RIKEN QUANTUM COMPUTING

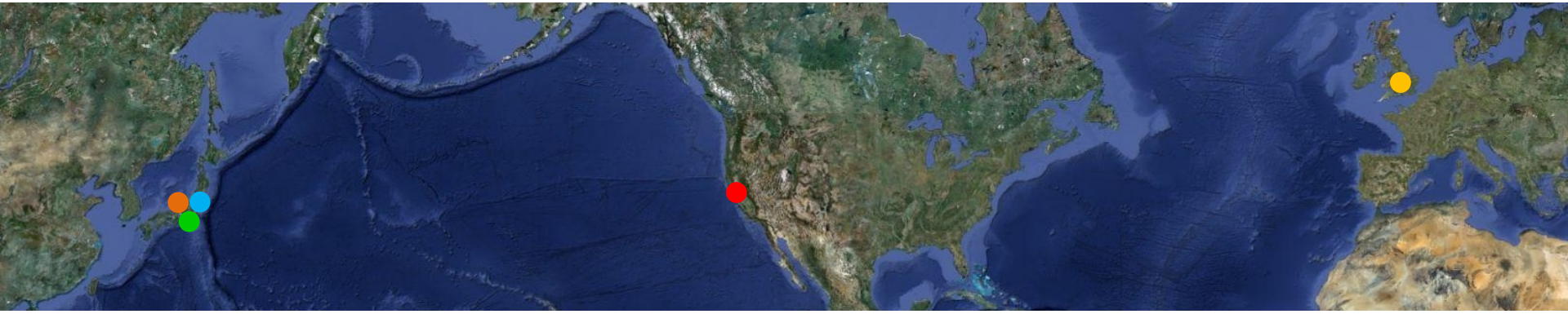
RIKEN

量子コンピューティングの基礎理論

阿部英介
理化学研究所 量子コンピュータ研究センター

2021年8月20日(バーチャル開催)
VLSI夏の学校「LSI技術者のための量子コンピューティング講座」
日本学術振興会シリコン超集積システム第165委員会

自己紹介



© Google Earth

- **2001.4 – 2006.3 (慶應)** → スピンコヒーレンス(シリコン)
- **2006.4 – 2009.12 (東大物性研)** → 量子輸送現象(ゲート制御型量子ドット)
- **2010.1 – 2011.6 (Oxford)** → スピンを用いた共振器QED
- **2011.7 – 2015.3 (Stanford)** → 量子ネットワーク(光学活性量子ドット)
- **2015.4 – 2019.1 (慶應)** → 量子センシング(ダイヤモンド)
- **2019.2 – Present (理研)** → 量子コンピューティング(超伝導量子回路)

講義内容

- **イントロダクション**
  - 半導体デバイスと量子
  - 量子ドット中の電子の振る舞い
- **量子コンピューティングの基礎**
  - 量子ビットと量子ゲート
  - 量子アルゴリズム
  - 量子コンピューティングの難しさ

講義内容

- **イントロダクション**
  - 半導体デバイスと量子
  - 量子ドット中の電子の振る舞い
- **量子コンピューティングの基礎**
  - 量子ビットと量子ゲート
  - 量子アルゴリズム
  - 量子コンピューティングの難しさ

トンネルダイオード

New Phenomenon in Narrow Germanium *p-n* Junctions

LEO ESAKI

Tokyo Tsushin Kogyo, Limited, Shinagawa, Tokyo, Japan

(Received October 11, 1957)

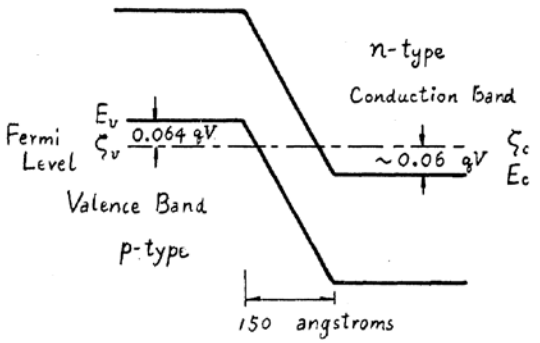


FIG. 2. Energy diagram of the *p-n* junction at 300°K and no bias voltage.

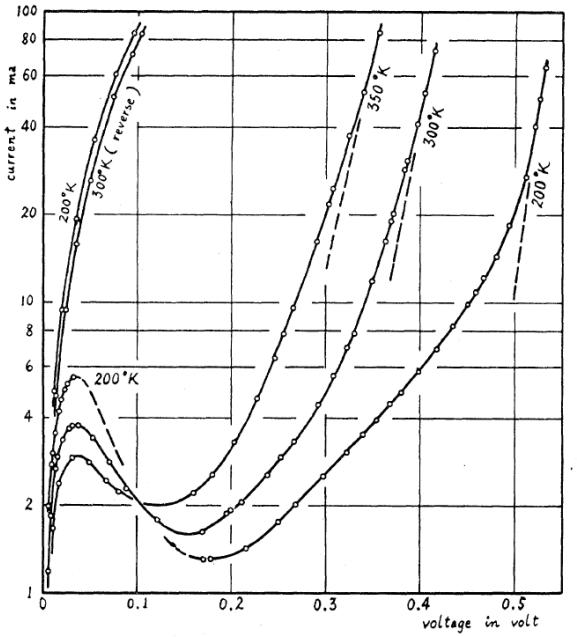


FIG. 1. Semilog plots of the measured current-voltage characteristic at 200°K, 300°K, and 350°K.

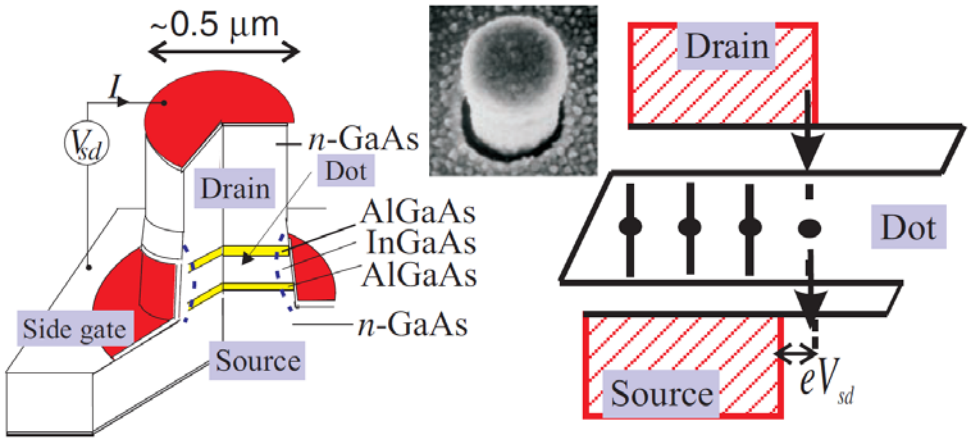
L. Esaki
(Nobel Phys. 1973)

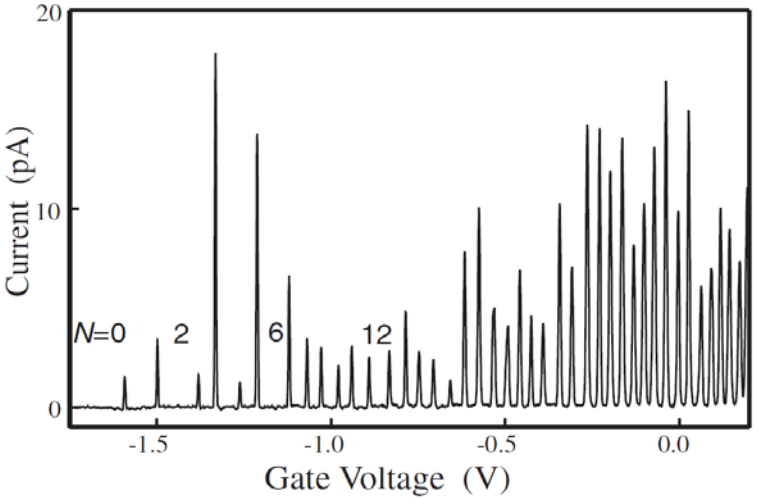
- トンネル現象
  → 電子は**波**

Phys. Rev. **109**, 603 (1958) Esaki

縦型量子ドット

共鳴トンネルダイオード → 縦型量子ドット (1996)





- トンネル現象
  → 電子は**波**
- 単電子トランジスタ
  → 電子は**粒子**

Rep. Prog. Phys. **64**, 701 (2001) Kouwenhoven *et al.*

高移動度トランジスタ

JAPANESE JOURNAL OF APPLIED PHYSICS
VOL. 19, NO. 5, MAY, 1980 pp. L225–L227

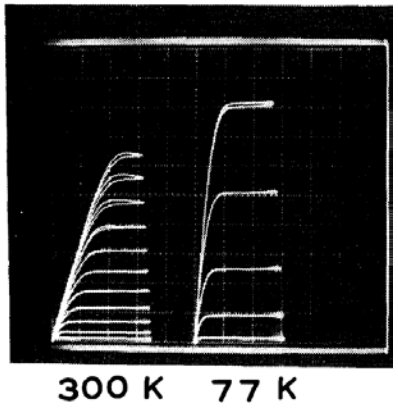
A New Field-Effect Transistor with Selectively Doped GaAs/n-$Al_xGa_{1-x}As$ Heterojunctions

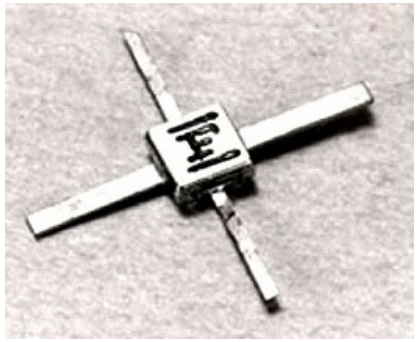
Takashi MIMURA, Satoshi HIYAMIZU, Toshio FUJII and Kazuo NANBU

Fujitsu Laboratories Ltd.,
1015, Kamikodanaka, Nakahara-ku, Kawasaki 211

(Received March 24, 1980)

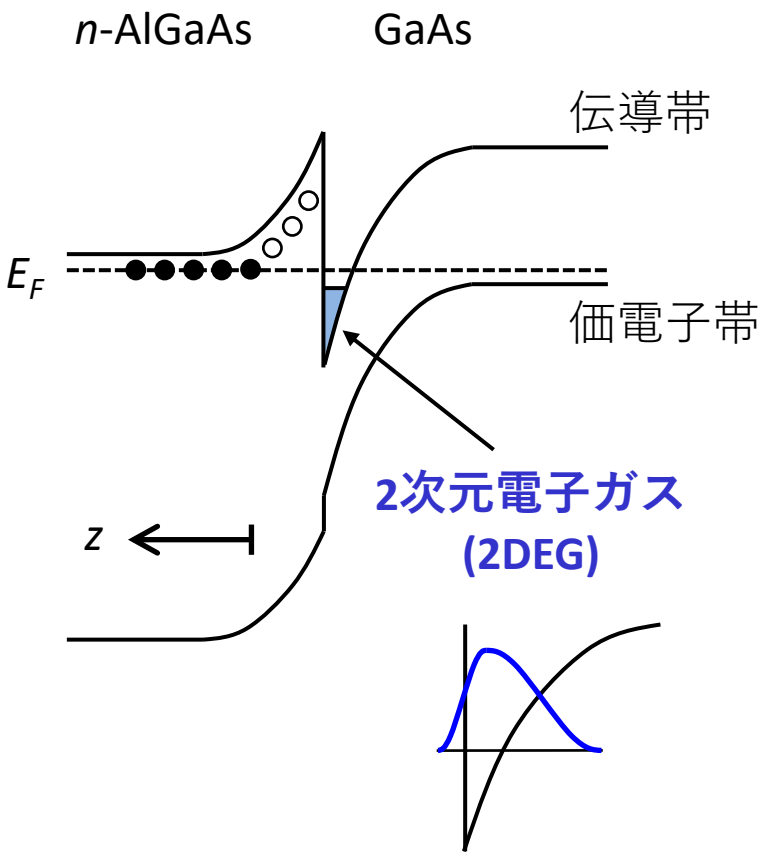
Studies of field-effect control of the high mobility electrons in MBE-grown selectively doped GaAs/n-$Al_xGa_{1-x}As$ heterojunctions are described. Successful fabrication of a new field-effect transistor, called a high electron mobility transistor (HEMT), with extremely high-speed microwave capabilities is reported.





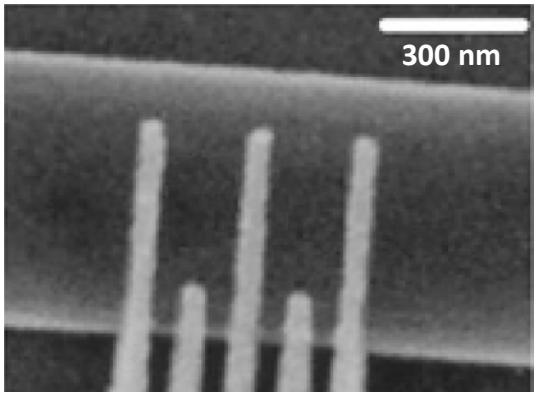
© Fujitsu

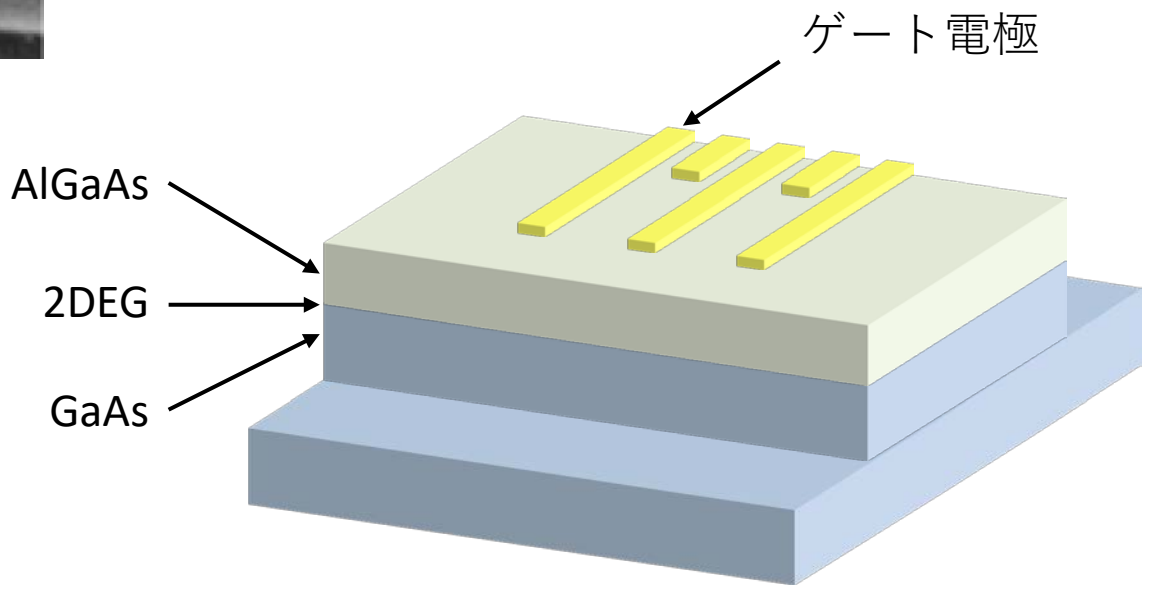
変調ドープヘテロ界面



Jpn. J. Appl. Phys. **19**, L225 (1980) Mimura *et al.*

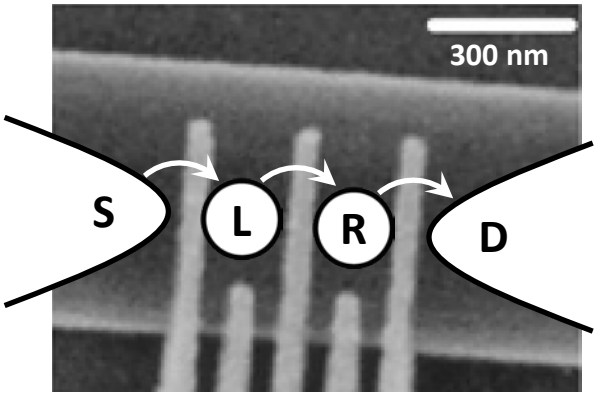
横型二重量子ドット

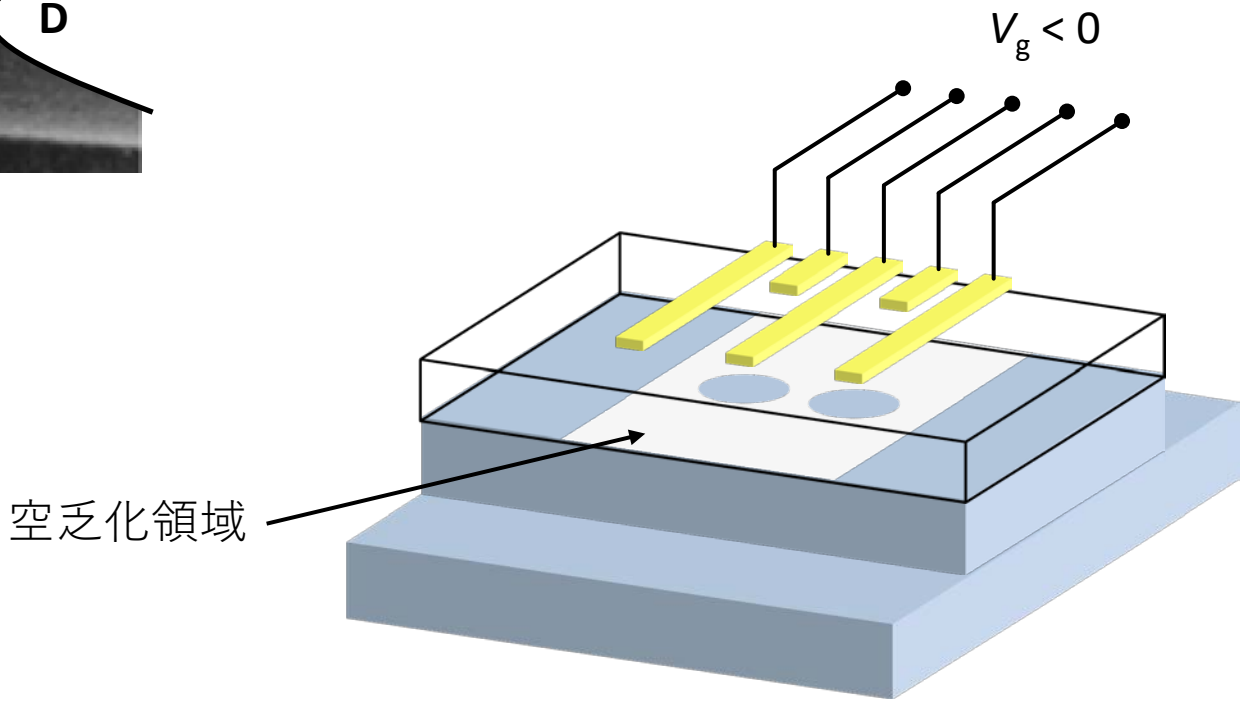




Rep. Prog. Phys. **69**, 759 (2006) Fujisawa *et al.*

横型二重量子ドット





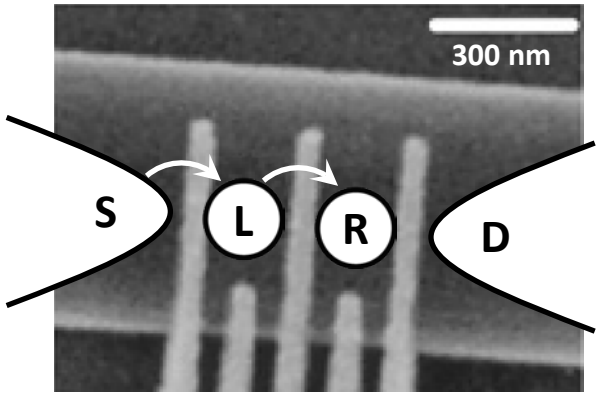
Rep. Prog. Phys. **69**, 759 (2006) Fujisawa *et al.*

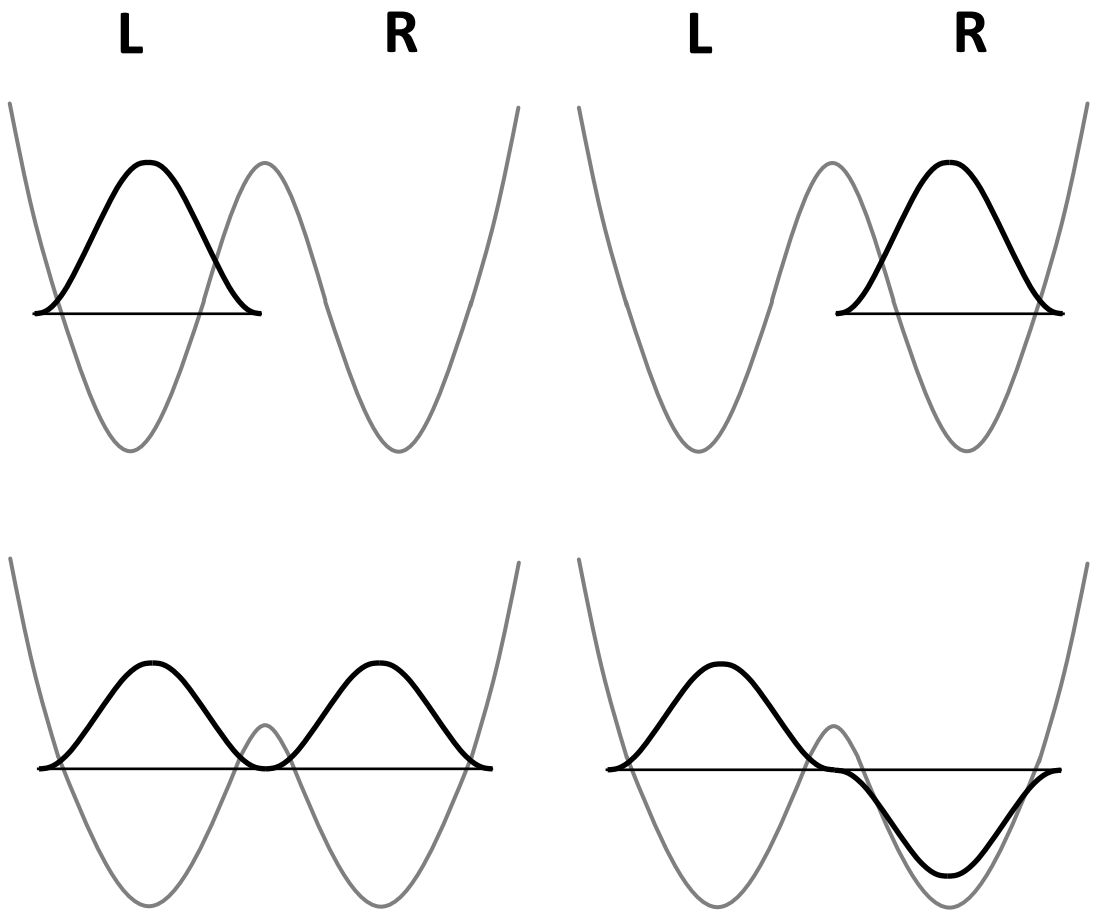
講義内容

- **イントロダクション**
  - 半導体デバイスと量子
  - 量子ドット中の電子の振る舞い
- **量子コンピューティングの基礎**
  - 量子ビットと量子ゲート
  - 量子アルゴリズム
  - 量子コンピューティングの難しさ

DWポテンシャル中の単一電子

(二重井戸)





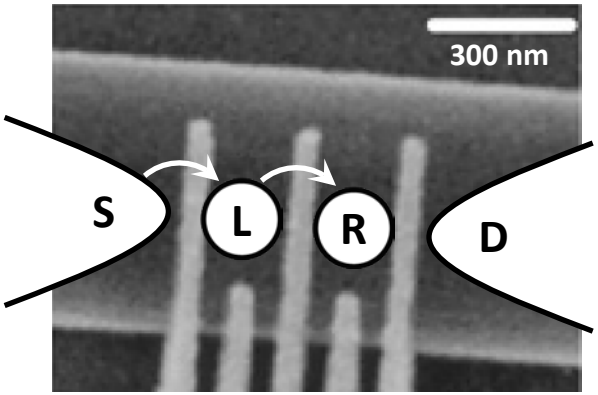
単一電子が2つの量子ドットにまたがって存在してもよい

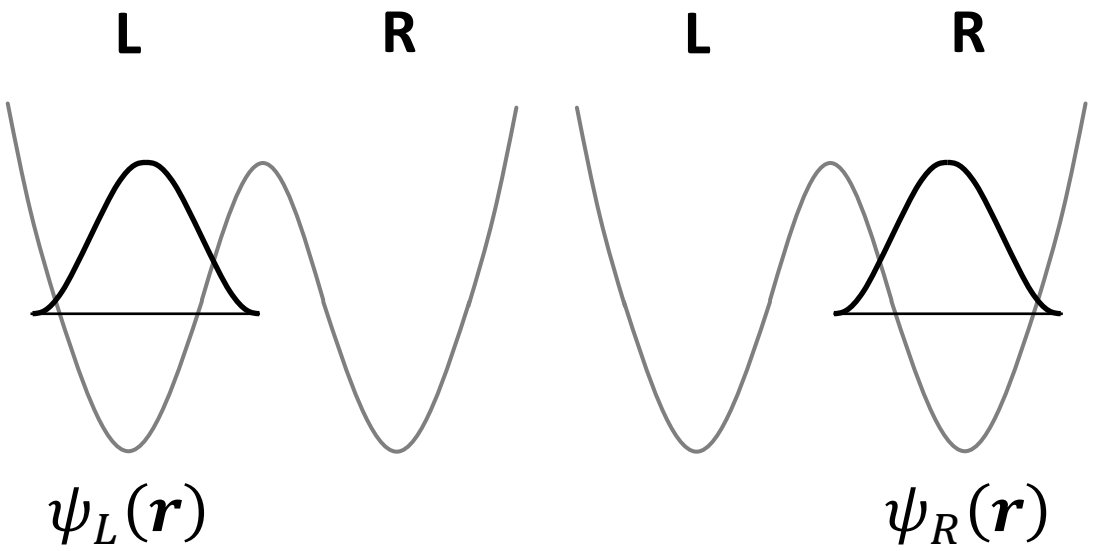
(結合状態・反結合状態)

Rep. Prog. Phys. **69**, 759 (2006) Fujisawa *et al.*

DWポテンシャル中の単一電子

(二重井戸)





規格化条件

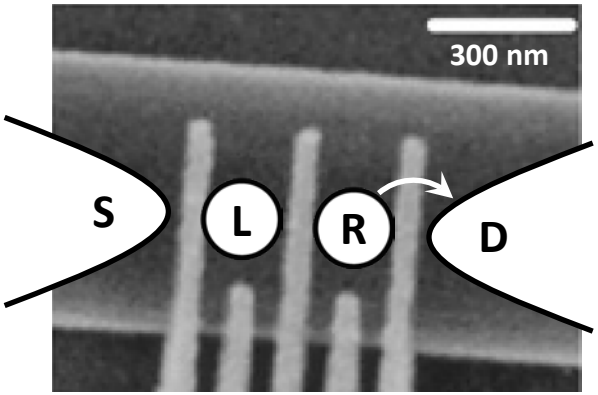
$$\int |\psi_L(\boldsymbol{r})|^2 d\boldsymbol{r} = \int |\psi_R(\boldsymbol{r})|^2 d\boldsymbol{r} = 1$$

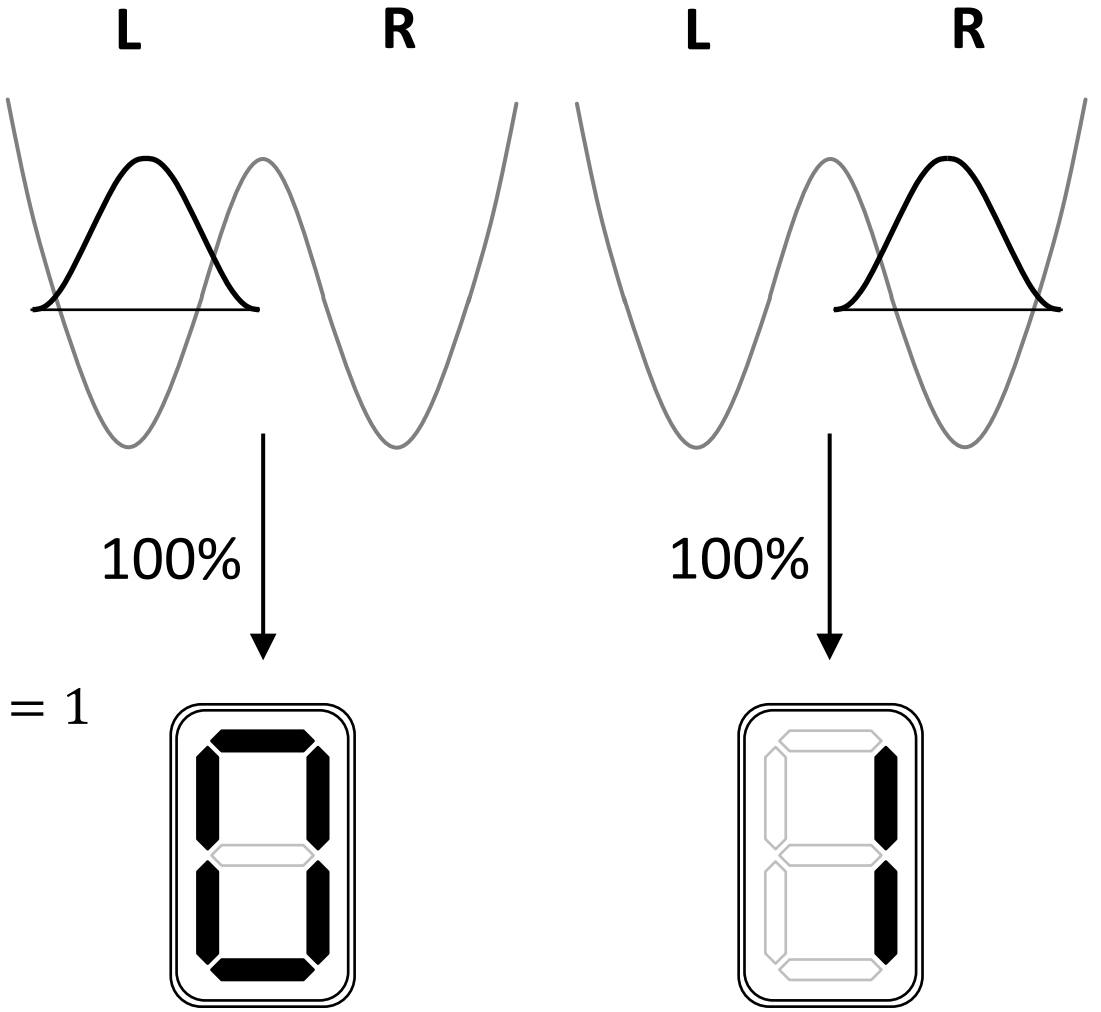
直交性

$$\int \psi_R^*(\boldsymbol{r})\psi_L(\boldsymbol{r}) d\boldsymbol{r} = 0$$

Rep. Prog. Phys. **69**, 759 (2006) Fujisawa *et al.*

電子の居場所を調べる





規格化条件

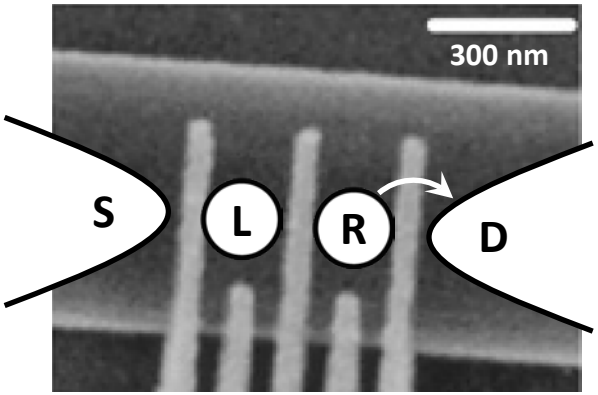
$$\int |\psi_L(\boldsymbol{r})|^2 d\boldsymbol{r} = \int |\psi_R(\boldsymbol{r})|^2 d\boldsymbol{r} = 1$$

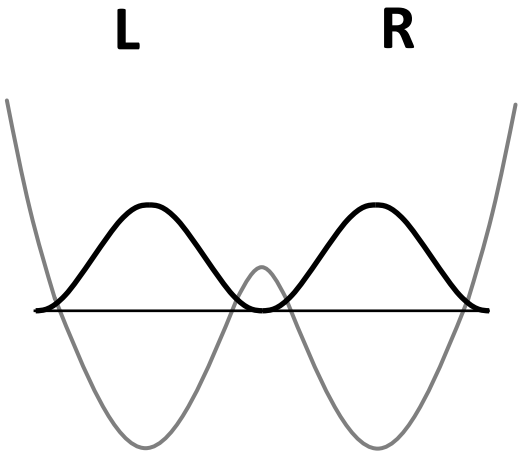
直交性

$$\int \psi_R^*(\boldsymbol{r})\psi_L(\boldsymbol{r}) d\boldsymbol{r} = 0$$

Rep. Prog. Phys. **69**, 759 (2006) Fujisawa *et al.*

電子の居場所を調べる





ボルン則(確率解釈)

$$\left| \int \psi_B^*(\boldsymbol{r}) \psi_L(\boldsymbol{r}) d\boldsymbol{r} \right|^2 = 0.5$$

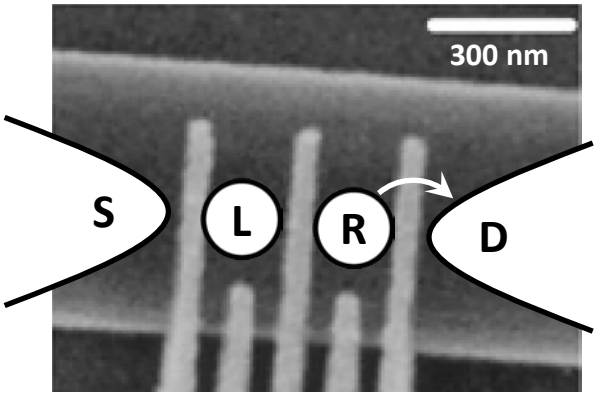
$$\left| \int \psi_B^*(\boldsymbol{r}) \psi_R(\boldsymbol{r}) d\boldsymbol{r} \right|^2 = 0.5$$

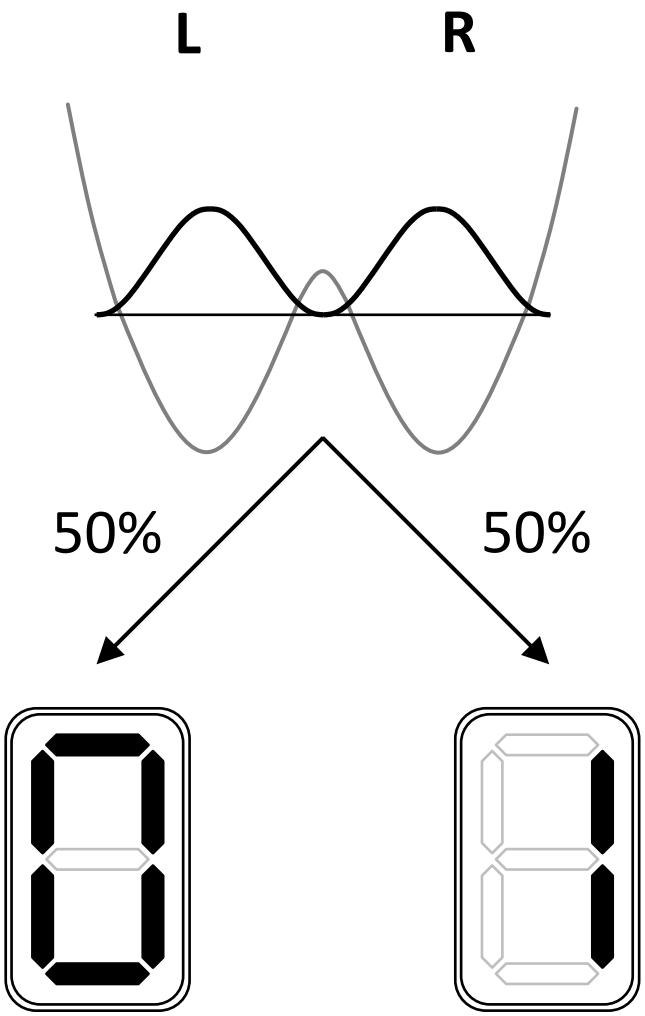
$$\psi_B(\boldsymbol{r}) = \frac{1}{\sqrt{2}} [\psi_L(\boldsymbol{r}) + \psi_R(\boldsymbol{r})]$$

結合状態

Rep. Prog. Phys. **69**, 759 (2006) Fujisawa *et al.*

電子の居場所を調べる





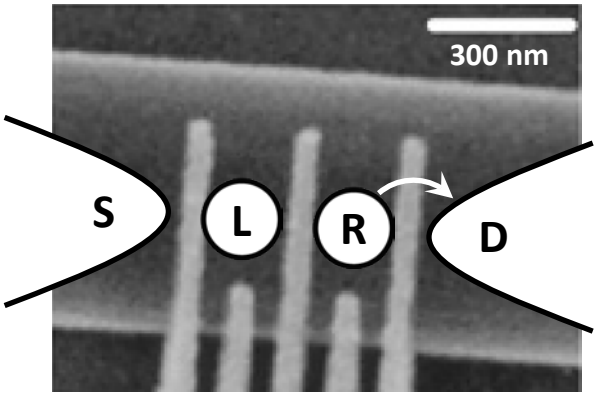
ボルン則(確率解釈)

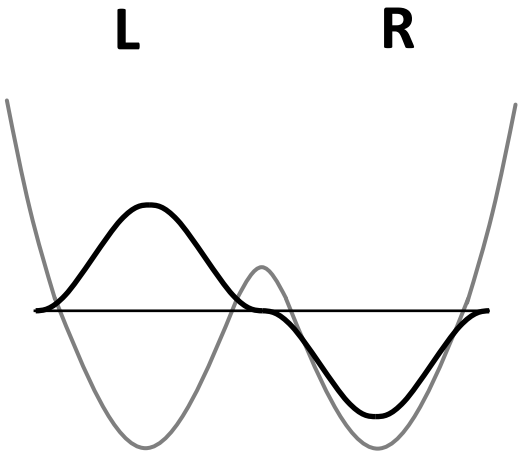
$$\left| \int \psi_B^*(\boldsymbol{r}) \psi_L(\boldsymbol{r}) d\boldsymbol{r} \right|^2 = 0.5$$

$$\left| \int \psi_B^*(\boldsymbol{r}) \psi_R(\boldsymbol{r}) d\boldsymbol{r} \right|^2 = 0.5$$

Rep. Prog. Phys. **69**, 759 (2006) Fujisawa *et al.*

電子の居場所を調べる





ボルン則(確率解釈)

$$\left| \int \psi_A^*(\boldsymbol{r}) \psi_L(\boldsymbol{r}) d\boldsymbol{r} \right|^2 = 0.5$$

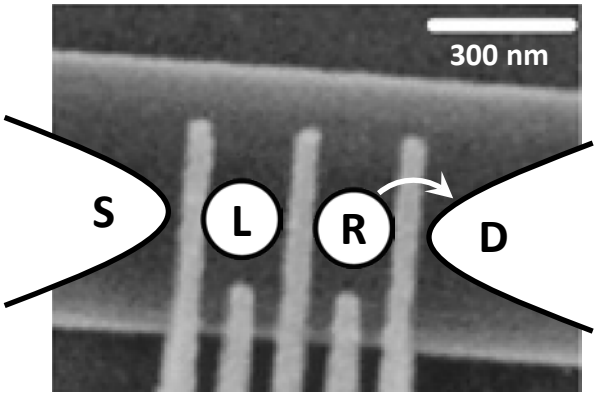
$$\left| \int \psi_A^*(\boldsymbol{r}) \psi_R(\boldsymbol{r}) d\boldsymbol{r} \right|^2 = 0.5$$

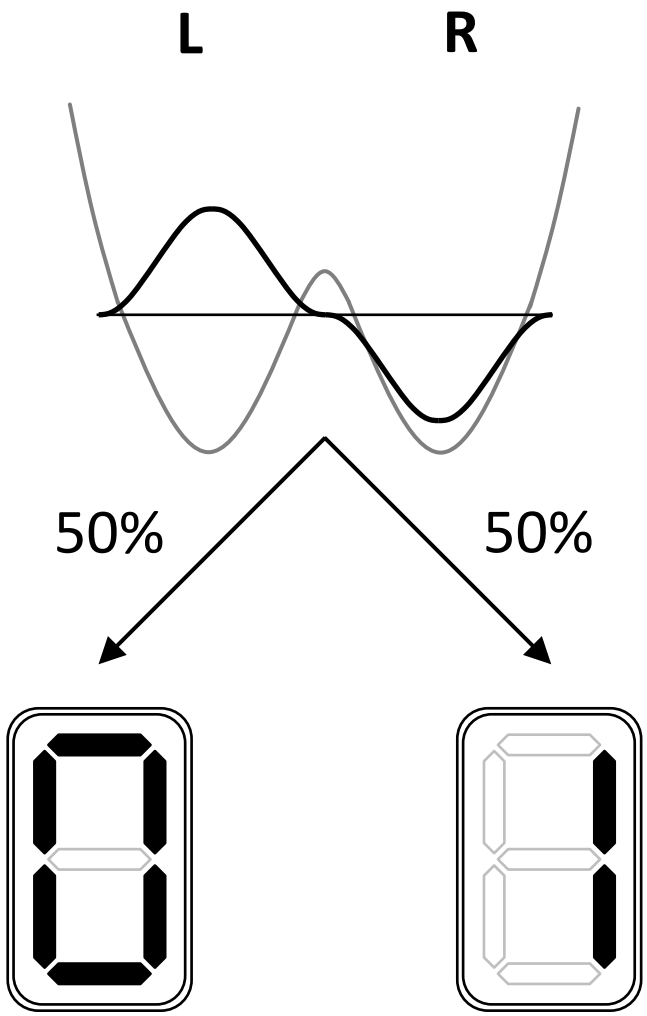
$$\psi_A(\boldsymbol{r}) = \frac{1}{\sqrt{2}} [\psi_L(\boldsymbol{r}) - \psi_R(\boldsymbol{r})]$$

反結合状態

Rep. Prog. Phys. **69**, 759 (2006) Fujisawa *et al.*

電子の居場所を調べる





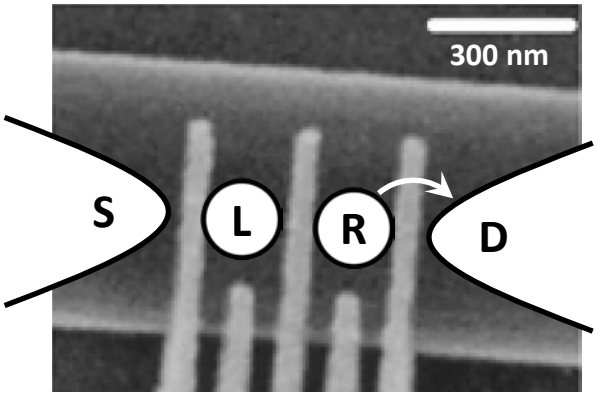
ボルン則(確率解釈)

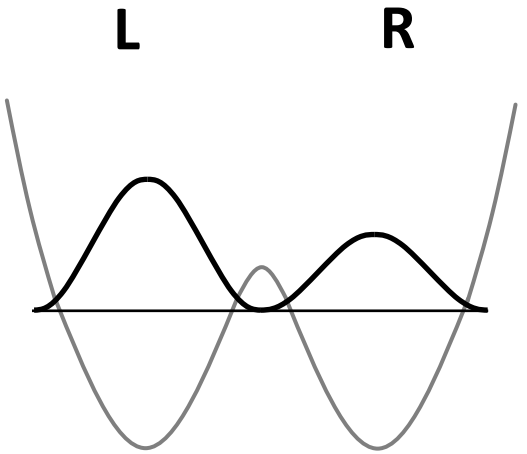
$$\left| \int \psi_A^*(\boldsymbol{r}) \psi_L(\boldsymbol{r}) d\boldsymbol{r} \right|^2 = 0.5$$

$$\left| \int \psi_A^*(\boldsymbol{r}) \psi_R(\boldsymbol{r}) d\boldsymbol{r} \right|^2 = 0.5$$

Rep. Prog. Phys. **69**, 759 (2006) Fujisawa *et al.*

電子の居場所を調べる





$$\psi(\boldsymbol{r}) = \frac{\sqrt{3}}{2}\psi_L(\boldsymbol{r}) + \frac{1}{2}\psi_R(\boldsymbol{r})$$

重ね合わせ状態

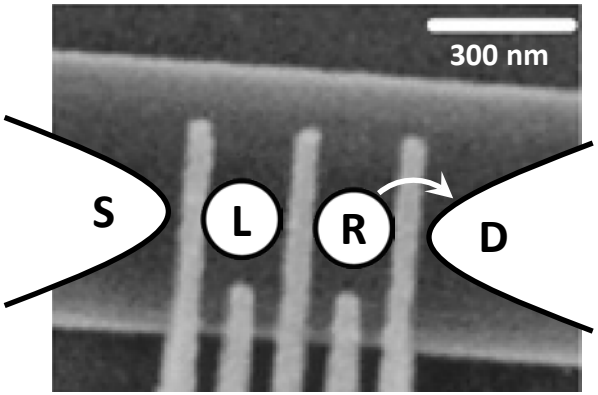
ボルン則(確率解釈)

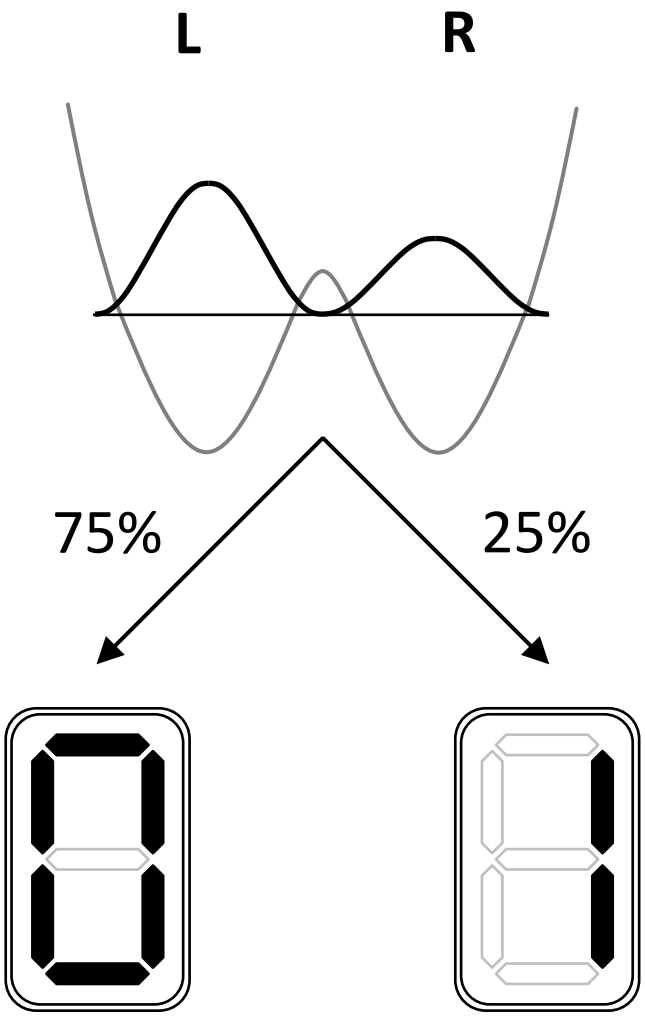
$$\left|\int \psi^*(\boldsymbol{r})\psi_L(\boldsymbol{r})d\boldsymbol{r}\right|^2 = 0.75$$

$$\left|\int \psi^*(\boldsymbol{r})\psi_R(\boldsymbol{r})d\boldsymbol{r}\right|^2 = 0.25$$

Rep. Prog. Phys. **69**, 759 (2006) Fujisawa *et al.*

電子の居場所を調べる





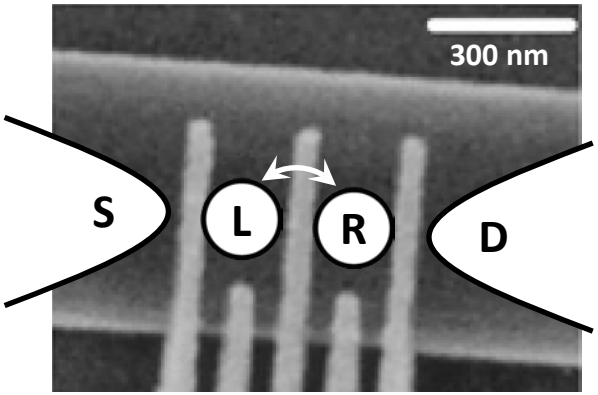
ボルン則(確率解釈)

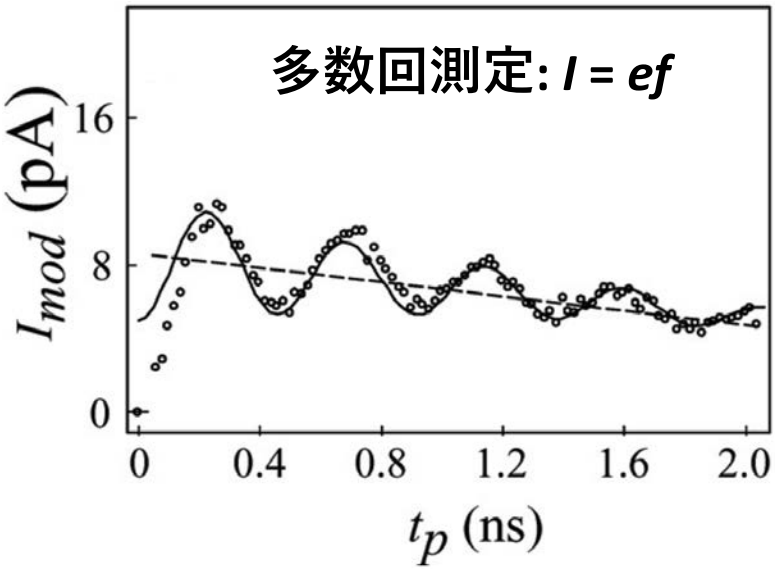
$$\left| \int \psi^*(\boldsymbol{r}) \psi_L(\boldsymbol{r}) d\boldsymbol{r} \right|^2 = 0.75$$

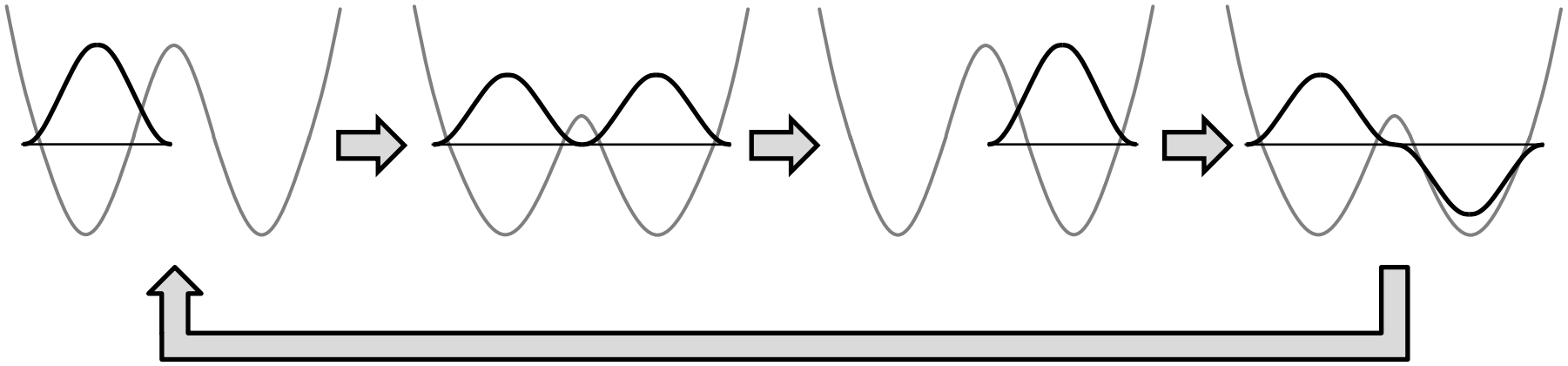
$$\left| \int \psi^*(\boldsymbol{r}) \psi_R(\boldsymbol{r}) d\boldsymbol{r} \right|^2 = 0.25$$

Rep. Prog. Phys. **69**, 759 (2006) Fujisawa *et al.*

電子の居場所を調べる







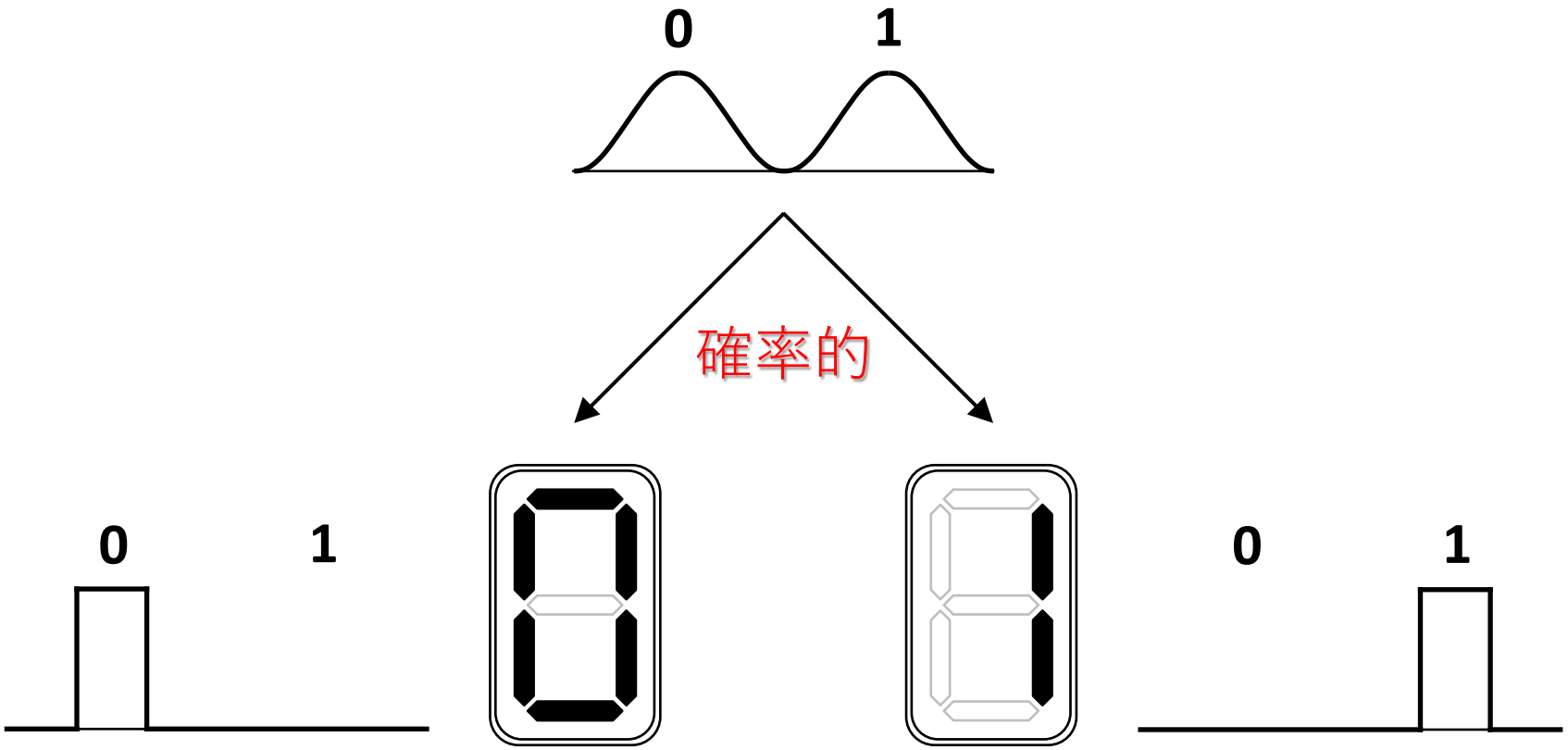
Rep. Prog. Phys. **69**, 759 (2006) Fujisawa *et al.*

講義内容

- **イントロダクション**
  - 半導体デバイスと量子
  - 量子ドット中の電子の振る舞い
- **量子コンピューティングの基礎**
  - 量子ビットと量子ゲート
  - 量子アルゴリズム
  - 量子コンピューティングの難しさ

量子ビット

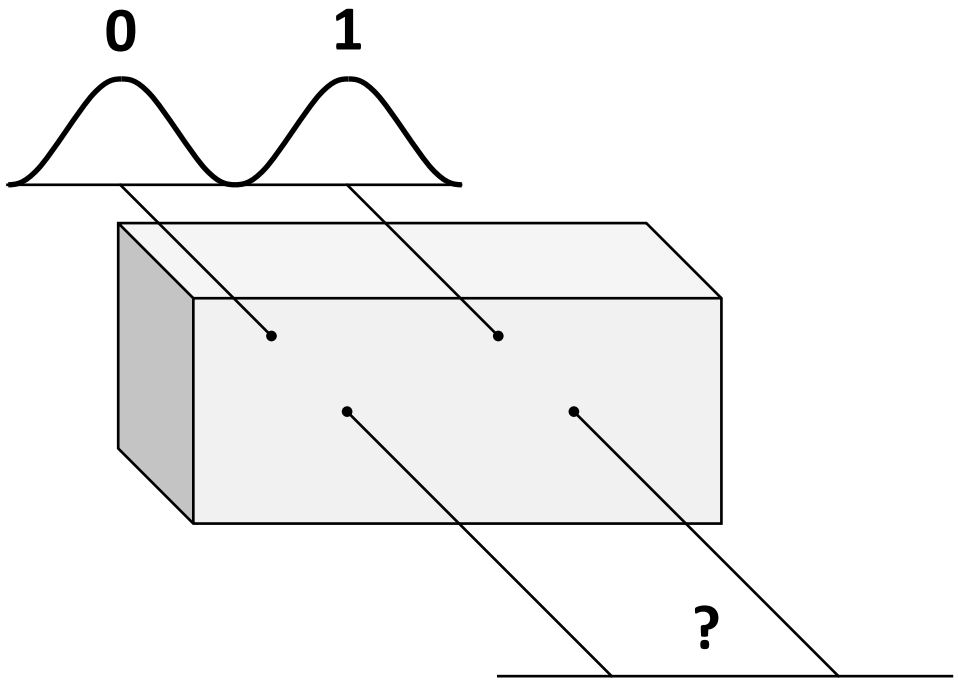
電子の波としての性質を計算に用いることができないか?



ただし“測定”によって電子の位置は確定する(局在 = 粒子)

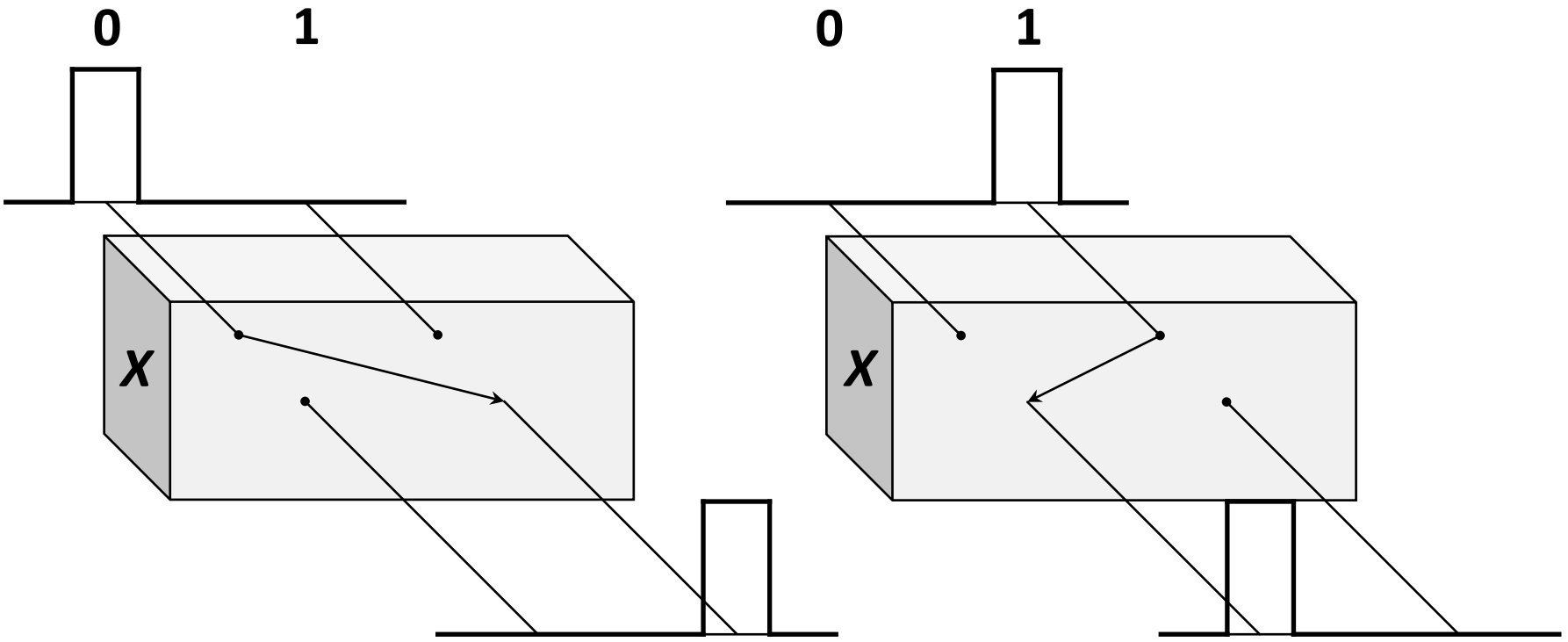
量子ビット

ビットがあるだけでは計算はできない



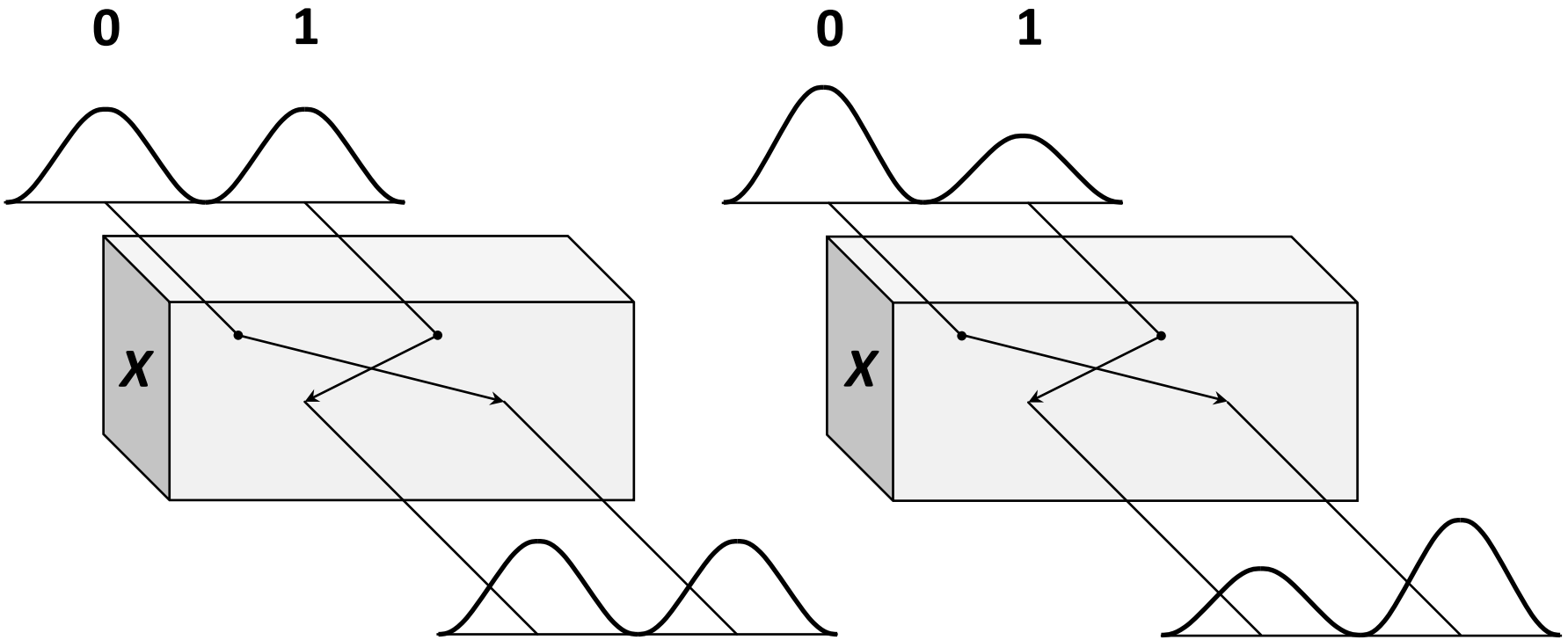
量子ビットに対して可能な演算(ゲート)とは?

Xゲート(NOT)



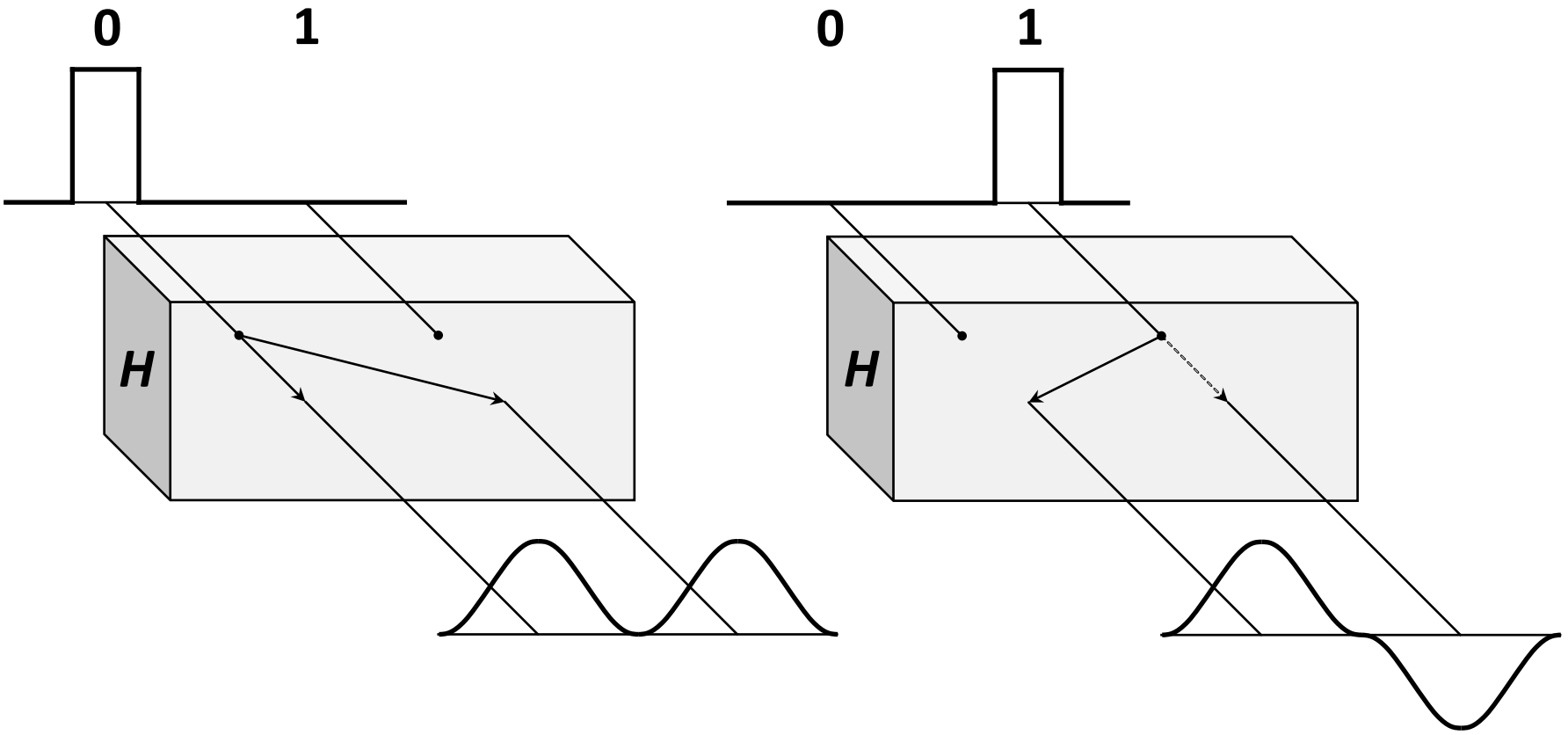
古典計算で1ビットに可能な演算はNOTだけ

*X*ゲート(NOT)

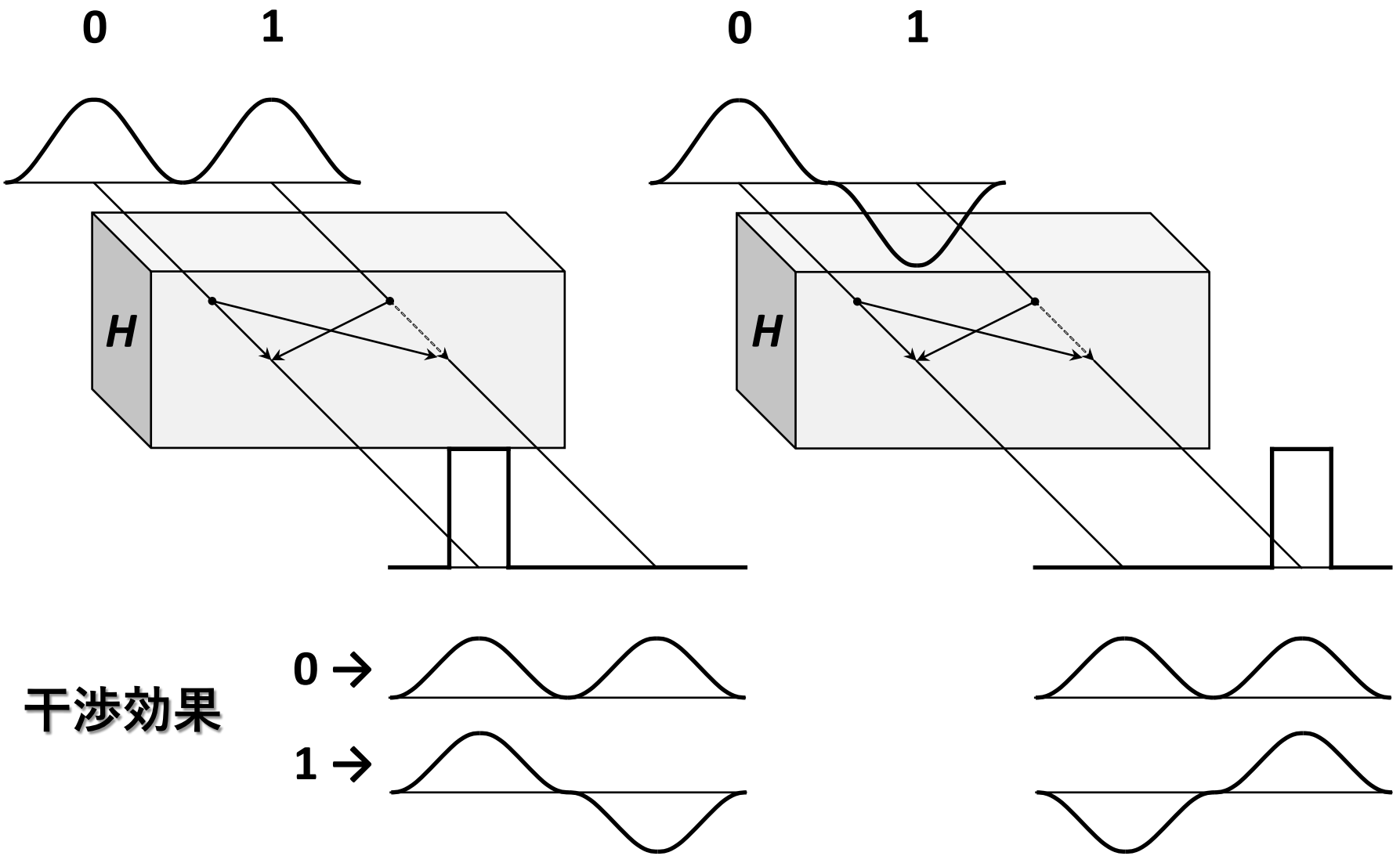


処理内容は同じだが重ね合わせ状態を入力できる

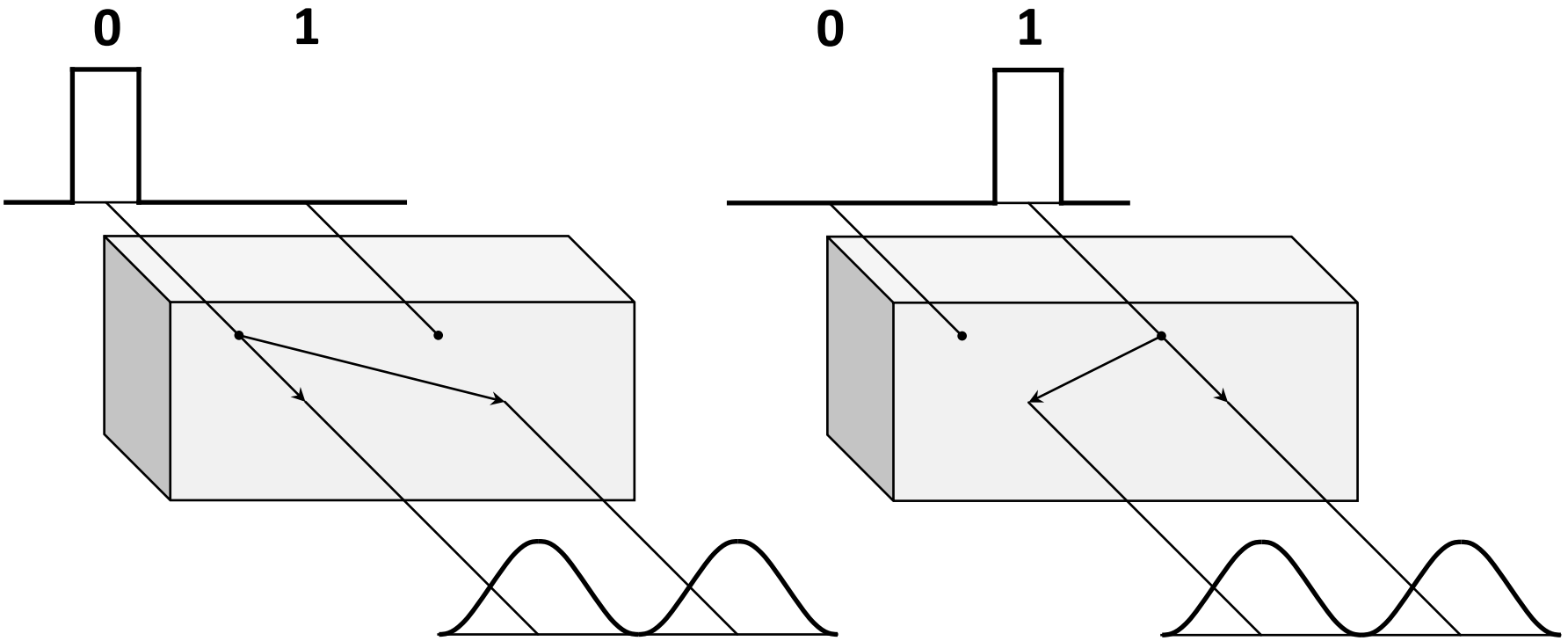
*H*ゲート



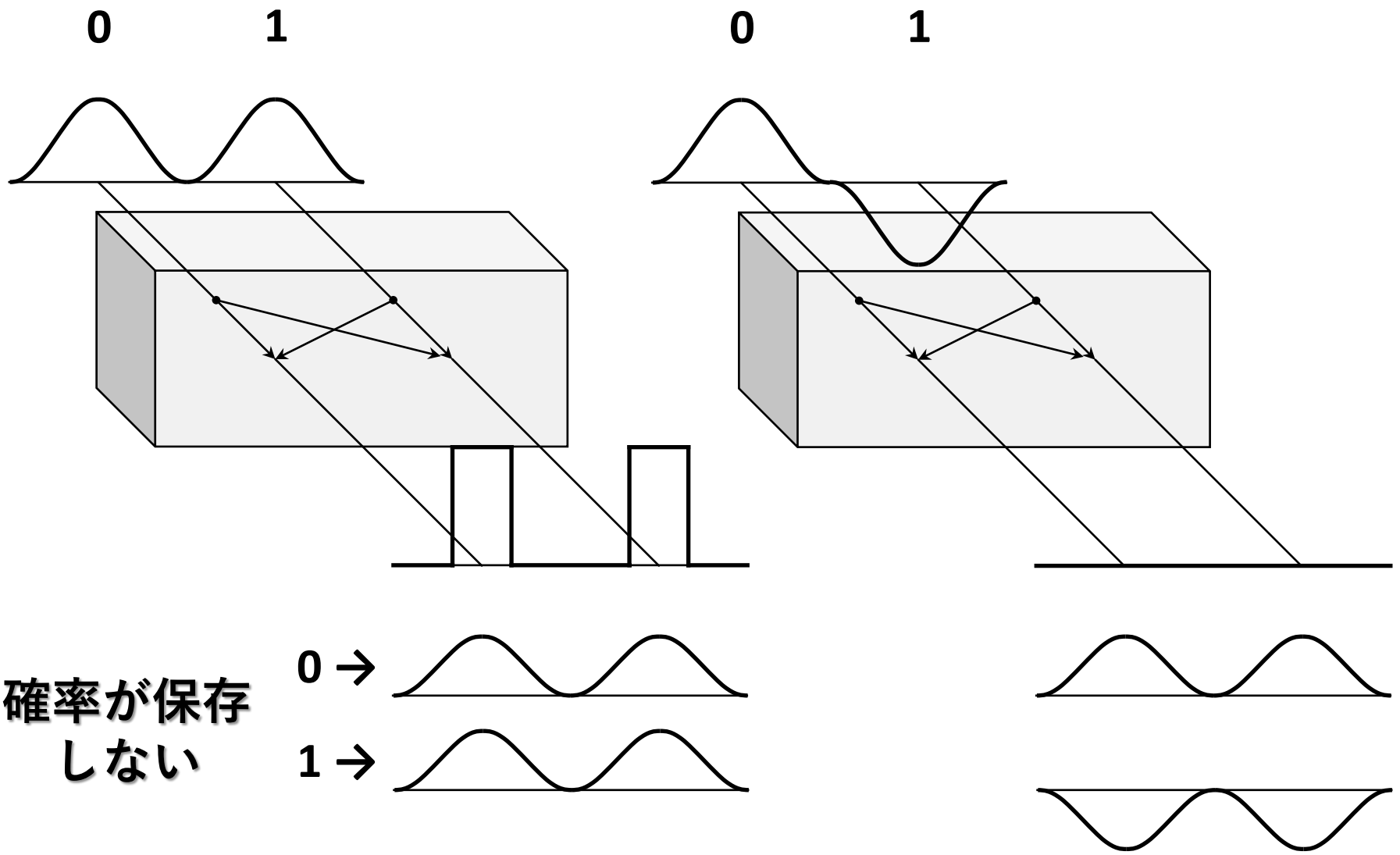
*H*ゲート



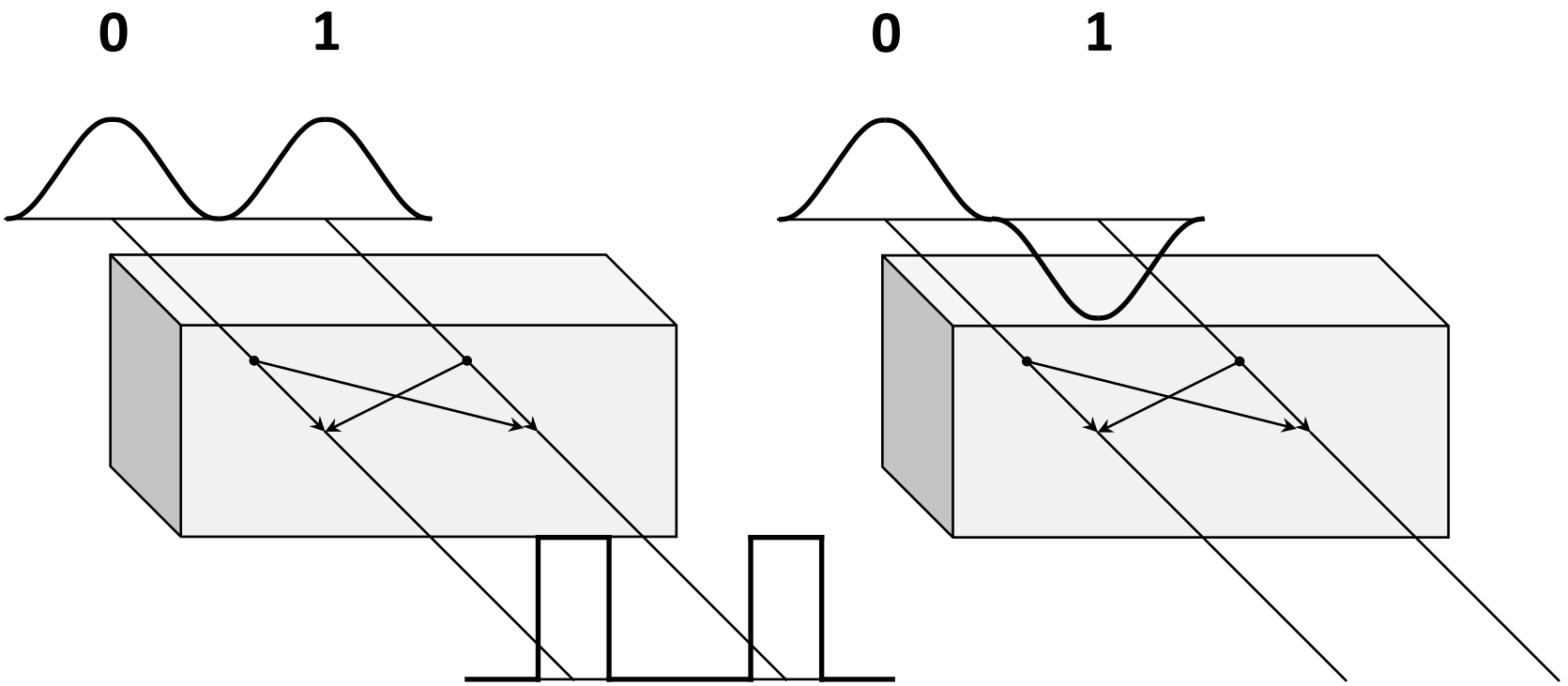
実現できないゲート



実現できないゲート



実現できないゲート

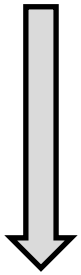


量子力学のルールに従って実現可能なゲートを
ユニタリゲートと呼ぶ(*X*, *H*…)

量子ビット

ベクトル表示

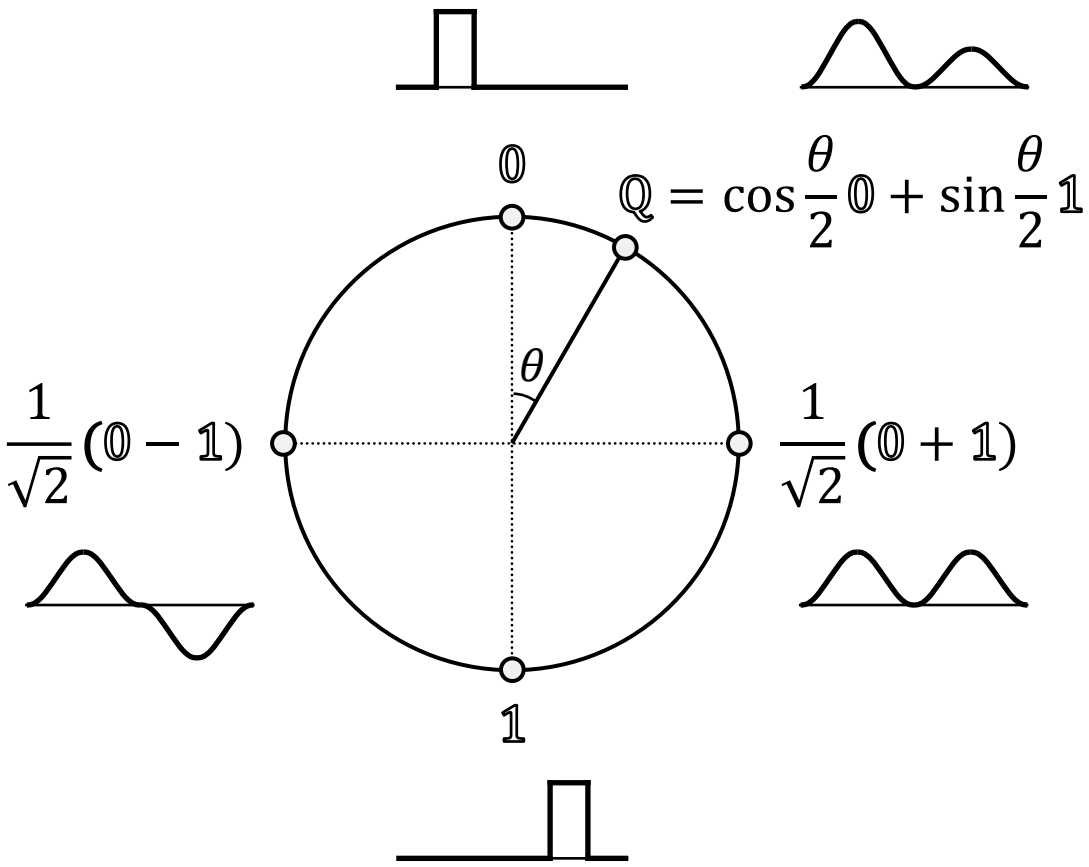
$$\mathbb{0} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \mathbb{1} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$



重ね合わせ状態

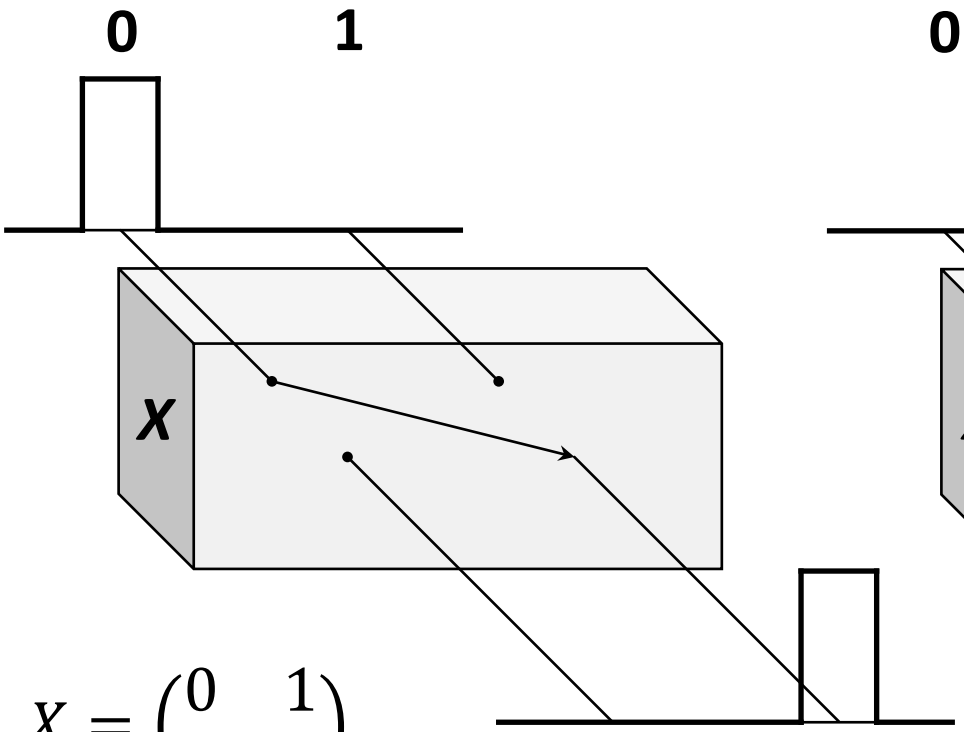
$$\mathbb{Q} = a\,\mathbb{0} + b\,\mathbb{1} = \begin{pmatrix} a \\ b \end{pmatrix}$$

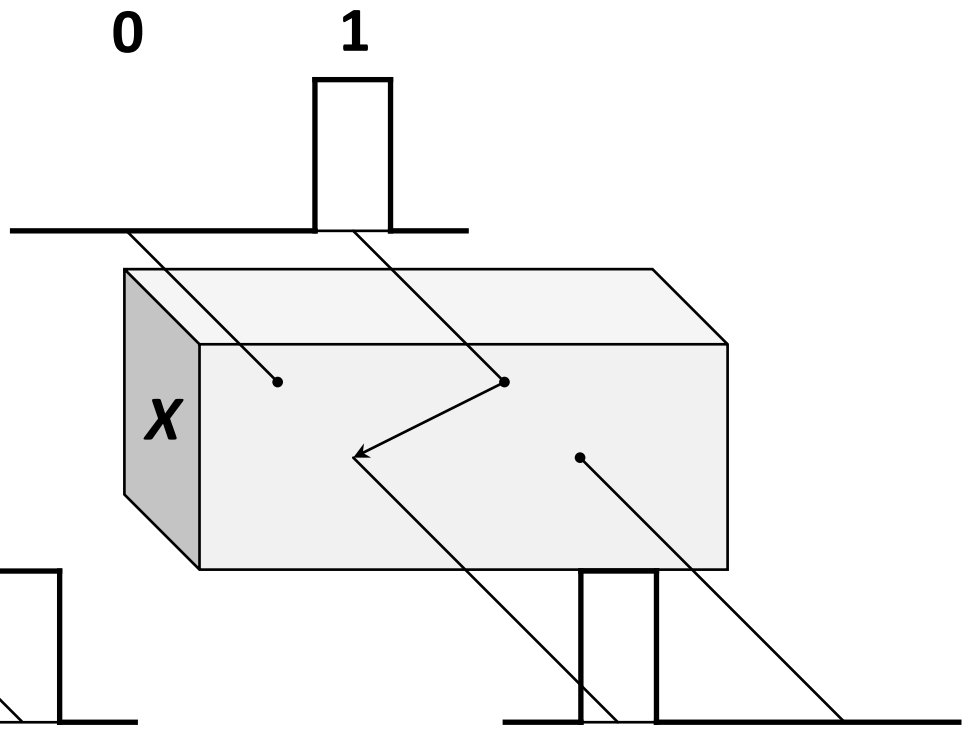
$$|a|^2 + |b|^2 = 1$$



厳密に言うと$\mathbb{0}$, $\mathbb{1}$を特別な点とみなすことは正しくないがここでは気にしない

量子ビット



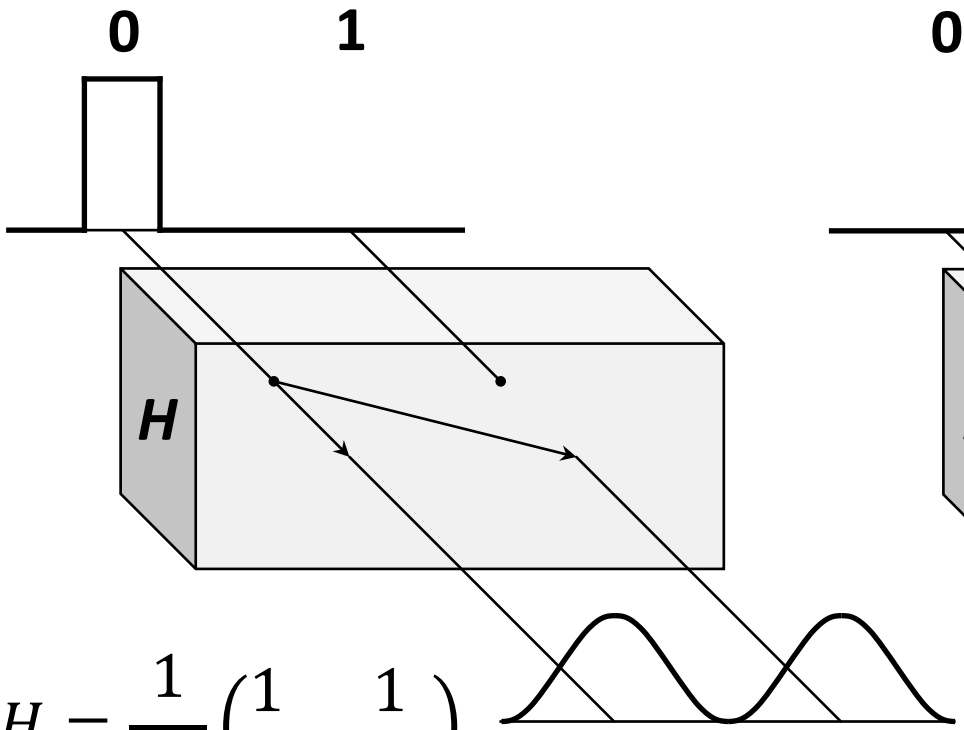


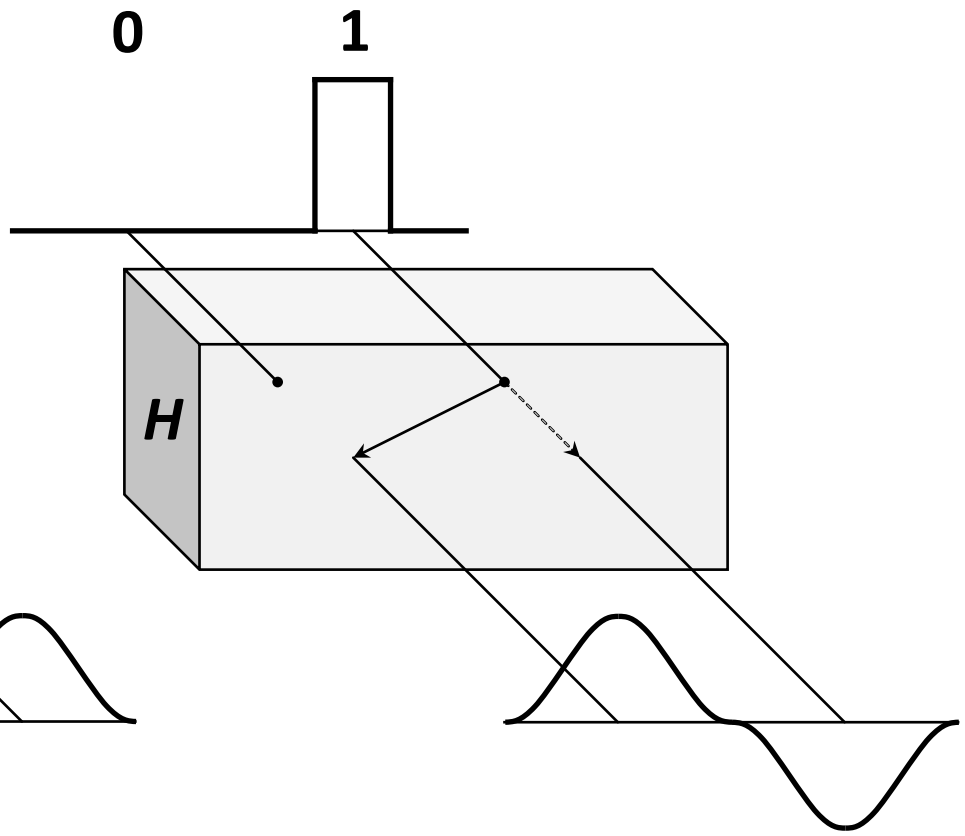
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$X\mathbb{0} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \mathbb{1} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$X\mathbb{1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \mathbb{0} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Hゲート



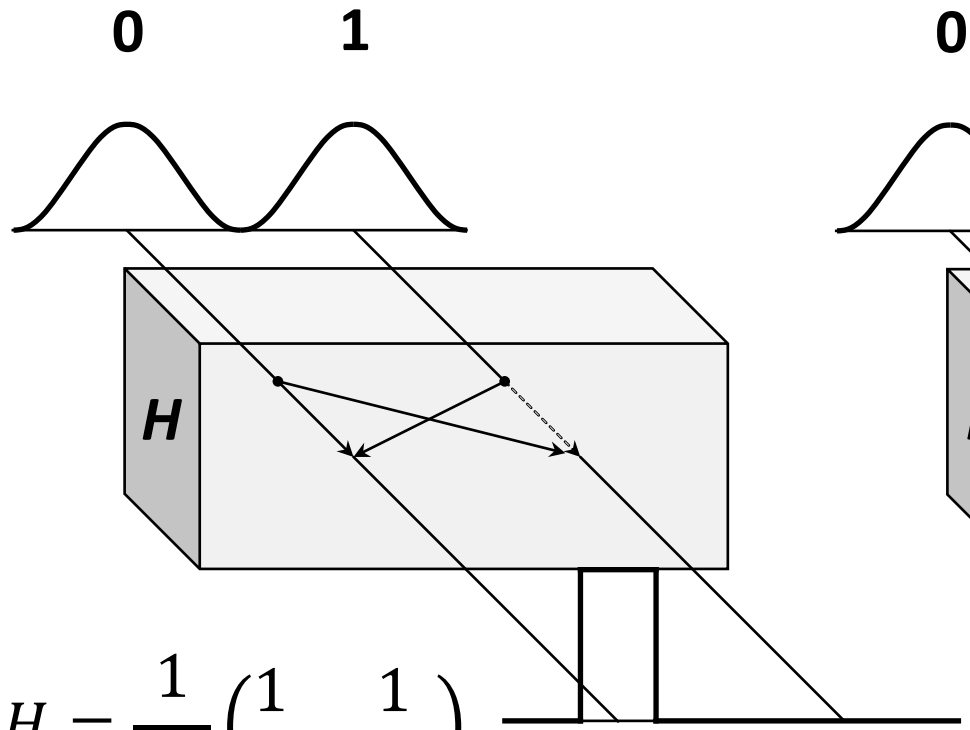


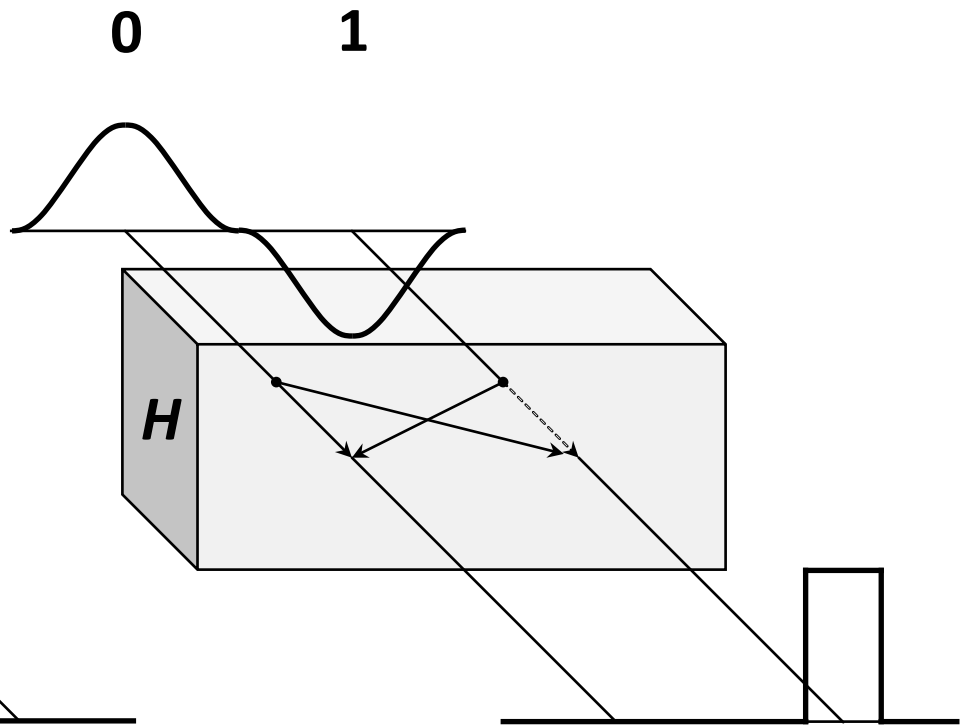
$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

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

Hゲート

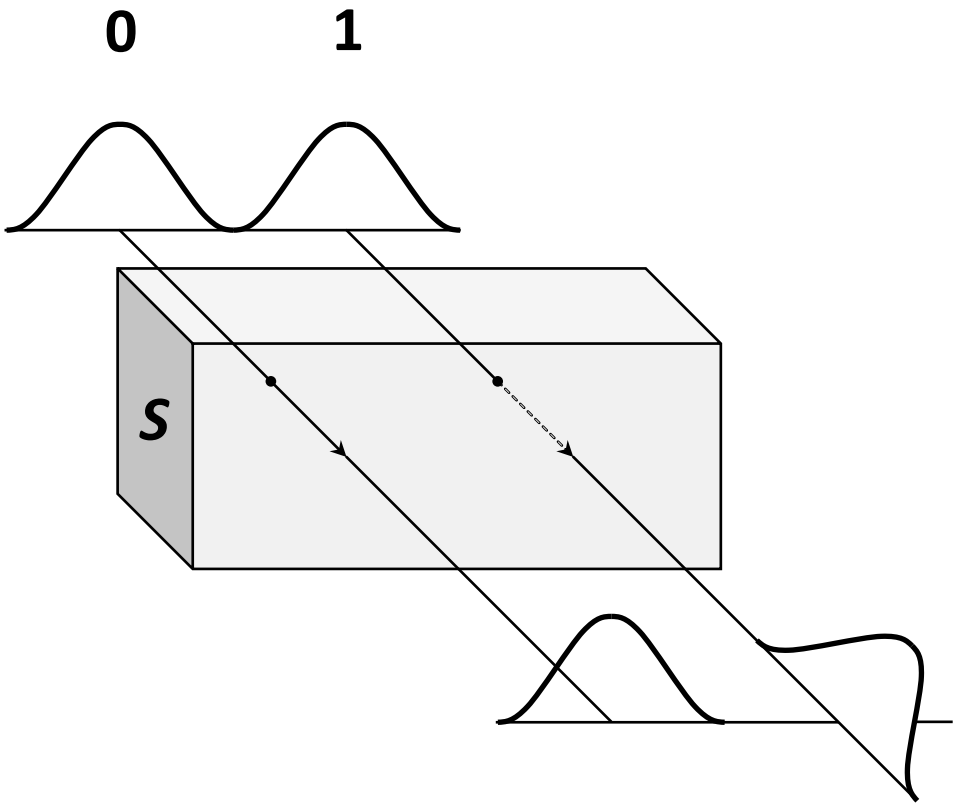




$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H\frac{1}{\sqrt{2}}(\mathbb{0} \pm \mathbb{1}) = \frac{1}{2}(\mathbb{0} + \mathbb{1} \pm \mathbb{0} \mp \mathbb{1}) = \begin{cases} \mathbb{0} \\ \mathbb{1} \end{cases}$$

Sゲート



$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

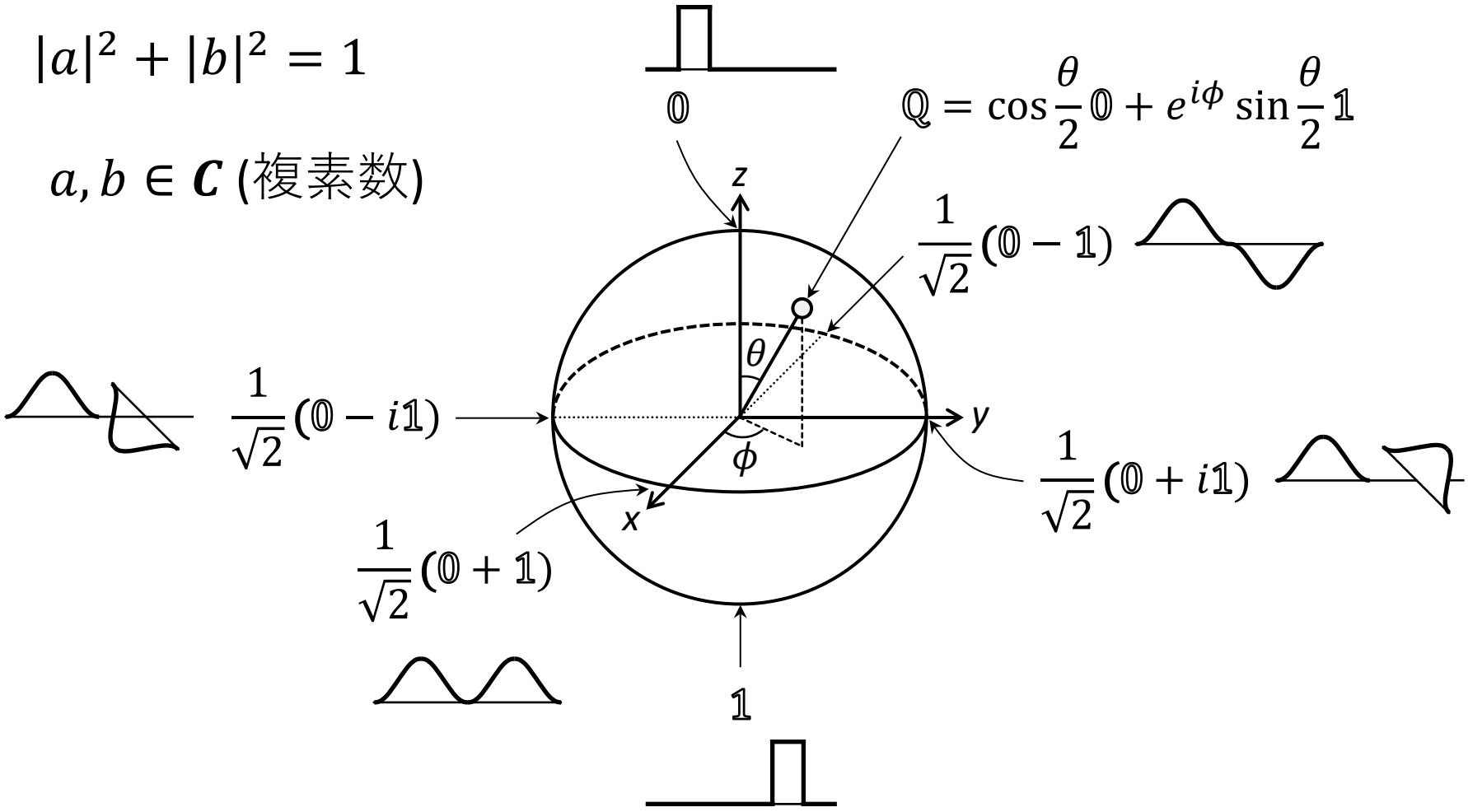
$$S\frac{1}{\sqrt{2}}(\mathbb{0} + \mathbb{1}) = \frac{1}{\sqrt{2}}(\mathbb{0} + i\mathbb{1})$$

ひっくり返すだけが位相ではない

量子ビット(ブロッホ球)

$|a|^2 + |b|^2 = 1$

$a, b \in \boldsymbol{C}$ (複素数)



2量子ビット

2量子ビットの状態の記述

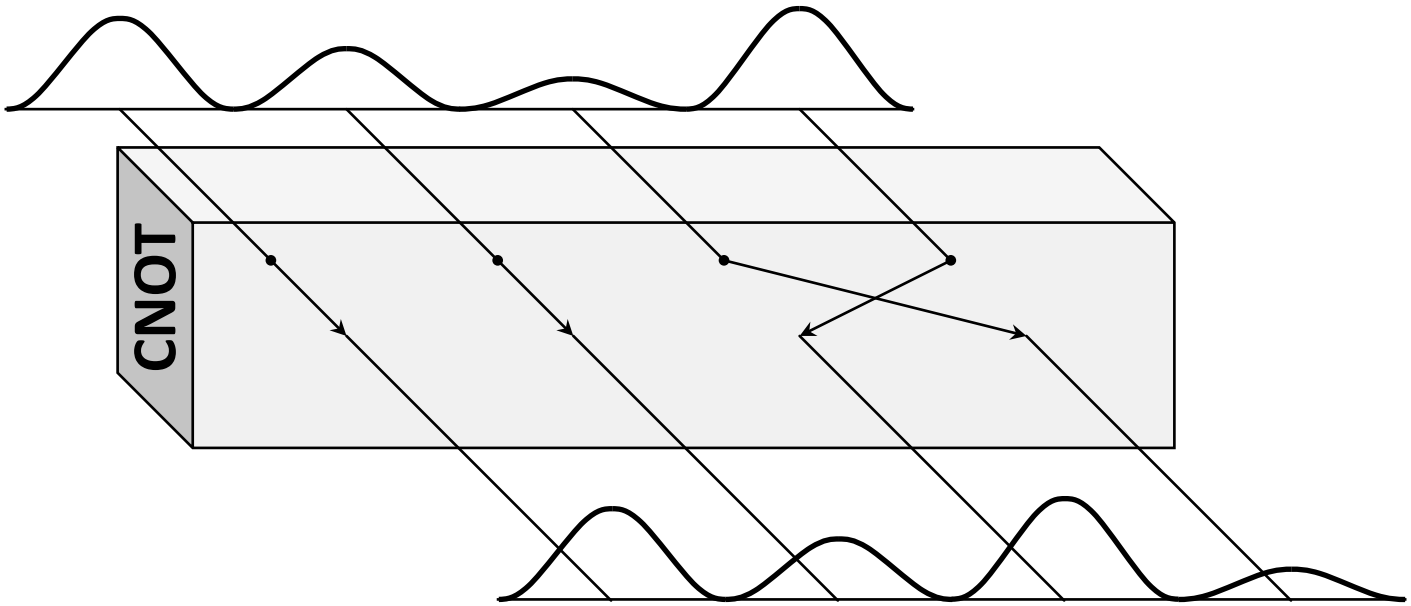
$$\mathbb{00} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \mathbb{01} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \mathbb{10} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \mathbb{11} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\mathbb{Q} = a\,\mathbb{00} + b\,\mathbb{01} + c\,\mathbb{10} + d\,\mathbb{11} = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$$

CNOTゲート

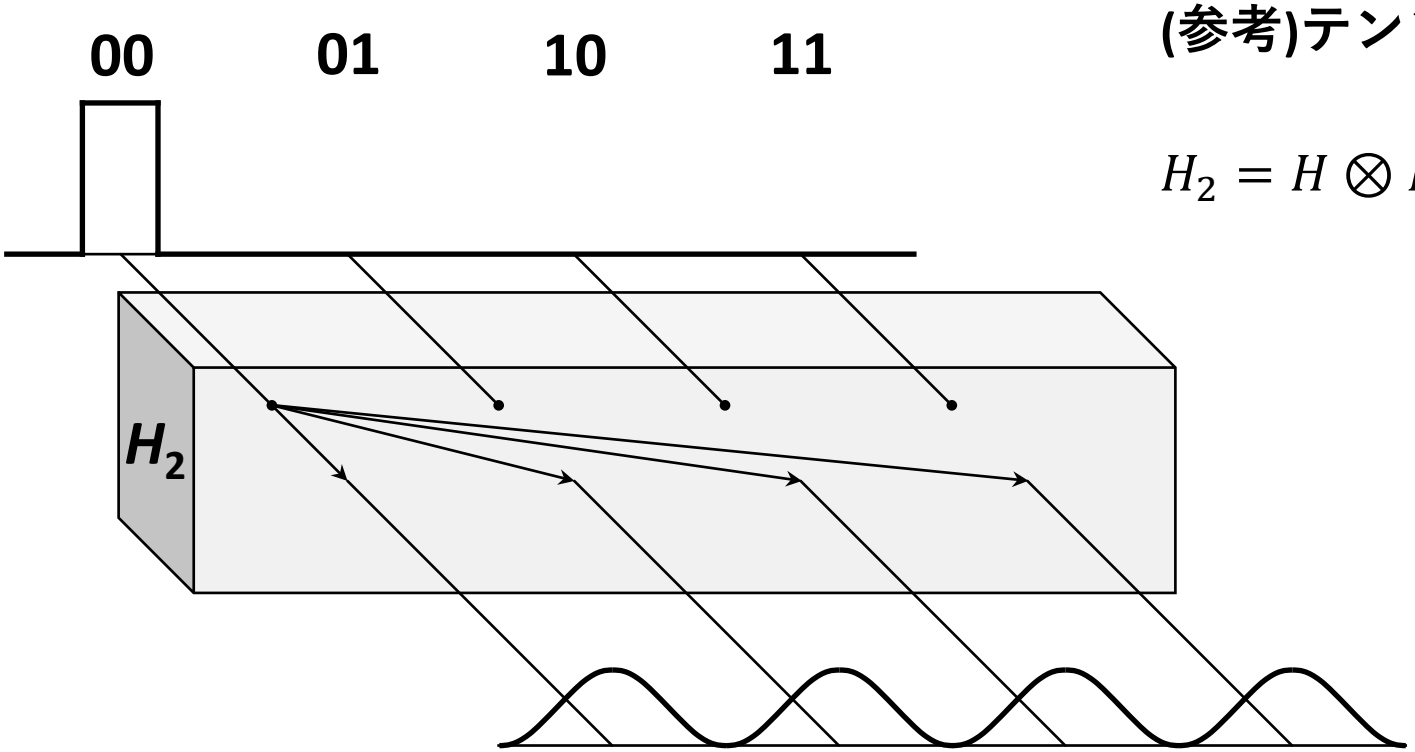
1番目のビットの値に応じて
2番目のビットをNOT



$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathrm{CNOT} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ d \\ c \end{pmatrix}$$

H_2ゲート



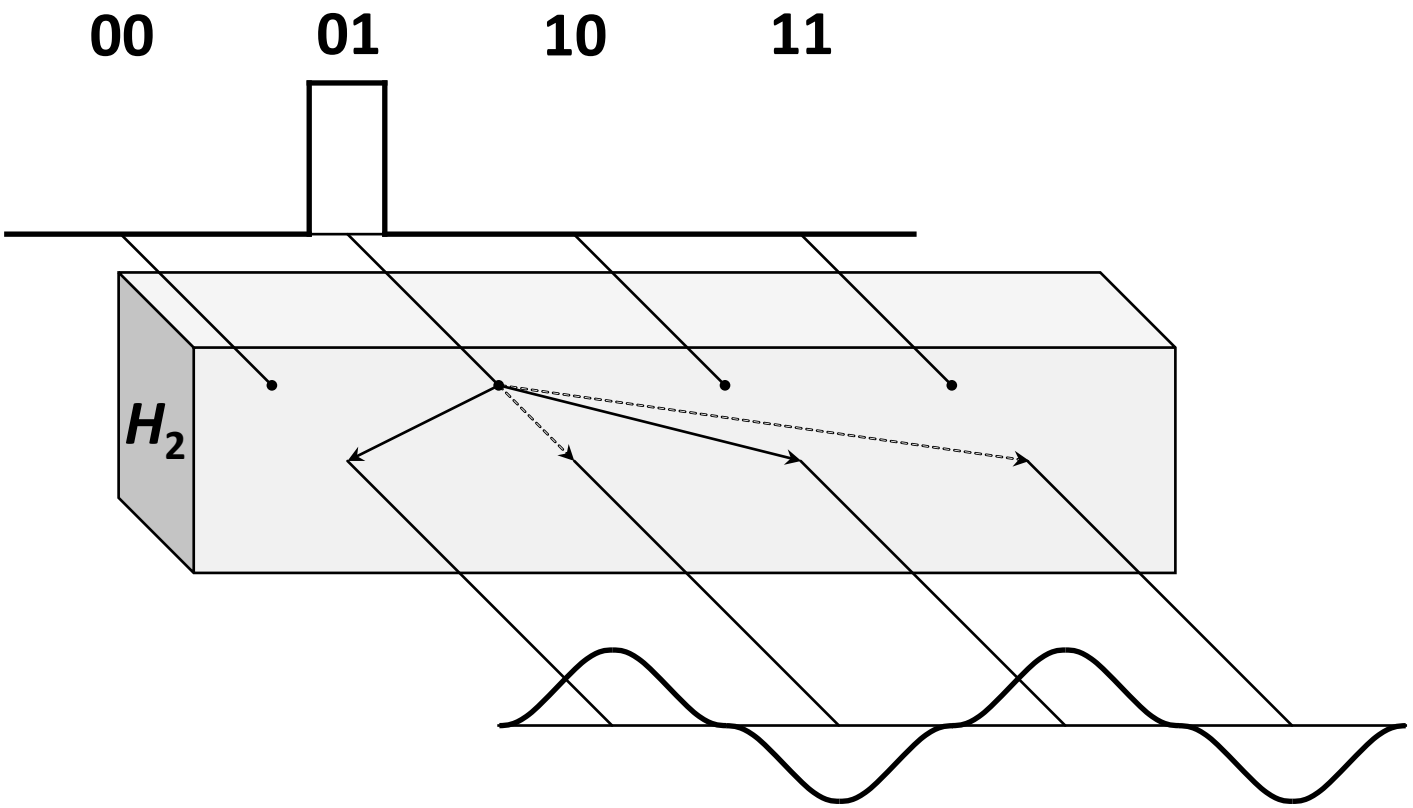
(参考)テンソル積

$$H_2 = H \otimes H = \frac{1}{\sqrt{2}}\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$$

$$H_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_2 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

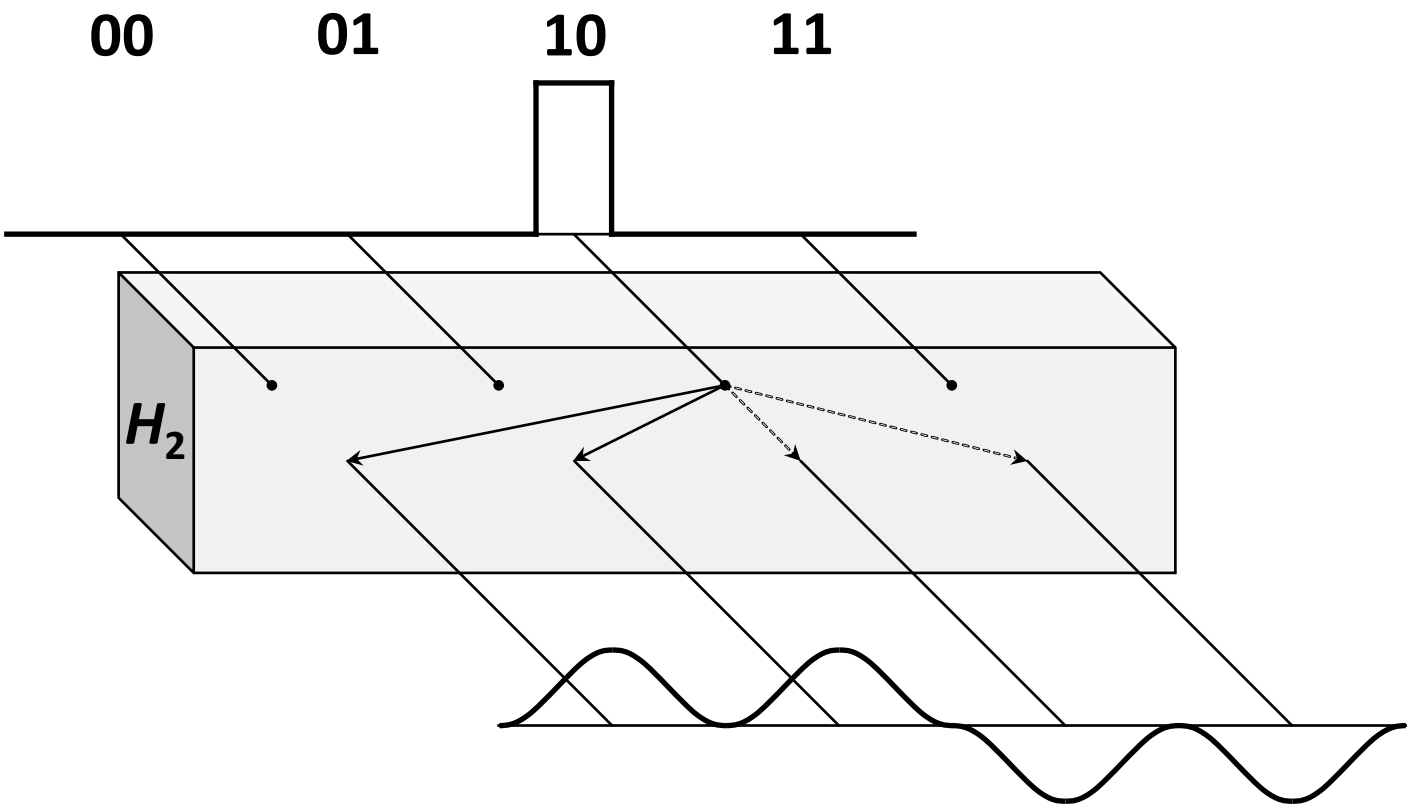
H_2ゲート



$$H_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

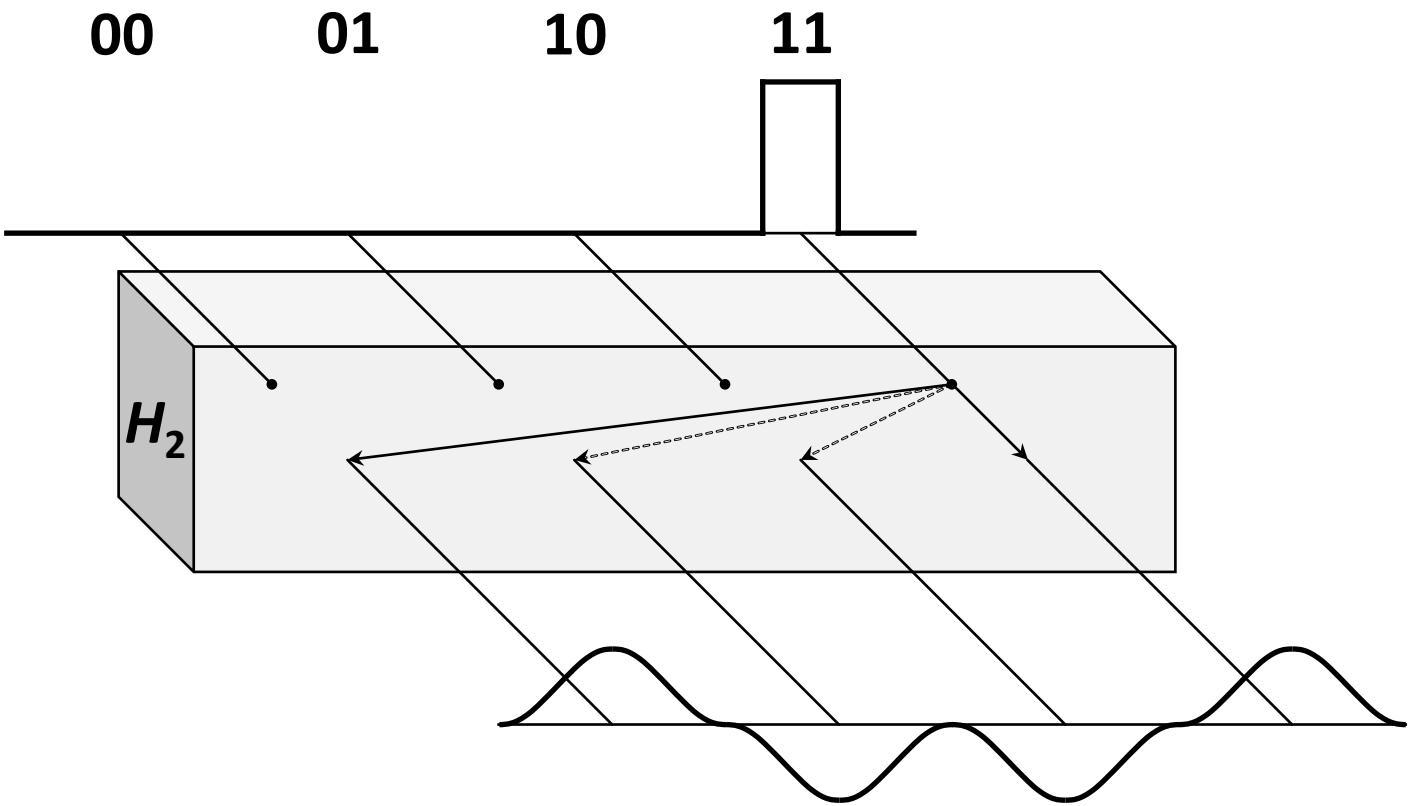
H_2ゲート



$$H_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}$$

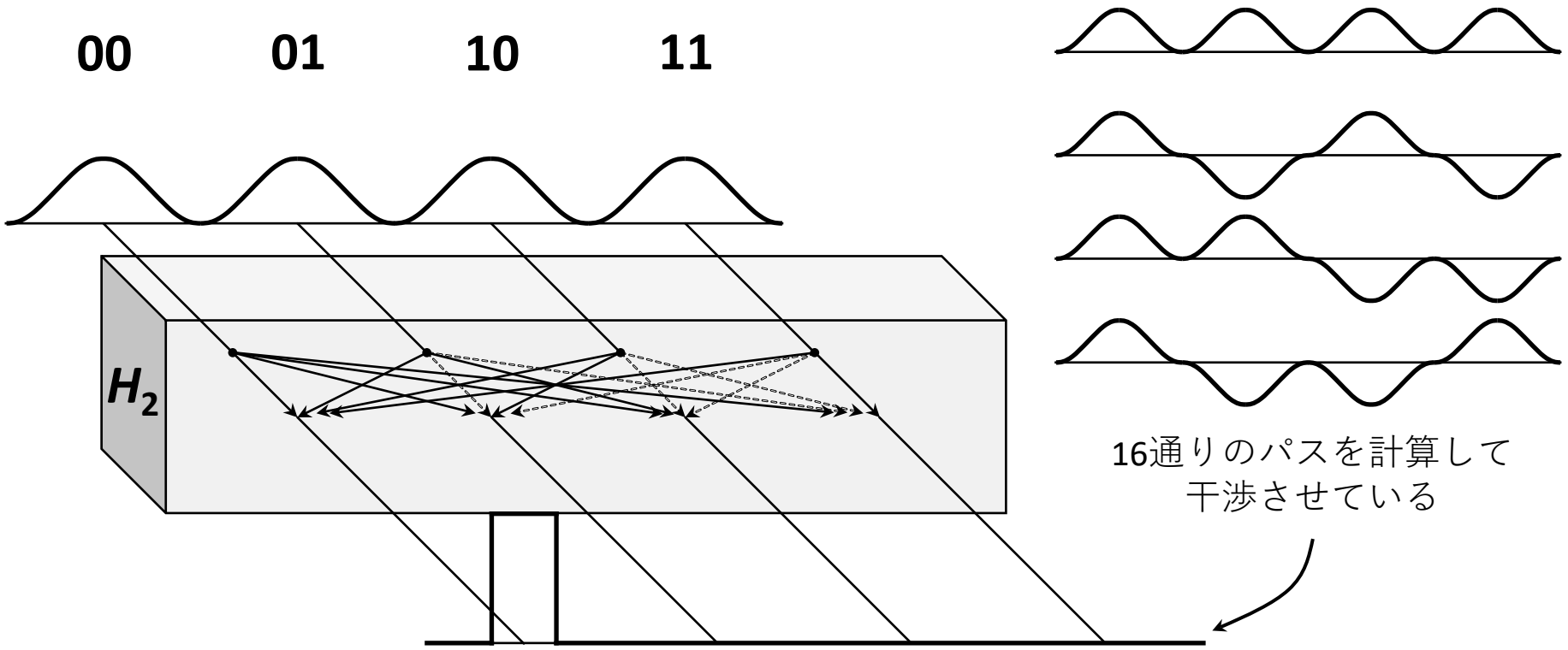
H_2ゲート



$$H_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_2 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}$$

H_2ゲート



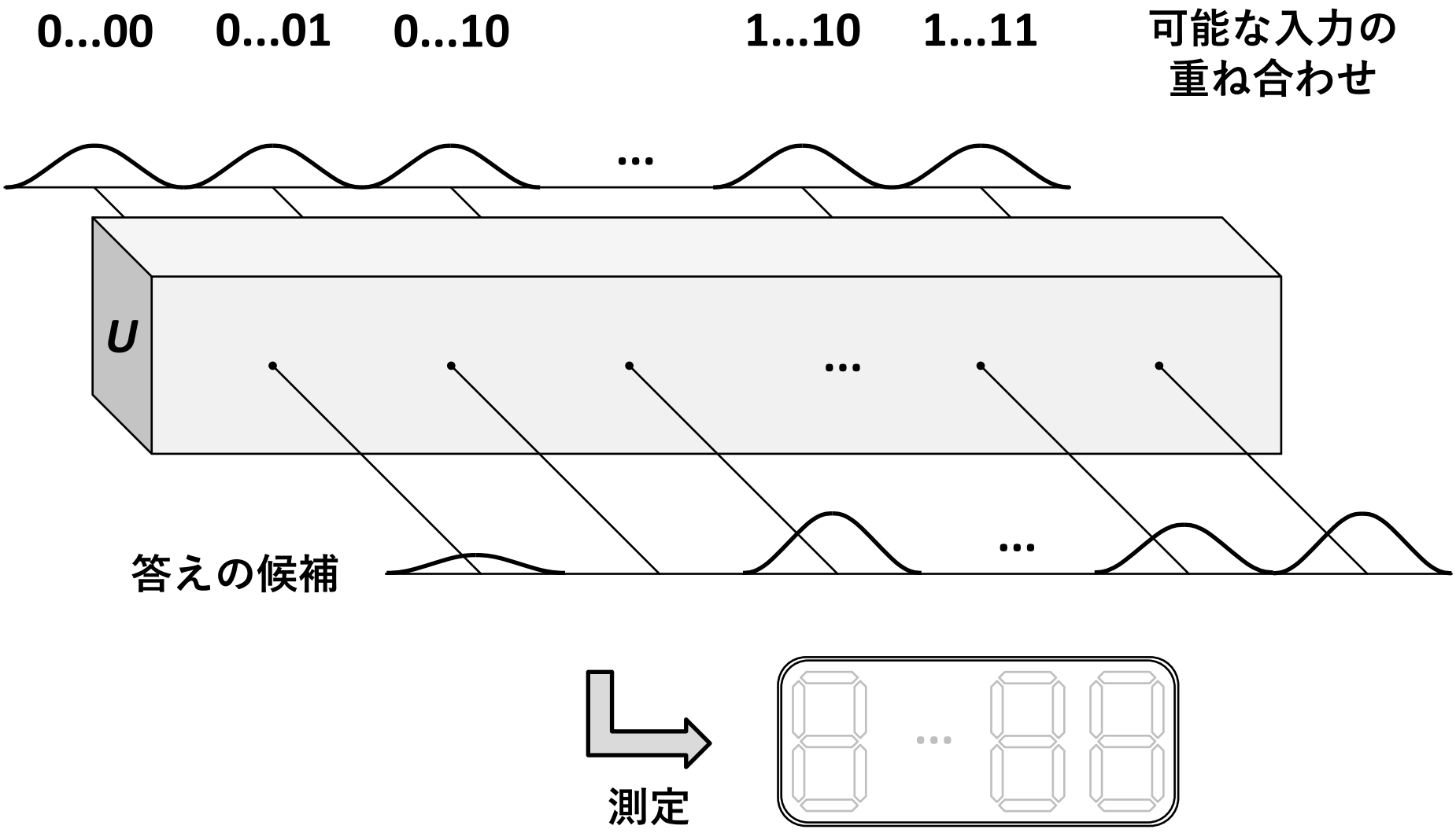
$$H_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H_2 \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

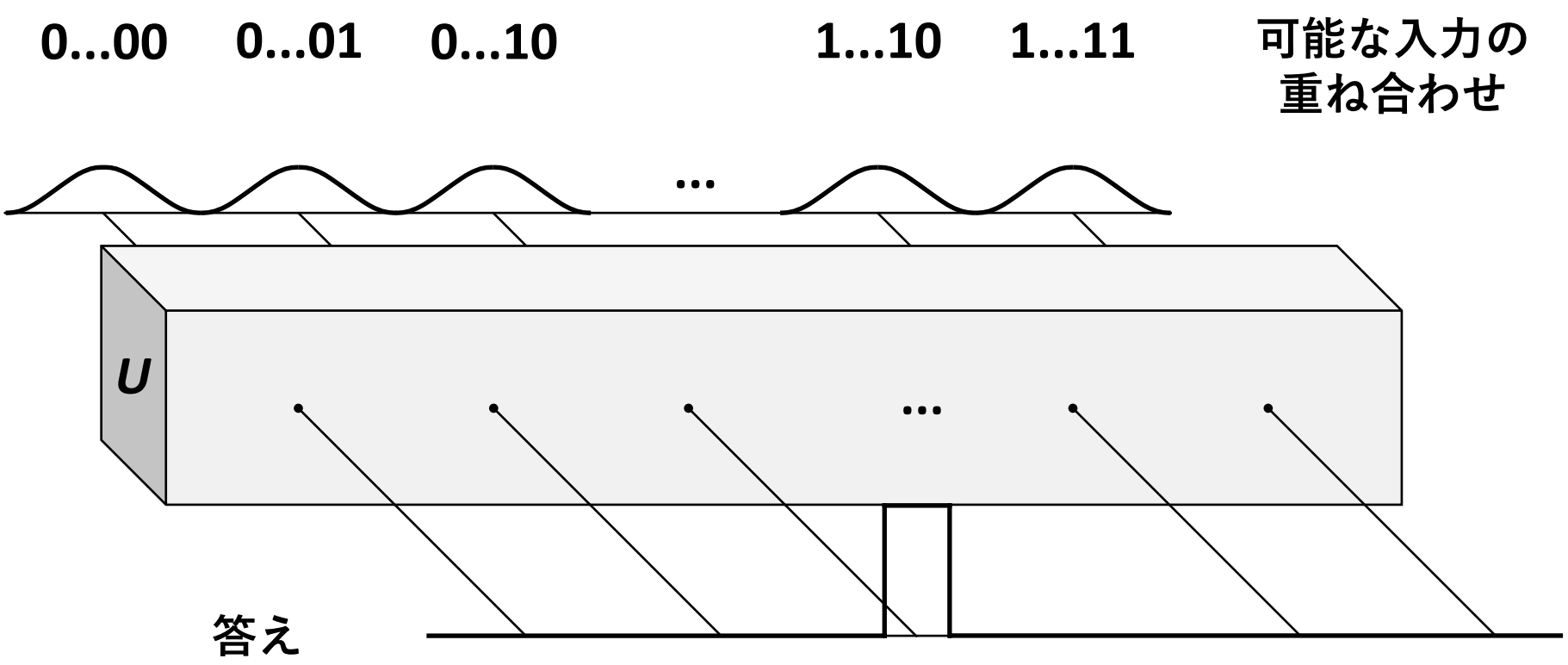
講義内容

- **イントロダクション**
  - 半導体デバイスと量子
  - 量子ドット中の電子の振る舞い
- **量子コンピューティングの基礎**
  - 量子ビットと量子ゲート
  - 量子アルゴリズム
  - 量子コンピューティングの難しさ

量子計算のアイディア

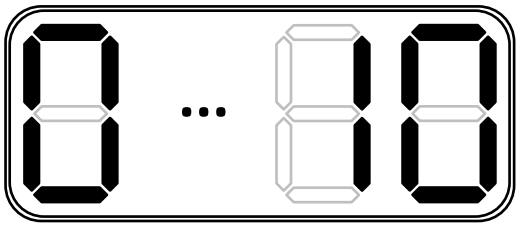


量子計算のアイディア



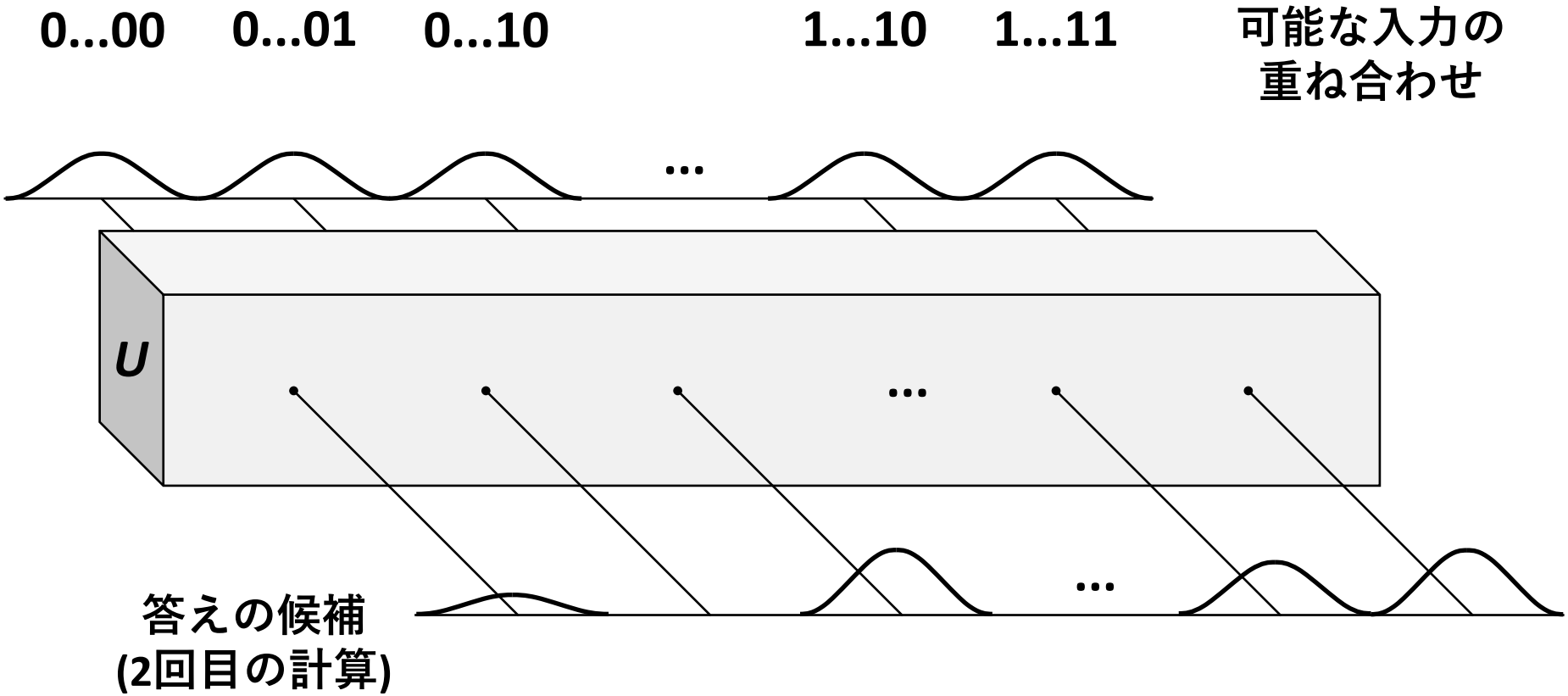
あまりうれしくない

測定

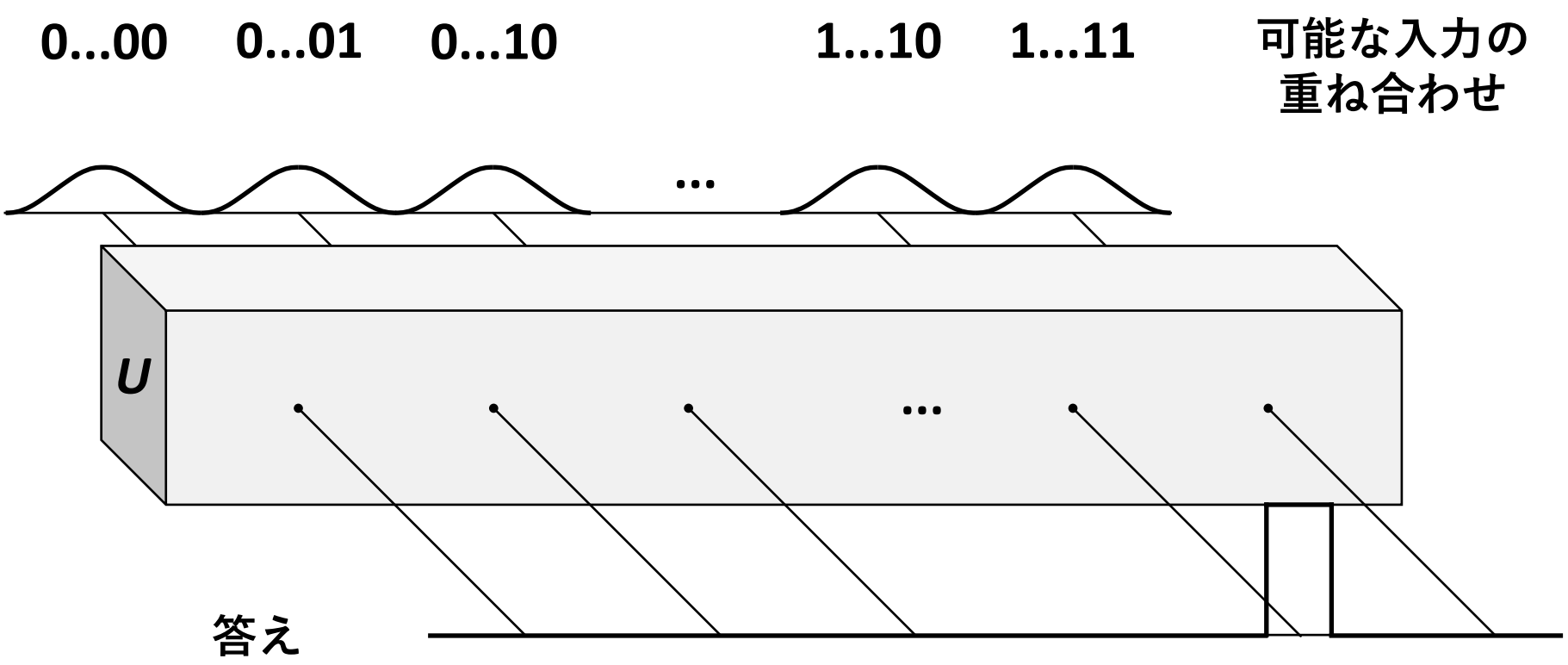


(20%...)

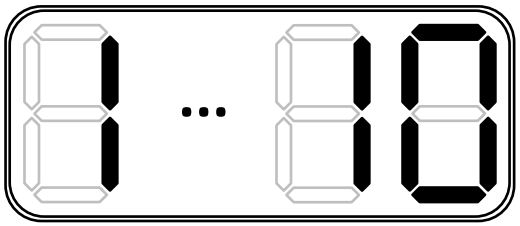
量子計算のアイディア



量子計算のアイディア

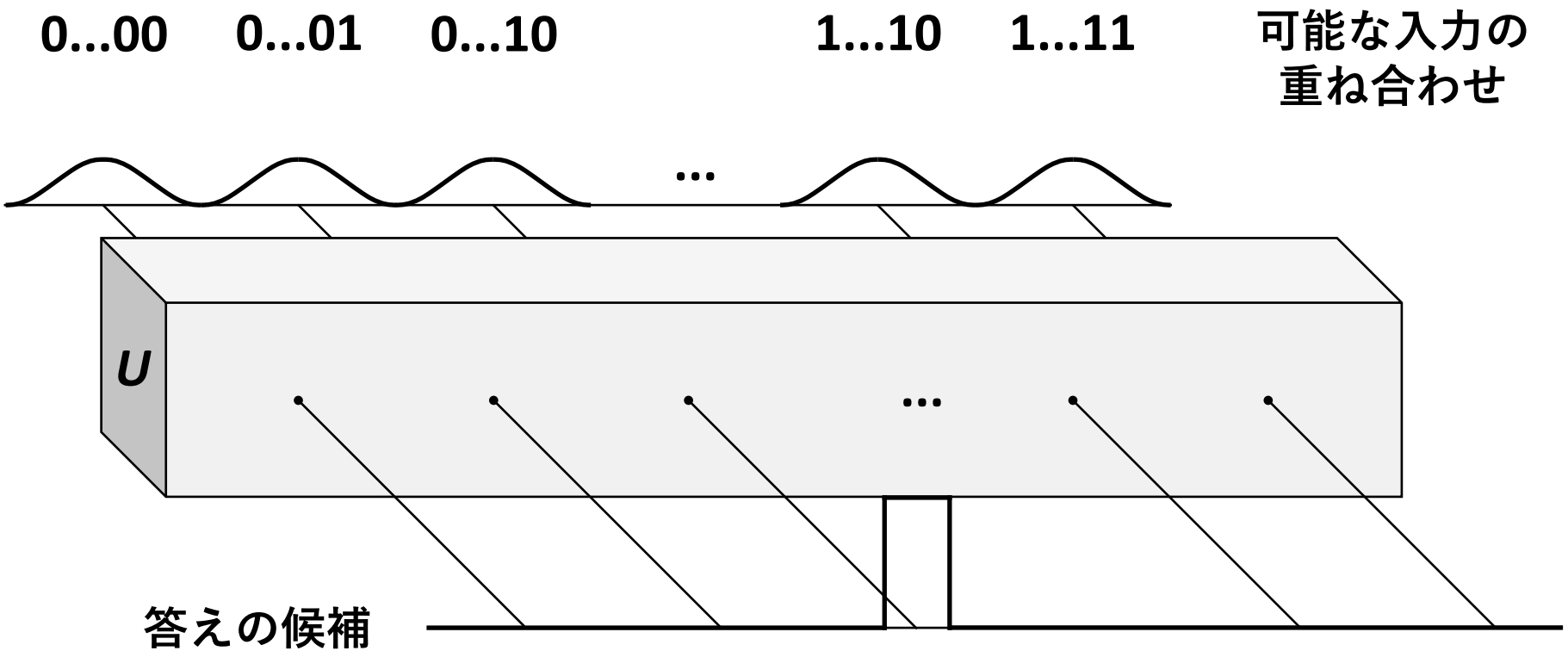


2回目の測定



(15%...)

量子計算のアイディア

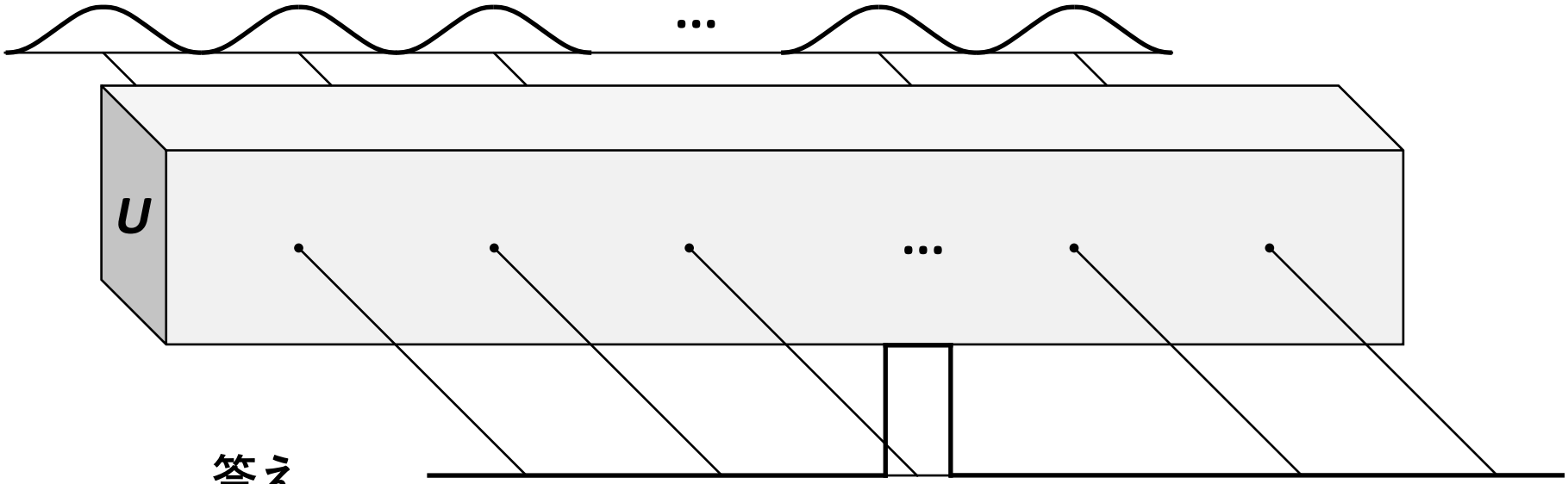


計算が終わった(測定前の“**候補**”) の時点に**答えの状態**になっていて欲しい

量子計算のアイディア

0…00　0…01　0…10　…　1…10　1…11

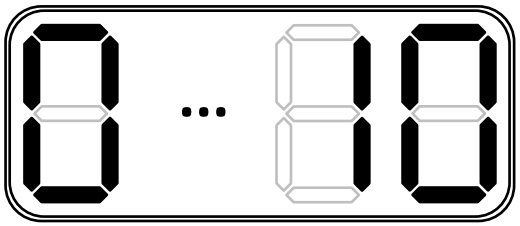
可能な入力の重ね合わせ



答え

うれしい

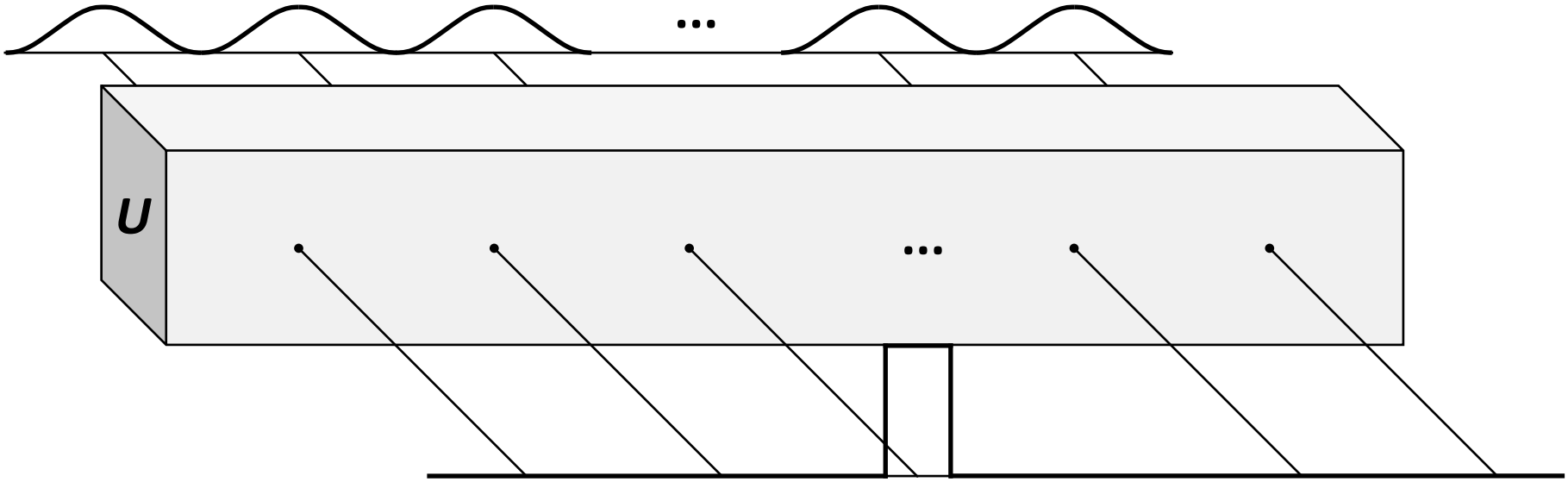
測定



(100%!)

量子アルゴリズム

- 重ね合わせ状態(**量子並列性**)から始めて、解の状態の確率振幅が大きくなるよう(**量子干渉**)にユニタリ変換し、最後に**測定**
- **ドイチェ–ジョザ**、グローバー(データ検索)、ショア(素因数分解)...

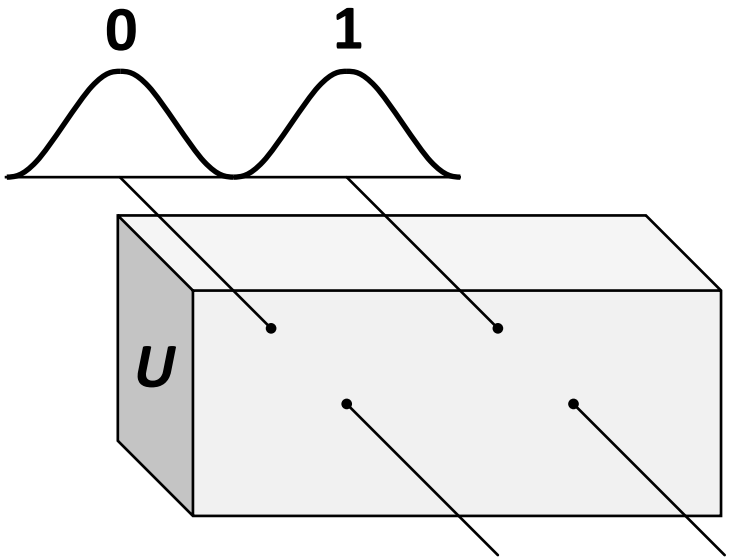


量子ビット・ゲートの表し方

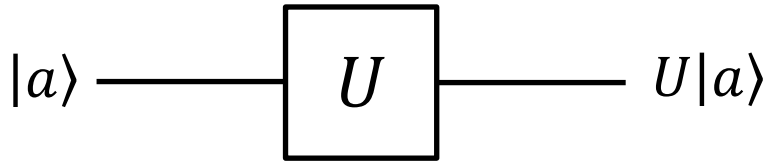
$$\mathbb{0} = \begin{pmatrix}1\\0\end{pmatrix} \quad \mathbb{1} = \begin{pmatrix}0\\1\end{pmatrix} \quad \Rightarrow \quad |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad |1\rangle = \begin{pmatrix}1\\0\end{pmatrix}$$

$$a\,\mathbb{0} + b\,\mathbb{1} \qquad a|0\rangle + b|1\rangle$$

量子力学でケットベクトルと呼ぶもの
ここでは単なる記法と思えばよい



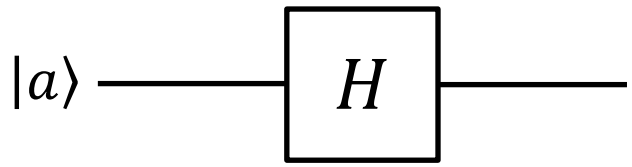
$\Rightarrow$



$a = 0,1$

“ワイヤ”の数が*n*本で済むことに注意
(左の図だと2^n本必要)

Hゲート

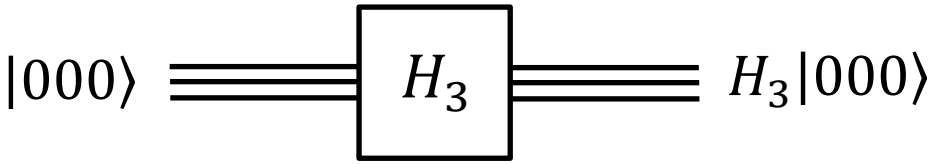


$$\frac{1}{\sqrt{2}}\sum_{b=0,1}(-1)^{a\cdot b}|b\rangle = \frac{|0\rangle + (-1)^a|1\rangle}{\sqrt{2}}$$

$a = 0,1$

$$\begin{cases} H|0\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}} \\ H|1\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} \end{cases} \Leftrightarrow \begin{cases} H\begin{pmatrix}1\\0\end{pmatrix} = \dfrac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \\ H\begin{pmatrix}0\\1\end{pmatrix} = \dfrac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \end{cases} \Leftrightarrow H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$$

H_3ゲート



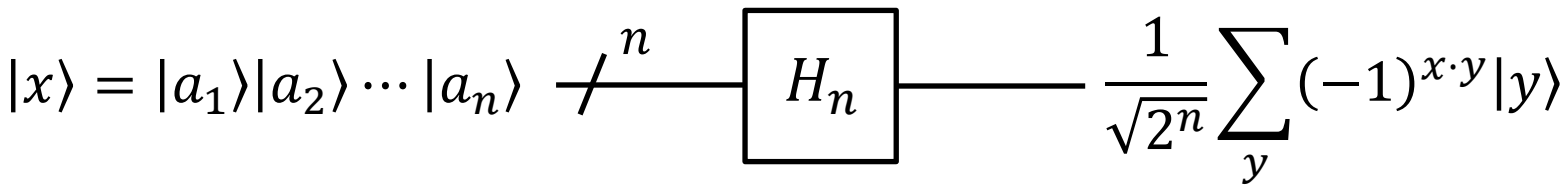
$H_3|000\rangle$

$$= \frac{1}{\sqrt{2^3}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$

$$= \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

$$= \frac{1}{\sqrt{2^3}} \sum_{a,b,c=0,1} |abc\rangle = \frac{1}{\sqrt{2^3}} \sum_{x=0}^{2^3-1} |x\rangle$$

H_nゲート



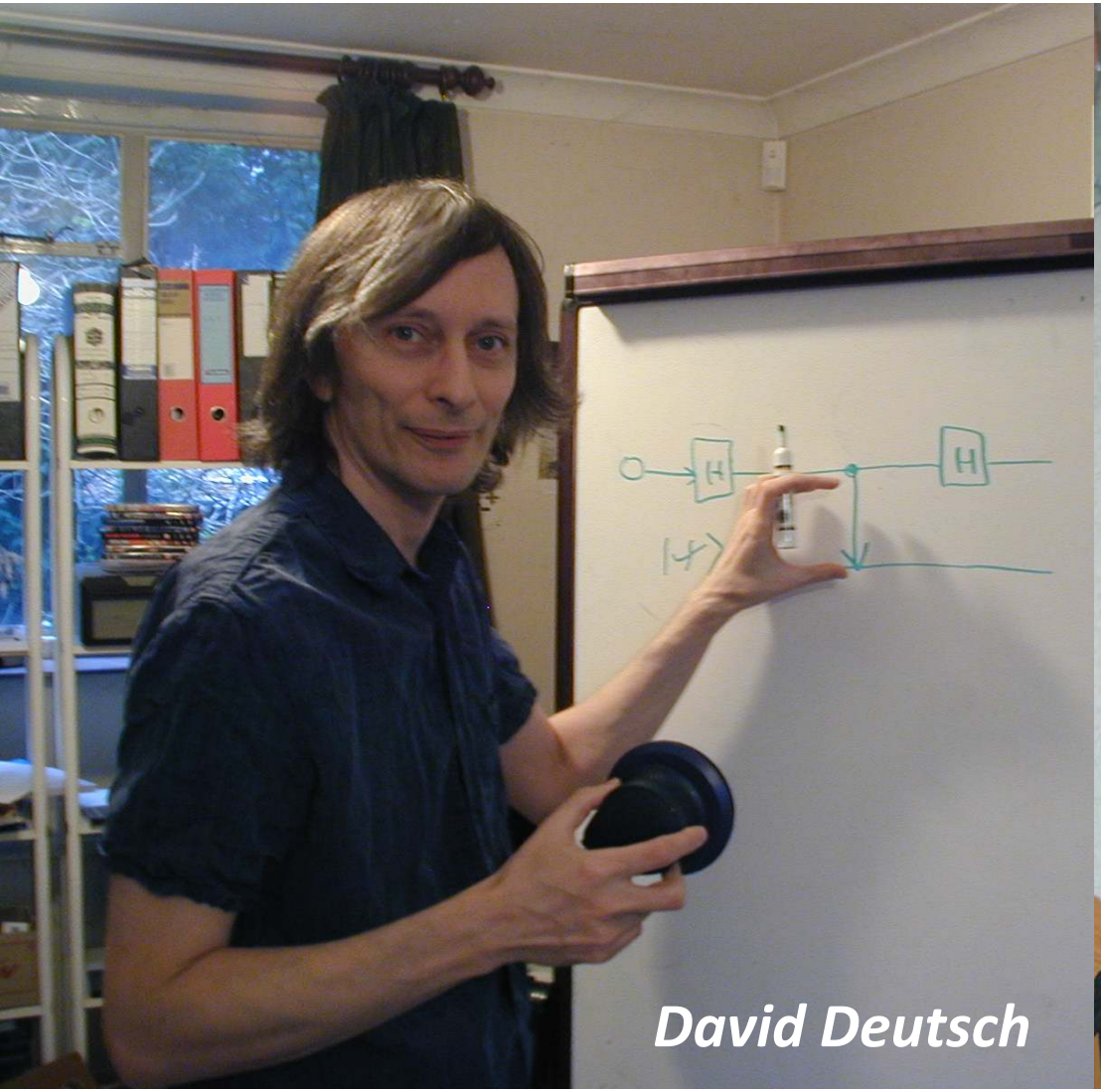
$x \cdot y \equiv a_1 \cdot b_1 + a_2 \cdot b_2 + \cdots + a_n \cdot b_n$

$$H_n|x\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{b_1=0,1} (-1)^{a_1 \cdot b_1} |b_1\rangle \right) \cdots \left(\sum_{b_n=0,1} (-1)^{a_n \cdot b_n} |b_n\rangle \right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{b_1, b_2 \cdots b_n} (-1)^{a_1 \cdot b_1 + a_2 \cdot b_2 + \cdots + a_n \cdot b_n} |b_1 b_2 \cdots b_n\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_y (-1)^{x \cdot y} |y\rangle$$

ドイチェ–ジョザのアルゴリズム



David Deutsch

Richard Jozsa

ドイチェの問題

定義: 二値関数$f(x)$について、全ての入力xに対して同じ出力(全て0か全て1)を返すものを**“一定(constant)”**、0・1半々となるものを**“均等(balanced)”**と呼ぶ

例:

一定

x	$f(x)$
0	0
1	0
2	0
3	0

均等

x	$f(x)$
0	0
1	1
2	1
3	0

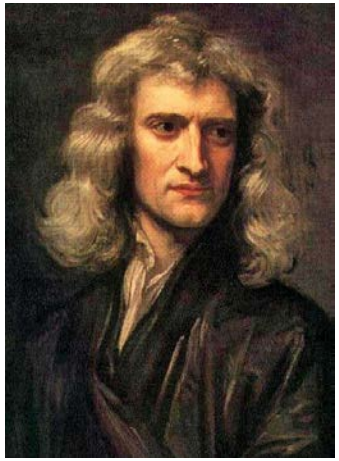
どちらでもない

x	$f(x)$
0	0
1	1
2	1
3	1

ドイチェの問題

ドイチェは**一定**か**均等**のビットデータ列$f(x)$を持っている。**ニュートン**と**シュレディンガー**は、$f(x)$が一定か均等かを判定するために**何回の問い合わせ**が必要か?

“古典”問い合わせ



I. Newton
By Godfrey Kneller

$x = 0$

$f(0) = 0$

$x = 1$

$f(1) = 0$

⋮

最大(半分+1)回

x	$f(x)$
0	0
1	0
2	0
3	0

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

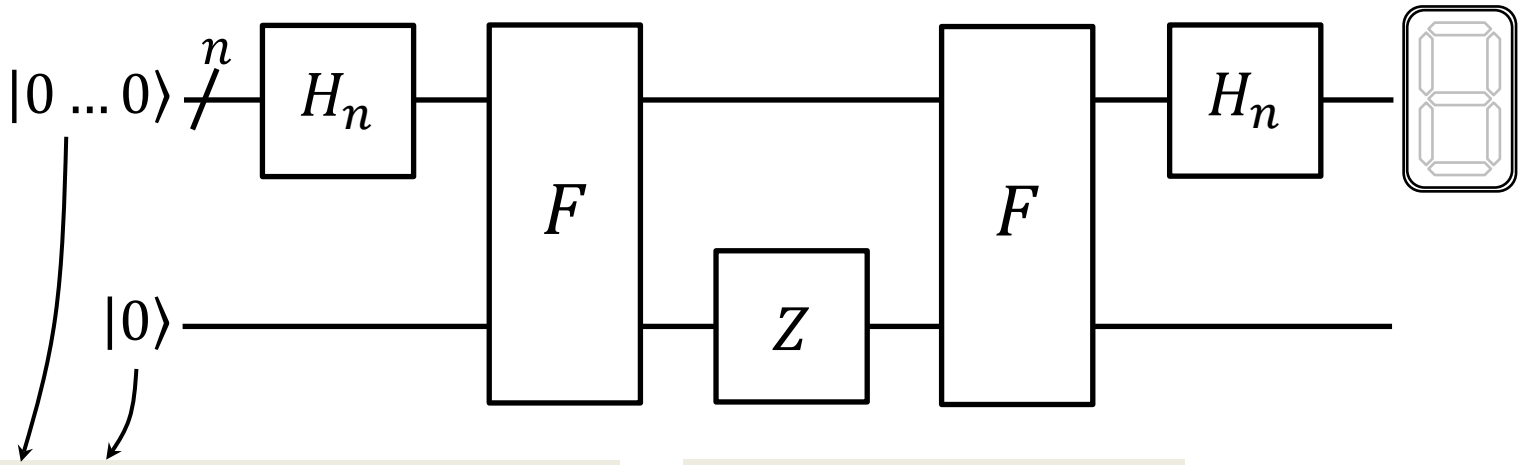
$|\Psi\rangle$

常に1回

“量子”問い合わせ

E. Schrödinger
©Nobel Foundation

ドイチェ–ジョザのアルゴリズム



$F|x\rangle|a\rangle = |x\rangle|a \oplus f(x)\rangle$

$Z|a\rangle = (-1)^a|a\rangle$

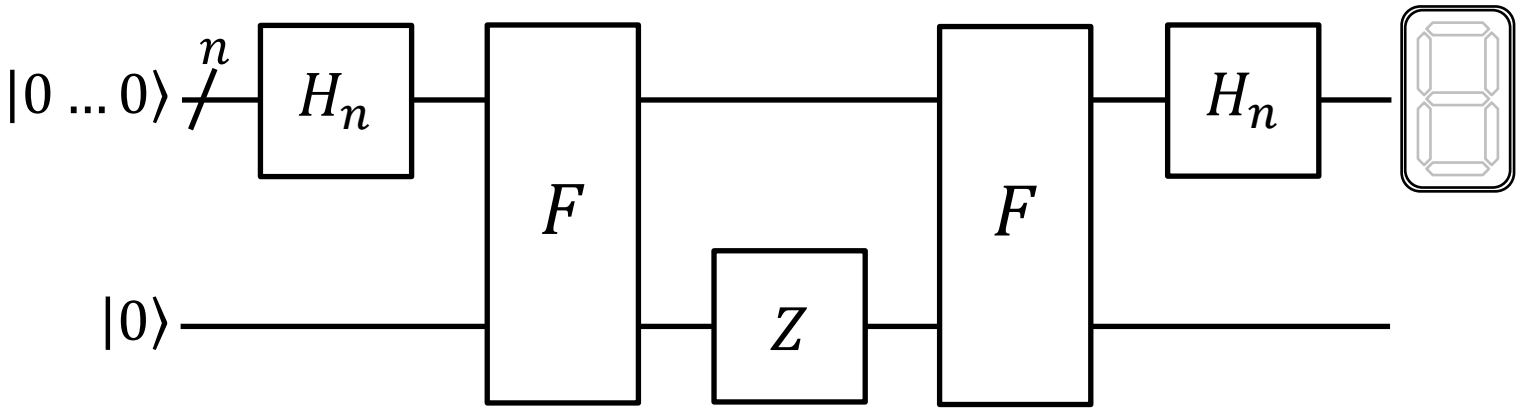
$f(x)$の情報を全て含む
量子もつれ状態

$$|0 \ldots 0\rangle|0\rangle \xrightarrow{H_n} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle \xrightarrow{F} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$$

$$\xrightarrow{Z} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle|f(x)\rangle$$

$f(x)$の情報を**位相**
に書き込む

ドイチェ–ジョザのアルゴリズム



$$F|x\rangle|a\rangle = |x\rangle|a \oplus f(x)\rangle$$

$f(x)$の情報を下の
ビットから**消去**

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle|f(x)\rangle \xrightarrow{F} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle|0\rangle$$

$$\xrightarrow{H_n} \sum_y\left(\sum_x \frac{(-1)^{f(x)+x\cdot y}}{2^n}\right)|y\rangle|0\rangle$$

$$H_n|x\rangle = \frac{1}{\sqrt{2^n}}\sum_y(-1)^{x\cdot y}|y\rangle$$

ドイチェ–ジョザのアルゴリズム

$|0 \ldots 0\rangle$に戻る確率振幅

$$\sum_{x=0}^{2^n-1} \frac{(-1)^{f(x)+x\cdot 0}}{2^n} = \begin{cases} \pm 1 & (\text{一定}) \\ 0 & (\text{均等}) \end{cases}$$

***n* = 2, 一定**　　干渉による強め合い

$$\sum_{x=0}^{3} \frac{(-1)^{f(x)}}{2^n} = \frac{(-1)^0 + (-1)^0 + (-1)^0 + (-1)^0}{4} = 1$$

***n* = 2, 均等**　　干渉による弱め合い

$$\sum_{x=0}^{3} \frac{(-1)^{f(x)}}{2^n} = \frac{(-1)^0 + (-1)^1 + (-1)^1 + (-1)^0}{4} = 0$$

講義内容

- **イントロダクション**
  - 半導体デバイスと量子
  - 量子ドット中の電子の振る舞い
- **量子コンピューティングの基礎**
  - 量子ビットと量子ゲート
  - 量子アルゴリズム
  - 量子コンピューティングの難しさ

量子コンピューティングの難しさ

- 量子情報を**位相**に書き込み、**量子干渉**により解の状態を抜き出す
  → 計算中に**量子コヒーレンス**を保つことが必要

- 量子状態は複製できない(**複製禁止定理**)
  → **量子誤り訂正符号 & 誤り耐性量子計算**

(フォールトトレラント, fault tolerant)

複製禁止定理

任意の状態$|\psi\rangle$に対して$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$となる
ユニタリゲートUは存在しない

LETTERS TO NATURE

A single quantum cannot be cloned

W. K. Wootters*

Center for Theoretical Physics, The University of Texas at Austin, Austin, Texas 78712, USA

W. H. Zurek

Theoretical Astrophysics 130-33, California Institute of Technology, Pasadena, California 91125, USA

If a photon of definite polarization encounters an excited atom, there is typically some nonvanishing probability that the atom will emit a second photon by stimulated emission. Such a photon is guaranteed to have the same polarization as the original photon. But is it possible by this or any other process to amplify a quantum state, that is, to produce several copies of a quantum system (the polarized photon in the present case) each having the same state as the original? If it were, the amplifying process could be used to ascertain the exact state of a quantum system: in the case of a photon, one could determine its polarization by first producing a beam of identically polarized copies and then measuring the Stokes parameters[1]. We show here that the linearity of quantum mechanics forbids such replication and that this conclusion holds for all quantum systems.

Note that if photons could be cloned, a plausible argument could be made for the possibility of faster-than-light communication[2]. It is well known that for certain non-separably correlated Einstein–Podolsky–Rosen pairs of photons, once an observer has made a polarization measurement (say, vertical versus horizontal) on one member of the pair, the other one, which may be far away, can be for all purposes of prediction regarded as having the same polarization[3]. If this second photon could be replicated and its precise polarization measured as above, it would be possible to ascertain whether, for example, the first photon had been subjected to a measurement of linear or circular polarization. In this way the first observer would be able to transmit information faster than light by encoding his message into his choice of measurement. The actual impossibility of cloning photons, shown below, thus prohibits superluminal communication by this scheme. That such a scheme must fail for some reason despite the well-established existence of long-range quantum correlations[6–8], is a general consequence of quantum mechanics[9].

A perfect amplifying device would have the following effect on an incoming photon with polarization state $|s\rangle$:

$$|A_0\rangle|s\rangle \rightarrow |A_s\rangle|ss\rangle \quad (1)$$

Here $|A_0\rangle$ is the 'ready' state of the apparatus, and $|A_s\rangle$ is its final state, which may or may not depend on the polarization of the original photon. The symbol $|ss\rangle$ refers to the state of the radiation field in which there are two photons each having the polarization $|s\rangle$. Let us suppose that such an amplification can in fact be accomplished for the vertical polarization $|\updownarrow\rangle$ and for the horizontal polarization $|\leftrightarrow\rangle$. That is,

$$|A_0\rangle|\updownarrow\rangle \rightarrow |A_{vert}\rangle|\updownarrow\updownarrow\rangle \quad (2)$$

and

$$|A_0\rangle|\leftrightarrow\rangle \rightarrow |A_{hor}\rangle|\leftrightarrow\leftrightarrow\rangle \quad (3)$$

According to quantum mechanics this transformation should be representable by a linear (in fact unitary) operator. It therefore follows that if the incoming photon has the polarization given by the linear combination $\alpha|\updownarrow\rangle+\beta|\leftrightarrow\rangle$—for example, it could be linearly polarized in a direction 45° from the vertical, so that $\alpha=\beta=2^{-1/2}$—the result of its interaction with the apparatus will be the superposition of equations (2) and (3):

$$|A_0\rangle(\alpha|\updownarrow\rangle+\beta|\leftrightarrow\rangle) \rightarrow \alpha|A_{vert}\rangle|\updownarrow\updownarrow\rangle+\beta|A_{hor}\rangle|\leftrightarrow\leftrightarrow\rangle \quad (4)$$

If the apparatus states $|A_{vert}\rangle$ and $|A_{hor}\rangle$ are not identical, then the two photons emerging from the apparatus are in a mixed state of polarization. If these apparatus states are identical, then the two photons are in the pure state

$$\alpha|\updownarrow\updownarrow\rangle+\beta|\leftrightarrow\leftrightarrow\rangle \quad (5)$$

In neither of these cases is the final state the same as the state with two photons both having the polarization $\alpha|\updownarrow\rangle+\beta|\leftrightarrow\rangle$. That state, the one which would be required if the apparatus were to be a perfect amplifier, can be written as

$$2^{-1/2}(\alpha a^*_{vert}+\beta a^*_{hor})^2|0\rangle=\alpha^2|\updownarrow\updownarrow\rangle+2^{1/2}\alpha\beta|\updownarrow\leftrightarrow\rangle+\beta^2|\leftrightarrow\leftrightarrow\rangle$$

which is a pure state different from the one obtained above by superposition [equation (5)].

Thus no apparatus exists which will amplify an arbitrary polarization. The above argument does not rule out the possibility of a device which can amplify two special polarizations, such as vertical and horizontal. Indeed, any measuring device which distinguishes between these two polarizations, a Nicol prism for example, could be used to trigger such an amplification.

The same argument can be applied to any other kind of quantum system. As in the case of photons, linearity does not forbid the amplification of any given state by a device designed especially for that state, but it does rule out the existence of a device capable of amplifying an arbitrary state.

* Present address: Department of Physics and Astronomy, Williams College, Williamstown, Massachusetts 01267, USA.

Milonni (unpublished work) has shown that the process of stimulated emission does not lead to quantum amplification, because if there is stimulated emission there must also be—with equal probability in the case of one incoming photon—spontaneous emission, and the polarization of a spontaneously emitted photon is entirely independent of the polarization of the original.

It is conceivable that a more sophisticated amplifying apparatus could get around Milonni's argument. We have therefore presented the above simple argument, based on the linearity of quantum mechanics, to show that no apparatus, however complicated, can amplify an arbitrary polarization.

We stress that the question of replicating individual photons is of practical interest. It is obviously closely related to the quantum limits on the noise in amplifiers[10,11]. Moreover, an experiment devised to establish the extent to which polarization of single photons can be replicated through the process of stimulated emission is under way (A. Gozzini, personal communication; and see ref. 12). The quantum mechanical prediction is quite definite; for each perfect clone there is also one randomly polarized, spontaneously emitted, photon.

We thank Alain Aspect, Carl Caves, Ron Dickman, Ted Jacobson, Peter Milonni, Marlan Scully, Pierre Meystre, Don Page and John Archibald Wheeler for enjoyable and stimulating discussions.

This work was supported in part by the NSF (PHY 78-26592 and AST 79-22012-A1). W.H.Z. acknowledges a Richard Chace Tolman Fellowship.

Received 11 August; accepted 7 September 1982.

1. Born, M. & Wolf, E. *Principles of Optics* 4th edn (Pergamon, New York, 1970).
2. Herbert, N. *Found. Phys.* (in the press).
3. Einstein, A., Podolsky, B. & Rosen, N. *Phys. Rev.* **47**, 777–780 (1935).
4. Bohm, D. *Quantum Theory*, 611–623 (Prentice-Hall, Englewood Cliffs, 1951).
5. Kocher, C. A. & Commins, E. D. *Phys. Rev. Lett.* **18**, 575–578 (1967).
6. Freedman, S. J. & Clauser, J. R. *Phys. Rev. Lett.* **28**, 938–941 (1972).
7. Fry, E. S. & Thompson, R. C. *Phys. Rev. Lett.* **37**, 465–468 (1976).
8. Aspect, A., Grangier, P. & Roger, G. *Phys. Rev. Lett.* **47**, 460–463 (1981).
9. Bussey, P. J. *Phys. Lett.* **90A**, 9–12 (1982).
10. Haus, H. A. & Mullen, J. A. *Phys. Rev.* **128**, 2407–2410 (1962).
11. Caves, C. M. *Phys. Rev.* **D15**, (in the press).
12. Gozzini, A. *Proc. Symp. on Wave-Particle Dualism* (eds Diner, S., Fargue, D., Lochak, G. & Selleri, F) (Reidel, Dordrecht, in the press).

Nature **299**, 802 (1982) Wootters & Zurek

複製禁止定理

任意の状態$|\psi\rangle$に対して$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$となる
ユニタリゲートUは存在しない

証明: 存在するならば…

$$U|0\rangle|0\rangle = |0\rangle|0\rangle$$

$$U|1\rangle|0\rangle = |1\rangle|1\rangle$$

⇩

$$U(\underbrace{a|0\rangle + b|1\rangle}_{|\psi\rangle})|0\rangle = aU|0\rangle|0\rangle + bU|1\rangle|0\rangle$$

$$= a|0\rangle|0\rangle + b|1\rangle|1\rangle$$

$$\neq (a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle)$$

ディビンチェンゾの要請

量子コンピューティングを実現する物理系に求められる条件

1. **多数の量子ビットを用意すること**
2. **00...0状態を準備できること**
3. **重ね合わせ状態を長く保持できること**
4. **任意のユニタリゲートを実行できること**
5. **状態の測定ができること**

D. DiVincenzo

Fortschr. Phys. **48**, 771 (2000) DiVincenzo

もっと知りたい方へ

- **驚異の量子コンピュータ: 宇宙最強マシンへの挑戦**
  - 藤井啓祐 (2019, 岩波科学ライブラリー)

- **Quantum Computation and Quantum Information**
  - Michael A. Nielsen & Isaac L. Chuang (2000, Cambridge University Press)

- **量子コンピュータ授業(YouTube)**
  - https://www.youtube.com/playlist?list=PLB1324F2305C028F7
  - https://quantum.riken.jp/lecture.html#link2 (スライド有)

動画は2005年のもので、元々YouTube用に撮影されたものではないことを
ご了承下さい。なお、https://quantum.riken.jp/lecture.html内には
上記以外の阿部による量子情報関係の講義スライドもあります。