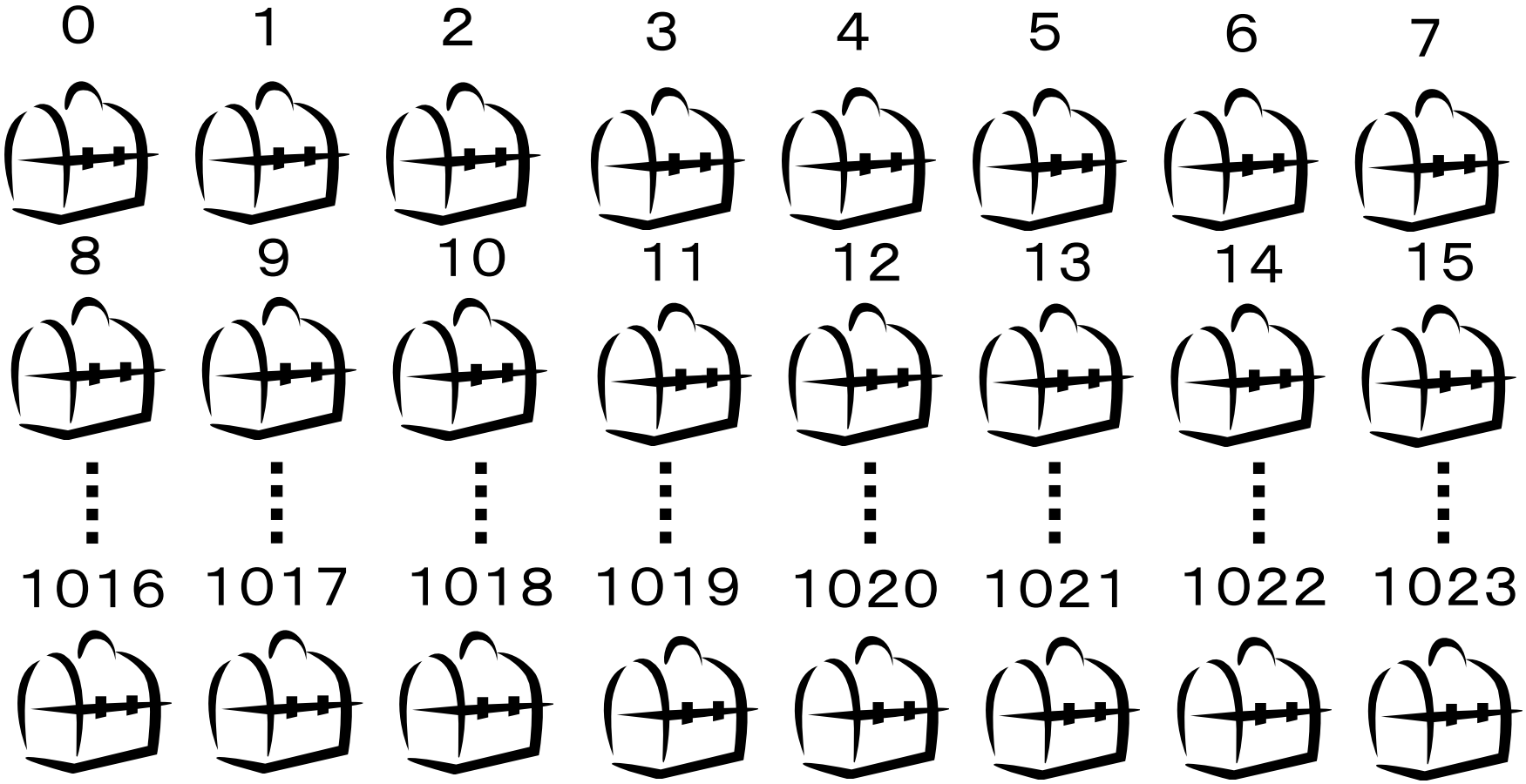
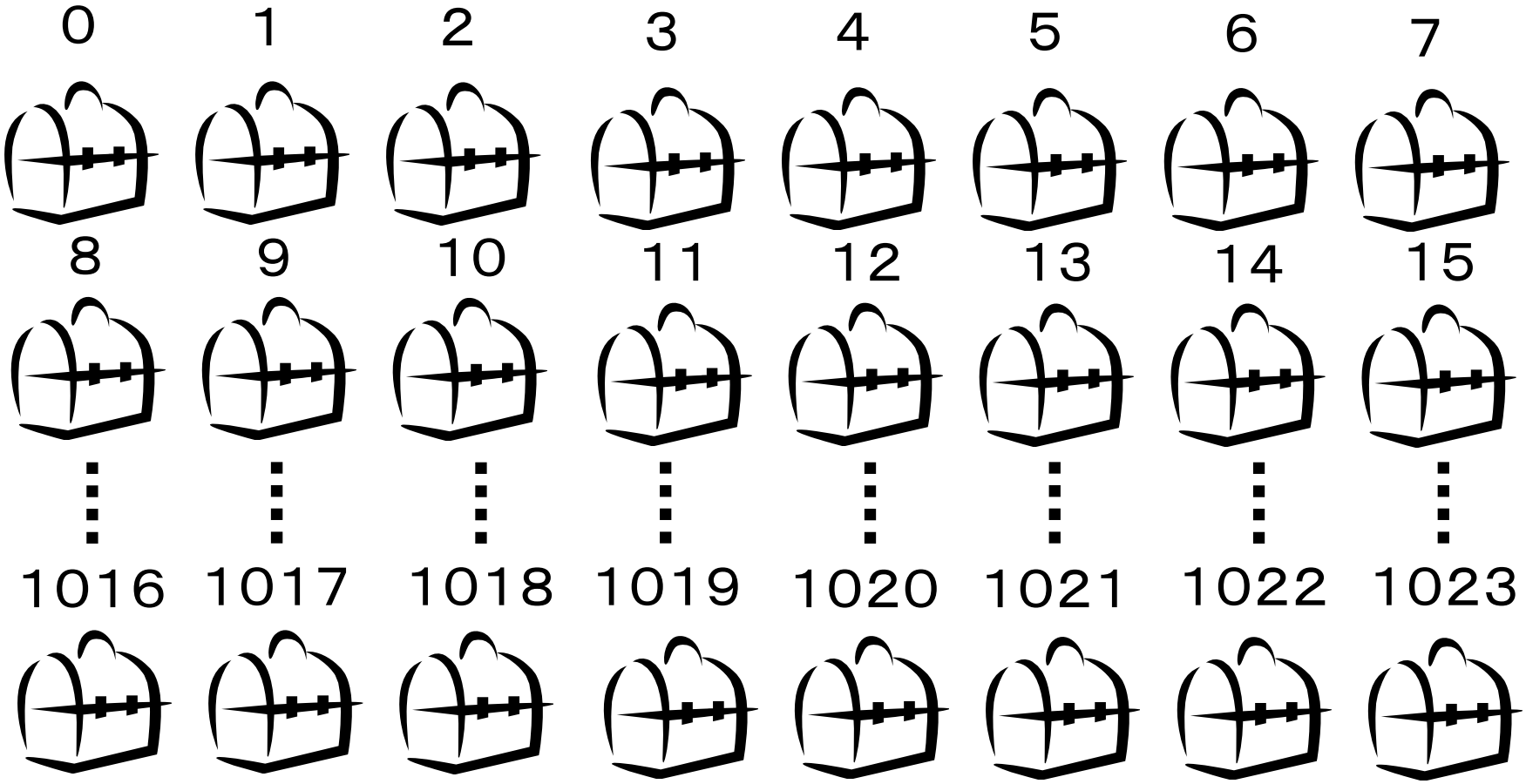
量子アルゴリズム

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 $f:\{0,1\}^n \to \{0,1\}$

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

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 $00\cdots0$ ～ $11\cdots1$ の $N := 2^n$ 個
  - $\left|00\cdots0\right\rangle$から中立的な状態$\left|\phi_0\right\rangle$を生成

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

  - この時点で測定した場合の成功確率

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

    ・・・一様ランダムに探すのと一緒

  - 成功確率 $\left|\left\langle x_0 \middle| \phi_0 \right\rangle\right|^2$ 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: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

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

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

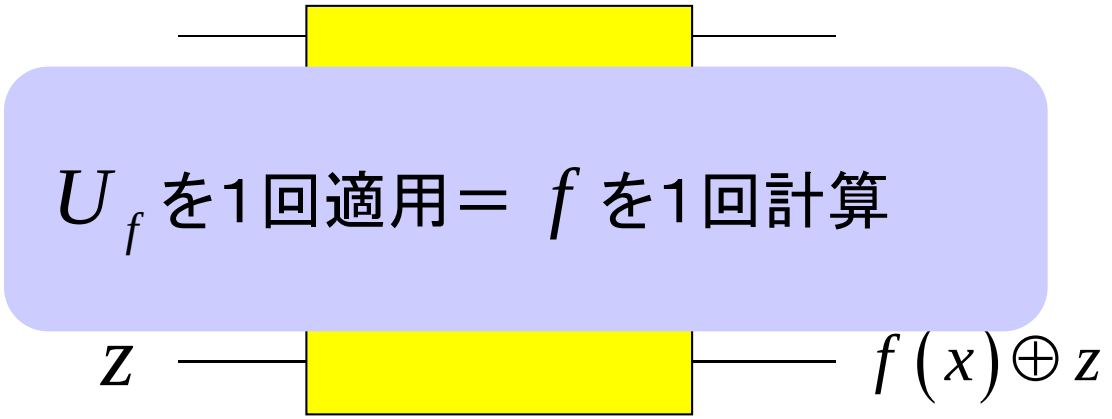
$$\begin{aligned} H^{\otimes n}\left|00\cdots0\right\rangle &= \left(H\left|0\right\rangle\right)\otimes\cdots\otimes\left(H\left|0\right\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right)\otimes\cdots\otimes\frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right) \\ &= \frac{1}{\sqrt{2^n}}\left(\left|0\cdots00\right\rangle + \left|0\cdots01\right\rangle + \cdots + \left|1\cdots11\right\rangle\right) \\ &= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}\left|x\right\rangle \end{aligned}$$

論理関数 ➔ ユニタリ変換

- f を計算するユニタリ変換 U_f

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

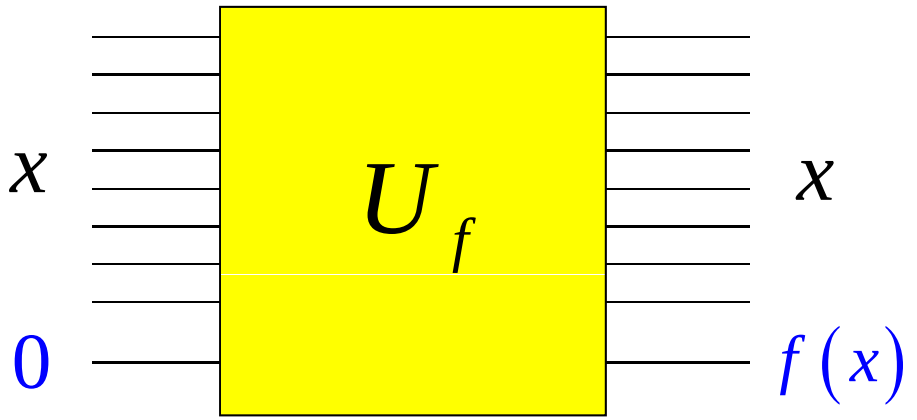
$$\left(x \in \{0,1\}^n, z \in \{0,1\}\right)$$



論理関数 ➔ ユニタリ変換

- f を計算するユニタリ変換 U_f

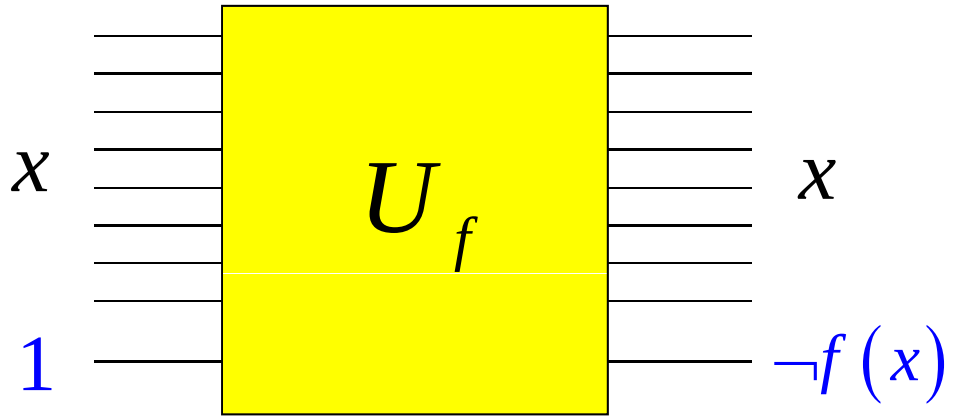
$$U_f \left|x\right\rangle \left|0\right\rangle = \left|x\right\rangle \left|f(x)\right\rangle$$



論理関数 ➔ ユニタリ変換

- f を計算するユニタリ変換 U_f

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



U_f を使って V_f を構成

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

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

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

第2レジスタは全く変化しない！（無視できる）

$$V_f \left|x\right\rangle = \begin{cases} \left|x\right\rangle & (f(x)=0 \text{の場合}) \\ -\left|x\right\rangle & (f(x)=1 \text{の場合}) \end{cases}$$

が実現可能

$$V_f = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & -1 & \\ & & & 1 \\ 0 & & & \ddots \\ & & & & 1 \end{pmatrix} < x_0$$

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

拡散変換

$$D = \begin{pmatrix} -1+\frac{2}{N} & & \frac{2}{N} \\ & -1+\frac{2}{N} & \\ \frac{2}{N} & & \ddots \\ & & -1+\frac{2}{N} \end{pmatrix}$$

$$D = -H^{\otimes n}\left(I - 2\left|0\cdots0\right\rangle\left\langle 0\cdots0\right|\right)H^{\otimes n}$$

$$= H^{\otimes n}\begin{pmatrix} 1 & & 0 \\ & -1 & \\ & & \ddots \\ 0 & & -1 \end{pmatrix}H^{\otimes n}$$

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

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

一回目の繰り返しを計算してみよう

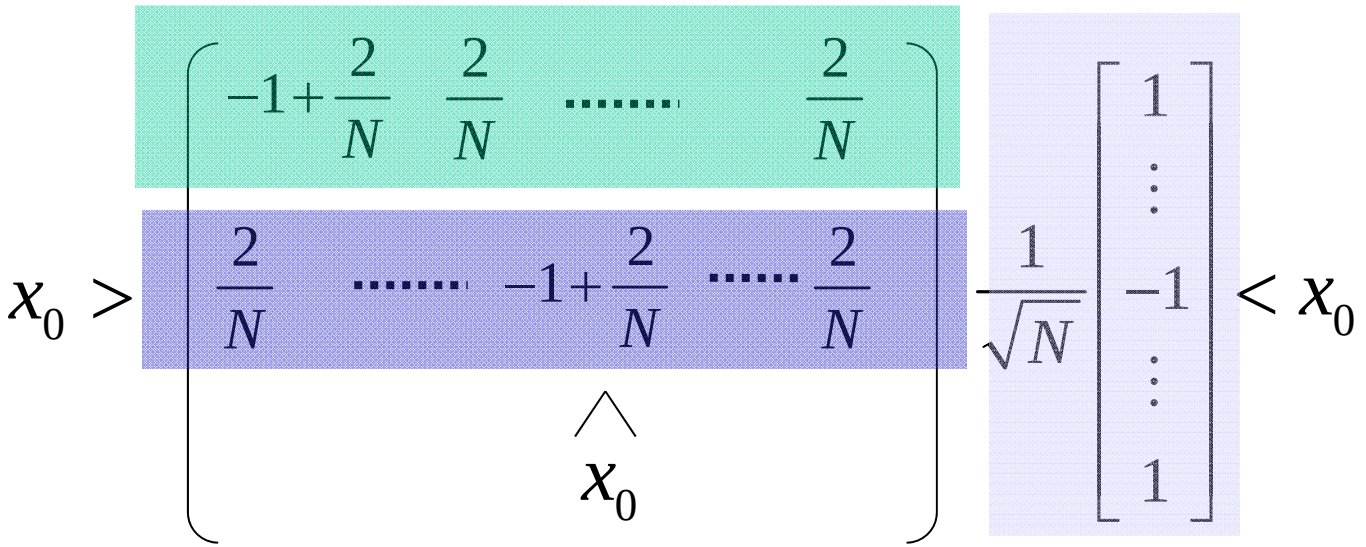
２　V_f でアタリの位相を反転

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

一回目の繰り返しを計算してみよう

３ 拡散変換を適用

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



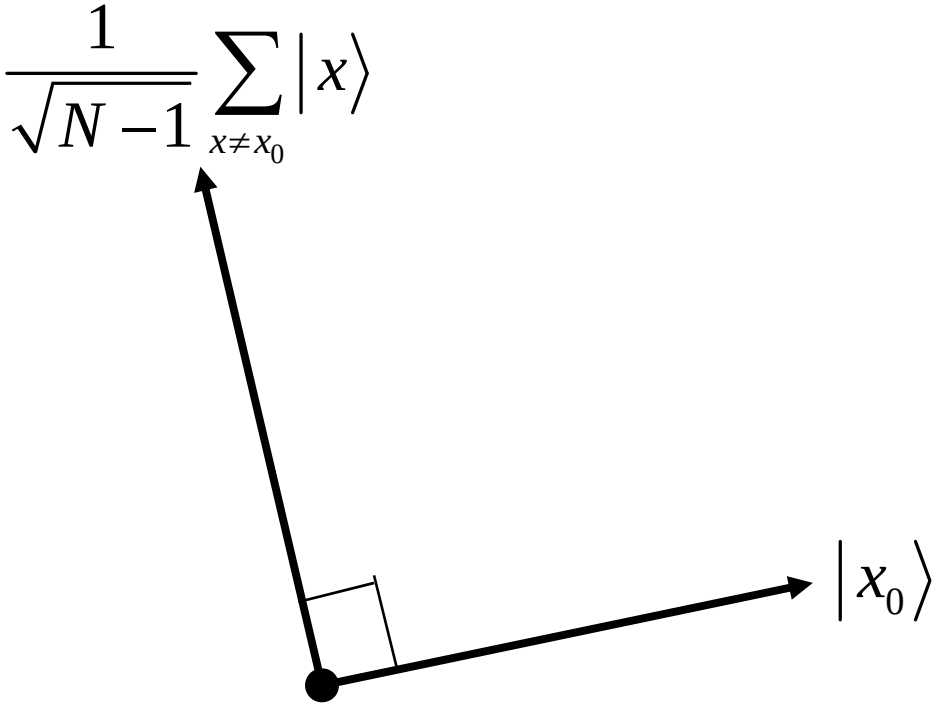
$$\times = \frac{1}{\sqrt{N}}\left(-1+\frac{2}{N}+\overbrace{\frac{2}{N}+\cdots+\frac{2}{N}}^{N-2}-\frac{2}{N}\right)=\frac{1}{\sqrt{N}}\left(1-\frac{4}{N}\right)$$

$$\times = \frac{1}{\sqrt{N}}\left(\overbrace{\frac{2}{N}+\cdots+\frac{2}{N}}^{N-1}+1-\frac{2}{N}\right)=\frac{1}{\sqrt{N}}\left(2-\frac{4}{N}\right)$$

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

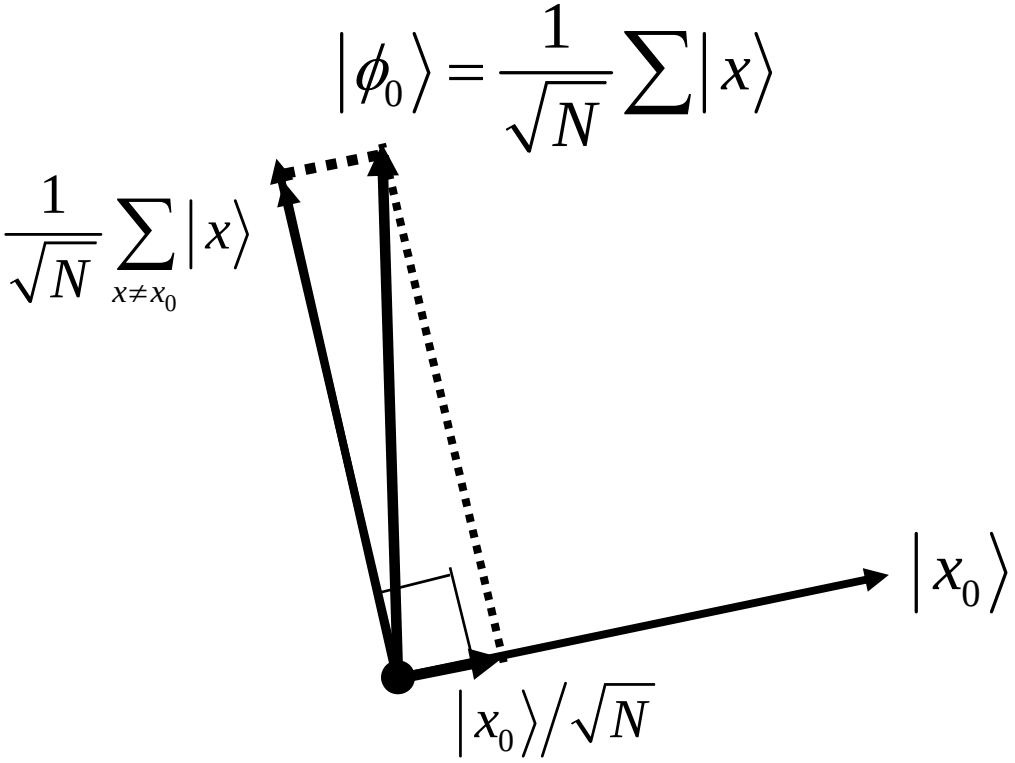
なぜ上手くいくの？？

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



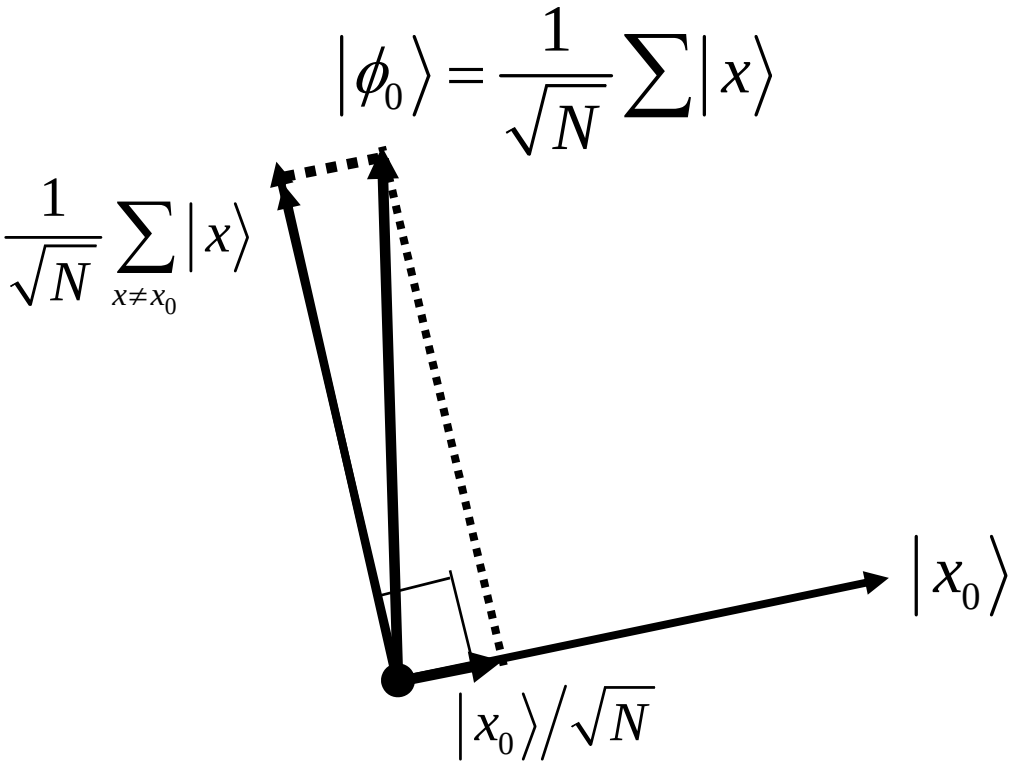
なぜ上手くいくの？？

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



なぜ上手くいくの？？

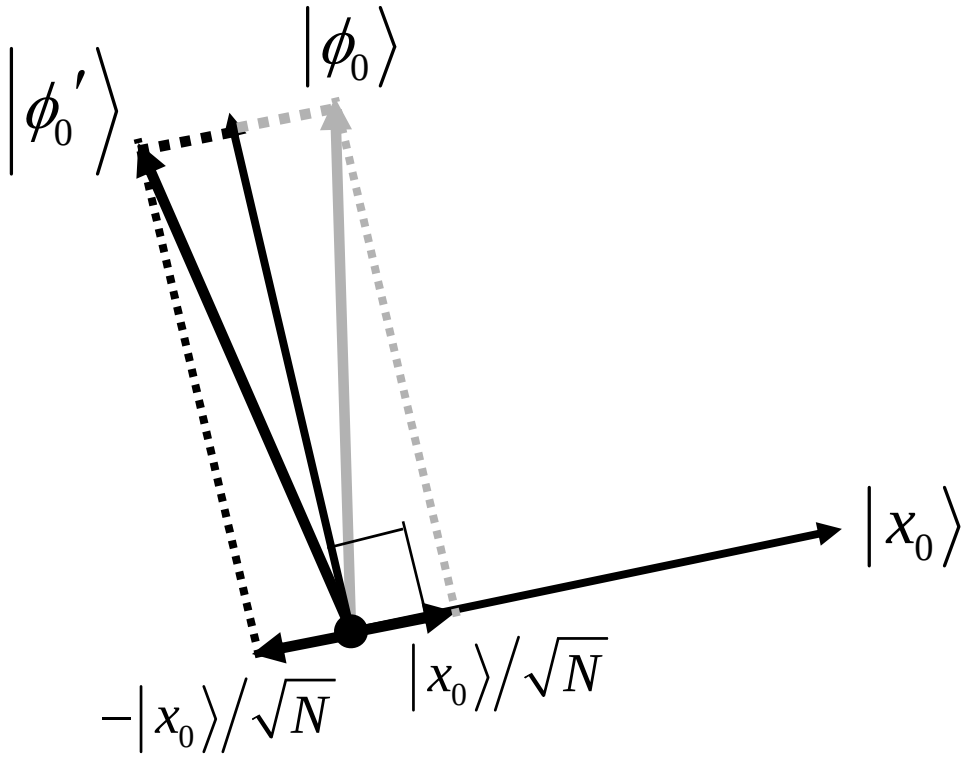
$V_f = I - 2|x_0\rangle\langle x_0|$ の適用



なぜ上手くいくの？？

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

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

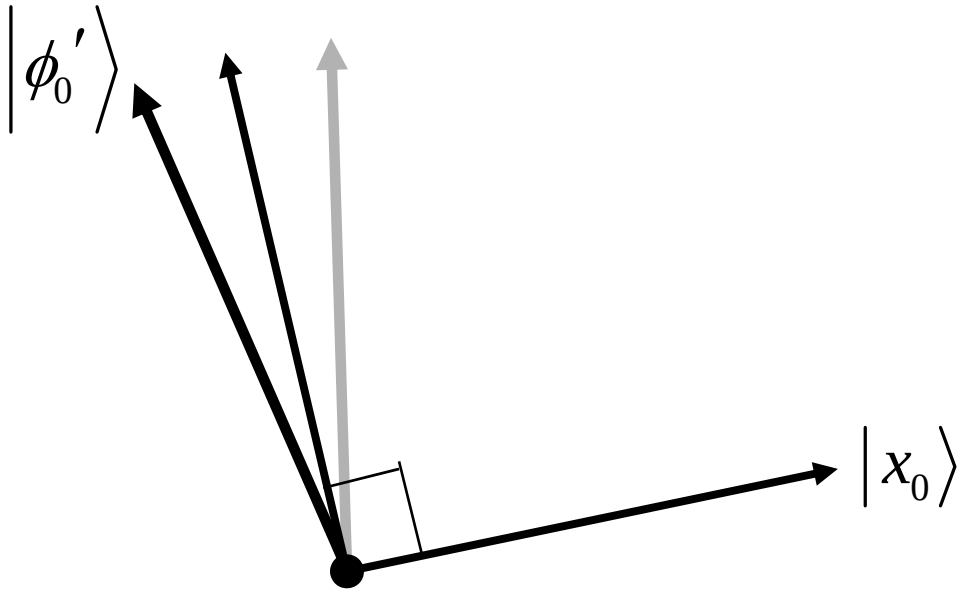


なぜ上手くいくの？？

拡散行列

$$D = -I + 2H^{\otimes n}\left|0\cdots0\right\rangle\left\langle 0\cdots0\right|H^{\otimes n} = -I + 2\left|\phi_0\right\rangle\left\langle\phi_0\right|$$

の適用



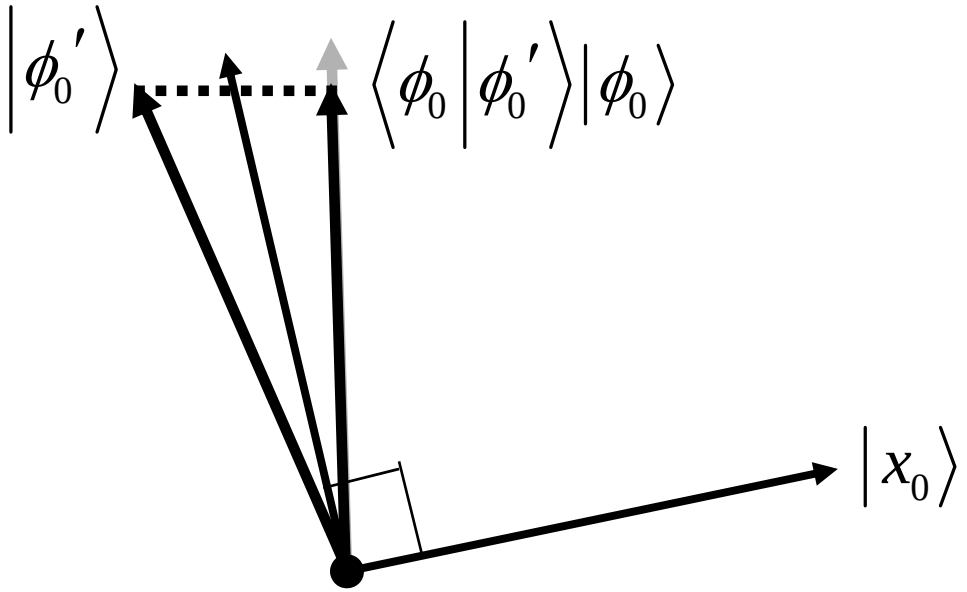
なぜ上手くいくの？？

拡散行列

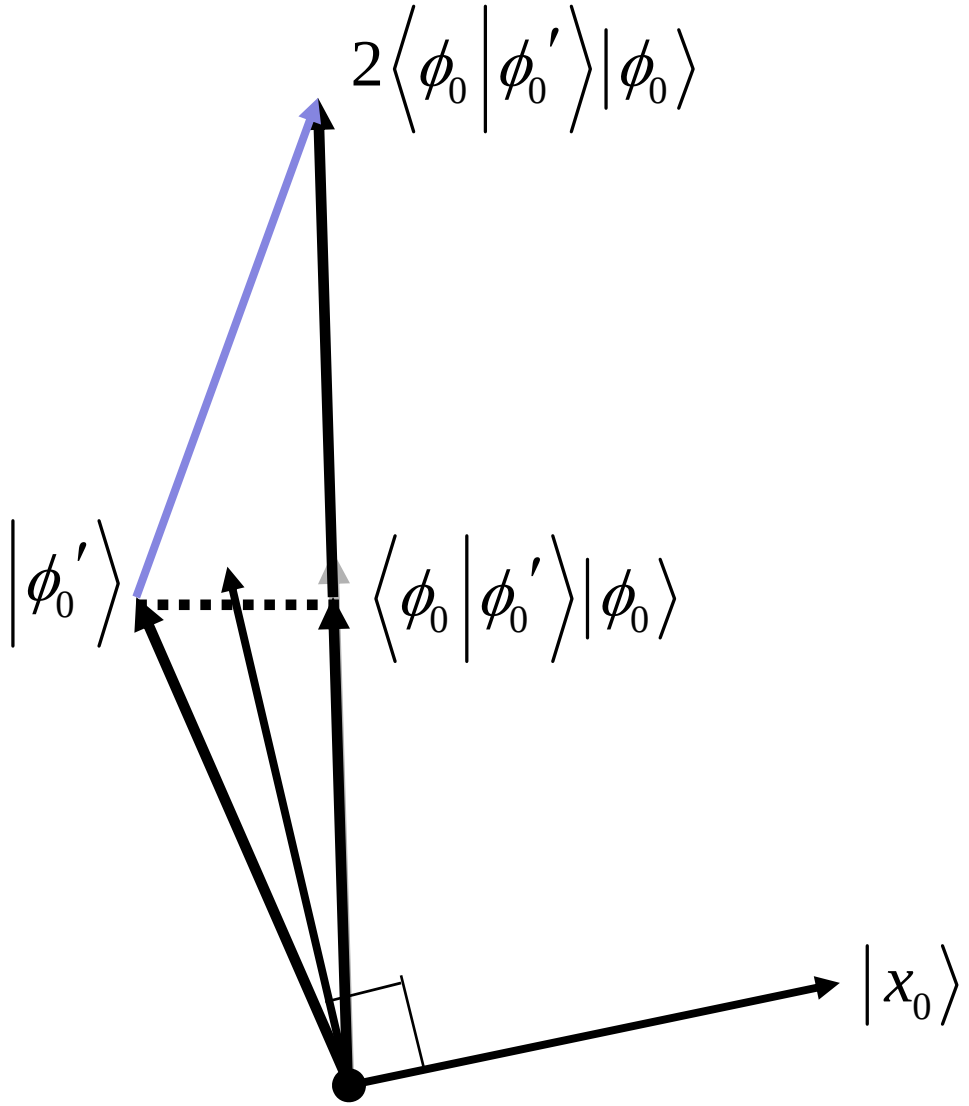
$$D = -I + 2H^{\otimes n}\left|0\cdots0\right\rangle\left\langle 0\cdots0\right|H^{\otimes n} = -I + 2\left|\phi_0\right\rangle\left\langle\phi_0\right|$$

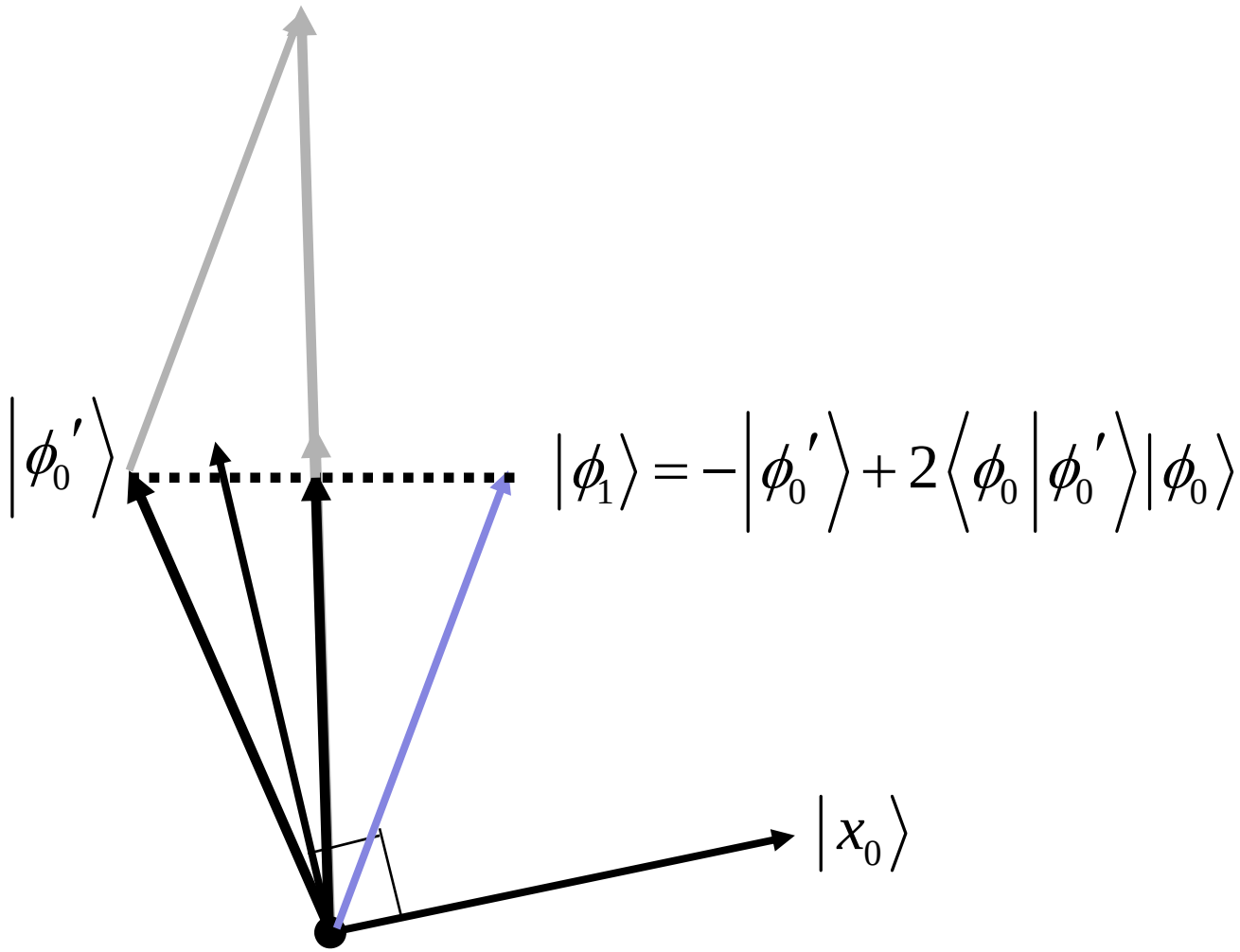
の適用

$$\left(-I + 2\left|\phi_0\right\rangle\left\langle\phi_0\right|\right)\left|\phi_0'\right\rangle = -\left|\phi_0'\right\rangle + 2\left\langle\phi_0\middle|\phi_0'\right\rangle\left|\phi_0\right\rangle$$



$$\left(-I+2\left|\phi_0\right\rangle\left\langle\phi_0\right|\right)\left|\phi_0'\right\rangle=-\left|\phi_0'\right\rangle+2\left\langle\phi_0\middle|\phi_0'\right\rangle\left|\phi_0\right\rangle$$

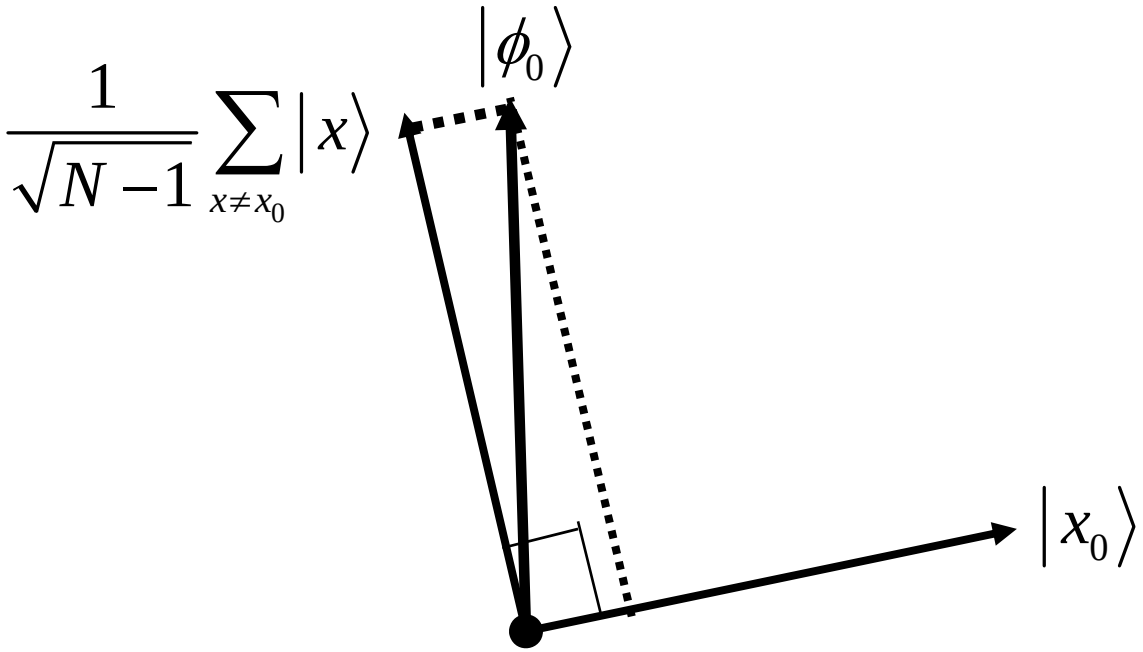



$|\phi_0'\rangle$
$|\phi_1\rangle = -|\phi_0'\rangle + 2\langle\phi_0|\phi_0'\rangle|\phi_0\rangle$
$|x_0\rangle$

おさらい

（1）一様な状態生成

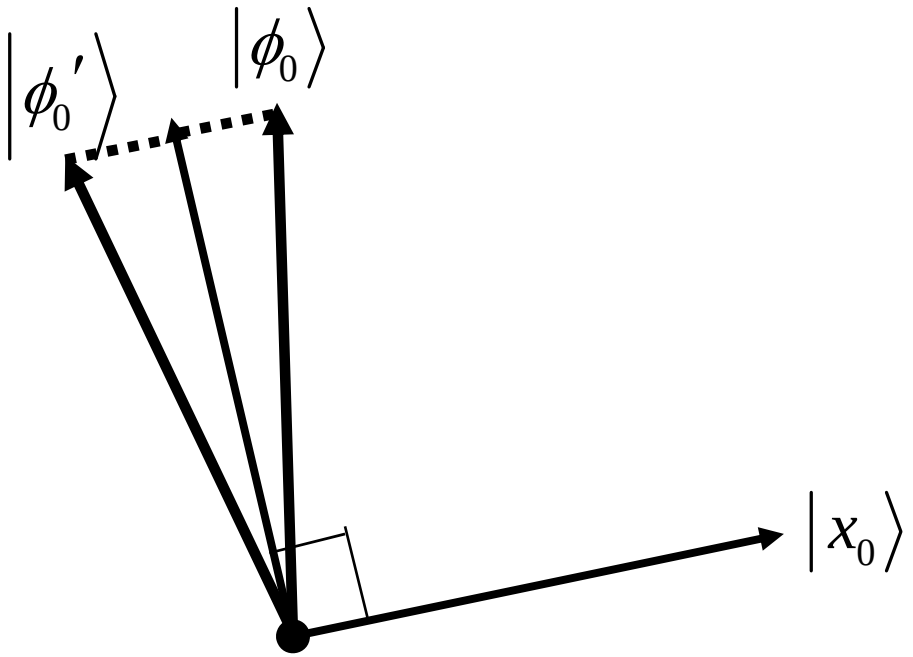
$$|\phi_0\rangle = \frac{1}{\sqrt{N}} \sum |x\rangle$$



おさらい

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

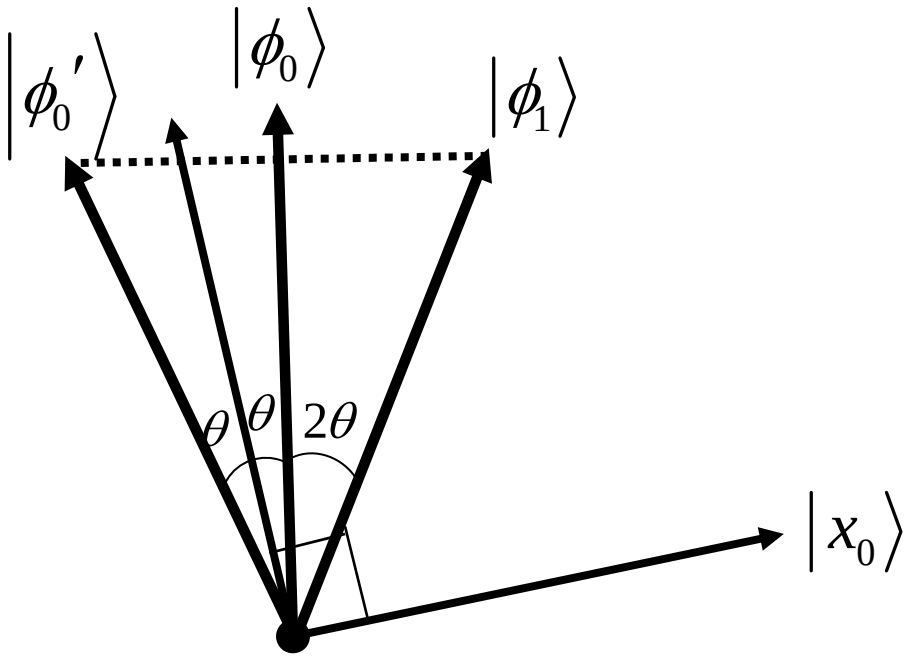
$$|\phi_0'\rangle = \frac{1}{\sqrt{N}}\left(-|x_0\rangle + \sum_{x\neq x_0}|x\rangle\right)$$



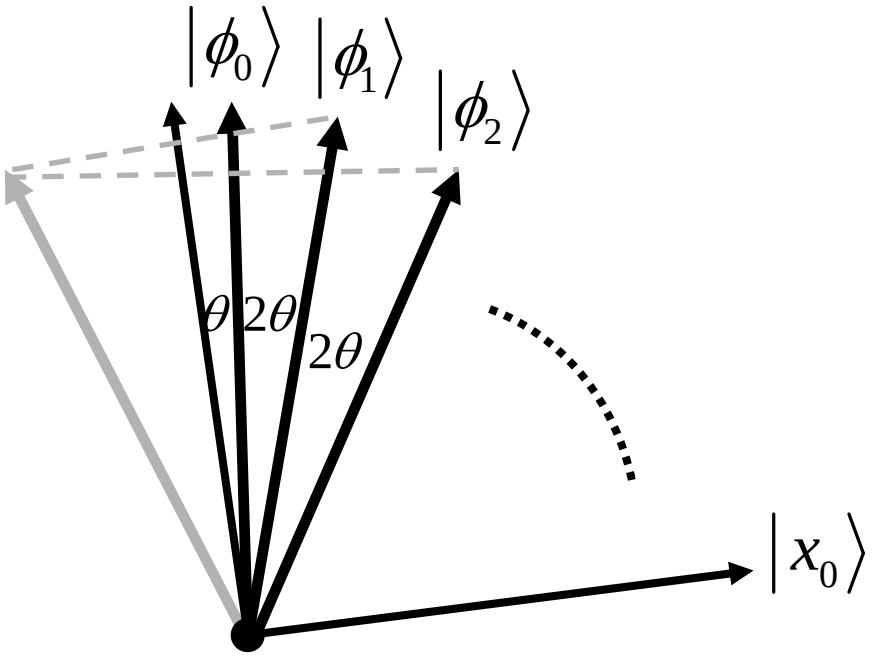
おさらい

（3）$|\phi_0\rangle$ で折り返し

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

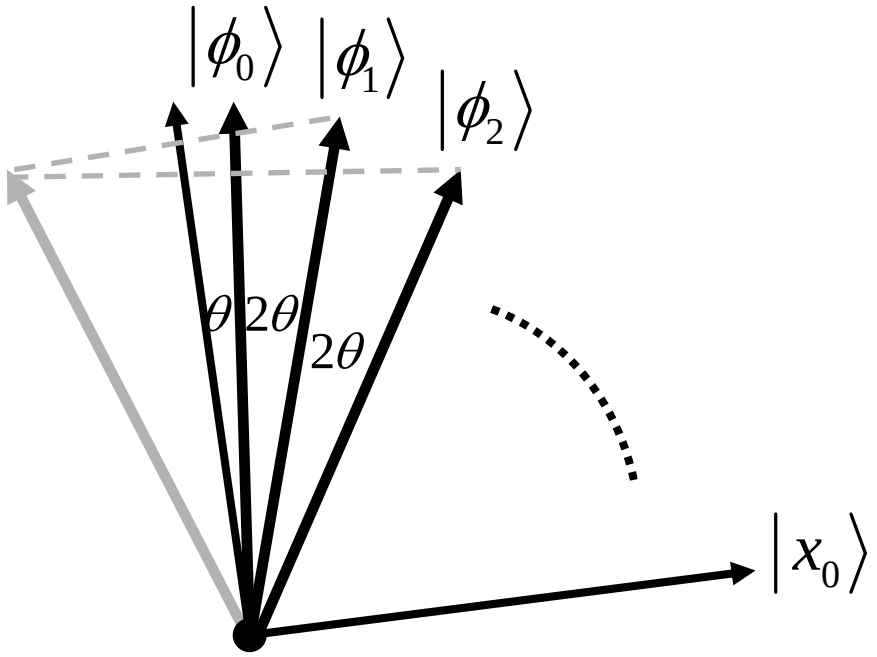


さらに繰り返していくと・・・



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

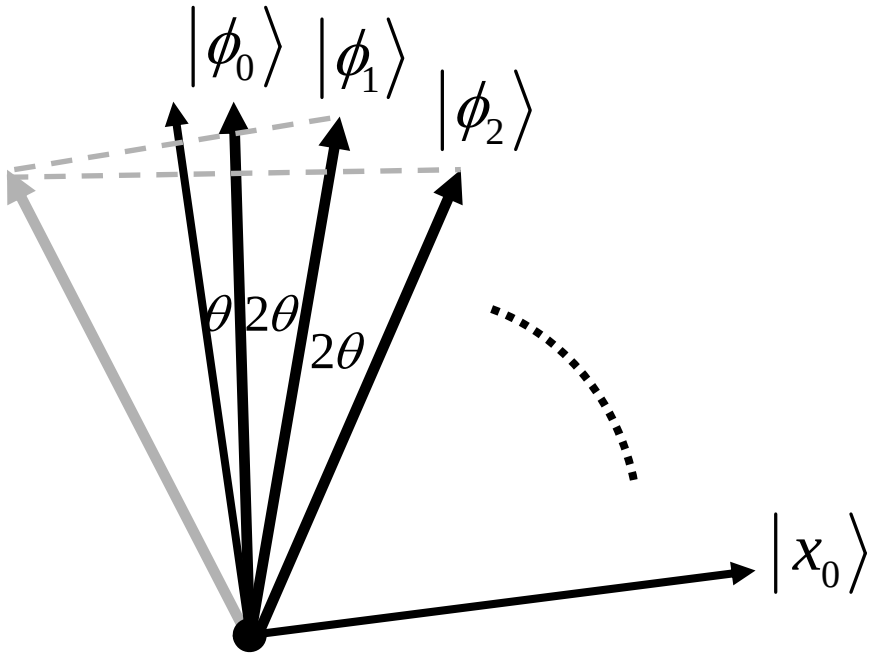
成功確率と繰り返し回数の解析



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

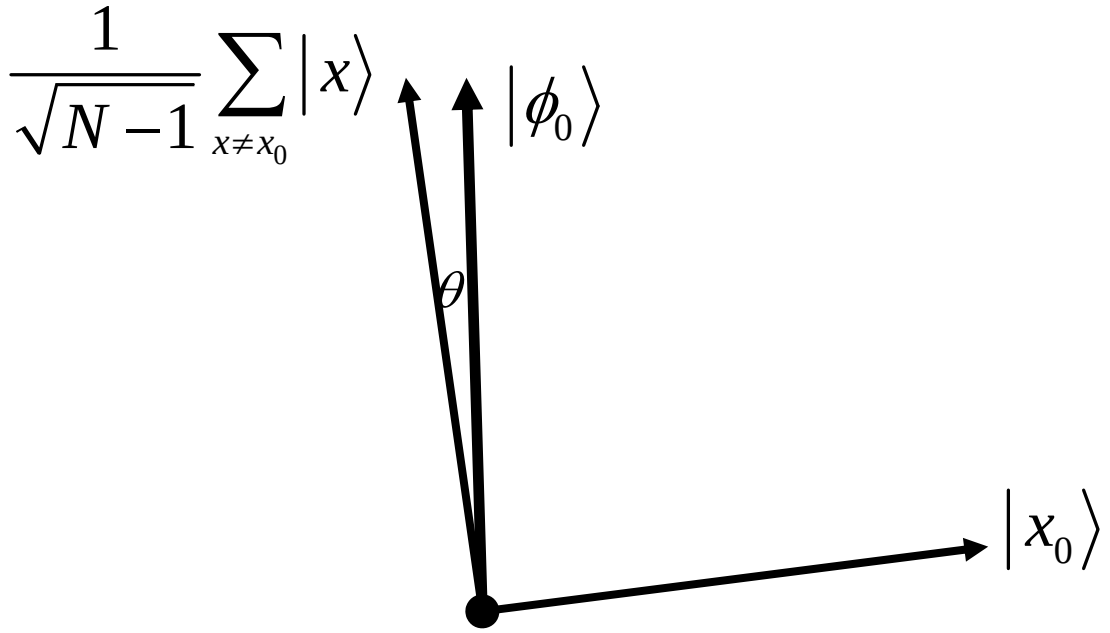
⇒ $|\phi_k\rangle$ を観測したときの成功確率＝ $\cos^2\left(\frac{\pi}{2}-(2k+1)\theta\right)$

$|\phi_k\rangle$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！

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



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

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

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

Grover のアルゴリズム

(Grover, 1996)

- 入力: 論理関数 $f:\{0,1\}^n \to \{0,1\}$

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

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？