態

- 電子, 光子, 原子などの量子状態を最小単位 (qubit) として制御することで計算

量子計算機の方式例

- 超電導・イオントラップ・中性原子・光など
  - それぞれの方式の詳細は本講演の範囲外
- コヒーレンス時間（量子情報を保持する時間）・速度・エラー率・動作温度が一長一短
- qubit を増やすだけでなく、エラー率の低減・大規模化・運用コストなども課題

誤り訂正

- 量子情報（重ね合わせ・位相）は外部環境の影響を受けやすく誤りが発生しやすい
- 誤り訂正の技術を使って複数の物理qubitで1個の論理qubitを表す
- 実際に計算できるためには誤り耐性量子計算FTQC（Fault-Tolerant QC）が必要
- 実用的なものは100万 qubit程度必要と言われている

量子計算機の実装例

超伝導方式

- Google: 2019年 53 qubit, 2024年 105 qubit
- IBMのロードマップ: 2021年 127 qubit, 2022年 433 qubit, 2023年 1121 qubit Condor
- 大阪大学: 2023年 64 quibit, 富士通と理研: 2025年 256 qubit

イオントラップ方式

- 2023/6: IonQが29 quibit, 2025: Quantinuum 56 qubit
- 2025/6: 1qubitで1/670万のエラー率

中性原子方式

- 2023/10: Atom Computing 1180 quibit
- 2025/9: 6100 qubit, 0.02%のエラー率
- その他: 電子, 光, マイクロ波 etc.

量子計算機に必要な線形代数の復習

行列

- 複素数を縦に n 個, 横に m 個並べた $A = (a_{ij})$ $(a_{ij} \in \mathbb{C})$ を n 行 m 列（複素）行列という
  - その全体を $M_{n,m}(\mathbb{C})$ と書く（$n = m$ のときは n 次正方行列で $M_n(\mathbb{C})$ と書く）
- $A \in M_{n,m}(\mathbb{C}), B \in M_{m,l}(\mathbb{C})$ に対して行列の積 $AB := \left(\left(\sum_{k=1}^{m} a_{ik}b_{kj}\right)_{ij} \in M_{n,l}(\mathbb{C})\right.$
- A^T: 行列 A の転置行列 $A^T := (a_{ji})$ は m 行 n 列の行列
- A のエルミート共役: $A^\dagger := \overline{A}^T = (\overline{a_{ji}})$（$\overline{a_{ji}}$ は a_{ij} の複素共役）
  - $(AB)^\dagger = (\overline{(AB)_{ji}}) = (\overline{\sum a_{jk}b_{ki}}) = B^\dagger A^\dagger$

ベクトル

- n 次元縦ベクトル $v, w \in M_{n,1}(\mathbb{C})$ の内積: $v \cdot w := v^\dagger w = \sum_{i=0}^{n} \overline{v_i} w_i \in \mathbb{C}$
- v のノルム（長さ）: $|v| := \sqrt{v \cdot v}$, 単位ベクトル: ノルムが1のベクトル
- n 個の n 次元縦ベクトル $e_1, \ldots, e_n$ が $e_i \cdot e_j = \delta_{ij}$ のとき $\{e_i\}$ を正規直交基底という
  - $\{e_i := (0, \ldots, 0, 1, 0, \ldots, 0)^T\}$（$i$ 番目だけ1）は標準基底

ユニタリ行列

量子力学の演算に必要な行列

- ユニタリ行列: $U^\dagger U = I$ を満たす n 次行列 U（I は単位行列）, その全体を $U(n)$ と書く
- $U \in U(n)$ なら $U^{-1} = U^\dagger$ なので U は可逆
- ユニタリ行列はベクトルの長さを変えない
  - v が $|v| = l$ なら $l^2 = v^\dagger v = v\dagger (U^\dagger U)v = (Uv)^\dagger (Uv) = |Uv|^2$ なので $|Uv| = l$
  - 同様に $\{e_i\}$ が正規直交基底なら $\{Ue_i\}$ も正規直交基底（$(Ue_i)^\dagger (Ue_j) = \delta_{ij}$）
  - 特に U は単位ベクトルを単位ベクトルに移す

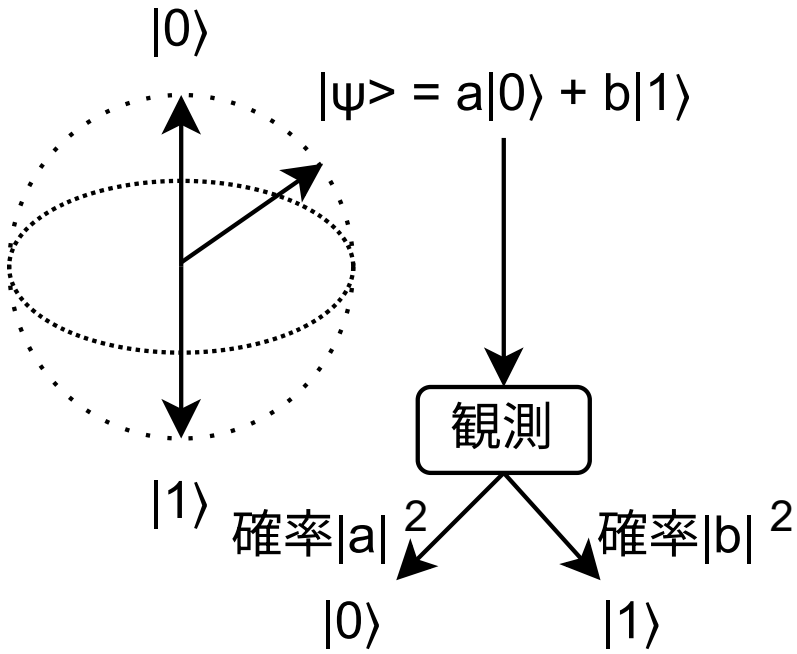
固有値と固有ベクトル

- A: 行列, v: ベクトル, $\lambda \in \mathbb{C}$ について $Av = \lambda v$ を満たすとき v: A の固有ベクトル, λ: 固有値
- A がユニタリ行列のとき $|v| = 1$ とすると $|v| = |Av| = |\lambda||v|$ なので $|\lambda| = 1$
  - ユニタリ行列の固有値は絶対値が1の複素数なので $\lambda = e^{i\theta}$ $(\theta \in \mathbb{R})$ と表せる

量子計算機の基礎

QC の演算の基本単位: 量子ビット (qubit)

- 1 qubitとは複素2次元単位ベクトル $v := (a, b)^T \in M_{2,1}(\mathbb{C})$
  - $|v| = 1$ より $|a|^2 + |b|^2 = 1$
  - $v = a(1, 0)^T + b(0, 1)^T$ は標準基底による表現
  - 慣習的にベクトル v と標準基底 $\left\{(1, 0)^T, (0, 1)^T\right\}$ を $|\psi\rangle, \{|0\rangle, |1\rangle\}$ と書き $|\psi\rangle = a|0\rangle + b|1\rangle$ と表記する
    $ab \neq 0$ のとき $|\psi\rangle$ は $|0\rangle, |1\rangle$ の混合状態という



観測の原理

- $|\psi\rangle$ を基底 $(|0\rangle, |1\rangle)$ に従って「観測」すると $|a|^2$ の確率で $|0\rangle$, $|b|^2$ の確率で $|1\rangle$ が得られる

位相

- $\theta \in [0, 1]$ について $|e^{i\theta}| = 1$ なので $|\psi'\rangle := e^{i\theta}|\psi\rangle$ の観測結果は $|\psi\rangle$ の観測結果と同じ分布
- $|\psi\rangle$ と $|\psi'\rangle$ は物理的に区別がつかない: 位相変換に対して不変, $e^{i\theta}$ を位相因子という

量子ゲート

qubitの状態を変換する演算

- 1 qubit $|\psi\rangle = (a, b)^T$ に対して $U \in U(2)$ を掛ける操作: $|\psi\rangle \mapsto U|\psi\rangle$ を量子ゲートという
  - U はユニタリ行列なので $|U|\psi\rangle| = ||\psi\rangle| = 1$ であり, $U|\psi\rangle$ もqubitの状態を表す
- ユニタリ行列は可逆なので量子ゲートは可逆な変換しかできない
  - 例えば古典の AND ゲートは不可逆なので量子ゲートでは実現できない
  - 後述する複数のqubitを用いて $(x, y, z) \mapsto (x, y, z \oplus (x \wedge y))$ のような形で実現する

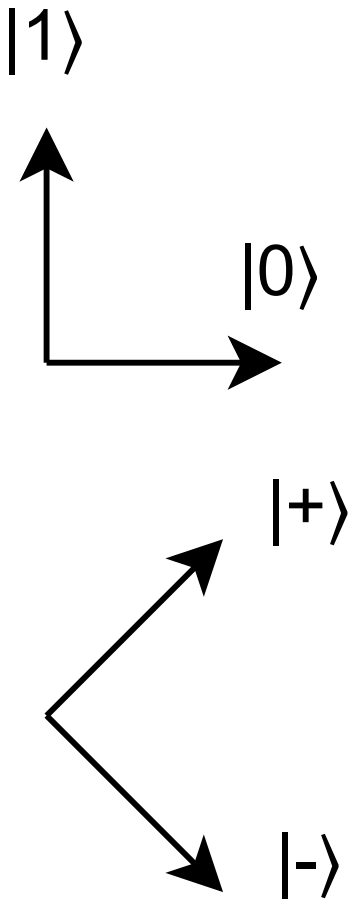
複製不可能性定理 (no-cloning theorem)

- 未知の量子状態の複製は不可能
- ユニタリ行列の性質から導かれる
  - 古典的な誤り訂正を適用できない
  - 量子誤り訂正符号という異なる手法・理論がひつよう

量子ゲートの例

代表的な量子ゲート

- X (NOT) ゲート: $X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
  - $X|0\rangle = |1\rangle = (1,0)^T, X|1\rangle = |0\rangle = (0,1)^T$: 基底の反転
- アダマールゲート: $H := (1/\sqrt{2}) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
  - $|+\rangle := H|0\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle) = (1/\sqrt{2})(1,1)^T$
  - $|-\rangle := H|1\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle) = (1/\sqrt{2})(1,-1)^T$
- 位相回転: $R(\theta) := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$
  - $R(\theta)|0\rangle = |0\rangle, R(\theta)|1\rangle = e^{i\theta}|1\rangle$
    - $|1\rangle$ の位相を θ だけ回転させる
  - $T := R(\pi/4), S := R(\pi/2)$ と略記することが多い（$T^2 = S$）



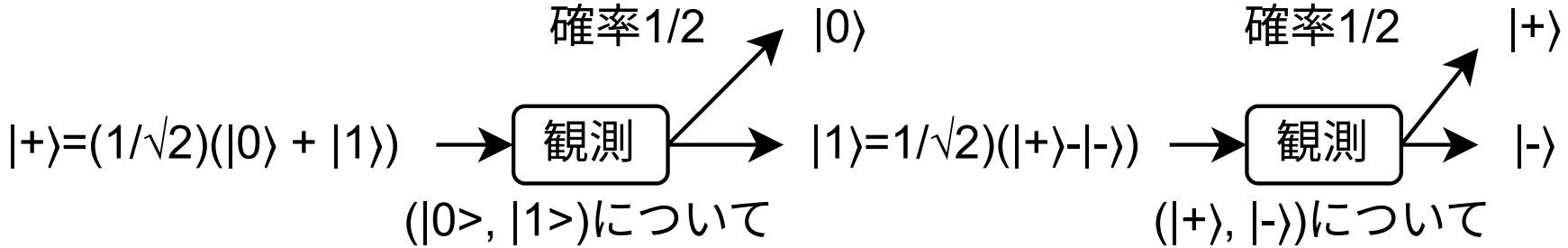
異なる基底での観測

相互関係

- $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle), |-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$
- $|0\rangle = (1/\sqrt{2})(|+\rangle + |-\rangle), |1\rangle = (1/\sqrt{2})(|+\rangle - |-\rangle)$

基底を取り替えて観測する

- $(|0\rangle, |1\rangle)$ 以外の基底でも観測できる
- $(|+\rangle, |-\rangle)$ も別の基底なので $|+\rangle, |-\rangle$ で観測してみる
- $|0\rangle$ を $(|0\rangle, |1\rangle)$ に関して観測すると確率 1 で $|0\rangle$
- $|0\rangle$ を $(|+\rangle, |-\rangle)$ に関して観測すると確率 $1/2$ で $|+\rangle$ か $|-\rangle$



複数個のqubit

テンソル積

- 2個の2次元ベクトルの基底を組み合わせて4次元ベクトル空間の基底を作る（合成系という）
  - $(a,b)\otimes(c,d) := (ac,ad,bc,bd)$ （表記の都合で横ベクトルで表す）
- 独立に準備された2個の1 qubit $|\psi_1\rangle$ と $|\psi_2\rangle$ がある状態を $|\psi_1\rangle\otimes|\psi_2\rangle$ と表す
- 複素4次元ベクトル空間 $\mathcal{H}$ の基底
  - $|00\rangle := |0\rangle\otimes|0\rangle = (1,0)\otimes(1,0) = (1,0,0,0)$
  - $|01\rangle := |0\rangle\otimes|1\rangle = (1,0)\otimes(0,1) = (0,1,0,0)$
  - $|10\rangle := |1\rangle\otimes|0\rangle = (0,1)\otimes(1,0) = (0,0,1,0)$
  - $|11\rangle := |1\rangle\otimes|1\rangle = (0,1)\otimes(0,1) = (0,0,0,1)$
- 一般に $\mathcal{H}$ の元は $c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$ $(c_{ij}\in\mathbb{C}, \sum|c_{ij}|^2 = 1)$ の形
  - この基底で観測したとき $|ij\rangle$ が得られる確率は $|c_{ij}|^2$
- n個のqubitの状態は 2^n 次元複素ベクトルとなる
  - $|i_0 i_1\cdots i_{n-1}\rangle$ を i を2進数展開$(i=\sum_k i_k 2^k)$ したものとみなして $|i\rangle$ と略記する

量子もつれ (Entanglement)

合成系の中でテンソル積で表現できない状態

- テンソル積で表現できる例
  - $(1/\sqrt{2})(|0\rangle + |1\rangle) \otimes |0\rangle = (1/\sqrt{2})(|00\rangle + |10\rangle)$
  - $(1/\sqrt{2})(|0\rangle + |1\rangle) \otimes (1/\sqrt{2})(|0\rangle + |1\rangle) = (|00\rangle + |01\rangle + |10\rangle + |11\rangle)/2$
- テンソル積で表現できない例
  - $|\psi\rangle := (1/\sqrt{2})(|00\rangle + |11\rangle)$
    - $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ と表現できない
      - $|\psi_1\rangle = a|0\rangle + b|1\rangle, |\psi_2\rangle = c|0\rangle + d|1\rangle$ とすると
        $ac = 1/\sqrt{2}, bd = 1/\sqrt{2}, ad = 0, bc = 0$ となり矛盾
- このように状態が各qubitの状態のテンソル積で表現できないとき
  $|\psi\rangle$ は量子もつれの状態にあるという

部分測定

部分測定の例

- $|\psi\rangle = s|00\rangle + t|01\rangle + u|10\rangle + v|11\rangle$ とする
- 1個目のqubitについて測定して $|0\rangle$ となるのは $s|00\rangle$ か $t|01\rangle$ のどちらかで確率は $|s|^2 + |t|^2$
  - 測定後の状態は $|\psi'\rangle = s|00\rangle + t|01\rangle$ を正規化したもの
    - ベクトル $v \neq 0$ の正規化とはノルムを1にすること: $v \mapsto v/|v|$
  - $||\psi'\rangle|^2 = |s|^2 + |t|^2$ なので $|\psi'_0\rangle := |\psi'\rangle/|\psi'| = (s|00\rangle + t|01\rangle)/\sqrt{|s|^2 + |t|^2}$
- 同様に $|1\rangle$ となる確率は $|u|^2 + |v|^2$, 測定後は $|\psi'_1\rangle := (u|10\rangle + v|11\rangle)/\sqrt{|u|^2 + |v|^2}$

テンソル積の場合

- $|\psi_1\rangle = a|0\rangle + b|1\rangle, |\psi_2\rangle = c|0\rangle + d|1\rangle$ で $a, b, c, d > 0, |\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ なら
  $s = ac, t = ad, u = bc, v = bd$ となり $|s|^2 + |t|^2 = |a|^2(|c|^2 + |d|^2) = |a|^2$
- 確率 a^2 で $|\psi'_0\rangle = (ac|00\rangle + ad|01\rangle)/a = |0\rangle \otimes |\psi_2\rangle$
- 確率 b^2 で $|\psi'_1\rangle = (bc|10\rangle + bd|11\rangle)/b = |1\rangle \otimes |\psi_2\rangle$. 第2qubitはどちらも同じ（独立）

部分測定後の独立性

量子もつれの場合

- $|\psi\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$ の場合
- 1個目のqubitを観測して $|0\rangle$ が得られる確率は $1/2$, 測定後の状態は $|00\rangle$
- 1個目のqubitを観測して $|1\rangle$ が得られる確率は $1/2$, 測定後の状態は $|11\rangle$
  - 1個目のqubitが $|0\rangle$ ならば2個目も $|0\rangle$, 1個目が $|1\rangle$ なら2個目も $|1\rangle$

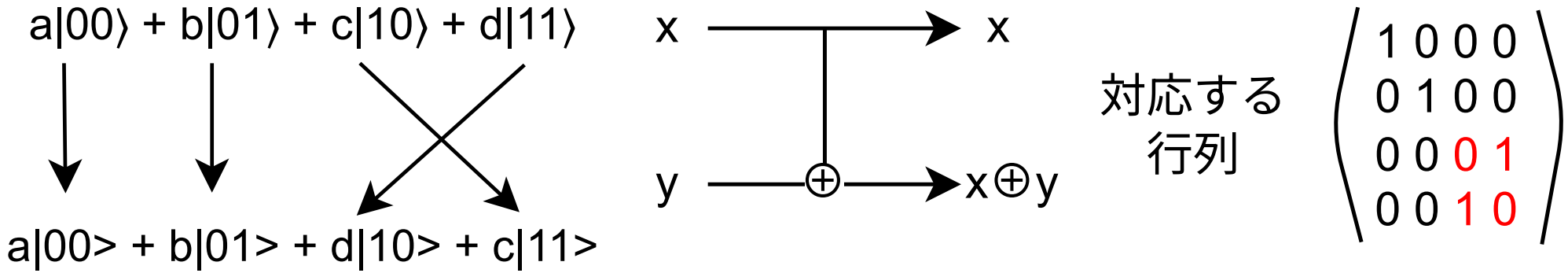
2個のqubitが独立でない

- 1個目のqubitの状態が決まると2個目の状態も決まる
  - 2個のqubitは離れた状態でも成り立つ
  - 量子テレポーテーションや量子暗号（量子鍵配送）のキーとなる現象

CNOT (Controlled NOT) ゲート

2個のqubitに対する量子ゲート

- $CNOT(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle) := a|00\rangle + b|01\rangle + d|10\rangle + c|11\rangle$
  - 後ろ2個の基底の係数が入れ代わる



  - 状態 $|xy\rangle$ $(x, y \in \{0, 1\})$ に対して $x = 0$ のとき y はそのまま, $x = 1$ のとき y は反転
  - $(x, y) \mapsto (x, x \oplus y)$ と表せる
- $x = (1/\sqrt{2})(|0\rangle + |1\rangle), y = |0\rangle$ とすると $x \otimes y = (1/\sqrt{2})(|00\rangle + |10\rangle)$
  - $CNOT(x \otimes y) = (1/\sqrt{2})(|00\rangle + |11\rangle)$ となり量子もつれの状態になる
- 量子計算の普遍性: $H, T, CNOT$ の組合せで任意の量子ゲートを近似できる
  - これら（と $S = T^2$ も追加して）を使って量子回路を組み立てる

CNOTを用いたSWAP

2個のqubitの入れ換え

- $(x, y) \overset{CNOT(1\to2)}{=} (x, x \oplus y) \overset{CNOT(2\to1)}{=} (x \oplus (x \oplus y), x \oplus y) = (y, x \oplus y)$
  $\overset{CNOT(1\to2)}{=} (y, (x \oplus y) \oplus y) = (y, x)$

古典的にも一時変数を使わない同様のSWAPがある

- int a, b; に対して
  - a = a ^ b;
  - b = a ^ b; // b = (a ^ b) ^ b = a
  - a = a ^ b; // a = (a ^ b) ^ a = b

CNOTを用いた量子ビットの冗長化

量子誤り訂正の基礎

- 量子状態の複製は不可能なので古典的な3重冗長化はできない
- 量子ビットの冗長化の例
  - $|\psi\rangle = a|0\rangle + b|1\rangle$ に $|00\rangle$ を付加して $|\psi\rangle \otimes |00\rangle = a|000\rangle + b|100\rangle$
  - 1, 2ビット目にCNOTゲートを適用: $(x, y) \mapsto (x, x \oplus y)$
    - $a|000\rangle + b|100\rangle \to a|000\rangle + b|110\rangle$
  - 1, 3ビット目にCNOTゲートを適用
    - $a|000\rangle + b|110\rangle \to a|000\rangle + b|111\rangle$
- $|000\rangle, |111\rangle$ を1個の論理qubit $|0_L\rangle, |1_L\rangle$ とみなして冗長化

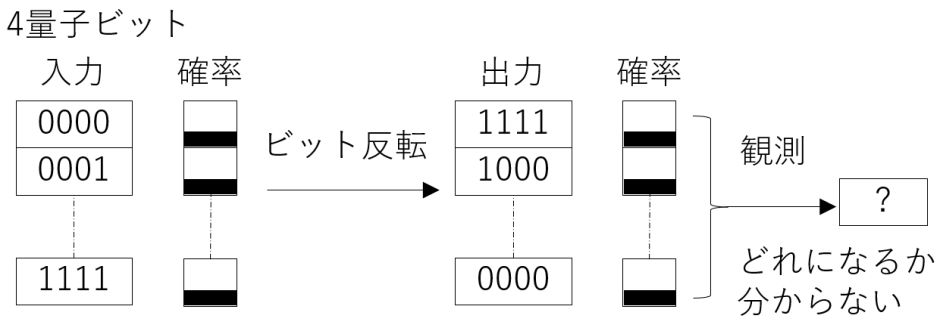
Shorコード: 1論理qubitを9個の物理qubitで表現

- 位相反転 $|+\rangle \leftrightarrow |-\rangle$ とビット反転 $|0\rangle \leftrightarrow |1\rangle$ のどちらかに耐性がある
  - $|0_L\rangle := (1/\sqrt{2^3})(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$
  - $|1_L\rangle := (1/\sqrt{2^3})(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$

量子計算機における計算

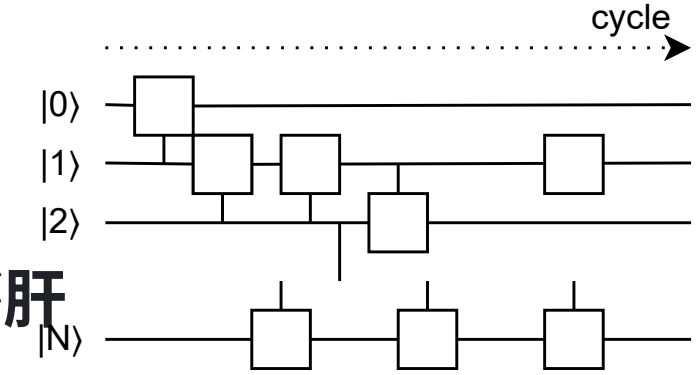
n qubitの状態は 2^n 通りの状態の重なり

- $|\psi\rangle = \sum_{i=0}^{2^n-1} c_i|i\rangle \ (c_i \in \mathbb{C}, \sum |c_i|^2 = 1)$
- $|\psi\rangle$ に標準量子ゲートなどを順番に作用させる回路を作る
  - 遠いところはSWAP演算などの組合せ



最終的には観測しないと結果を得られない

- そのとき $|c_i|^2$ の確率で $|i\rangle$ に確定し, これが計算結果
- もし $|c_0| = \cdots = |c_{2^n-1}|$ ならどの $|i\rangle$ が得られるかランダム



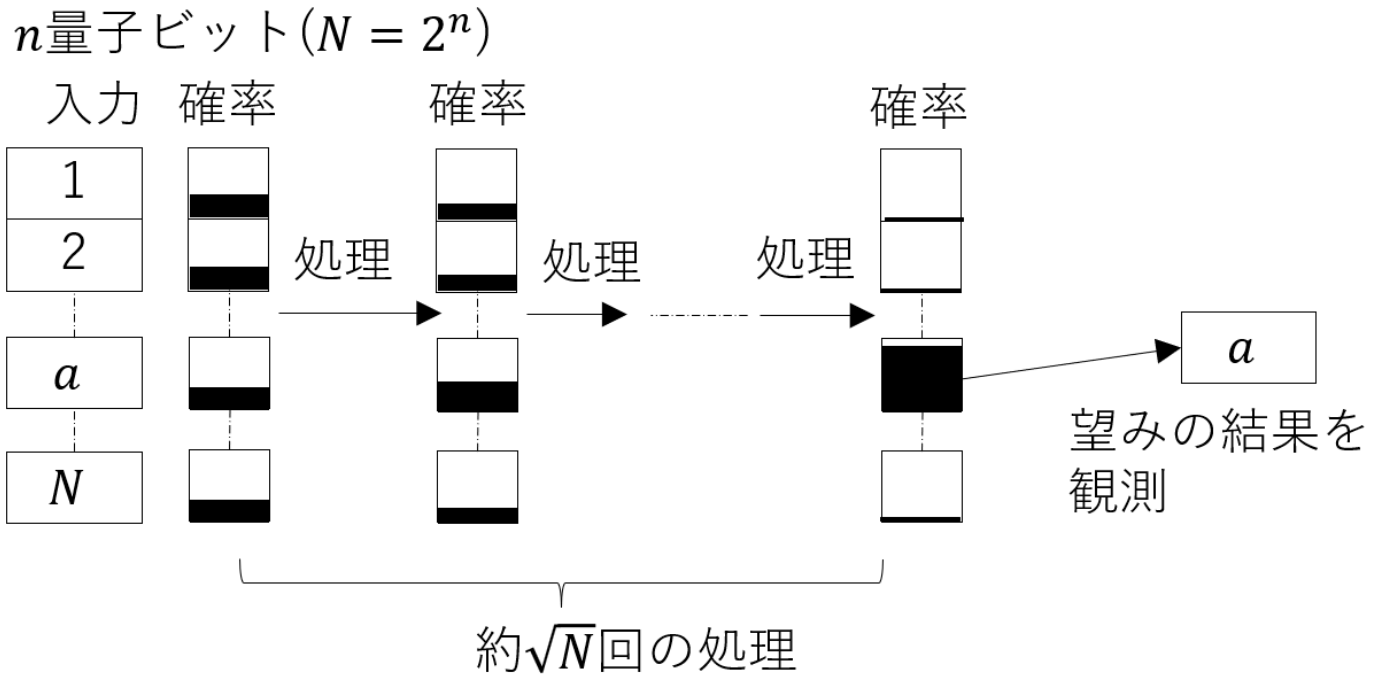
望ましい答えが観測されるように特定の $|c_i|$ を大きくするのが肝

- 古典計算機における分岐・ループ処理は存在しない
- 10回ループする処理は10回分の量子ゲートを展開する
- 任意回ループは基本的に不可能

Groverのアルゴリズム

N 個のデータから特定の条件を満たすものを一つ探す

- 関数 $f(x) = 1$ if $x = a$, それ以外は0 において $f(x) = 1$ となる $x = a$ を探す
- 古典計算機なら平均 $N/2$ 回の試行が必要
- Groverのアルゴリズムは $O(\sqrt{N})$ 回の量子クエリで可能
  - $O(\sqrt{N})$ 回のクエリで十分高い確率で $f(x) = 1$ なる x が見つかるということ



2qubitに対するアダマールゲート

$H \otimes H = H^{\otimes 2}$ と表記

- $H = (1/\sqrt{2}) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ なので$H^{\otimes 2} = (1/2) \begin{pmatrix} 1 \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} & 1 \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ 1 \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} & -1 \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{pmatrix} = (1/2) \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$
  - $H^{\otimes 2}|00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
  - $H^{\otimes 2}|01\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$
  - $H^{\otimes 2}|10\rangle = \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle)$
  - $H^{\otimes 2}|11\rangle = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$
- $H^{\otimes 2}|i\rangle = \frac{1}{2}\sum_{j=0}^{3}(-1)^{i \cdot j}|j\rangle \, (i = 0, 1, 2, 3)$
  - $i \cdot j$ は i, j を2進数展開したときの各桁の積の和（$\mathrm{mod}\ 2$）
  - 例えば $i = 2 = 10_2, j = 3 = 11_2$ のとき $i \cdot j = 1 \times 1 + 0 \times 1 = 1$
- $H^{\otimes n}|i\rangle = (1/2^{n/2})\sum_{j=0}^{2^n-1}(-1)^{i \cdot j}|j\rangle \, (i = 0, 1, \ldots, 2^n - 1)$

一般の関数に対する量子ゲート

補助ビット (ancilla) の導入

- 関数 $f : \{0,1\}^n \to \{0,1\}$ に対して
  $U_f : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle$ と定義する
  - x: n qubit, y: 1 qubit （y が補助ビット）
- このとき U_f はユニタリ行列になる
  - $U_f(U_f(|x\rangle \otimes |y\rangle)) = |x\rangle \otimes |y \oplus f(x) \oplus f(x)\rangle = |x\rangle \otimes |y\rangle$, つまり $U_f^{-1} = U_f$
- 位相キックバック
  - $|y\rangle := |-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$ とする
    - $f(x) = 0$ のとき $U_f(|x\rangle \otimes |-\rangle) = |x\rangle \otimes |-\rangle$
    - $f(x) = 1$ のとき $U_f(|x\rangle \otimes |-\rangle) = -|x\rangle \otimes |-\rangle$
    - つまり $U_f(|x\rangle \otimes |-\rangle) = (-1)^{f(x)}|x\rangle \otimes |-\rangle$
      $f(x)$ を位相部分に埋め込む演算 $U_f(|x\rangle) = (-1)^{f(x)}|x\rangle$ とみなす

Shorのアルゴリズム

$n = pq$ (p, q は素数) を素因数分解するアルゴリズム

- 位数計算問題: 与えられた $g \in [1, n-1]$ の位数を求める問題
  - g の位数: $g^r \equiv 1 \pmod{n}$ となる最小の正整数
- 位数が見つかり r が偶数ならば $(g^{r/2} - 1)(g^{r/2} + 1) \equiv 0 \pmod{n}$
  - このとき有意な確率で $g^{r/2} - 1$ と $g^{r/2} + 1$ のどちらかは n の非自明な約数を持つ
  - 見つからなければ別の g でやり直す
  - 最大公約数は古典計算機で高速に求められるので p, q が得られる
- 位数計算問題を量子計算機で解き, 全体で $O((\log n)^3)$ で素因数分解できる

QFT (Quantum Fourier Transform)

量子フーリエ変換

- 古典離散フーリエ変換DFTの量子版
- n qubit の $|x\rangle = \sum_{j=0}^{N-1} x_j |j\rangle, N := 2^n, w = w_N := \exp(2\pi\sqrt{-1}/N)$ に対して
- QFTは $|j\rangle$ を $(1/\sqrt{N}) \sum_{k=0}^{N-1} w^{jk} |k\rangle$ に変換する（$|j\rangle$ という状態と位相の相互変換）
  - $O(n^2)$ 個の量子ゲート, $O(n^2)$ ステップで実現可能

古典DFT

- $x_k \mapsto X_j := F(x_k) = (1/\sqrt{N}) \sum_{k=0}^{N-1} x_k w^{jk}$
- 逆変換は $X_j \mapsto x_k = (1/\sqrt{N}) \sum_{j=0}^{N-1} X_j w^{-jk}$
  - $\sum_j w^{j(l-k)} = N\delta_{lk}$

量子位相推定 QPE (Quantum Phase Estimation)

ユニタリ行列 U の固有値を求める

- U の固有値は絶対値が 1 なので $e^{2\pi i\theta}$ ($\theta \in [0, 1)$) と表せる
- U の固有ベクトル $|\psi\rangle$ が与えられたとき $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$ となる θ を m 桁の精度で求める
  - $N = 2^m, w = \exp(2\pi i/N)$

大まかな手順

- アダマールゲートを m qubitに作用: $|0^{\otimes m}\rangle|\psi\rangle \mapsto (1/\sqrt{N})\sum_{k=0}^{N-1}|k\rangle|\psi\rangle$
- U^k を作用: $|\psi\rangle \mapsto e^{2\pi i\theta k}|\psi\rangle = w^{Nk\theta}|\psi\rangle$ した結果: $(1/\sqrt{N})\sum_k w^{Nk\theta}|k\rangle \otimes |\psi\rangle$
- 逆QFTを作用: $|k\rangle \mapsto (1/\sqrt{N})\sum_j w^{-jk}|j\rangle$ した結果: $(1/N)\sum_{k,j} w^{k(N\theta-j)}|j\rangle \otimes |\psi\rangle$
- 測定:
  - ある j について $N\theta = j$ なら $|j\rangle|\psi\rangle$ が観測されるので j が求まる
  - そうでなくても $\theta \approx j/N$ なら40%程度の確率で $|j\rangle|\psi\rangle$ になることが示される

QPEを用いた位数計算の概略

演算 $U|x\rangle := |gx \bmod n\rangle$

- このとき固有ベクトル $|w_j\rangle := (1/\sqrt{r})\sum_{k=0}^{r-1}\exp(-2\pi ikj/r)|g^k \bmod n\rangle$ に対して固有値 $\lambda_j = \exp(2\pi ij/r)$, つまり $U|w_j\rangle = \exp(2\pi ij/r)|w_j\rangle$
  - $g^r \equiv 1$ なので U は $|g^k \bmod n\rangle$ を $|g^{(k+1) \bmod r} \bmod n\rangle$ に移す.
  - $\sum$ の添え字 k は $k-1$ に置き換えられて exp の要素 $\exp(-2\pi i(-1)j/r) = \lambda_j$ が出る
- 固有値の位相に j/r が含まれている
- QPEにより j/r の近似値が求まる
  - $(1/\sqrt{r})\sum_j |w_j\rangle = |1\rangle$ なので $|w_j\rangle$ を知らなくても $|1\rangle$ に対してQPEを適用できる
  - 連分数展開の技法を使って正確な値を求める
- QPEで必要な $U^{2^k}|x\rangle = |g^{2^k}x \bmod n\rangle$ は $g^{2^k}x \bmod n$ を古典計算機で事前に求めておく

量子計算機によるECDLPの解読

ECDLPからQPEへ

- $\langle P \rangle$: $E(\mathbb{F}_p)$ 上の素数位数 n の巡回群. $Q \in \langle P \rangle$ に対して $Q = xP$ となる x を見つける
- $|0,0\rangle|0\rangle$ にアダマールゲートを作用させて $(1/n)\sum_{a,b}|a,b\rangle|0\rangle$ を作る
- $U|a,b\rangle|0\rangle := |a,b\rangle|aP+bQ\rangle$ を作用させる
  - 結果: $(1/n)\sum_{a,b}|a,b\rangle|aP+bQ\rangle = (1/n)\sum_{R\in S_R}|a,b\rangle|R\rangle$,
    $S_R := \{(a,b) \mid aP+bQ = R\}$
- 3番目のqubitを測定すると ある $R = cP$ が選ばれ $(1/\sqrt{|S_R|})\sum_{(a,b)\in S_R}|a,b\rangle|R\rangle$ になる
  （以降 $|R\rangle$ は固定なので省略）
- 1, 2番目のqubitに2次元版逆QFTを作用させる
  - $|a,b\rangle \mapsto (1/n)\sum_{j,k}\exp(-2\pi i(aj+bk)/n)|j,k\rangle$
  - 結果: $(1/(n\sqrt{|S_R|}))\sum_{j,k}(\sum_{(a,b)\in S_R}\exp(-2\pi i(aj+bk)/n))|j,k\rangle$
  - この状態を観測する

確率の大きいところ

$|j, k\rangle$ が観測される確率

- 全体の係数を無視すると、$v_{j,k} := \sum_{(a,b)\in S_R} \exp(-2\pi i(aj+bk)/n)$ の絶対値の2乗
- $(a,b) \in S_R$ ならば$aP + b(xP) = cP$ より $a \equiv c - bx \pmod{n}$
- $aj + bk \equiv (c-bx)j + bk = cj + b(k-xj) \pmod{n}$
- $k - xj \equiv 0 \pmod{n}$ ならば $v_{j,k} = \sum_b \exp(-2\pi icj/n) = n\exp(-2\pi icj/n)$
  - 位相が揃って確率が最大化. それ以外は打ち消しあって小さくなる
  - つまり $k \equiv xj \pmod{n}$ となる k, j が選ばれる確率が高い
  - x が求まらなければリトライ
- 全体で $O((\log p)^3)$ で解けることが知られている
- ビット数が少ない分, 原理的に素因数分解よりも効率よく求められる

素因数分解の評価

理論的には

- Beauregard (2003)の見積もりで n bitの数の素因数分解に $2n+3$ bit必要

実際に必要なqubitの見積もり

- Gidney and Ekerå (2019) : 2048 bit RSAを解くにはエラー率0.1% 2000万 qubit, 8時間
- Gidney (2025)（未査読）: 2048 bit RSAを解くにはエラー率0.1% 100万 qubit, 1週間

実際に解読できたパターン

- 2001 IBM : 15 = 3x5
- 2012 Josephson phase qubi : 21 = 3x7
- 2019 IBM : 35を素因数分解しようとしたが失敗
- (DLP) 2020 NICT : $2^x \equiv 1 \pmod 2$ は解けたが $4^x \equiv 2 \pmod 7$ は失敗
- ただし解けた素因数分解は素因数の情報を使ってる（CRYPTREC : それはありなのか）
- もっと大きい素因数分解に成功したものもあるがそれも全数探索 or 素数の性質を使ってる

共通鍵暗号への影響

量子オラクル

- 量子重ね合わせを受け付ける暗号処理のブラックボックス

攻撃モデル

- Q1: 攻撃者は古典オラクルのみを使う（公開鍵暗号は事実上こちらのモデルのみ）
- Q2: 攻撃者は量子オラクルを使う
  - 共通鍵暗号はこちらのモデルを使うこともある（実際に攻撃できないことが多い）

共通鍵暗号の素朴な安全性評価

- 共通鍵暗号の鍵空間が 2^n なら古典では $O(2^n)$
- Groberのアルゴリズムを使う（Q2）と、$O(2^{n/2})$ で解読
- ハッシュ関数の衝突（$h(x) = h(x')$ となる $x \neq x'$）を求める問題
  - 古典 $O(2^{n/2})$ で解ける
  - Q2 : $O(2^{n/3})$ で解ける, ただしメモリは $O(2^{n/3})$: 現実的でない → 当面大丈夫

量子暗号

量子鍵配送 QKD (Quantum Key Distribution)

- 秘密鍵を共有する技術: 暗号化方式ではない
- 観測の不可逆性（観測すると状態が変わる）や量子もつれやを利用して盗聴を検出する
  - 盗聴されていれば鍵を破棄してやり直す
- 代表的なプロトコル: BB84（実用化済み）, E91

通信距離と速度

- 光ファイバー中の減衰や雑音の影響により50~150km, 10Mbps程度が実用的な限界
  - 中継地点で一度古典的に復号して再送する（中継地点が盗聴される可能性はある）
    - 中国では北京〜上海間2000kmのネットワーク
    - 人工衛星を信頼ノードとして利用し、地上局と鍵交換
- Twin-Field QKDで1000km達成 (2023)
  - 両端からパルスを発生させて中間地点で干渉させる手法