０と１を超える世界：量子コンピュータ入門

副題：量子をつかむっ！！

第二回
「量子計算はどう動いているのか」

大野木哲也

大阪大学大学院理学研究科

講義プラン

5月25日（月）　第一回「なぜ量子コンピュータか？」

6月29日（月）　第二回「量子計算はどう動いているのか」

7月27日（月）　第三回「現実の量子コンピュータ」

はじめに

前回の内容：

- 「計算」とは一定の規則に従う「物理的運動」と「結果の測定」で表現される。
  （例：そろばん「玉を動かす」、「結果を読む」）
- 量子力学は「状態」「重ね合わせ」「シュレーディンガー方程式」「測定」がキーワード。
- 量子力学特有の性質を用いて新しい種類の計算機ができないか？ ➔ 量子コンピュータ

今回の内容：

- 計算の基礎の「量子回路」と「量子アルゴリズム」について解説。

第二回　目次

1. 量子力学と線形代数
2. 論理回路
3. 素因数分解：Shorのアルゴリズム
4. まとめ、参考図書など

1. 量子力学と線形代数

量子力学は線形代数の言葉で書かれる。線形代数とはベクトルや行列を扱う数学である。

1) 状態はベクトルで表される。
例) N個の独立な状態が許される量子系の場合

$$\psi = \begin{pmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{N-1} \end{pmatrix} \qquad |\psi_0|^2 + |\psi_1|^2 + \cdots + |\psi_{N-1}|^2 = 1$$

2) 状態の時間発展はNxN ユニタリ行列の掛け算（長さを変えない行列の掛け算

$$\psi \longrightarrow U\psi$$

で与えられる。

N次元状態ベクトルの基底をいつも成分で書くのは煩雑なので、$|I\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$

と表記する。(I=0,1,…, N-1)

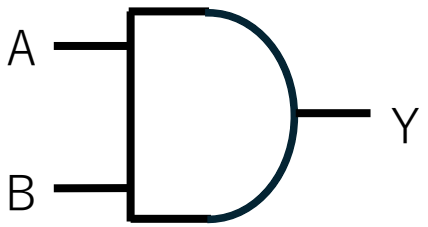
3) 1回の測定で状態 ψ は、$|\psi_I|^2$ の確率で $\psi \to |I\rangle$ と変化する。

2. 論理回路

古典論理回路とは「0」と「1」の信号を用いて
AND, OR, NOT, XORなどの論理演算を行うもの

入力1	入力2	出力
A	B	Y
0	0	0
0	1	0
1	0	0
1	1	1

ANDゲート



量子論理回路とは「０」と「１」に対応する状態の重ね合わせを信号に用いて、さまざまな論理演算を行うもの

重ね合わせ状態

- １量子ビット（２成分ベクトル）

$$\psi = \begin{pmatrix} \psi_0 \\ \psi_1 \end{pmatrix} = \psi_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \psi_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \psi_0 |0\rangle + \psi_1 |1\rangle$$

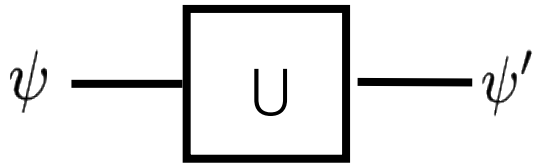
「０」状態　　「１」状態

これにより、複数個の入力値を一度に取り扱える。

ただし、『量子コンピュータは並列計算だから速い』は間違い

論理演算:状態ベクトルに行列をかける操作に対応

- 1量子ビットのとき

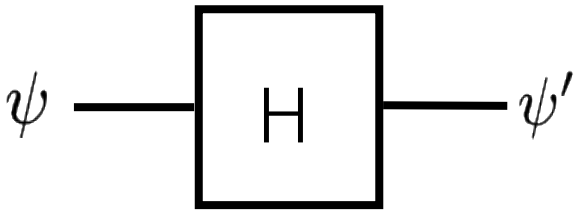


ψ：量子ゲートの入力
ψ'：量子ゲートの出力

$$\psi \longrightarrow \psi' = U\psi$$

2成分ベクトル　　2x2行列

例）アダマールゲート



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

重ね合わせ状態

- 2量子ビット（2つの２成分ベクトルの組み合わせ）のとき

$$\psi = \psi_{00}\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} + \psi_{01}\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} + \psi_{10}\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix} + \psi_{11}\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}$$

1つ目の量子が「０」で
2つ目の量子も「０」

ここで⊗ とは、「2つのベクトルを組み合わせること」
を意味する記号で『ベクトルのテンソル積』という。

✓ 2量子ビットは４個の独立な状態があるので、
４成分ベクトルで書くこともできる。

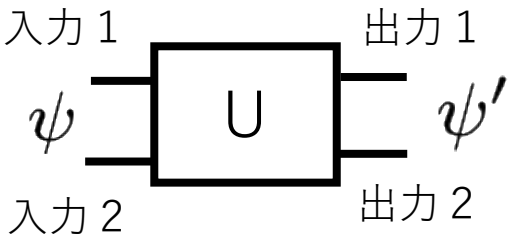
$$\psi = \begin{pmatrix}\psi_{00}\\ \psi_{01}\\ \psi_{10}\\ \psi_{11}\end{pmatrix}$$

✓N量子ビット➔ 2^N 成分ベクトル

論理演算:状態ベクトルに行列をかける操作に対応

- 2量子ビットのとき

$$\psi = \begin{pmatrix} \psi_{00} \\ \psi_{01} \\ \psi_{10} \\ \psi_{11} \end{pmatrix} \longrightarrow \psi' = \begin{pmatrix} \quad 4\text{x}\,4\ \text{行列} \quad \end{pmatrix} \begin{pmatrix} \psi_{00} \\ \psi_{01} \\ \psi_{10} \\ \psi_{11} \end{pmatrix}$$



ψ ：量子ゲートの入力 1 , 2
ψ' ：量子ゲートの出力 1 , 2

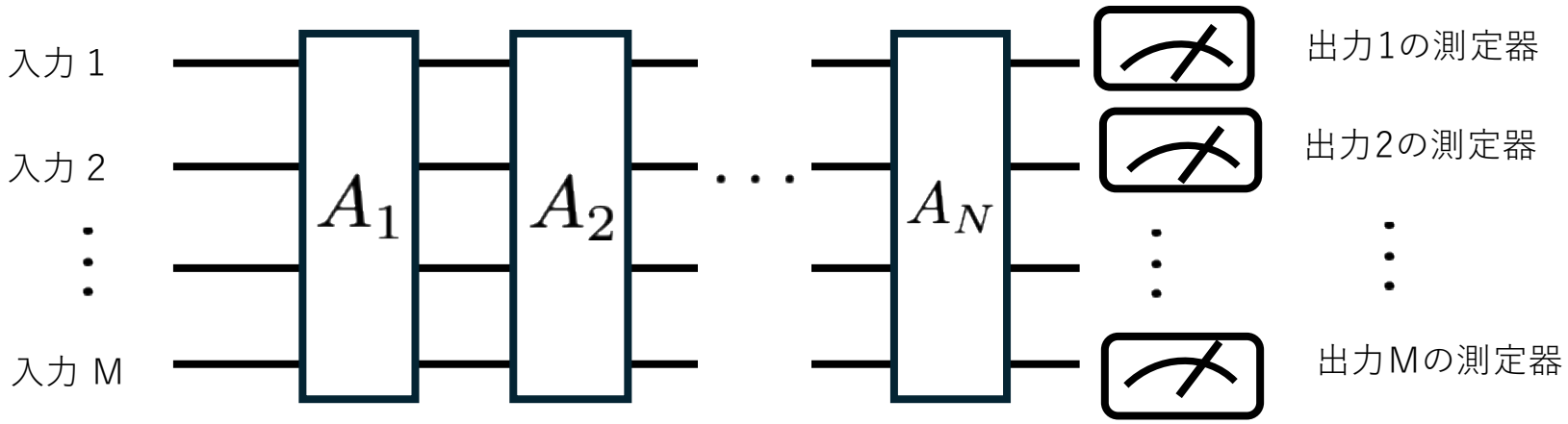
例）CNOTゲート(コントロール ノット ゲート)

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

- 入力 1 ベクトルが「0」の状態の部分に対しては
  出力2 = 入力 2
- 入力 1 ベクトルがが「1」の状態の部分に対しては
  出力2 は 入力 2 を反転したもの

実際の量子計算

複数個(M個）の入力ベクトルに量子ゲートに対応する様々な行列を掛け（N回）、最後に測定をおこなう。



上にある行列は
- 1つのベクトルにだけ作用する（例：アダマールゲート）
- あるいは2つのベクトルの組に作用する（例：CNOTゲート）

など色々可能。（その場合、残りのベクトルはそのまま素通り）

3. 素因数分解: Shorのアルゴリズム

RSA暗号とは文字列を「公開鍵」で変換し、秘密鍵で復元する。

Rivest-Shamir-Adleman

準備：

1. N は非常に大きな2つの素数p, qの積 N=p q

2. (p-1)(q-1)という数字から「エンコーダ」e,「デコーダ」dが作れる。

3. e, Nは公開鍵、dは秘密鍵

使い方：

1. 公開鍵 N, e だけを知っている人が暗号を送る
   1. 文字列を 2進数の数字 aに変換　“onogi”=01101111011011100110111101100111011010010000101O
   2. e（エンコーダ） で暗号 $b = Mod(a^e, N)$ を生成
   3. bを送信

a^eをNで割った余り

2. 秘密鍵 d も知っている人が暗号を受け取る
   1. d（デコーダ） で　$a = Mod(b^d, N)$ を復元

Nが素因数分解されたら、秘密鍵dまでバレてしまう。

「素因数分解が現実的時間で不可能」がRSA暗号の大前提。

素因数分解の計算量

- Shor のアルゴリズムの計算量は $n = \log N$ とおいて、およそ以下の程度 $\dfrac{n^2}{\log n \ \log(\log n)}$

- 古典計算機による素因数分解のアルゴリズムの計算量は
  - 素朴な方法　$\sqrt{N}$
  - ロー法　$N^{1/4} \log N$
  - 数体ふるい法　$\exp(cn^{1/3}(logn)^{2/3})$

- RSA暗号の典型的なp,qの典型的な大きさは1024ビットで、
  Nで言うと10進数で600桁。

$$N \sim 10^{600} \qquad n = \log_2 N = 600 \log_2 10 \sim 2000$$

アルゴリズム	計算量
素朴な方法	10^154
ロー法	10^77
数体ふるい法	10^26
Shorのアルゴリズム	10^10

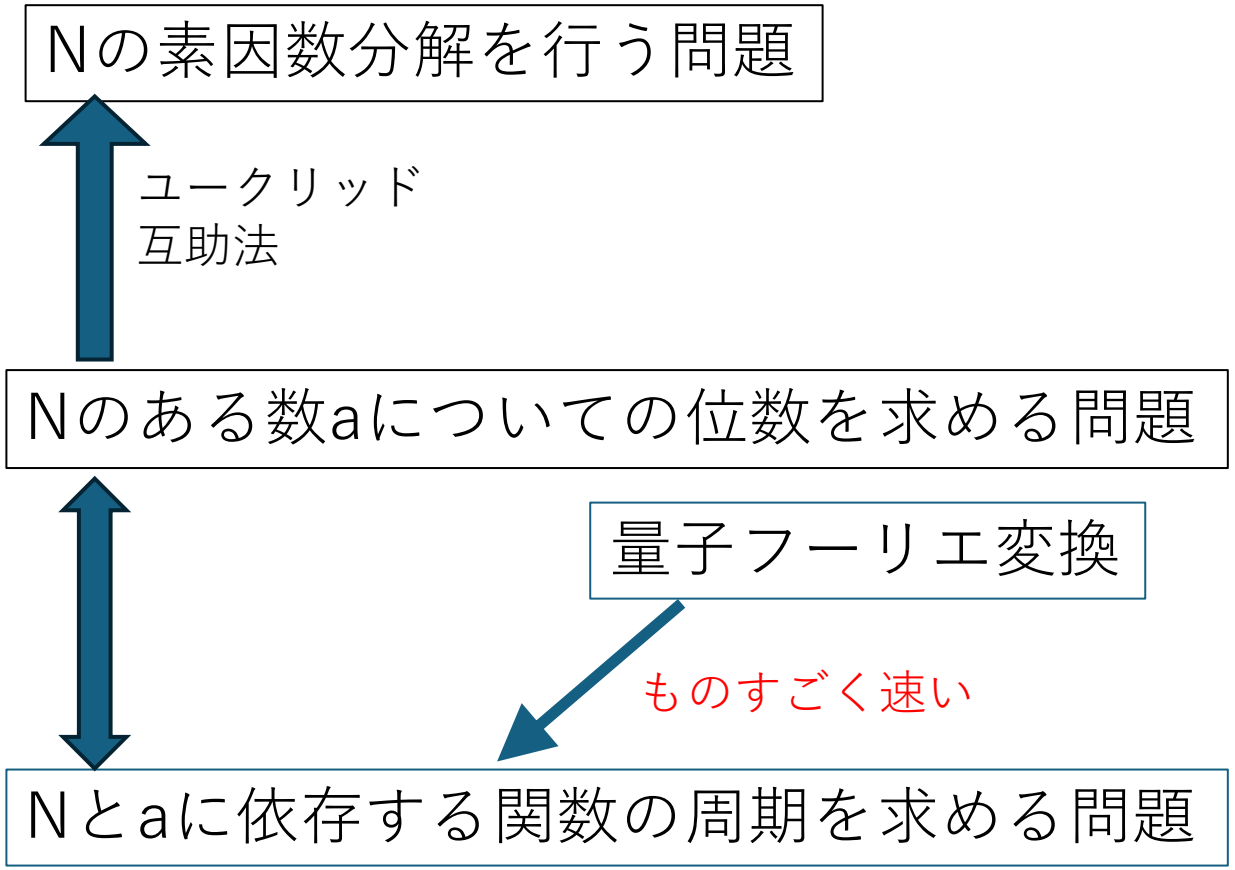
宇宙年齢で、
ぎりぎり？

パソコンで宇宙年齢時間計算した計算量

$$1\mathrm{Gflop/sec} \times 10^7 \mathrm{sec/year} \times 10^{10} \mathrm{year}$$
$$= 10^{26} \mathrm{flop}$$

N=pq の素因数分解の求め方

量子計算



クイズ１（素因数分解の問題）

N=21を素因数分解せよ。

答え：N= 3 x 7

クイズ2（位数の問題）

11^n をN=21 で割った余りが1になるnは？

a=11は適当に選んだ数

上の問題のゼロでない最小のnを「位数」という。

数学的には
「 $f(n) := \mathrm{mod}(11^n, 21) - 1$ がゼロとなるn を求めよ。」
と同等。

答え：n =0, 6, 12, …

位数は 6 。

$$11^6 = 1771561$$
$$= 84360 \times 21 + 1$$

一旦、位数が 6 と分かったとする

$$\underbrace{11^6-1}_{=(11^3+1)(11^3-1)=1332\times1330} = 84360 \times 21$$

左辺＝右辺なので、1332と1330は21と公約数を持つはず。

21と1332の最大公約数=3

21と1330の最大公約数=7

従って21の約数は3と 7 。

➔ 素因数分解ができた。

最大公約数は「ユークリッドの互助法」で素早く求められる。

どうやって位数が 6 であることを知るかが問題。
Nが10の600乗程度の場合は直接計算では絶望的。

これを一般化すると以下のようになる

NをN=pqと素因数分解する代わりに、ある数aを適当に選んで

$$a^r = 1 \pmod{N}$$

を満たす　r（Nのaについての位数）を求めれば

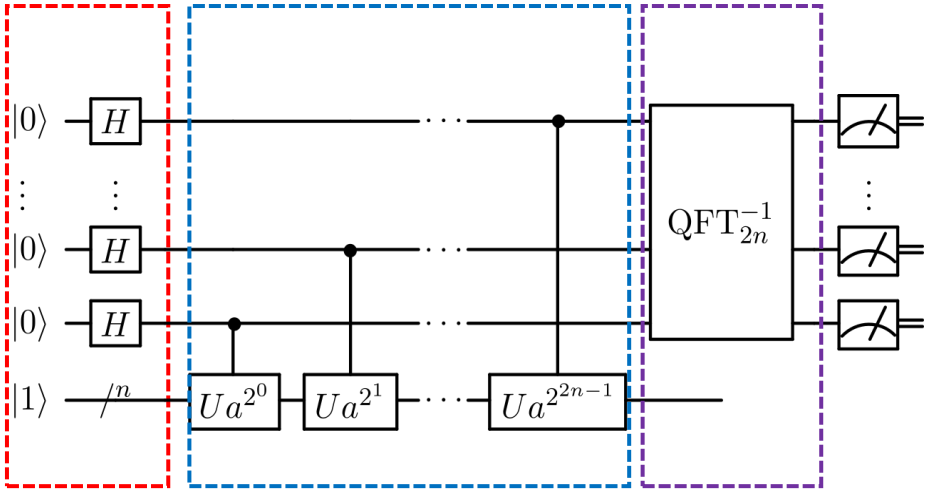
$$(a^{r/2}+1)(a^{r/2}-1) = kN$$　kはある整数

が成り立つので、pやqはN と $a^{r/2}+1,\ a^{r/2}-1$ の最大公約数から求まる。

位数を求めるには関数　$f_{a,N}(x) := a^x \pmod{N}$　の周期を求めれば良い。

位数（周期）を求める量子回路

1. 素因数分解したいN とそれと素なある整数aを用意
2. Nの 2 進数表記の桁数はn
3. 初期状態を準備
4. 制御ユニタリゲートを使って、位数を周期とする重ね合わせ状態を生成
5. 量子フーリエ変換を行なう。
6. 数回の測定を行うことで、周期（位数）を求める



位数を求める量子回路　Wikipediaより

3. アダマールゲートをうまく使って、初期状態を用意する。
すべての|x>が網羅されている。

$$\psi = \frac{1}{\sqrt{2048}} \sum_{x=0}^{2047} |x\rangle \otimes |1\rangle$$

4. 制御ユニタリゲートとして
となるものを用意する。

$$U_{11,21}|x\rangle \otimes |1 \pmod{21}\rangle := |x\rangle \otimes |11^x \pmod{21}\rangle$$

初期状態に制御ユニタリゲートをかけると

$$\begin{aligned}
\psi \xrightarrow{U_{11,21}} \sum_{x=0}^{2047} |x\rangle \otimes |11^x \pmod{21}\rangle \quad &= (|0\rangle + |6\rangle + |12\rangle + \cdots + |2046\rangle) \otimes |1 \pmod{21}\rangle \\
&+(|1\rangle + |7\rangle + |13\rangle + \cdots + |2047\rangle)|11 \pmod{21}\rangle \\
&+(|2\rangle + |8\rangle + |14\rangle + \cdots + |2042\rangle)|16 \pmod{21}\rangle \\
&+(|3\rangle + |9\rangle + |15\rangle + \cdots + |2043\rangle)|8 \pmod{21}\rangle \\
&+(|4\rangle + |10\rangle + |16\rangle + \cdots + |2044\rangle)|4 \pmod{21}\rangle \\
&+(|5\rangle + |11\rangle + |17\rangle + \cdots + |2045\rangle)|2 \pmod{21}\rangle
\end{aligned}$$

周期 6 の和にまとまっている量子もつれ状態が生成された。
しかしこのまま測定を行なっても、2048個の状態のどれか 1 つが選ばれるだけで、
本質的な情報は得られない。

5. 量子フーリエ変換

ここまでで得られた状態は、6個跳びの数に対応する状態の重ね合わせの形をしている。
そこで、以下で定義される「フーリエ変換」を考える。

$$|x\rangle = \frac{1}{\sqrt{2048}} \sum_{s=0}^{2047} \left[\cos\left(\frac{2\pi x s}{2048}\right) + i \sin\left(\frac{2\pi x s}{2048}\right) \right] |s\rangle$$

すると6個跳びの重ね合わせは

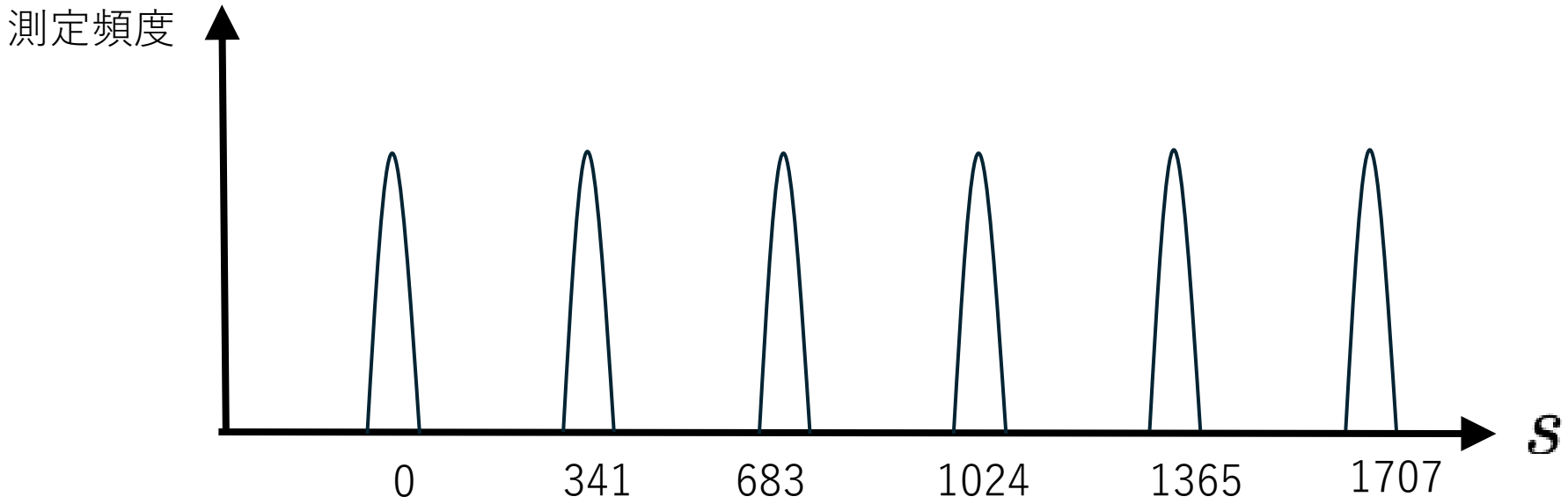
$$|0\rangle + |6\rangle + |12\rangle + \cdots + |2046\rangle$$

$$= \frac{1}{\sqrt{2048}} \sum_{s=0}^{2047} \left[1 + \cos\left(\frac{2\pi\ 6s}{2048}\right) + \cos\left(\frac{2\pi\ 12s}{2048}\right) + \cdots + \cos\left(\frac{2\pi\ 2046s}{2048}\right) \right.$$

$$\left. + i \left\{ \sin\left(\frac{2\pi\ 6s}{2048}\right) + \sin\left(\frac{2\pi\ 12s}{2048}\right) + \cdots + + \sin\left(\frac{2\pi\ 2046s}{2046}\right) \right\} \right] |s\rangle$$

各状態 |s>に対して、いろんな値の コサイン、サインが足し合わされる。
これは波の重ね合わせと似ている。sの値が特別でないときはほぼゼロになる。

しかし $\frac{2048}{6} = 341.333\cdots$ なので、sが0または341.33..やその倍数に近いとき
コサイン、サインの中身は2πのほぼ整数倍になり、波の重ね合わせの結果
ゼロにならずに生き残る。波の干渉における干渉縞の明るいところが測定される。



数回測定を行えば、どのsが干渉縞のピークかがわかり、
それから周期が6（すなわち位数が6）であることがわかる。

量子計算の何が本質的だったか？

- 解きたい問題が、多くの可能性の中から正解探す探索問題である。

- アダマールゲートを使って、すべての必要な計算を同時に行える状態を用意した。
- 制御ゲートを使って、うまい量子もつれ状態を作った。

- 量子フーリエ変換など、干渉効果を使って、正解に対応する状態の振幅が圧倒的に大きくなるように、最終処理を行なった。

これらの考え方は、量子探索問題で用いられるGroverのアルゴリズムなど他の場合にも共通である。

量子計算に対する誤解

- すべての計算が速くなる。➔ NO!
  探索問題が得意。サイズが大きくなると他では太刀打ちできなくなる。つまり、速さは、問題の種類とサイズに強く依存する。

- 並列計算だから速い➔ NO!
  そこまで速くはない。並列で計算できても、結果も重ね合わせなので、そこから干渉効果を使って、正解を浮き立たせるのが重要。そのステップの分だけ余計に時間がかかる。

- どんな問題でも使える。➔ NO!
  その問題に良い量子アルゴリズムが存在することが重要。まだ用途は限られている。ここは情報科学の研究者が世界中で研究中。これから解ける問題がじわじわと増えていくだろう。

4. まとめと参考文献

- 量子コンピュータは量子ゲートを用いて作動する。
- 初期状態はあらゆる可能な状態が含まれるようにしておく。
- 結果が確率的に出現するのが問題となる。量子もつれのある状態を作り、適切な操作と干渉効果を使って正解の振幅が大きくなるようにすると、正解が効率よく得られる。
- 今回は素因数分解のアルゴリズムを紹介したが、他にも量子暗号、量子探索問題、化学計算などの応用がある。AIも最適化問題の一種なので、量子AIも有望な応用かもしれない。

嶋田義皓「量子コンピューティング」オーム社

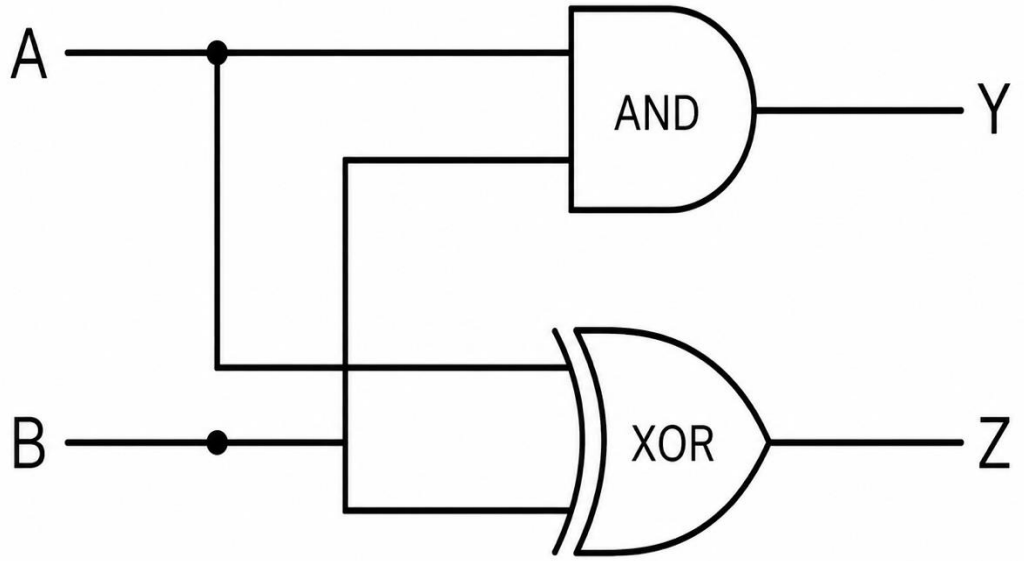
Backup Slides

応用例：２進法の足し算

0や1の足し算
- 0+0=0(=00)
- 0+1=1(=01)
- 1+0=1(=01)
- 1+1=2(=10)

繰り上がりも考慮

A	B	Y	Z
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0



. 論理回路

論理回路が演算の命令「AとBを足せ」
あとは具体的な入力があれば、自動的に結果が出力される。

ただし、一つ一つ入力していくしかない。