4. 量子アルゴリズム：グローバー探索と応用

2025/07/16

Ryota MAEDA
IJDS

自己紹介

- 名前：前田　良太（まえだ　りょうた）
- 経歴：大学院の修士課程まで数学（整数論）を専攻
- 所属：IJDS（日本IBMグループ）のSE

講義4. 量子アルゴリズム：
グローバー探索と応用

アジェンダ

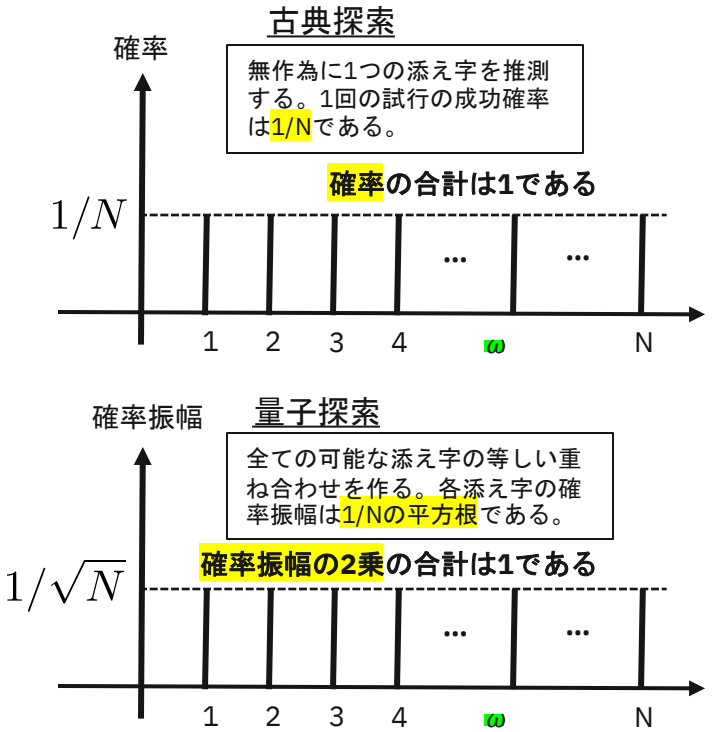
- 04-06：導入
- 07-13：グローバー探索
- 14-21：グローバー探索の量子回路

導入

- グローバー探索はLov K. Groverにより1996年に考案された、量子探索アルゴリズムの1つである。
  - 整理されていないデータベースの探索がしばしば例として使われる。
  - さらに、探索アルゴリズムを用いる多くの古典アルゴリズムを高速化するためにも使われる。
- 探索問題：ある1つのリストLからωを見つける。
  - Lは大きさNのリストで、ωは答えまたは「良い」添え字と呼ばれる。
- リストLからどうやってωを見つけ出すのか？
  - 古典計算においては、答えが見つかるまでLの各要素を確認する。
    - 最悪の場合、$O(N)$の計算量が必要となる。
  - 量子計算においては、グローバー探索を用いる！
    - $O(\sqrt{N})$の計算量が必要となる。
- 2次の高速化であって、指数関数的な高速化ではない。

古典的および量子的な探索アルゴリズム

- 探索問題
  - N個の添え字の中から、1つの良い添え字ωを見つける。
  - 各添え字が「良い」か否かを答えられるブラックボックスが与えられているとする。このブラックボックスはしばしば「オラクル」と呼ばれる。
- 古典探索アルゴリズム
  - 無作為に1～Nの中から1つの添え字を選ぶ。その添え字についてオラクルに尋ねる。
  - 成功確率は$1/N$である。
- 量子探索アルゴリズム
  - 全ての添え字の重ね合わせについて量子オラクルに尋ねる。
  - 量子オラクルへの問い合わせを使うことで、依然として成功確率は$1/N$であるが、測定前の確率振幅は$1/\sqrt{N}$である。



確率と確率振幅

- 古典アルゴリズムの成功確率
  - 1回の試行の成功確率が$1/N$のとき、k回の試行の成功確率は約k/Nである。
  - 最大でNと同程度のオーダーまで繰り返す必要がある。
- 量子アルゴリズムの確率振幅
  - 全ての可能な添え字の量子重ね合わせを作る。

$$\frac{1}{\sqrt{N}}|0\rangle + \frac{1}{\sqrt{N}}|1\rangle + \cdots + \frac{1}{\sqrt{N}}|\omega\rangle + \cdots + \frac{1}{\sqrt{N}}|N-1\rangle$$

オラクルに良い/悪い添え字をマークするように問い合わせて、結果を2番目のレジスタに保存する

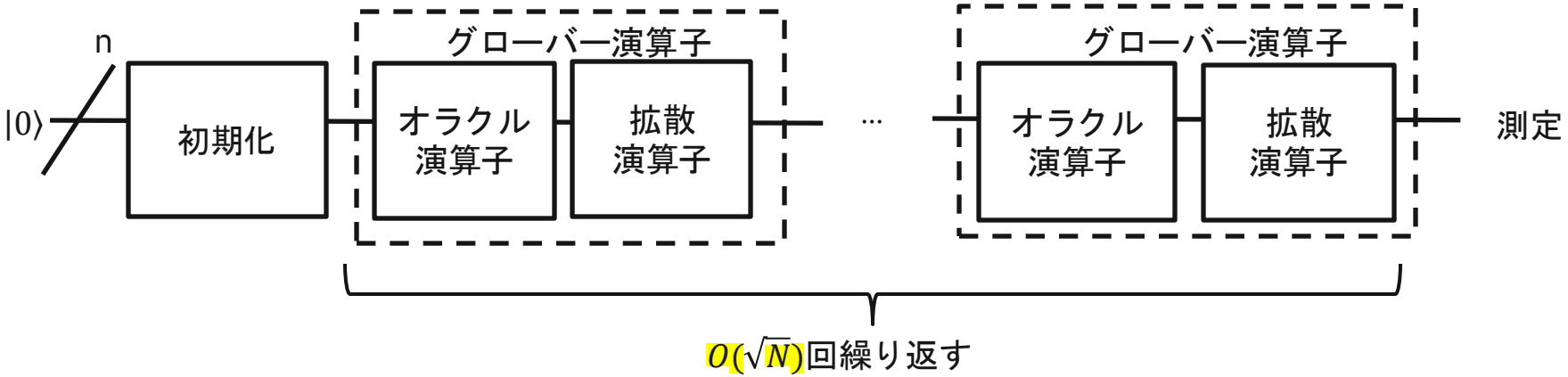
$$\frac{1}{\sqrt{N}}|0\rangle|bad\rangle + \frac{1}{\sqrt{N}}|1\rangle|bad\rangle + \cdots \frac{1}{\sqrt{N}}|\omega\rangle|good\rangle + \cdots + \frac{1}{\sqrt{N}}|N-1\rangle|bad\rangle$$

  - もしその直後に測定した場合、結果は古典アルゴリズムと同様になる。
  - しかし、もし確率振幅を加えたり集めたりすることができる場合、2次の速さで良い状態を増幅することができる。
  - k回の繰り返しによって確率振幅は$k/\sqrt{N}$となり、成功確率はk^2/Nとなる。
  - 最大で$\sqrt{N}$と同程度のオーダーまでしか繰り返す必要がない。

グローバー探索

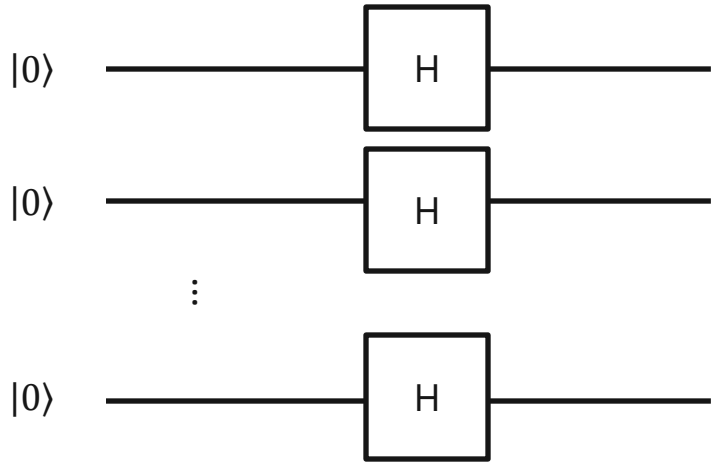
概要

- グローバー探索は3つの部分から成る。
  1. 初期化
  2. オラクル演算子を適用する
  3. 拡散演算子を適用する
- 初期化後に、上記の2と3を$O(\sqrt{N})$回繰り返す。



初期化

- 全ての可能な状態である$|00\ldots0\rangle, \ldots, |11\ldots1\rangle$が同じ振幅となっている重ね合わせを作る。
- アダマールゲートHを各量子ビットに適用する。



- 状態が$|00\ldots0\rangle$から$|s\rangle = \sum_{x\in\{0,1\}^n}^{n} \frac{1}{\sqrt{2^n}} |x\rangle$に変化する。

オラクル演算子

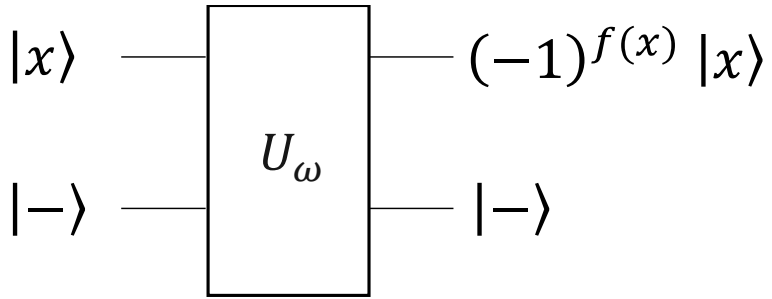
- オラクル演算子においてオラクルを使う。
- オラクルとは：ブラックボックス関数fを以下で定める。

$$f(x) = 1 \ (x = \omega),$$
$$f(x) = 0 \ (x \neq \omega).$$

- オラクル演算子とは：ブラックボックス演算子U_ωを以下で定める。

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle.$$

- 位相キックバックを使うことにより、$x = \omega$のときオラクル演算子は$|x\rangle$の位相を変化させる。



- しかし、答えωを知らない状態で、オラクル演算子をどうやって作るのか？

拡散演算子

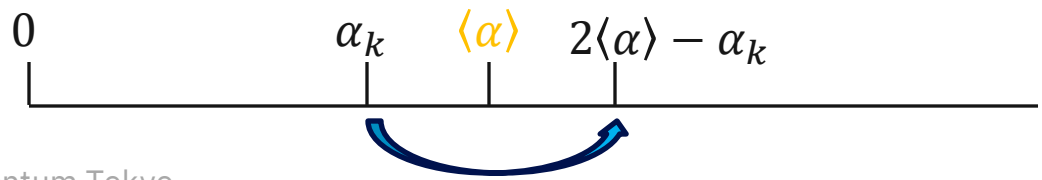
- 拡散演算子：$U_s = 2|s\rangle\langle s| - I.$
- これは平均に関する転倒を行う演算子である。
  - どういうことか？

$$(2|s\rangle\langle s| - I)\sum_k \alpha_k |k\rangle$$

$$= 2N^{-1}\sum_{i,j,k} \alpha_k |i\rangle\langle j|k\rangle - \sum_k \alpha_k |k\rangle$$

$$= 2N^{-1}\sum_{i,k} \alpha_k |i\rangle - \sum_k \alpha_k |k\rangle$$

$$= \sum_k (2\langle\alpha\rangle - \alpha_k)|k\rangle$$



n 量子ビットが与えられたとして、$N = 2^n$とおく。

$$|s\rangle = N^{-1/2}\sum_{i\in\{0,1\}^n}^{n} |i\rangle.$$

$$\langle s| = N^{-1/2}\sum_{j\in\{0,1\}^n}^{n} \langle j|.$$

$$\langle j|i\rangle = \delta_{ij}.$$

$$\langle\alpha\rangle = N^{-1}\sum_k \alpha_k.$$

2量子ビットグローバー探索の例

- $\omega = 2$とする。
- 初期化：全ての可能な状態が同じ振幅となっている重ね合わせを得る。

$$s = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|\omega\rangle + \frac{1}{2}|11\rangle.$$

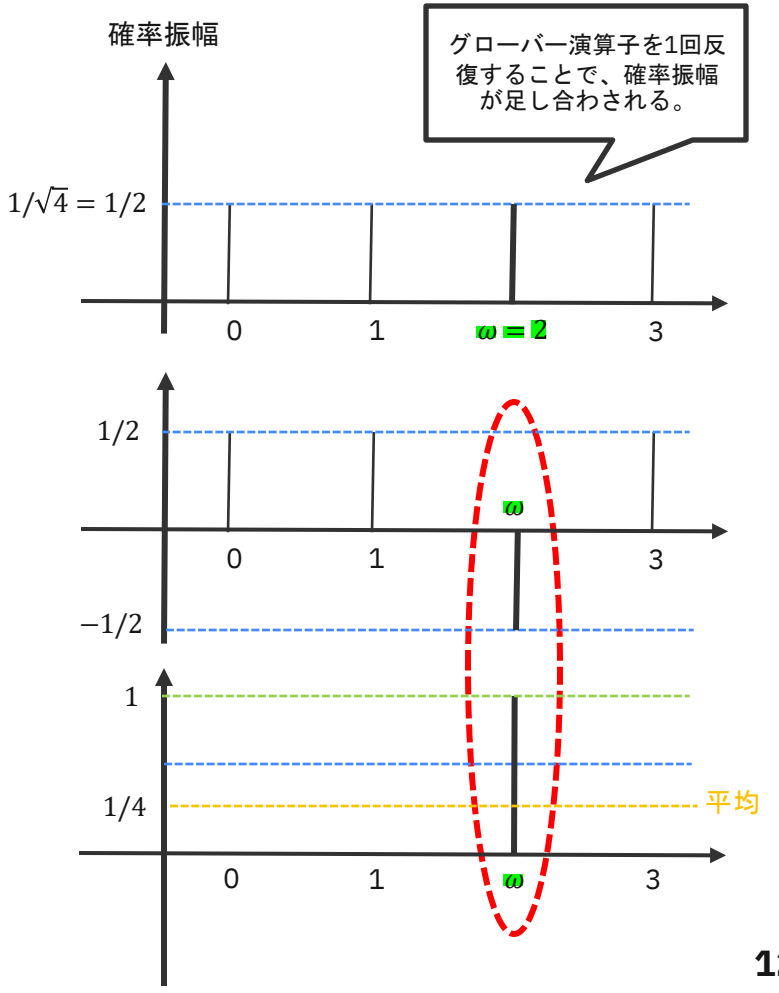
- オラクル演算子U_ωを適用する：ωの位相を変化させる。

$$U_\omega|s\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|\omega\rangle + \frac{1}{2}|11\rangle.$$

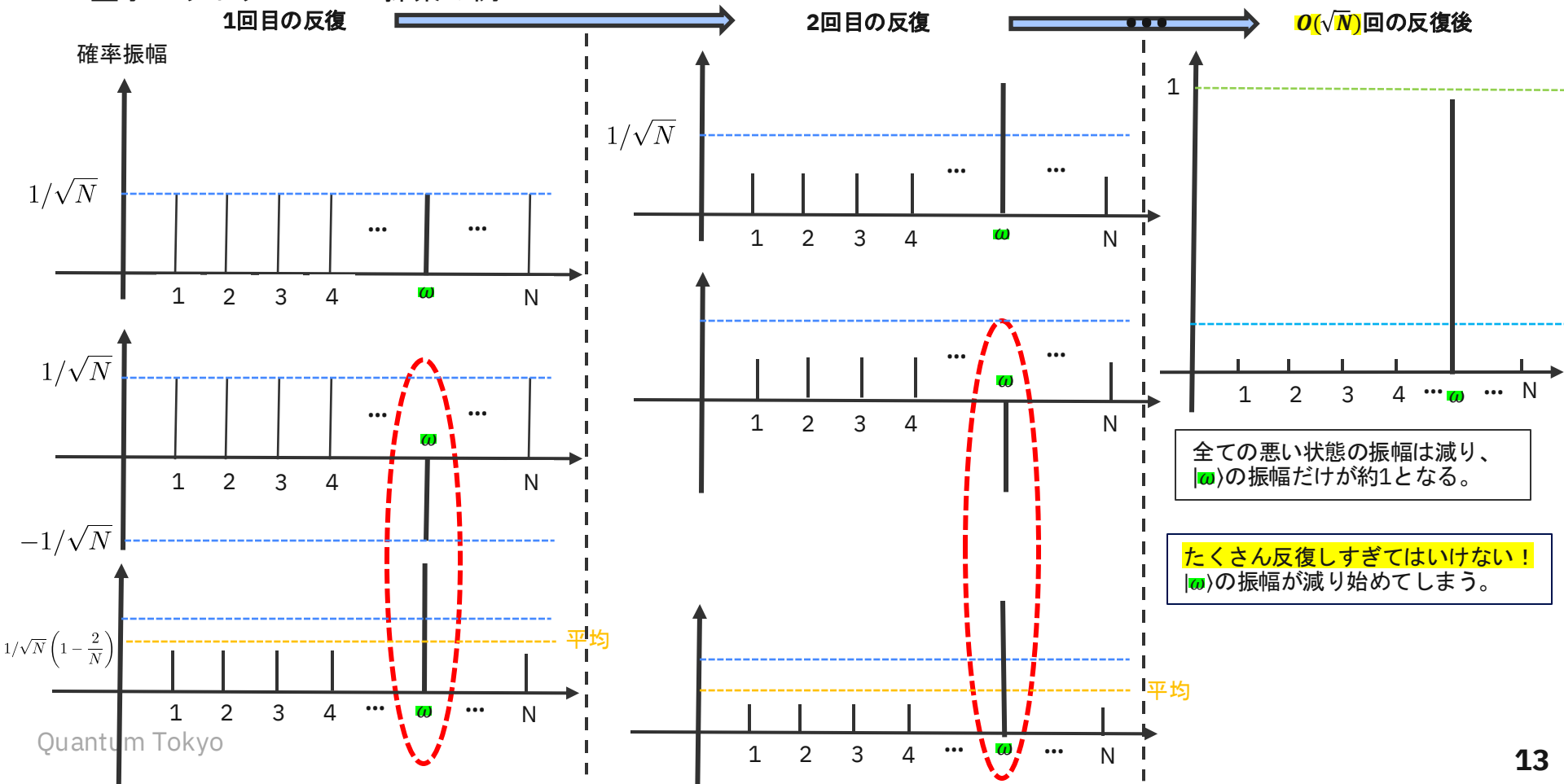
- 拡散演算子U_sを適用する：平均に関して転倒させる。

$$U_s U_\omega|s\rangle = 0|00\rangle + 0|01\rangle + 1|\omega\rangle + 0|11\rangle.$$

2量子ビットのグローバー探索では、たった1度の反復だけが必要となる。



n量子ビットグローバー探索の例

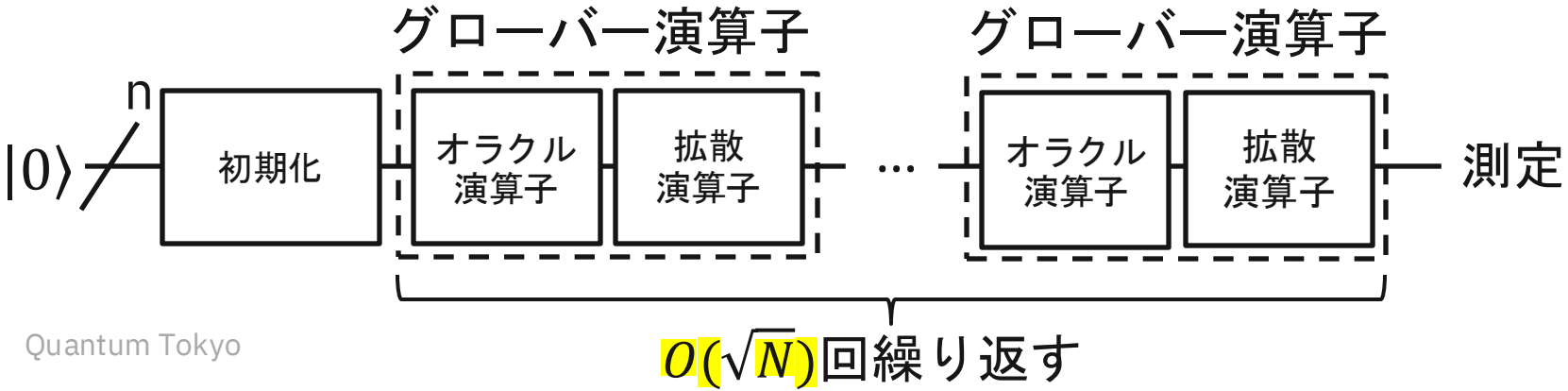


グローバー探索の量子回路

グローバー探索の量子回路をどうやって作るのか？

- 初期化：各量子ビットにアダマールゲートHを適用する。（易しい。）
- 拡散演算子：$U_s = 2|s\rangle\langle s| - I$を作る。（できそう。）
- オラクル演算子：$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle$を作る。

★これはどうやって行うのか？
これを作れるということは、答えを知っているということにならないか？
→そうではない！
答えを知っていることと答えを判定できることには、明確な差異がある。



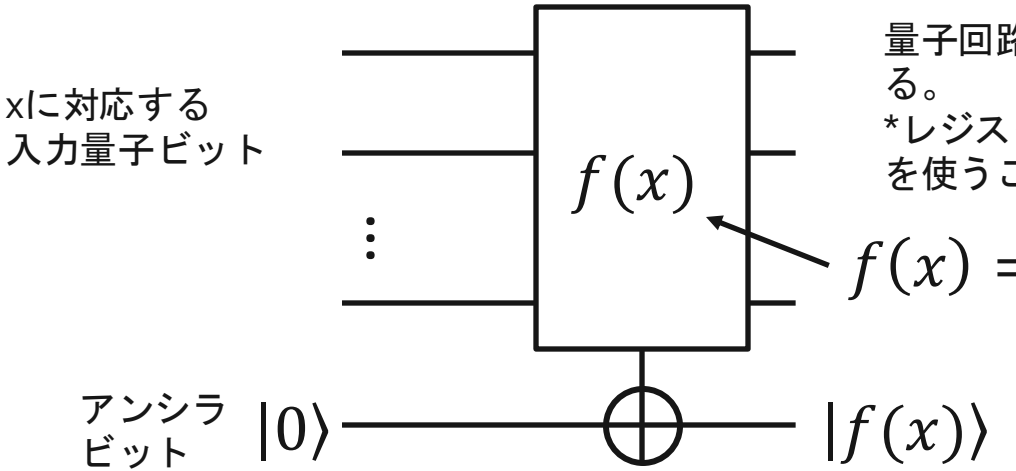
オラクルをどうやって作るのか？

- オラクルは次のようなブラックボックス関数fである。

  $f(x) = 1\ (x = \omega)$,

  $f(x) = 0\ (x \neq \omega)$.

- これをどうやって作るのか？
  - 量子回路にfを実装しさえすればよい！



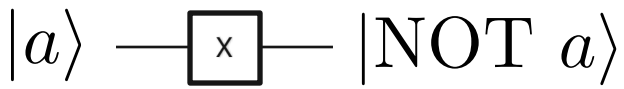
量子回路に、いかなる論理関数fも実装することができる。
*レジスタとして追加の量子ビット（アンシラビット）を使うこともある。

$$f(x) = (x_1 \vee \overline{x_2} \vee x_2) \wedge \ldots$$

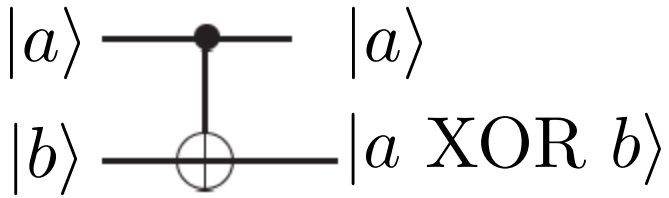
可逆論理ゲート

- 0か1の値をとるaとb(バイナリ)に対し、可逆的な量子回路によって次の演算を計算することができる。

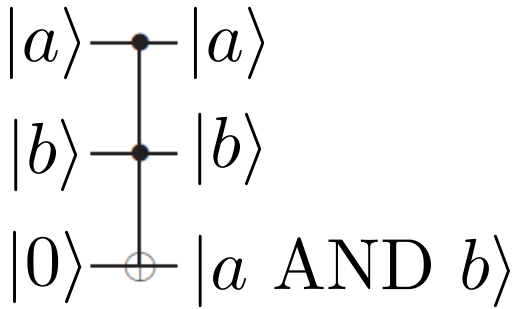
NOTゲート（Xゲート）



XORゲート（CNOTゲート）



ANDゲート（CCNOTゲート）

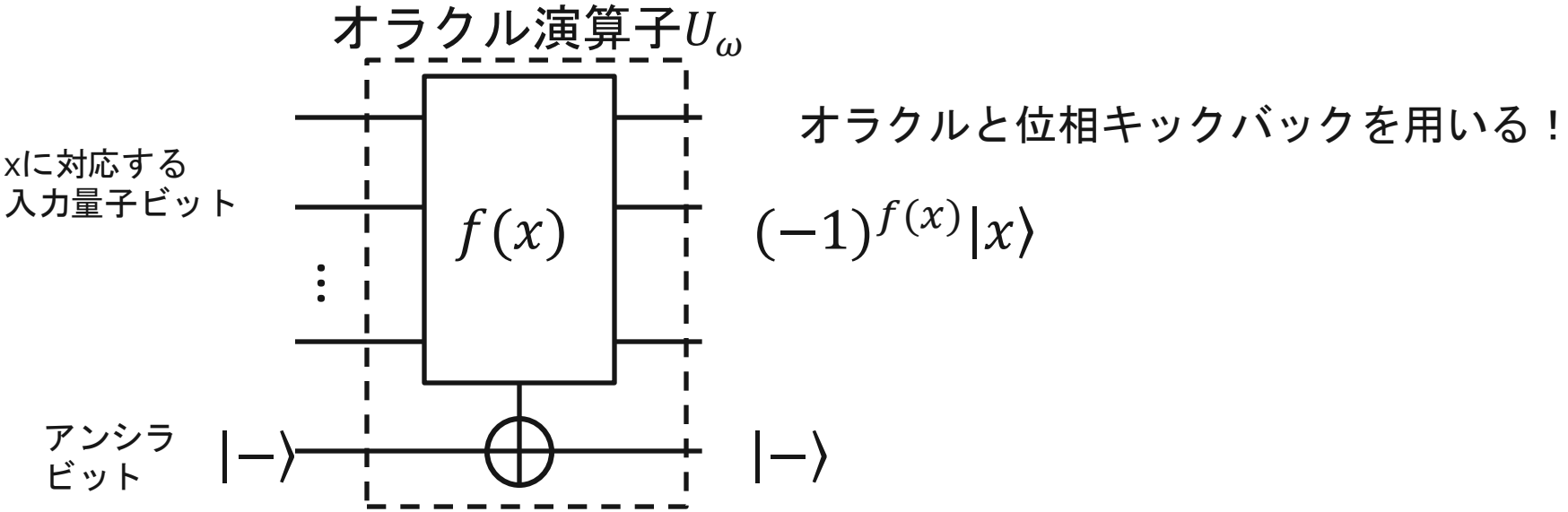


オラクル演算子の作り方

- オラクル演算子：ブラックボックス演算子U_ωを以下で定める。

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle.$$

位相キックバックを使うことにより、$x = \omega$のときオラクル演算子は$|x\rangle$の位相を変化させる。

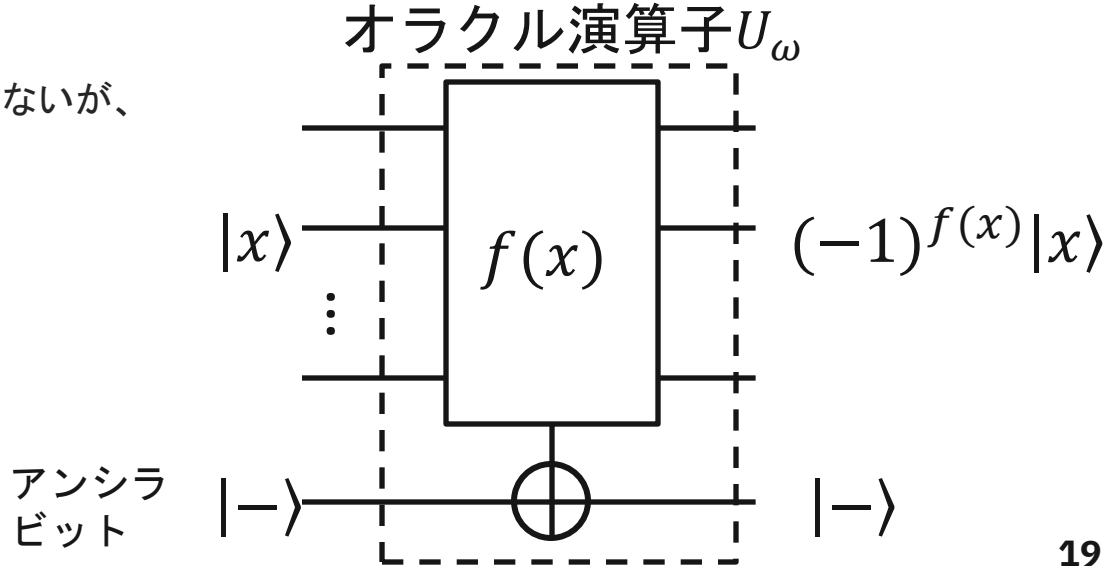


位相キックバック

|−⟩はXゲートを表す行列の固有ベクトルの1つで、固有値として−1を持つものである。

- $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$.
- Xゲートを表す行列は$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$である。
- $X|-\rangle = -1 * |-\rangle$.

|−⟩にXゲートを適用すると、状態は変わらないが、
位相が−1倍される。



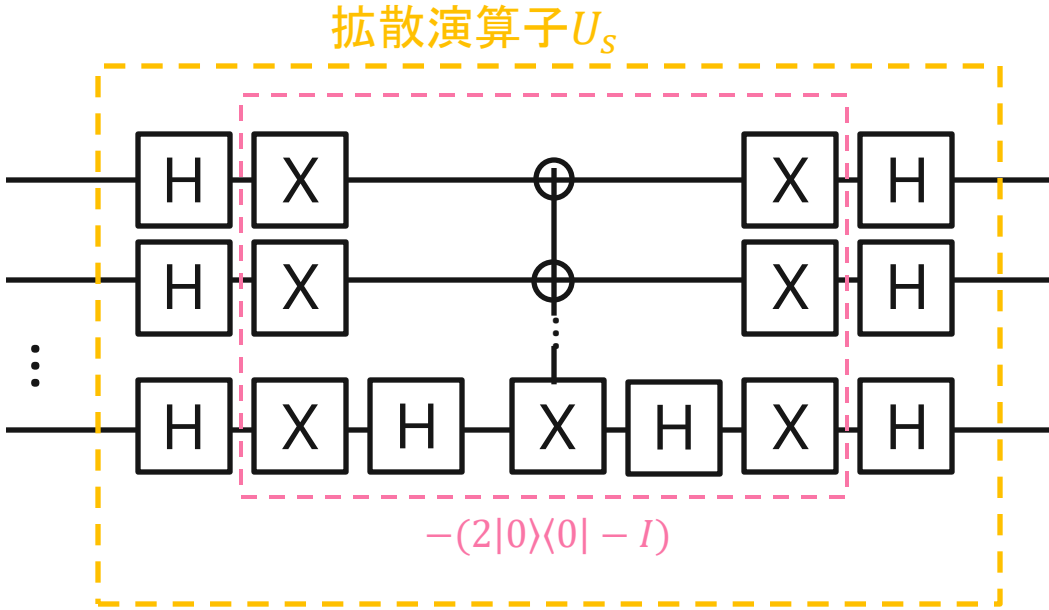
拡散演算子はどうやって作るのか？

- 拡散演算子：$U_s = 2|s\rangle\langle s| - I$.
- $2|s\rangle\langle s| - I = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}$.
- Hは$HH = I$を満たす。
- 次の作用素を考える。

$$-(2|0\rangle\langle 0| - I) = \begin{bmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

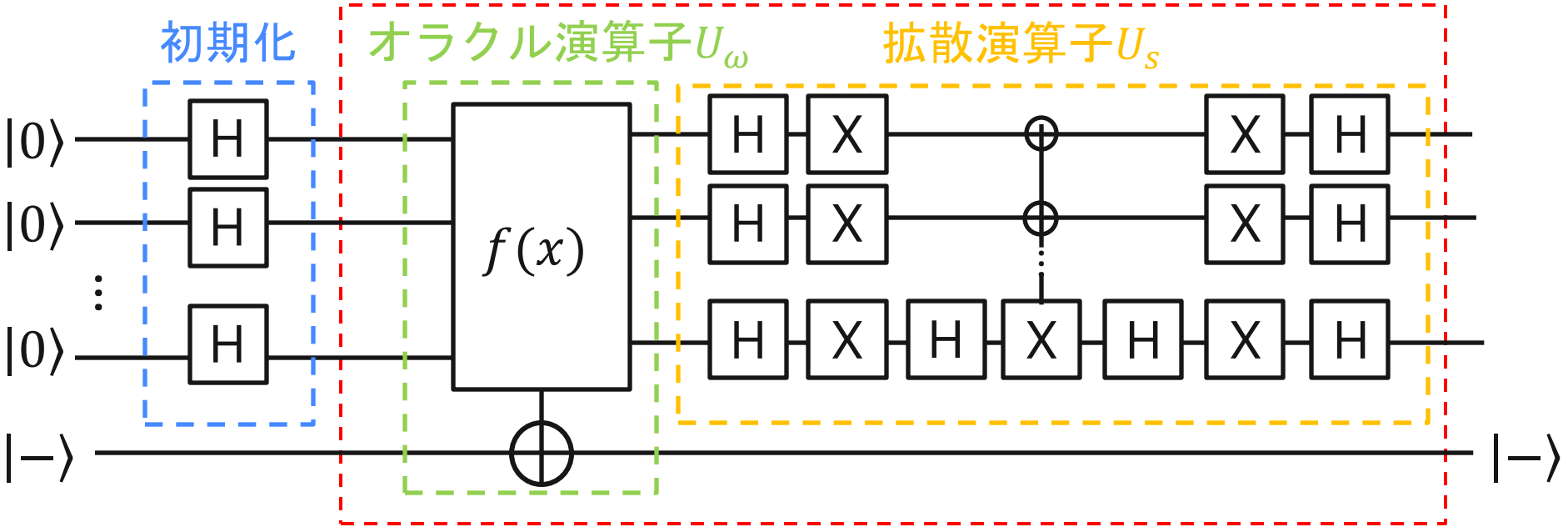
これはグローバル位相に関して、
$(2|0\rangle\langle 0| - I)$と等しい。

$$|s\rangle = N^{-1/2} \sum_{x\in\{0,1\}^n}^{n} |x\rangle$$



グローバー探索の量子回路

これらの回路を組み合わせることにより、次の量子回路を得る。



EoF