# 量子コンピュータ

## その仕組みと応用

情報理論　2023-7-21

# 古典コンピュータの論理

電圧が低い(0V)　→　0

電圧が高い(3V)　→　1

2進数を表現する

□　0か1が入る箱

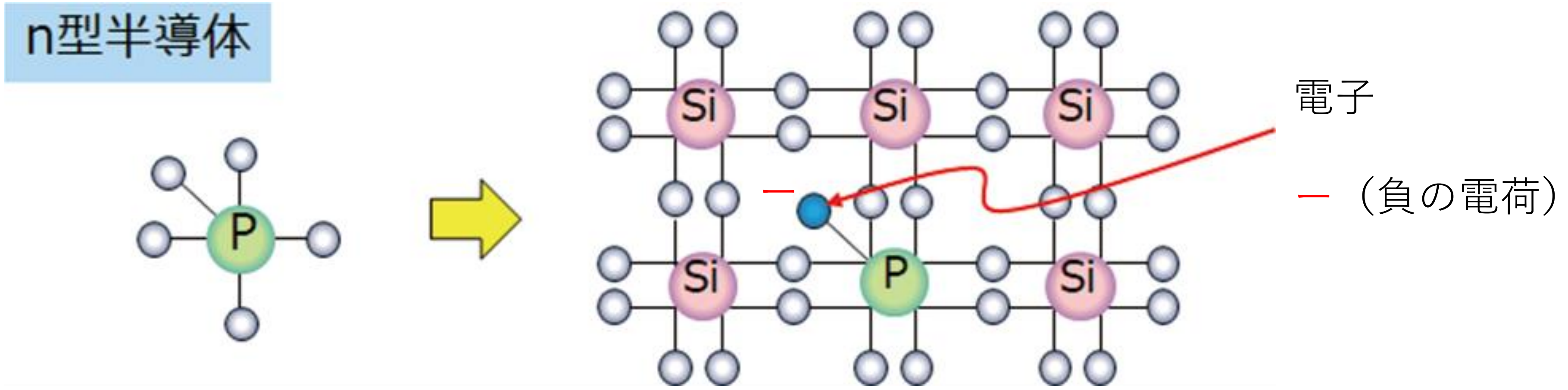
1 bit

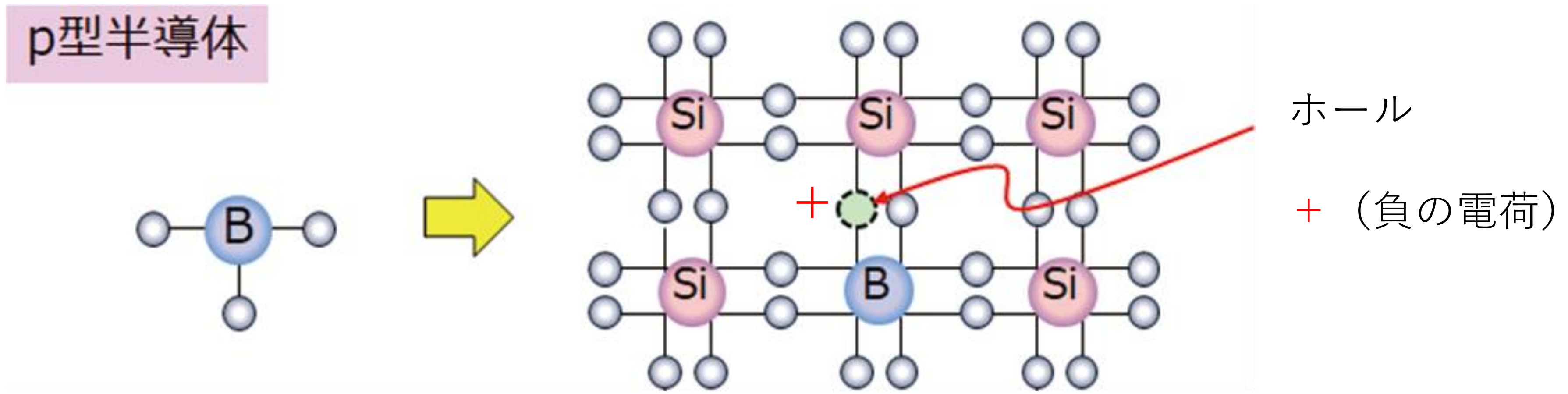
□□□□□□□□

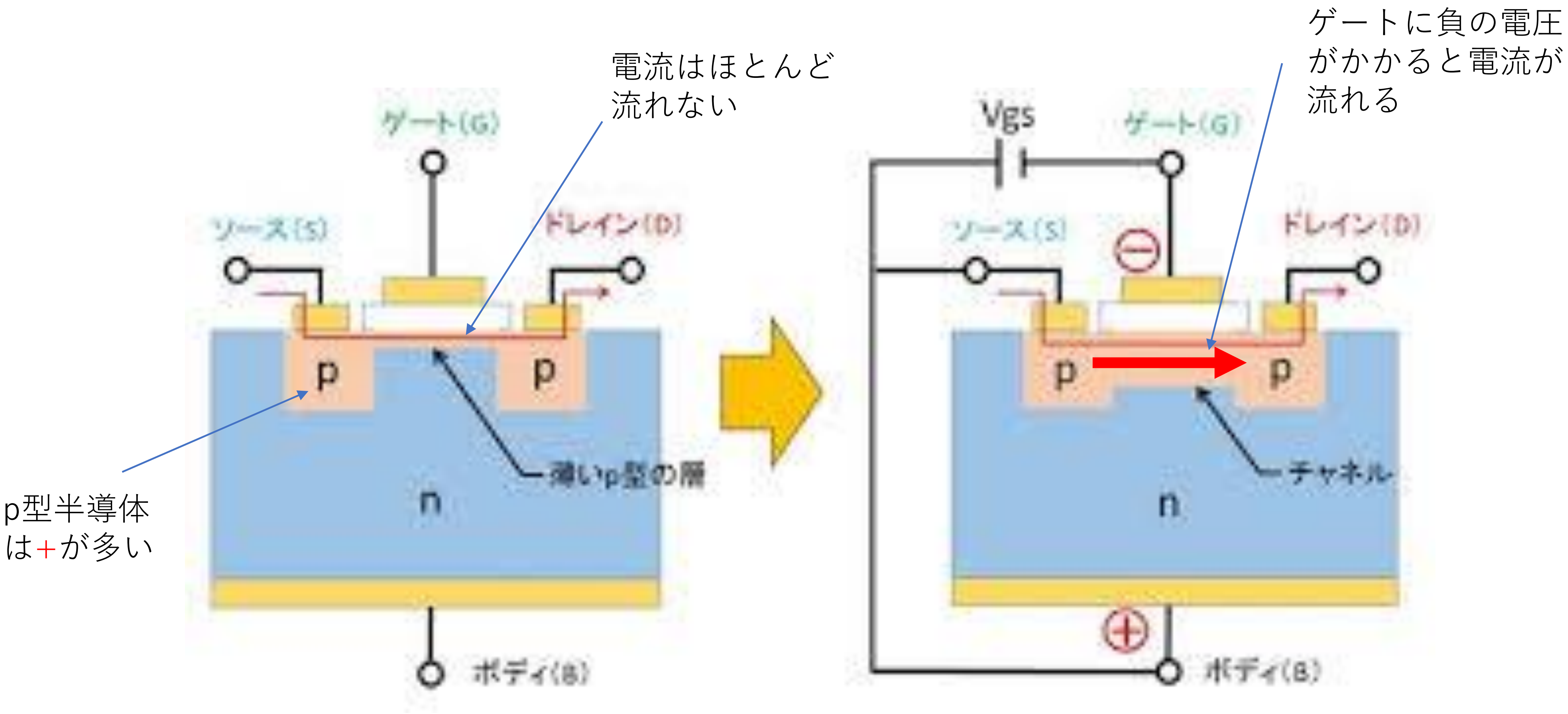
8 bit ＝ 1byte

0～255の 256通り

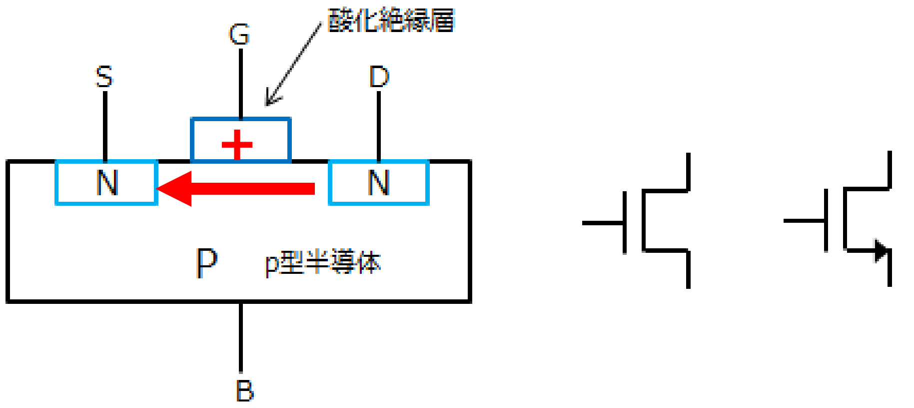
# 半導体



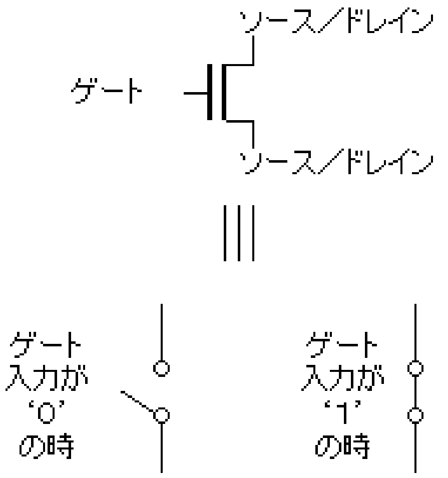


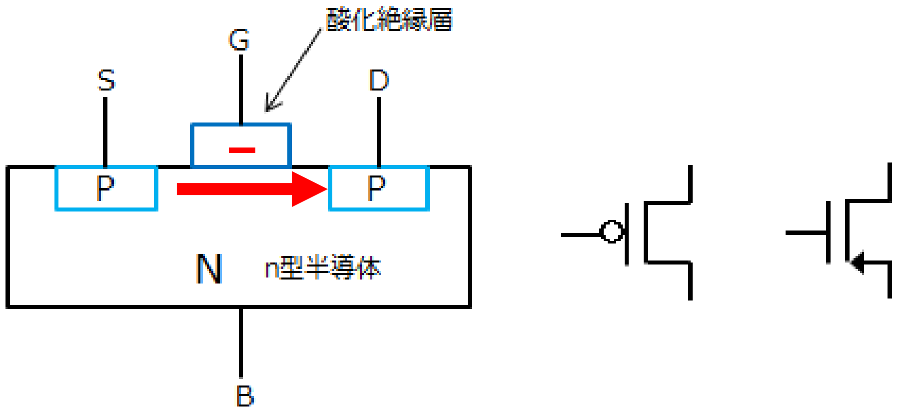

pチャネル MOS FET(金属酸化膜半導体電界効果トランジスタ)




**n チャネル MOS FETの構造と記号**

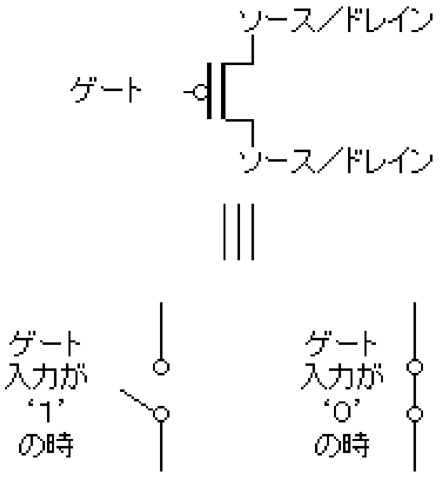
+(1と表す)で導通する
-(0と表す)で導通しない



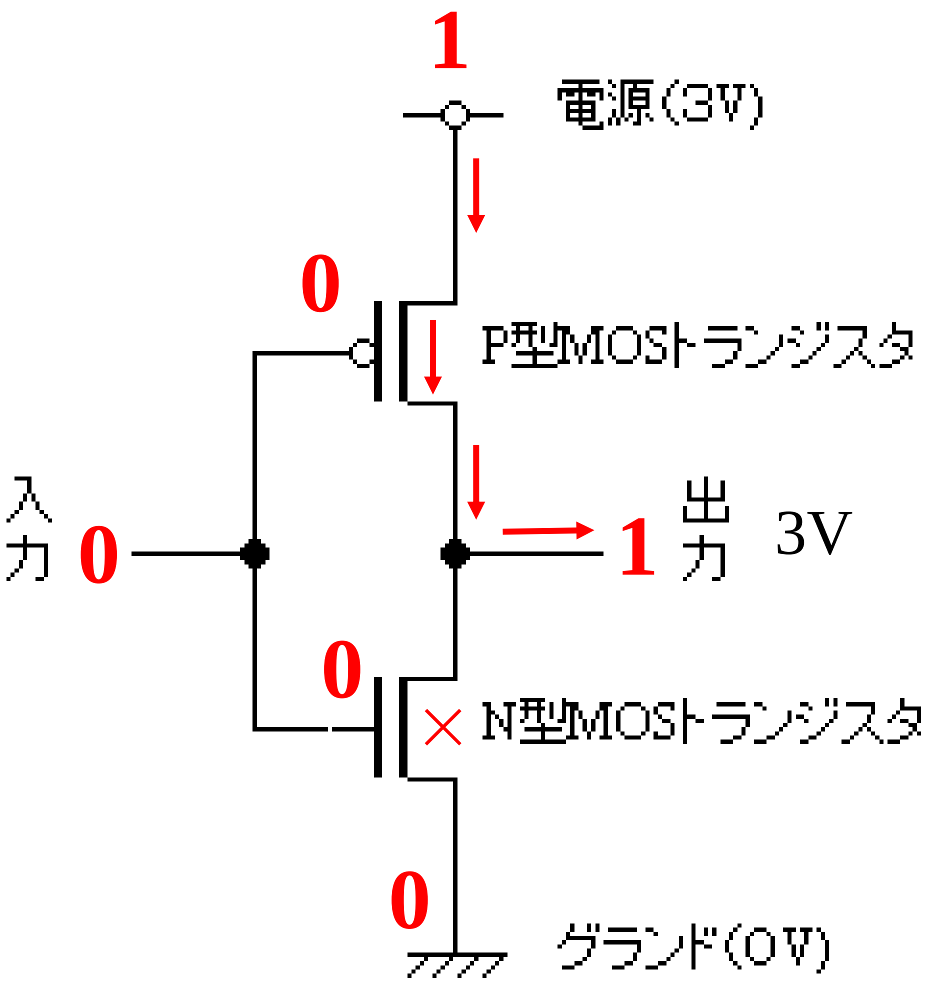



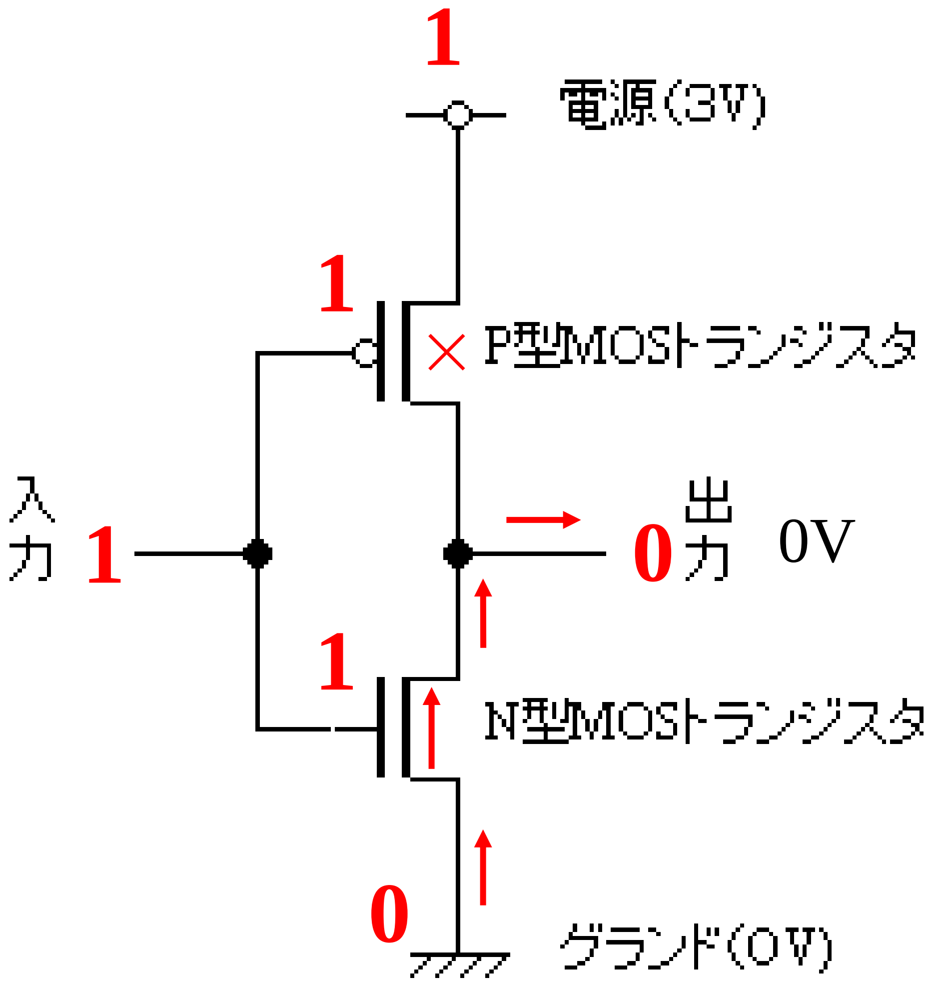

**pチャネル MOS FETの構造と記号**

-(0と表す)で導通する
+(1と表す)で導通しない



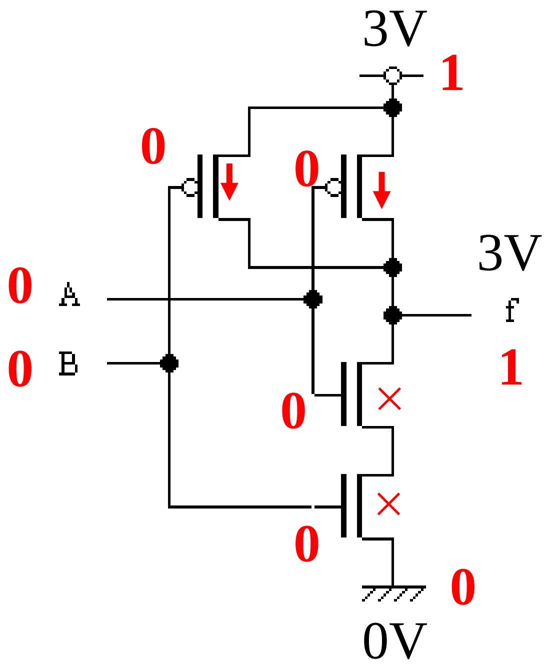
# NOT回路

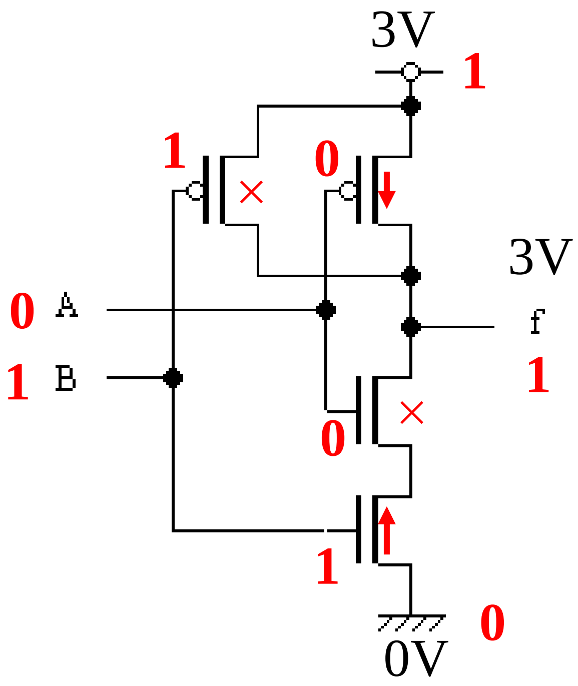


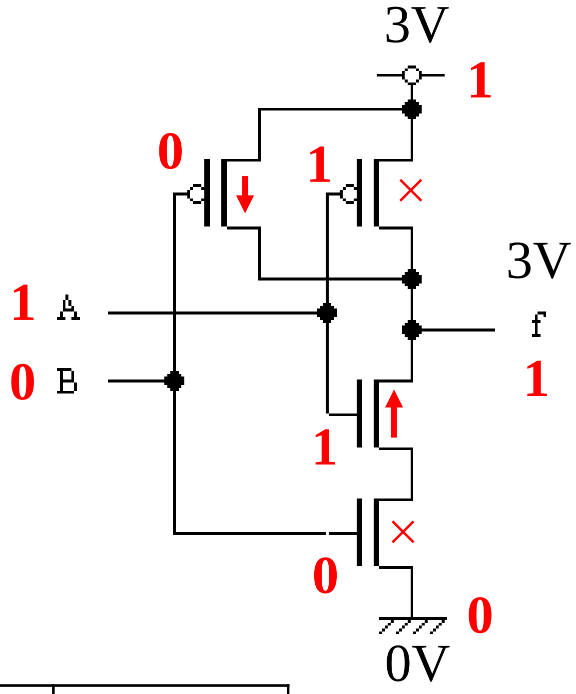



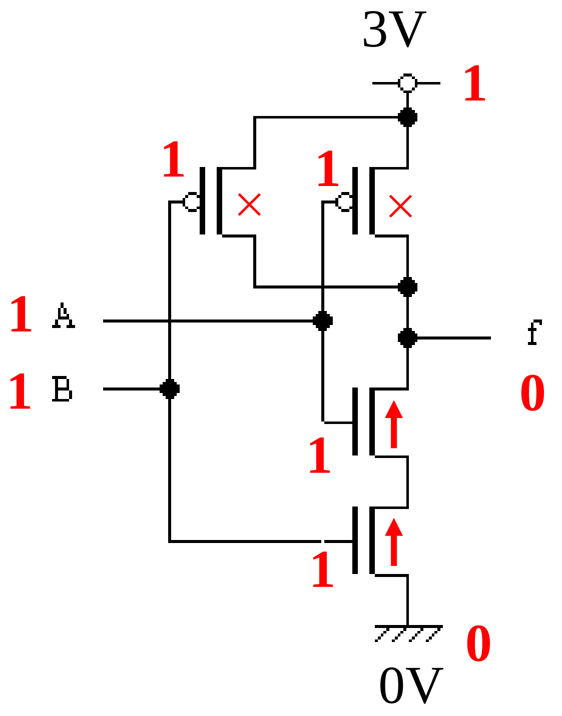

| 入力 | 出力 |
|---|---|
| 0 | 1 |
| 1 | 0 |

# NAND回路




| A | B | f |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

# 量子コンピュータの論理

スピンが上向き　→　|0>

スピンが下向き　→　|1>

|0>と |1>の重ね合わせ で表現する

$a_1|0> + b_1\ |1>$　　| >　0か1の状態を表す

1 qubit　1量子ビット

# 2 qubit　2量子ビット

$$(a_1|0\rangle + b_1\,|1\rangle)\ \ (a_2|0\rangle + b_2\,|1\rangle)$$

$$= \ a_1a_2|0\rangle|0\rangle + a_1b_2|0\rangle|1\rangle + b_1a_2|1\rangle|0\rangle + b_1b_2|1\rangle|1\rangle$$

$|0\rangle|0\rangle$，$|0\rangle|1\rangle$，$|1\rangle|0\rangle$，$|1\rangle|1\rangle$

の状態を一度に表せる

# 量子コンピュータのハードウェア（候補）

超伝導体

光学パルス

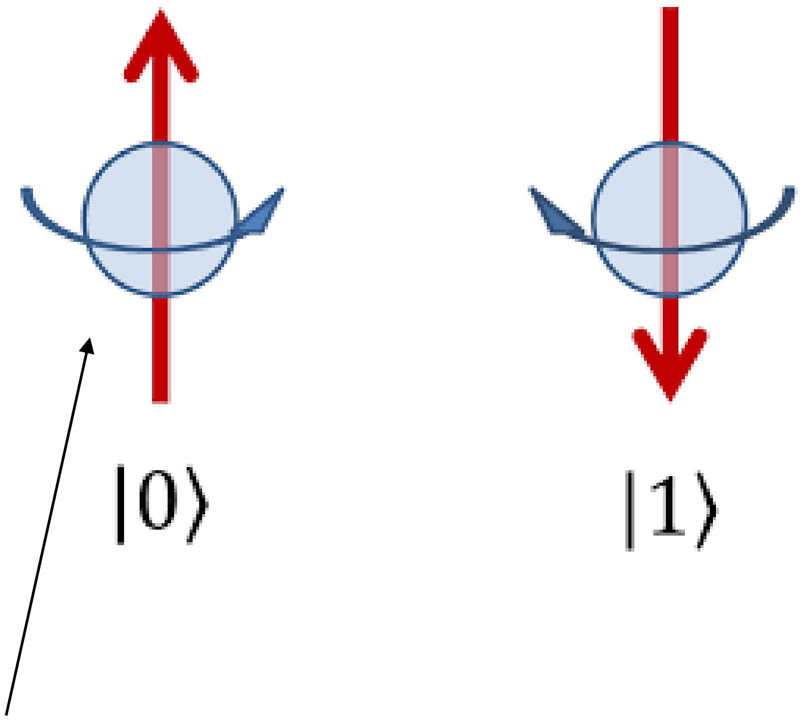
トラップイオン

量子ドット

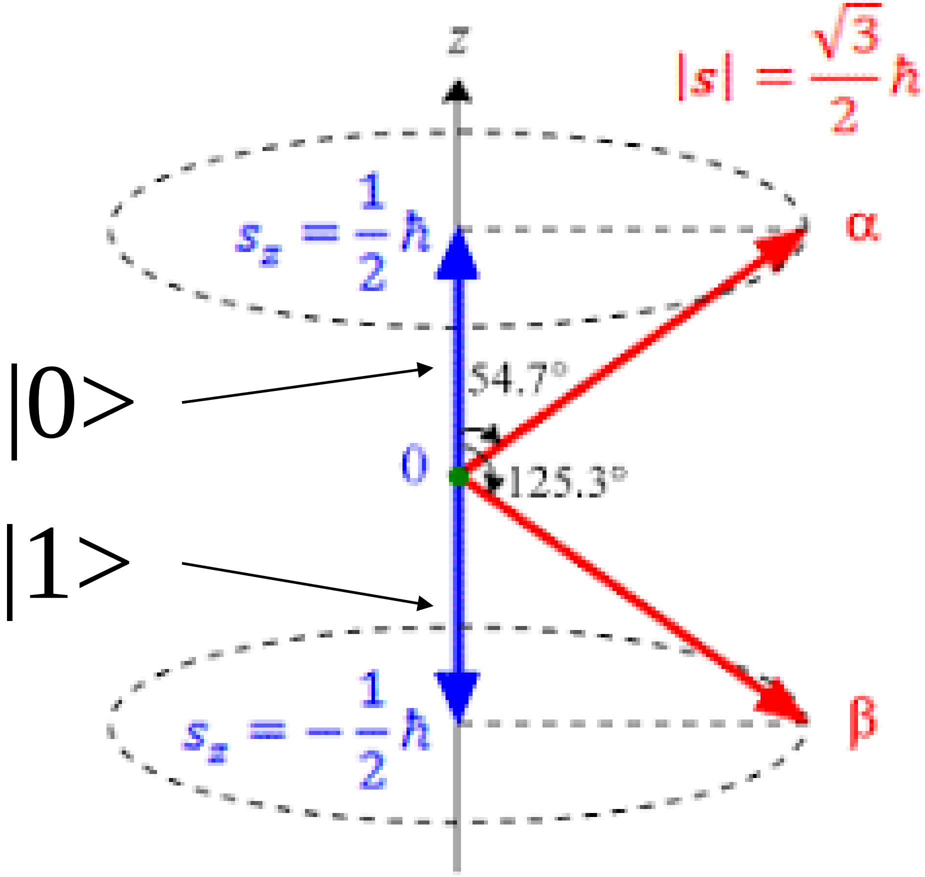
核磁気共鳴(NMR)

# 核磁気共鳴(NMR)

核スピン

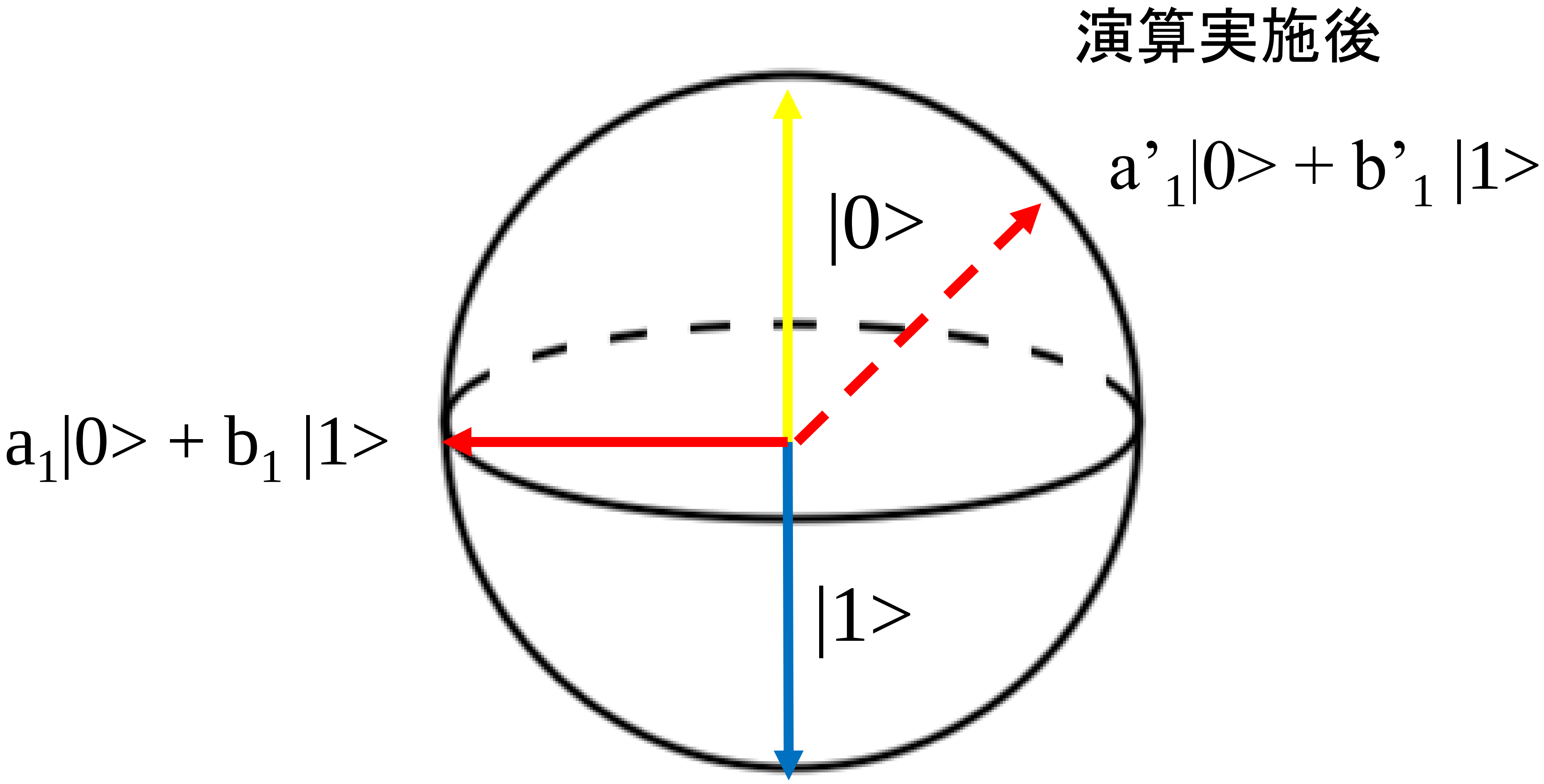


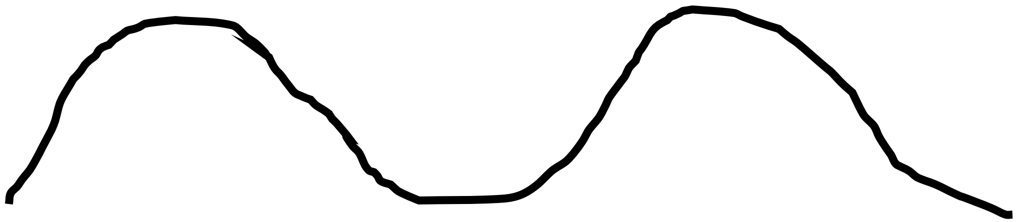

球は原子核を表す




$a_1|0> + b_1\ |1>$

演算は球の中でベクトルを動かす作用

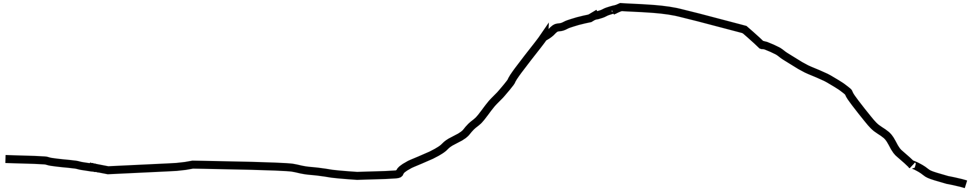




$|0\rangle$　　$|1\rangle$

$a_1|0\rangle + b_1\,|1\rangle$

$\downarrow$ 演算



$|0\rangle$　　$|1\rangle$

$|1\rangle$

8 量子ビット

|0>|0>|0>|0>|0>|0>|0>|0>　～　|1>|1>|1>|1>|1>|1>|1>|1>

0～255を一度に表せる

72量子ビット　$2^{72} = 4 \times 10^{21}$ を一度に表せる

量子コンピュータが古典コンピュータの能力を超える

現状は、汎用型で53量子ビット(IBM)

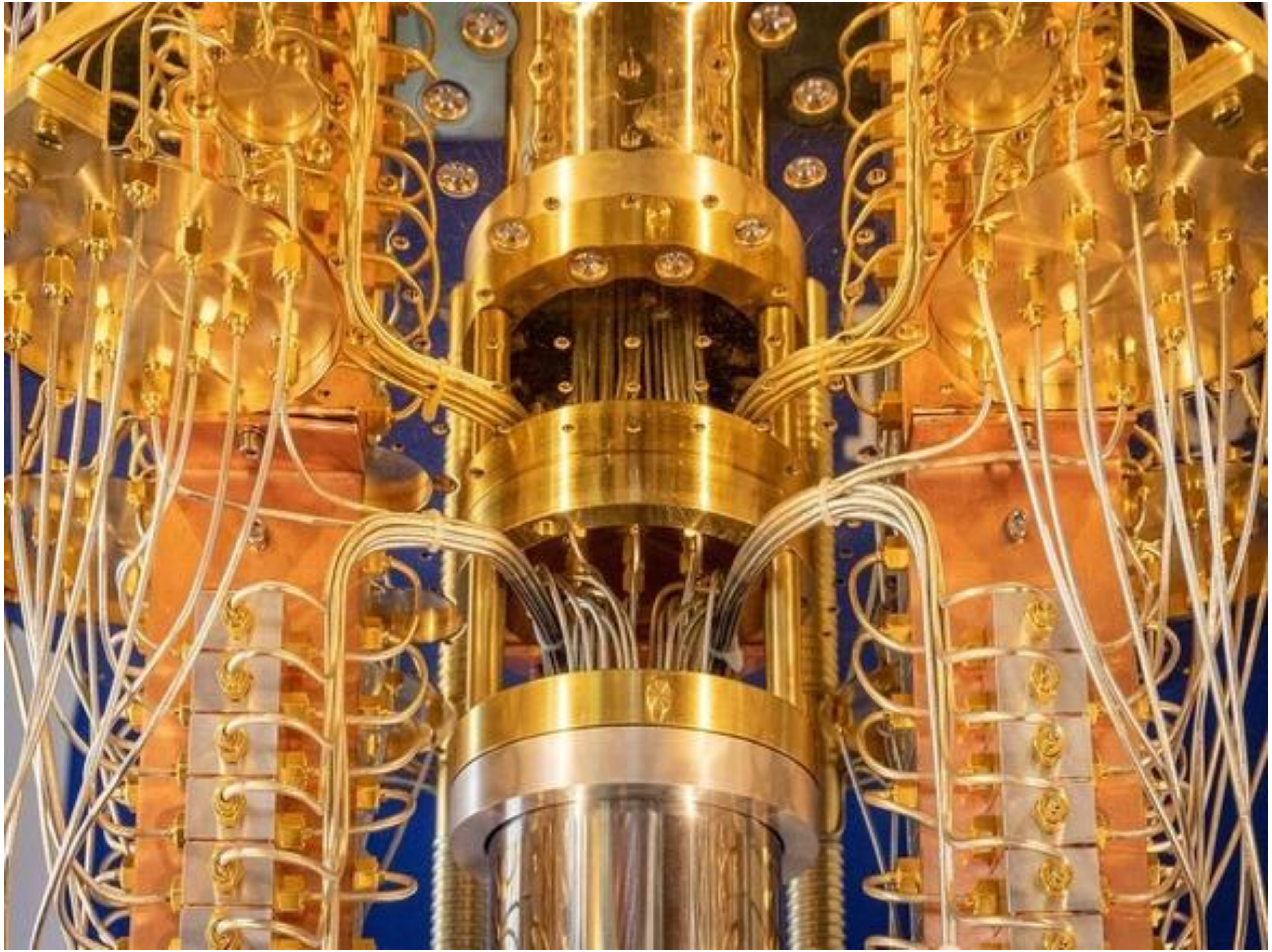
2023年には1000量子ビットを超えることを宣言

# 量子コンピュータ

IBM Q

超伝導量子ビット

53量子ビット



1量子ビット　$|0>$ や $|1>$ の状態は、行列で表す

$$|0> = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1> = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

演算子も、行列で表す

NOTゲート $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

# 行列の計算

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 1 \times 5 + 2 \times 6 \\ 3 \times 5 + 4 \times 6 \end{pmatrix}$$

$$= \begin{pmatrix} 5 + 12 \\ 15 + 24 \end{pmatrix} = \begin{pmatrix} 17 \\ 39 \end{pmatrix}$$

# 量子ゲート（演算子）

NOTゲート $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

NOTゲートを入力 $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ に作用

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

NOTゲートを入力 $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ に作用

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

NOT回路

| 入力 | 出力 |
|---|---|
| 0 | 1 |
| 1 | 0 |

NOTゲート

入力 出力

$|0\rangle \longrightarrow |1\rangle$

$|1\rangle \longrightarrow |0\rangle$

# 制御NOTゲート（演算子）

## CNOT(Control NOT) ゲート

2量子ビットを

|0> |0>　＝　|00>

|0> |1>　＝　|01>

|1> |0>　＝　|10>

|1> |1>　＝　|11>

と表すと、

CNOTゲートに2量子ビットを作用すると

| 入力 | | 出力 |
|---|---|---|
| \|00> | ⟶ | \|00> |
| \|01> | ⟶ | \|01> |
| \|10> | ⟶ | \|11> |
| \|11> | ⟶ | \|10> |

XOR回路

| A | B | C |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

# CNOTゲート　行列Xで表す

$$X = \begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix}$$

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

$$X \quad |00\rangle = |00\rangle$$

$$\begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$X \quad |01\rangle = |01\rangle$$

$$\begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$X \quad |10\rangle = |11\rangle$$

$$\begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$X \quad |11\rangle = |10\rangle$$

$$\begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

CNOTゲートを
作用すると

入力　　　　出力

A B　　　　A C

|00> ⟶ |00>

|01> ⟶ |01>

|10> ⟶ |11>

|11> ⟶ |10>

CNOTゲート

入力　　　　出力

| A | B | A | C = A⊕B |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 |

Aは制御ビット

A = 0 ならば　C = B

A = 1 ならば　C = $\overline{B}$

古典コンピュータでは、NAND回路ですべての論理回路を作れる。

量子コンピュータでは、1量子ビットに作用する5種類のゲートと
2量子ビットに作用するCNOTゲートですべての量子回路を作れる。

| Iゲート | Zゲート | Xゲート<br>(NOTゲート) | Yゲート | アダマールゲート |
| --- | --- | --- | --- | --- |
| $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ | $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ |

CNOTゲート $\begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix}$

# 量子コンピュータの今後の発展と課題

1. 大きな数の因数分解が瞬時にできるので、現在、暗号の主流であるRSA暗号が使えなくなる。量子の原理を利用した「量子暗号」が考案されている。

2. 高速にデータ検索ができる。

3. 化学シミュレーション　　新しい薬の設計

4. ナップサック問題、巡回セールスマン問題
を高速に解く

今後の課題

誤り訂正技術の確立、ノイズへの安定性