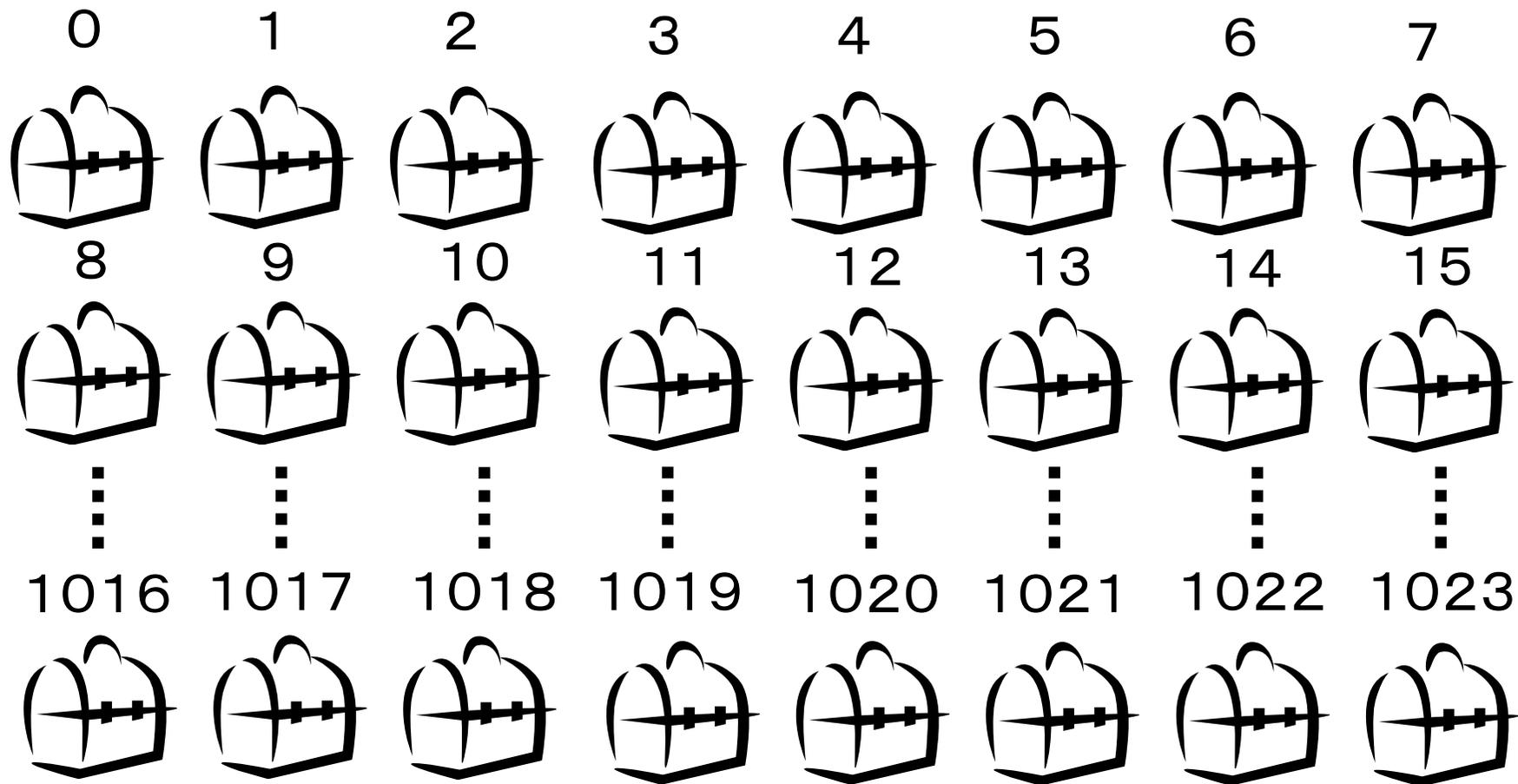


量子アルゴリズム

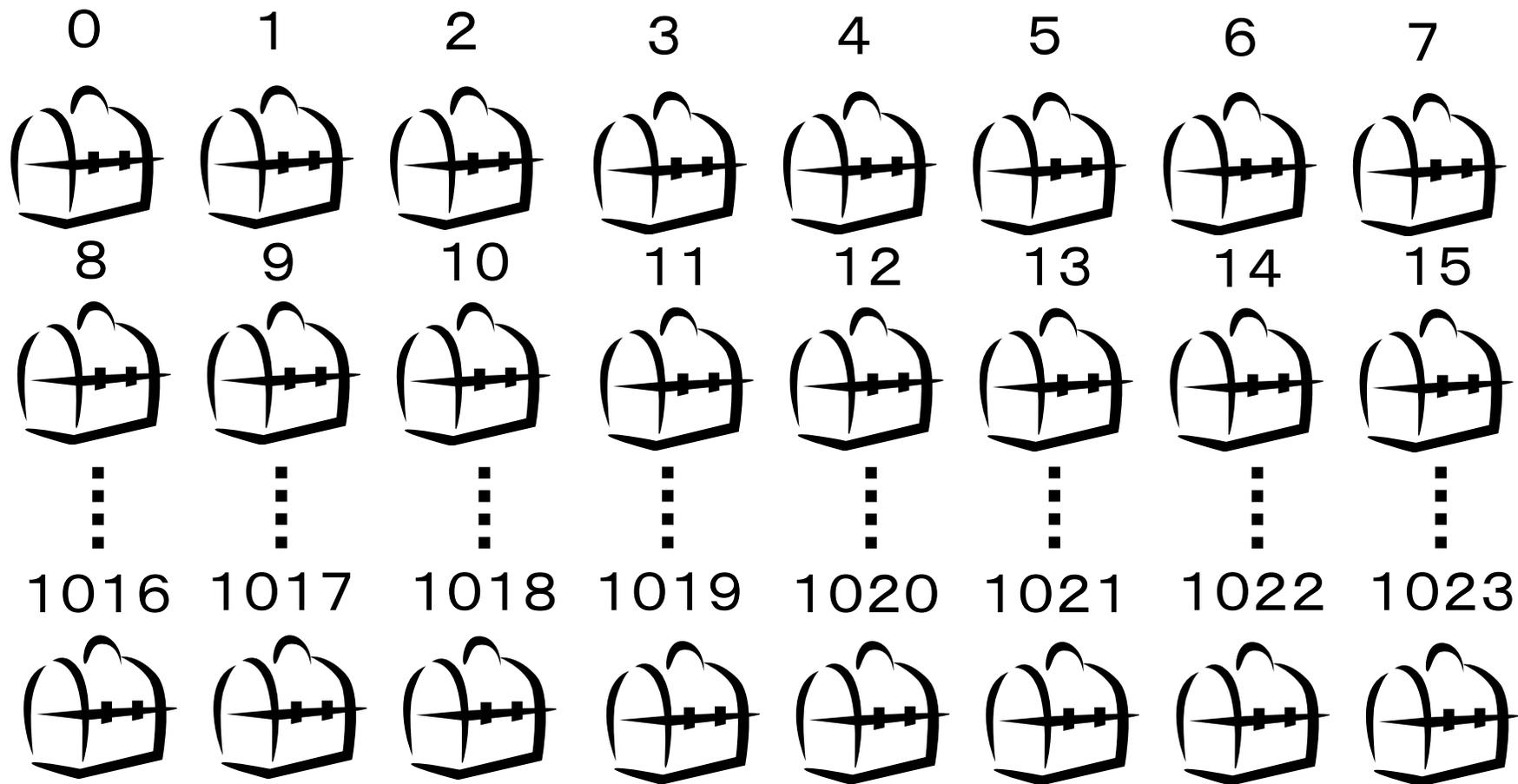
東京工業大学

河内 亮周

量子計算で高速検索！
～Groverのアルゴリズム～



アタリは一つだけ・・・どうやって探す??



片っ端から：最悪1024回開けるハメに！

一様ランダムに：512回で確率40%程度・・・

Groverのアルゴリズム：25回で確率99.9%以上！！

Grover のアルゴリズム

(Grover, 1996)

- 入力: 論理関数 $f : \{0,1\}^n \rightarrow \{0,1\}$
(但し $f(x_0)=1$ となる $x_0 \in \{0,1\}^n$ は唯一)
- 出力: n ビット列 $x_0 \in \{0,1\}^n$ s.t. $f(x_0) = 1$

Grover のアルゴリズムは

$$f \text{ の計算回数} = \lfloor \pi/4 \rfloor \sqrt{2^n} = O\left(\sqrt{2^n}\right)$$

$$\text{成功確率} \geq 1 - 2^{-n}$$

で上の問題を解くことが可能!

アルゴリズムの設計方針

- 答えの候補は $00\cdots 0 \sim 11\cdots 1$ の $N := 2^n$ 個
 - $|00\cdots 0\rangle$ から中立的な状態 $|\phi_0\rangle$ を生成

$$|\phi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

- この時点で測定した場合の成功確率

$$|\langle x_0 | \phi_0 \rangle|^2 = \left| \langle x_0 | \left(\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle \right) \right|^2 = \frac{1}{N}$$

…一様ランダムに探すのと一緒

- 成功確率 $|\langle x_0 | \phi_0 \rangle|^2$ を大きくしたい！

アルゴリズムの流れ

1 一様な状態を生成: $|\phi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$

2 f から構成される変換 V_f でアタリの位相反転

$$|\phi_0\rangle \xrightarrow{V_f} |\phi'_0\rangle = \frac{1}{\sqrt{N}} \left(-|x_0\rangle + \sum_{x \neq x_0} |x\rangle \right)$$

3 あるユニタリ変換 D (拡散変換) を適用

$$|\phi'_0\rangle \xrightarrow{D} |\phi_1\rangle = \frac{1}{\sqrt{N}} \left(\alpha |x_0\rangle + \beta \sum_{x \neq x_0} |x\rangle \right) \quad (\alpha > 1)$$

4 2-3を $k_0 = \lfloor \pi/4 \rfloor \sqrt{N}$ 回繰り返して測定

$$|\phi_{k_0}\rangle = \underbrace{DV_f \cdots DV_f}_{k_0} |\phi_0\rangle$$

一様な状態生成

Hadamard変換: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$\begin{aligned} H^{\otimes n}|00\dots 0\rangle &= (H|0\rangle) \otimes \dots \otimes (H|0\rangle) \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^n}}(|0\dots 00\rangle + |0\dots 01\rangle + \dots + |1\dots 11\rangle) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \end{aligned}$$

論理関数 \rightarrow ユニタリ変換

- f を計算するユニタリ変換 U_f

$$U_f |x\rangle |z\rangle = |x\rangle |f(x) \oplus z\rangle$$
$$(x \in \{0,1\}^n, z \in \{0,1\})$$



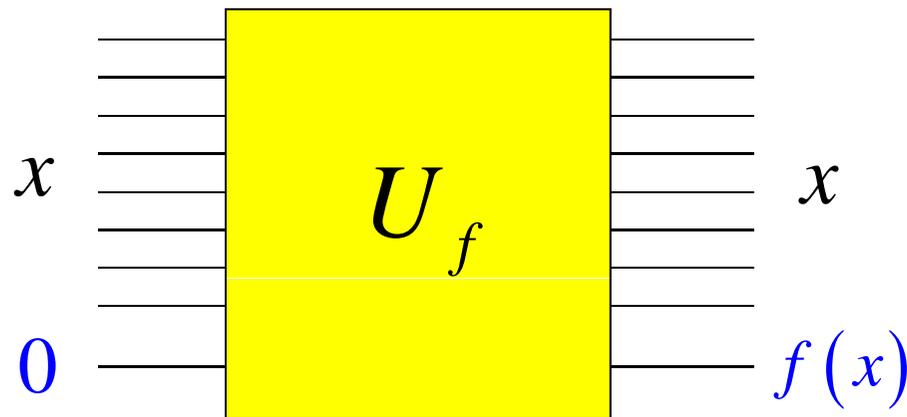
U_f を1回適用 = f を1回計算

z ——— $f(x) \oplus z$

論理関数 \rightarrow ユニタリ変換

- f を計算するユニタリ変換 U_f

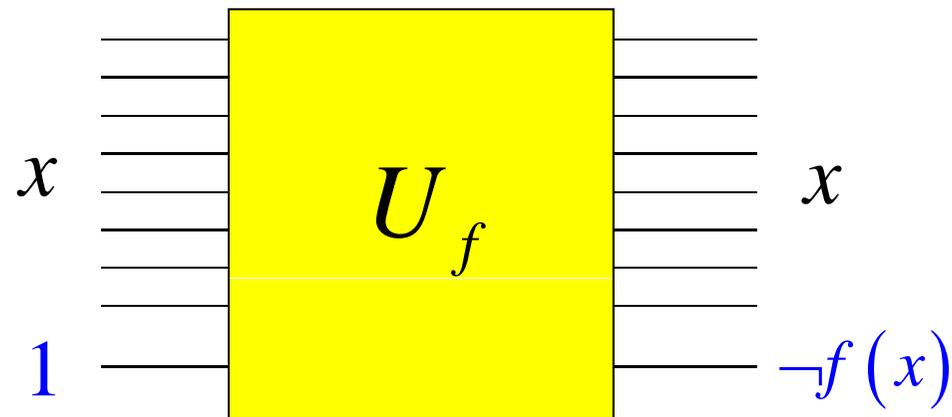
$$U_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$$



論理関数 \rightarrow ユニタリ変換

- f を計算するユニタリ変換 U_f

$$U_f |x\rangle |1\rangle = |x\rangle |\neg f(x)\rangle$$



U_f を使って V_f を構成

$$U_f |x\rangle |z\rangle = |x\rangle |f(x) \oplus z\rangle$$

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{U_f} \begin{cases} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & (f(x)=0 \text{ の場合}) \\ |x\rangle \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}} \right) = -|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & (f(x)=1 \text{ の場合}) \end{cases}$$

$H|1\rangle = \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$

第2レジスタは全く変化しない！（無視できる）

$$V_f |x\rangle = \begin{cases} |x\rangle & (f(x)=0 \text{ の場合}) \\ -|x\rangle & (f(x)=1 \text{ の場合}) \end{cases} \quad \text{が実現可能}$$

$$V_f = \left[\begin{array}{cc|c} 1 & & 0 \\ \hline & -1 & \\ \hline 0 & & 1 \end{array} \right] \langle x_0$$

The diagram shows a 3x3 matrix V_f enclosed in large square brackets. The matrix is partitioned into a central cross and four corner blocks. The top-left and bottom-right blocks are labeled '0'. The top-right and bottom-left blocks are also labeled '0'. The central cross, consisting of the middle row and middle column, is shaded light blue. The element at the center of this cross is '-1'. The four corners of the matrix (top-left, top-right, bottom-left, bottom-right) are labeled '1'. Dotted lines connect these '1's to the corners of the matrix, indicating they are part of the identity matrix structure. To the right of the matrix, the bra vector $\langle x_0$ is written. Below the matrix, a ket vector $|x_0\rangle$ is written, with a small wedge symbol pointing upwards from the ket to the center of the matrix's cross.

$$= I - 2|x_0\rangle\langle x_0|$$

一回目の繰り返しを計算してみよう

1 一様な状態を生成

$$|\phi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$$

一回目の繰り返しを計算してみよう

2 V_f でアタリの位相を反転

$$|\phi_0\rangle \xrightarrow{V_f} |\phi'_0\rangle = \frac{1}{\sqrt{N}} \left(-|x_0\rangle + \sum_{x \neq x_0} |x\rangle \right) = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 \\ \vdots \\ -1 \\ \vdots \\ 1 \end{bmatrix} \langle x_0$$

一回目の繰り返しを計算してみよう

3 拡散変換を適用

$$D|\phi_0'\rangle = \begin{pmatrix} -1 + \frac{2}{N} & & & & \frac{2}{N} \\ & -1 + \frac{2}{N} & & & \\ & & \dots & & \\ \frac{2}{N} & & & & -1 + \frac{2}{N} \end{pmatrix} \frac{1}{\sqrt{N}} \begin{bmatrix} 1 \\ \vdots \\ -1 \\ \vdots \\ 1 \end{bmatrix} \langle x_0$$

$$x_0 > \begin{bmatrix} -1 + \frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N} \\ \frac{2}{N} & \dots & -1 + \frac{2}{N} & \dots & \frac{2}{N} \end{bmatrix} \frac{1}{\sqrt{N}} \begin{bmatrix} 1 \\ \vdots \\ -1 \\ \vdots \\ 1 \end{bmatrix} < x_0$$

\wedge
 x_0

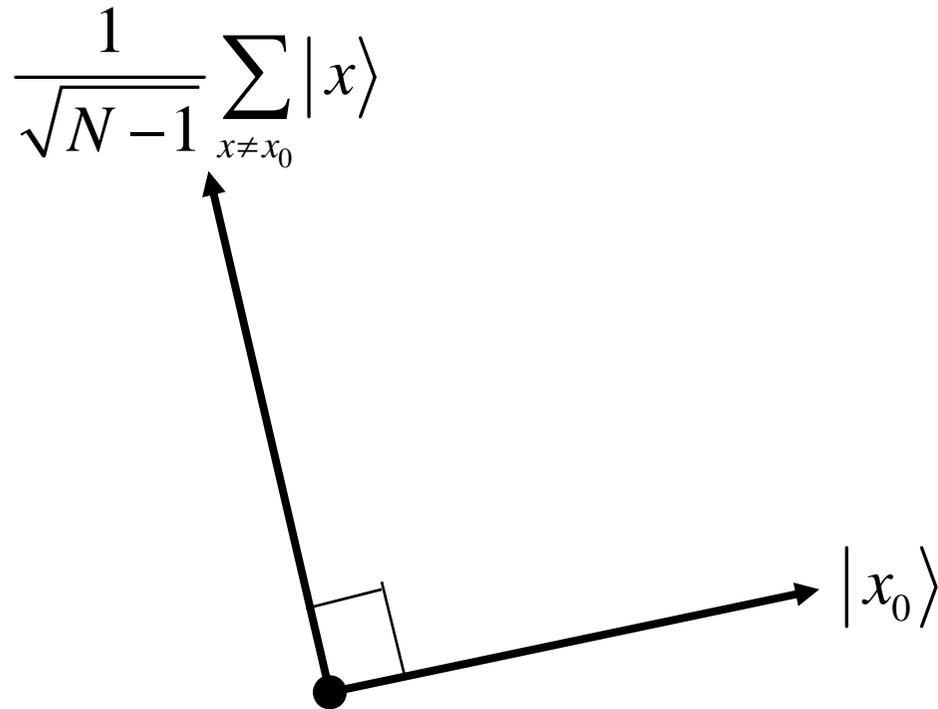
$$\begin{bmatrix} -1 + \frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N} \end{bmatrix} \times \begin{bmatrix} 1 \\ \vdots \\ -1 \\ \vdots \\ 1 \end{bmatrix} = \frac{1}{\sqrt{N}} \left(-1 + \frac{2}{N} + \overbrace{\frac{2}{N} + \dots + \frac{2}{N}}^{N-2} - \frac{2}{N} \right) = \frac{1}{\sqrt{N}} \left(1 - \frac{4}{N} \right)$$

$$\begin{bmatrix} \frac{2}{N} & \dots & -1 + \frac{2}{N} & \dots & \frac{2}{N} \end{bmatrix} \times \begin{bmatrix} 1 \\ \vdots \\ -1 \\ \vdots \\ 1 \end{bmatrix} = \frac{1}{\sqrt{N}} \left(\overbrace{\frac{2}{N} + \dots + \frac{2}{N}}^{N-1} + 1 - \frac{2}{N} \right) = \frac{1}{\sqrt{N}} \left(2 - \frac{4}{N} \right)$$

成功確率は $\frac{1}{N} \rightarrow \frac{4}{N} \left(1 - \frac{2}{N} \right)^2$ にUP!!

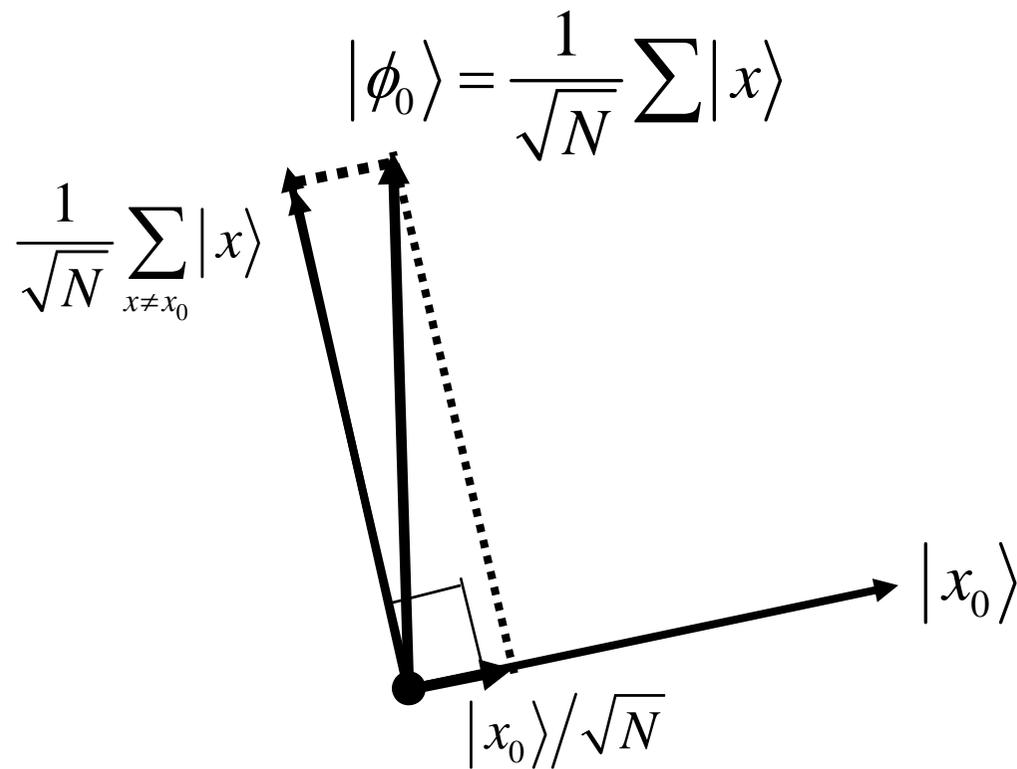
なぜ上手くいくの??

$\frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$ と $|x_0\rangle$ で張られる二次元空間



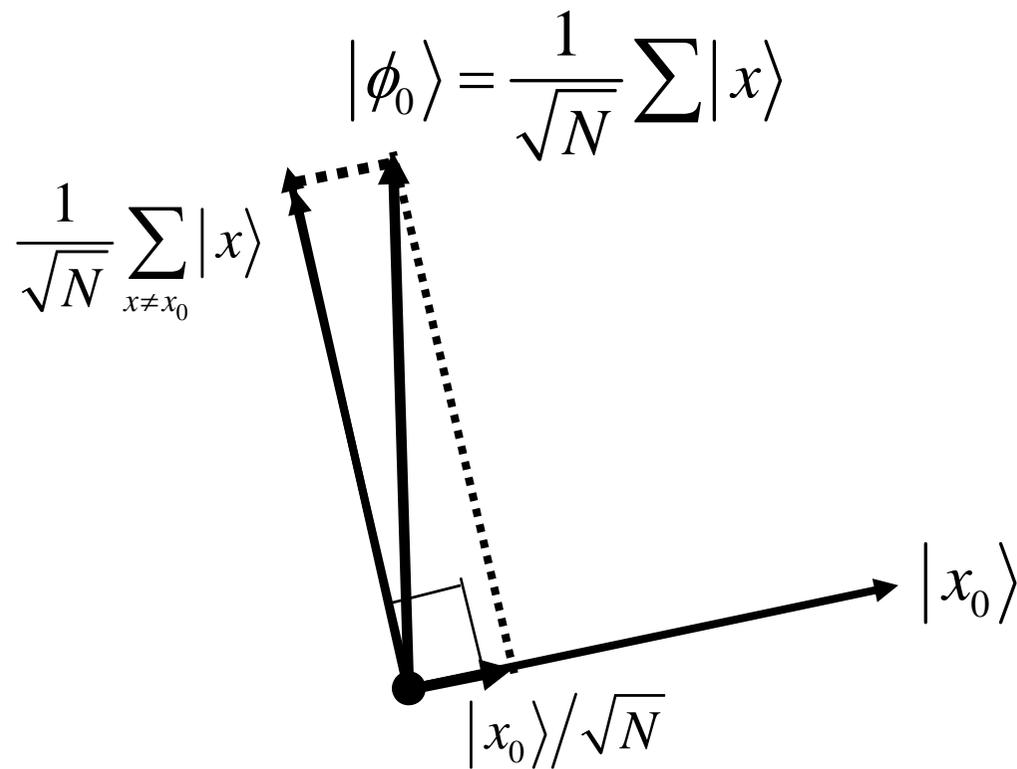
なぜ上手いくくの??

$\frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$ と $|x_0\rangle$ で張られる二次元空間



なぜ上手くいくの??

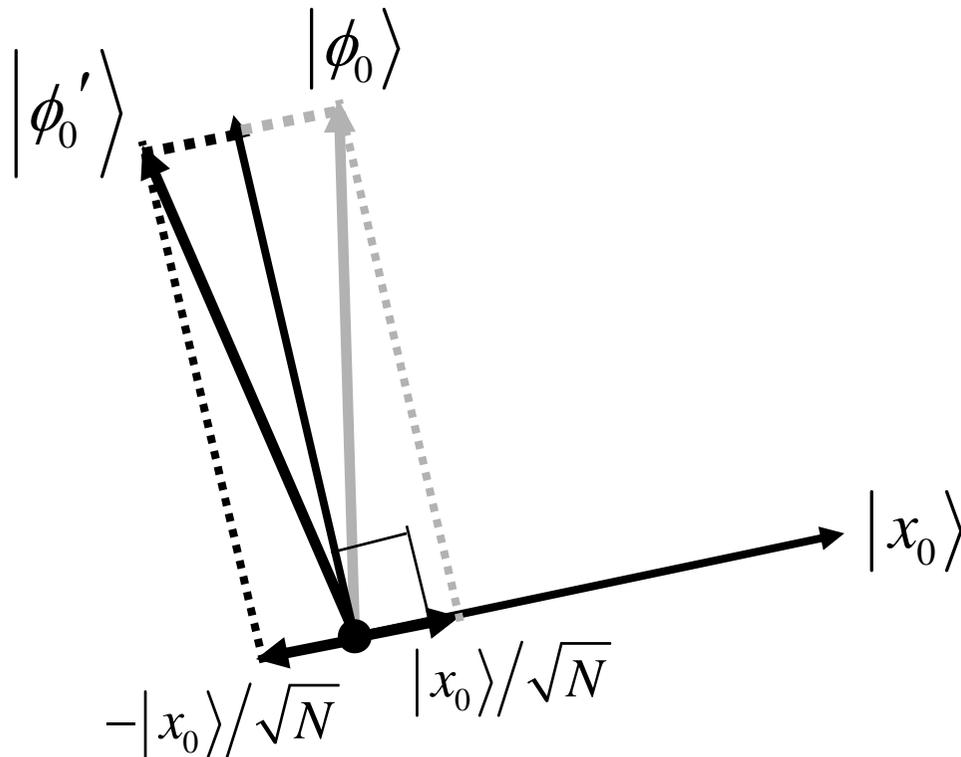
$$V_f = I - 2|x_0\rangle\langle x_0| \text{ の適用}$$



なぜ上手くいくの??

$V_f = I - 2|x_0\rangle\langle x_0|$ の適用

$$|\phi'_0\rangle = V_f |\phi_0\rangle = \frac{1}{\sqrt{N}} \left(-|x_0\rangle + \sum_{x \neq x_0} |x\rangle \right)$$

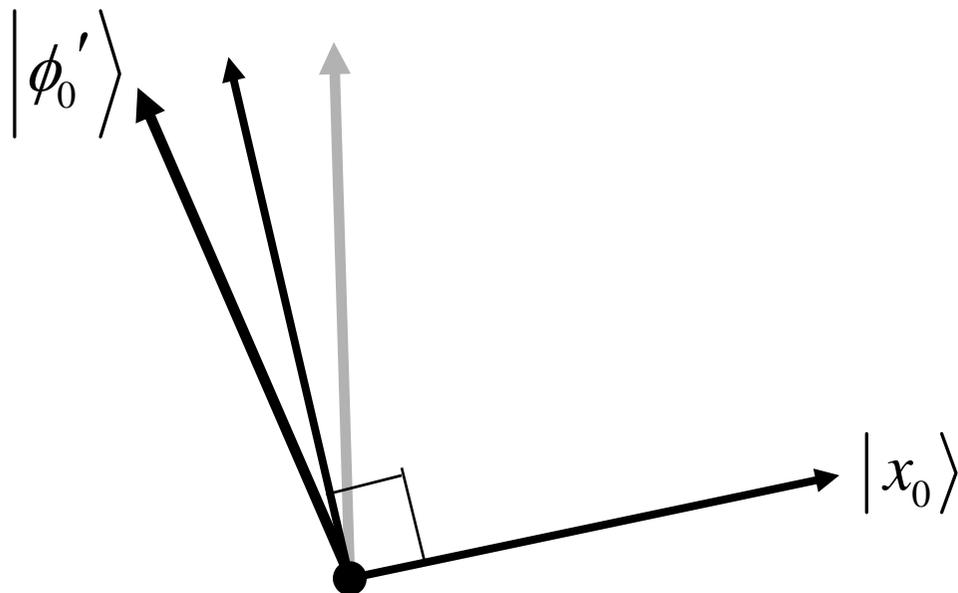


なぜ上手くいくの??

拡散行列

$$D = -I + 2H^{\otimes n} |0\dots 0\rangle\langle 0\dots 0| H^{\otimes n} = -I + 2|\phi_0\rangle\langle\phi_0|$$

の適用



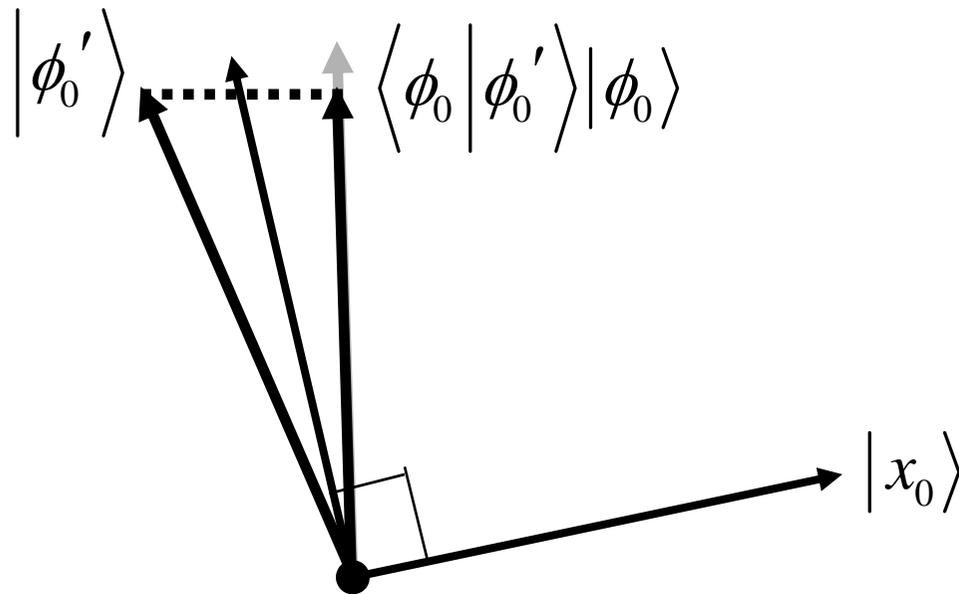
なぜ上手くいくの??

拡散行列

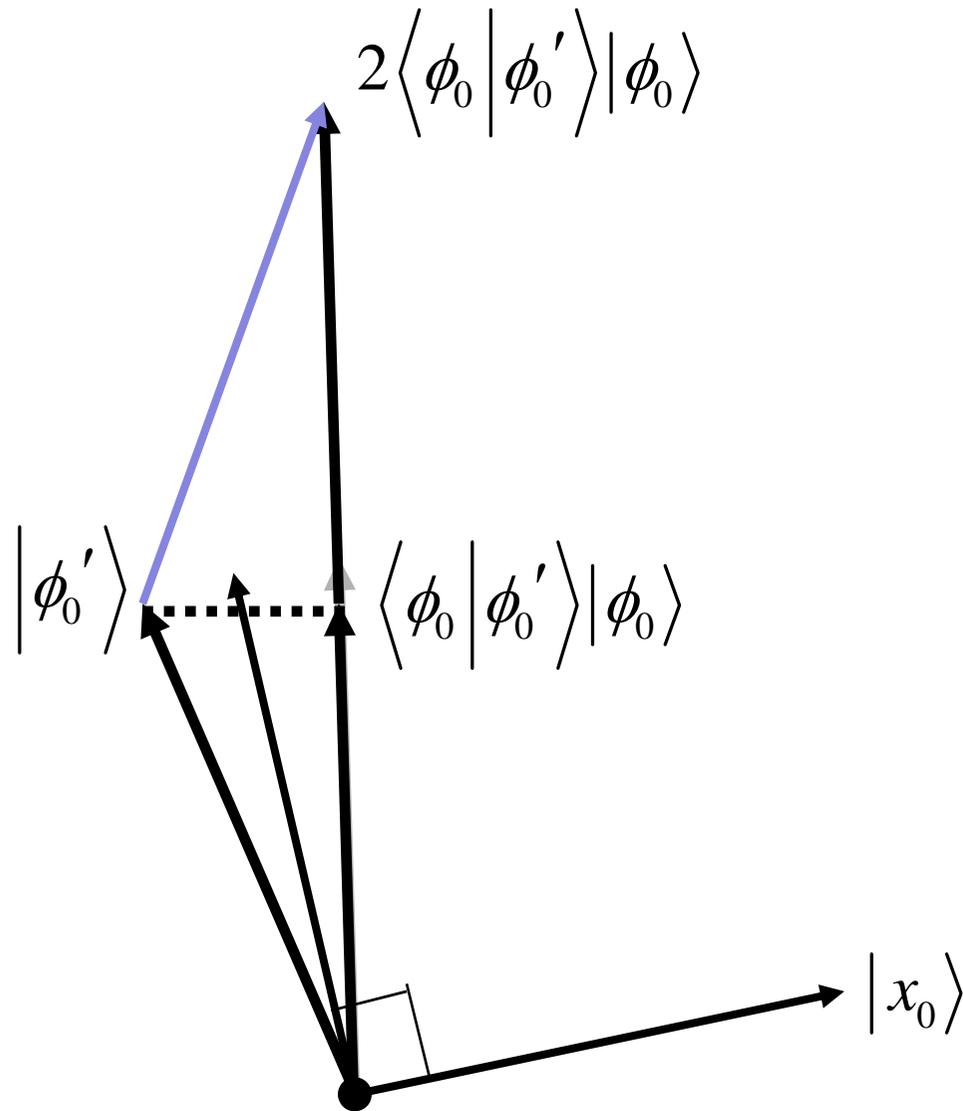
$$D = -I + 2H^{\otimes n} |0\dots 0\rangle\langle 0\dots 0| H^{\otimes n} = -I + 2|\phi_0\rangle\langle\phi_0|$$

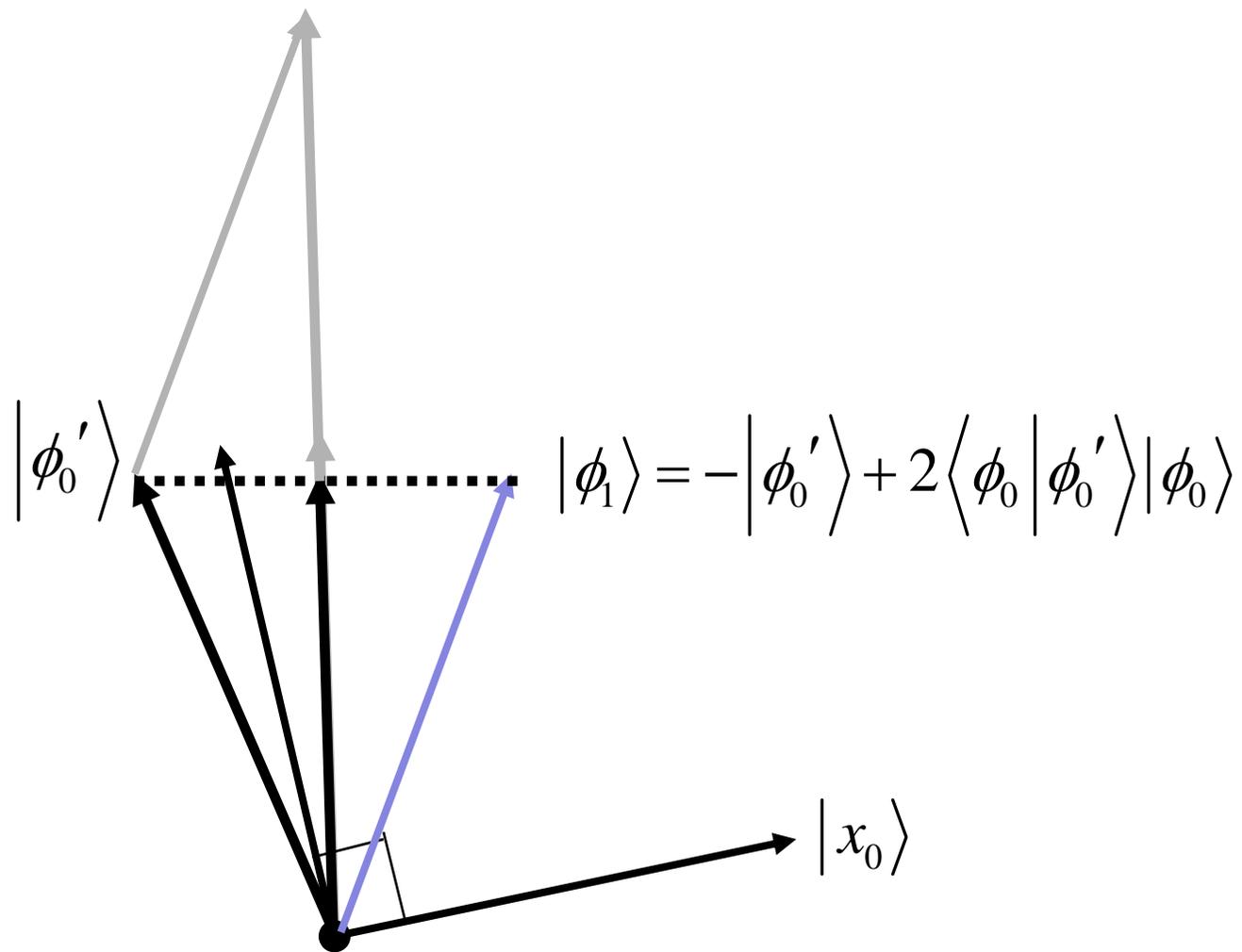
の適用

$$(-I + 2|\phi_0\rangle\langle\phi_0|)|\phi'_0\rangle = -|\phi'_0\rangle + 2\langle\phi_0|\phi'_0\rangle|\phi_0\rangle$$



$$(-I + 2|\phi_0\rangle\langle\phi_0|)|\phi'_0\rangle = -|\phi'_0\rangle + 2\langle\phi_0|\phi'_0\rangle|\phi_0\rangle$$

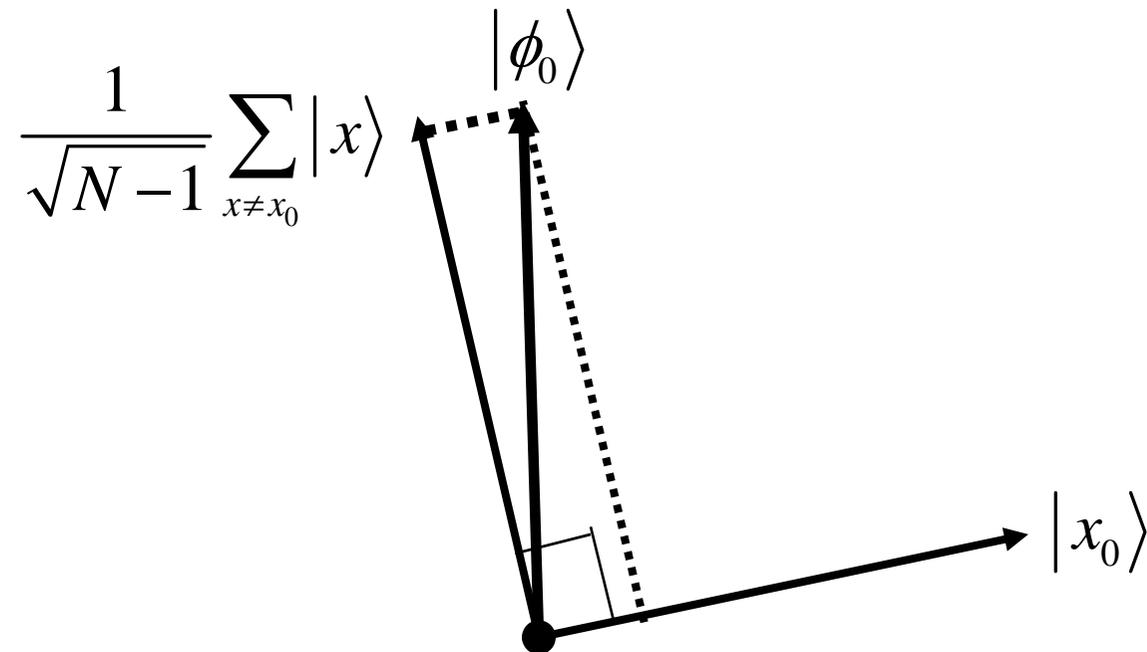




おさらい

(1) 一様な状態生成

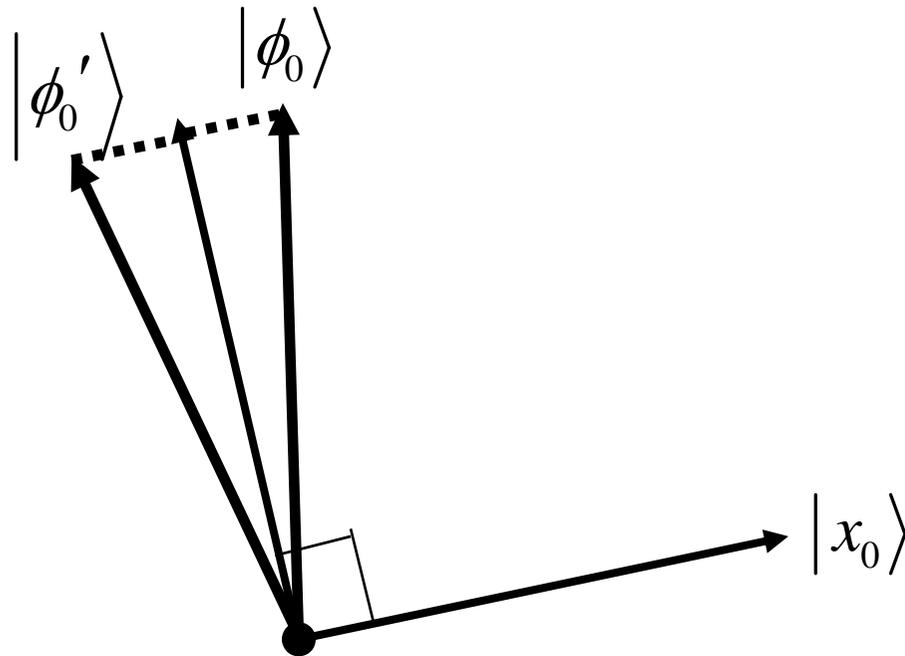
$$|\phi_0\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$



おさらい

(2) $\frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} |x\rangle$ で折り返し

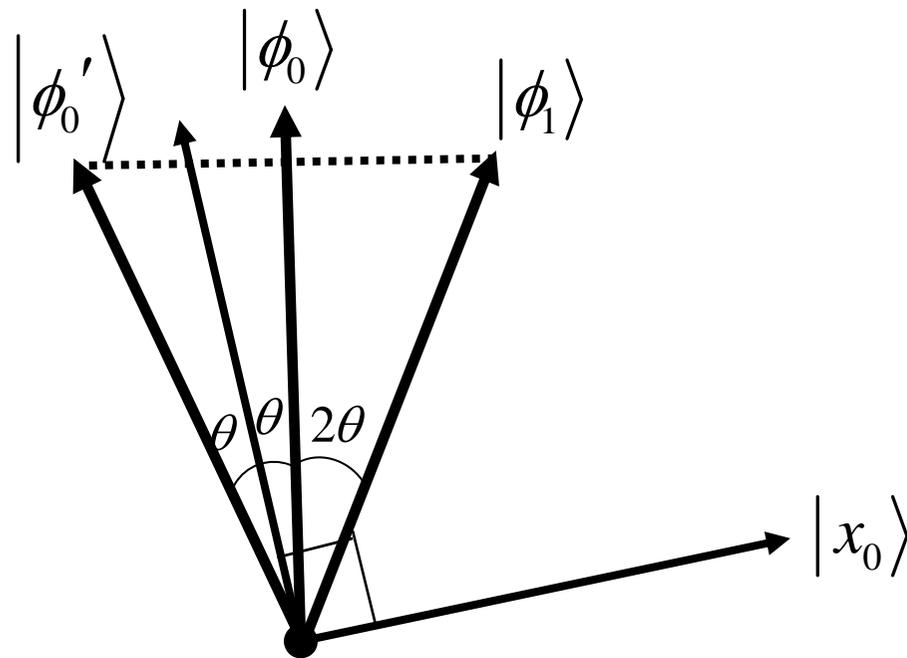
$$|\phi'_0\rangle = \frac{1}{\sqrt{N}} \left(-|x_0\rangle + \sum_{x \neq x_0} |x\rangle \right)$$



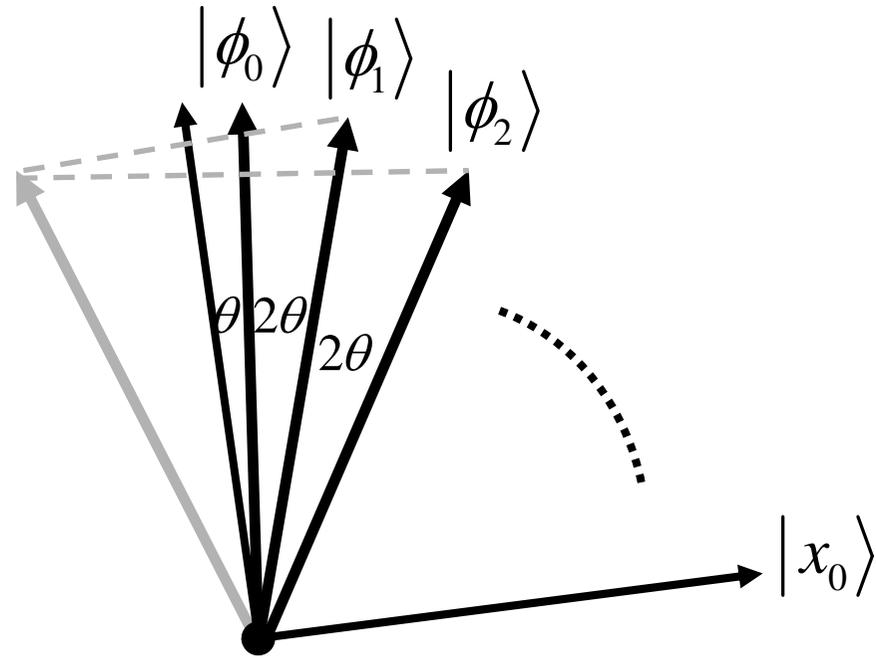
おさらい

(3) $|\phi_0\rangle$ で折り返し

$$|\phi_1\rangle = D|\phi_0'\rangle$$

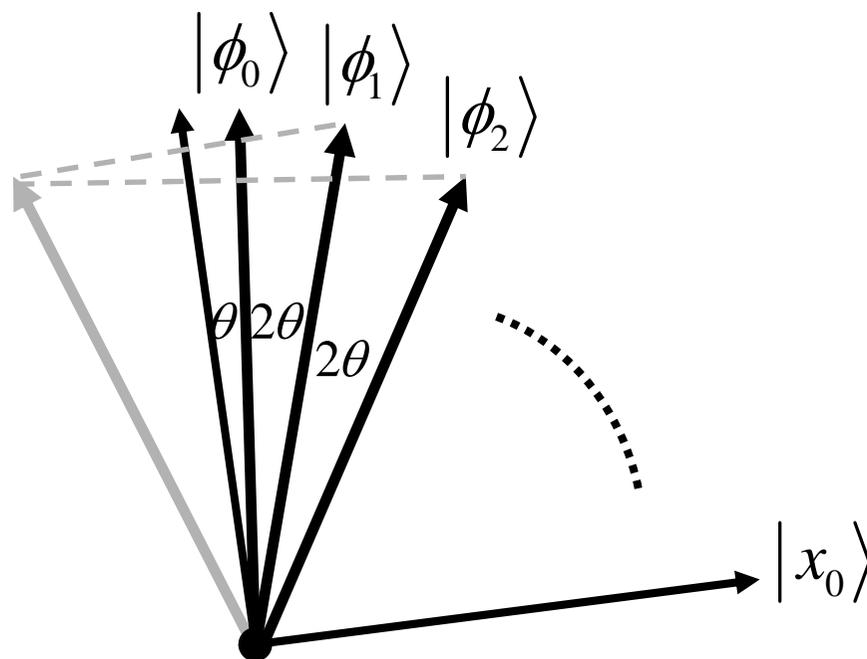


さらに繰り返していくと...



$|\phi_k\rangle$ は $|x_0\rangle$ に徐々に近づいていく!

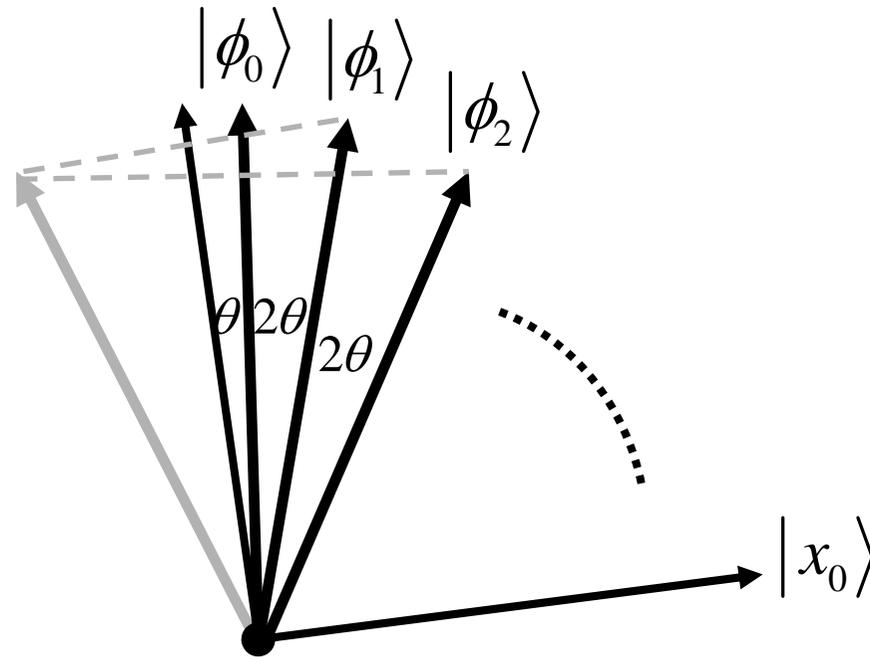
成功確率と繰り返し回数の解析



$|\phi_k\rangle$ と $|x_0\rangle$ の角度は $\frac{\pi}{2} - (2k + 1)\theta$

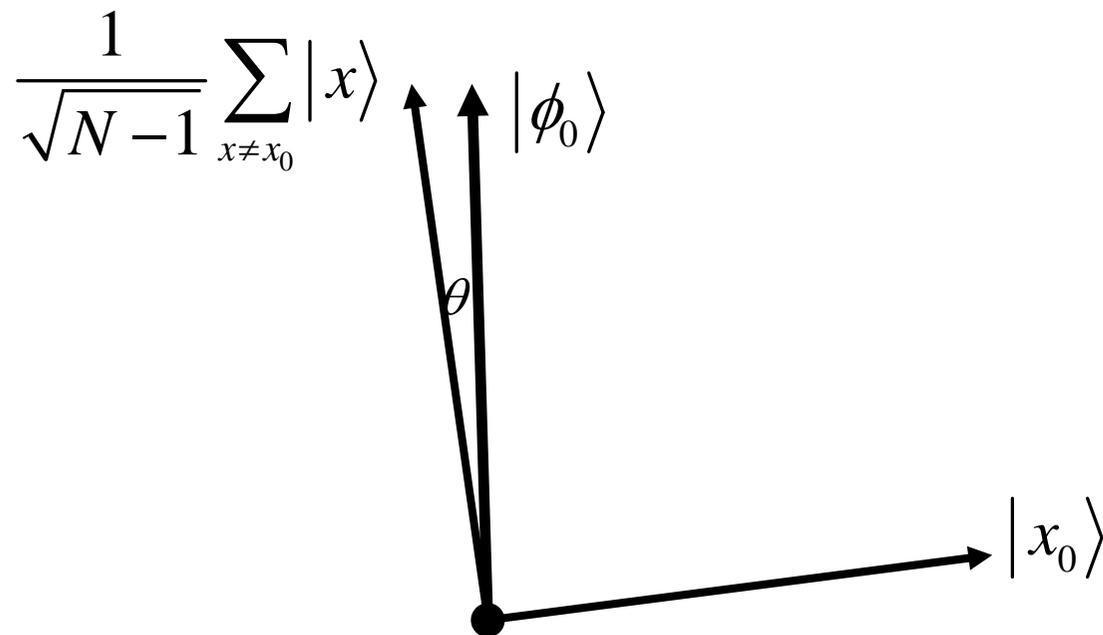
➡ $|\phi_k\rangle$ を観測したときの成功確率 = $\cos^2\left(\frac{\pi}{2} - (2k + 1)\theta\right)$

$$|\phi_k\rangle \text{ を観測したときの成功確率} = \cos^2\left(\frac{\pi}{2} - (2k+1)\theta\right)$$



$\frac{\pi}{2} \approx (2k+1)\theta$ であればほぼ確率1!

➡ $k \approx \frac{\pi}{4\theta} - \frac{1}{2}$



$$\cos \theta = \frac{1}{\sqrt{N-1}} \sum_{x \neq x_0} \langle x | \phi_0 \rangle = \frac{1}{\sqrt{N(N-1)}} \sum_{x \neq x_0} \sum_y \langle x | y \rangle = \sqrt{\frac{N-1}{N}}$$

$$\sin \theta = \sqrt{\frac{1}{N}}$$

N が十分大きいとき $\sin \theta \approx \theta$ なので $k \approx \frac{\pi}{4\theta} - \frac{1}{2} = O(\sqrt{N})$

Grover のアルゴリズム

(Grover, 1996)

- 入力: 論理関数 $f : \{0,1\}^n \rightarrow \{0,1\}$
(但し $f(x_0)=1$ となる $x_0 \in \{0,1\}^n$ は唯一)
- 出力: n ビット列 $x_0 \in \{0,1\}^n$ s.t. $f(x_0) = 1$

Grover のアルゴリズムは

$$f \text{ の計算回数} = \lfloor \pi/4 \rfloor \sqrt{2^n} = O\left(\sqrt{2^n}\right)$$

$$\text{成功確率} \geq 1 - 2^{-n}$$

で上の問題を解くことが可能!

一般化

- 解が複数個ある場合
 - 解の数が既知
 - 解の数が未知

まとめ

- 量子計算の基本モデル
 - 量子ビットと量子回路
- 量子アルゴリズムの例
 - Groverの高速検索アルゴリズム
- どんな問題が量子計算に向いている？