量子アルゴリズム

阿部 英介
理化学研究所 創発物性科学研究センター

応用物理情報特別講義A
2019年度春学期後半 金曜4限@14-202

参考書

- M. A. Nielsen & I. L. Chuang (2000)
  - “**Quantum Computation and Quantum Information**”

- **量子コンピュータ授業**
  - https://www.youtube.com/playlist?list=PLB1324F2305C028F7
  - http://www.appi.keio.ac.jp/Itoh_group/abe/

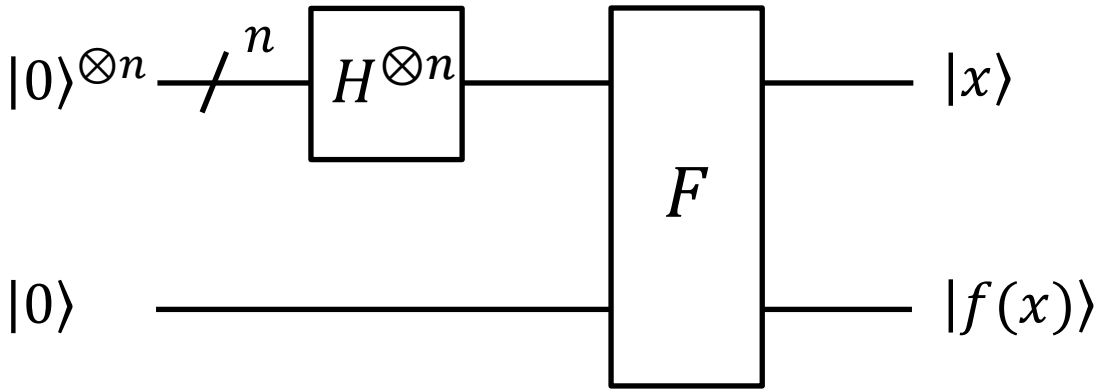
講義内容

- **量子並列性**
- **ドイチェ–ジョザのアルゴリズム**
- **量子フーリエ変換**
- **位数発見アルゴリズム**
- **素因数分解アルゴリズム**

講義内容

- **量子並列性**
- ドイチェ–ジョザのアルゴリズム
- 量子フーリエ変換
- 位数発見アルゴリズム
- 素因数分解アルゴリズム

量子並列性



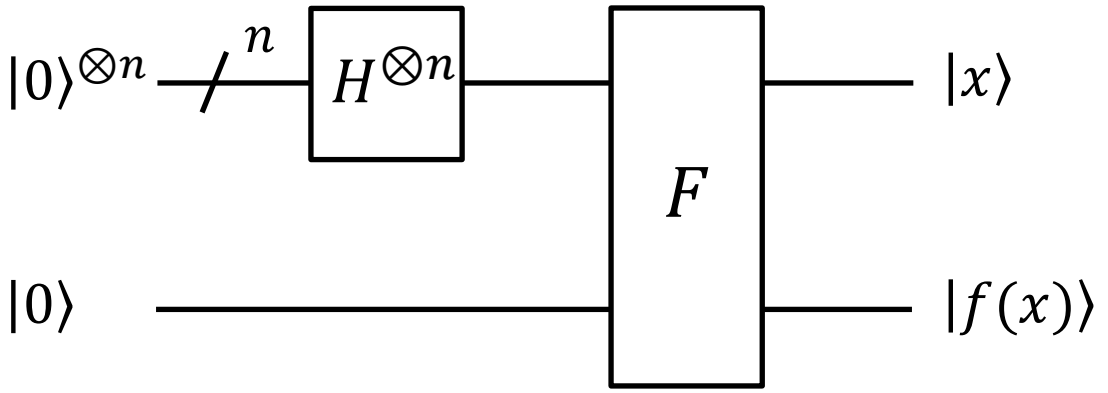
$f(x)$: 2値関数(ビットデータ列)

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

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

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

量子並列性



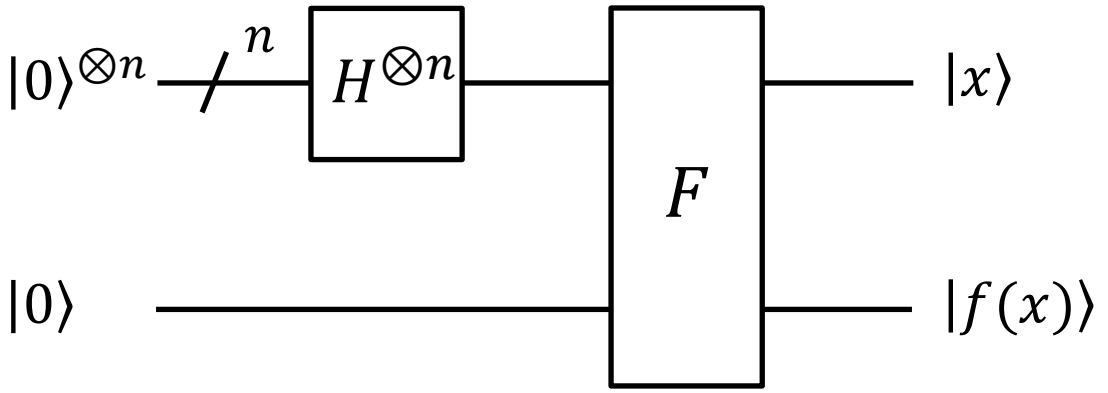
$$\frac{1}{\sqrt{2^2}}\sum_{x=0}^{2^2-1}|x\rangle|f(x)\rangle = \frac{1}{2}(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle + |2\rangle|f(2)\rangle + |3\rangle|f(3)\rangle)$$

$f(x)$の情報を全て含んだ量子もつれ状態

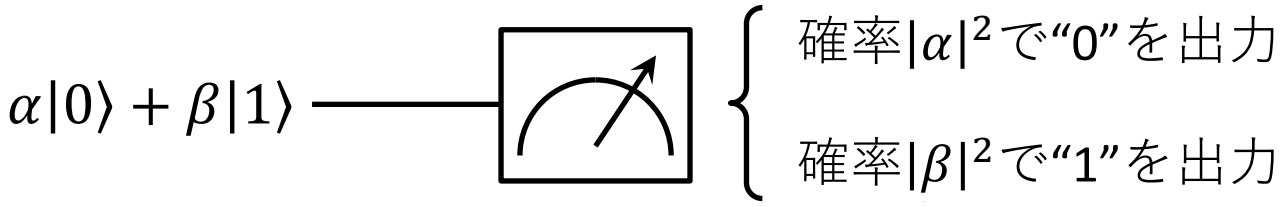
⇩

計算・情報処理の高速化に繋がる?

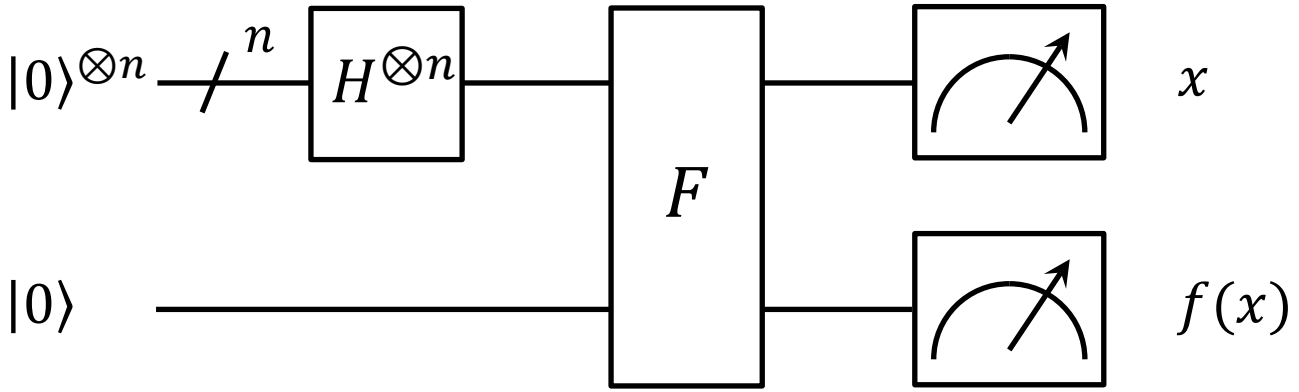
量子並列性と測定



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



量子並列性と測定



$$\frac{1}{\sqrt{2^2}}\sum_{x=0}^{2^2-1}|x\rangle|f(x)\rangle = \frac{1}{2}(\cancel{|0\rangle|f(0)\rangle} + |1\rangle|f(1)\rangle + \cancel{|2\rangle|f(2)\rangle} + \cancel{|3\rangle|f(3)\rangle})$$

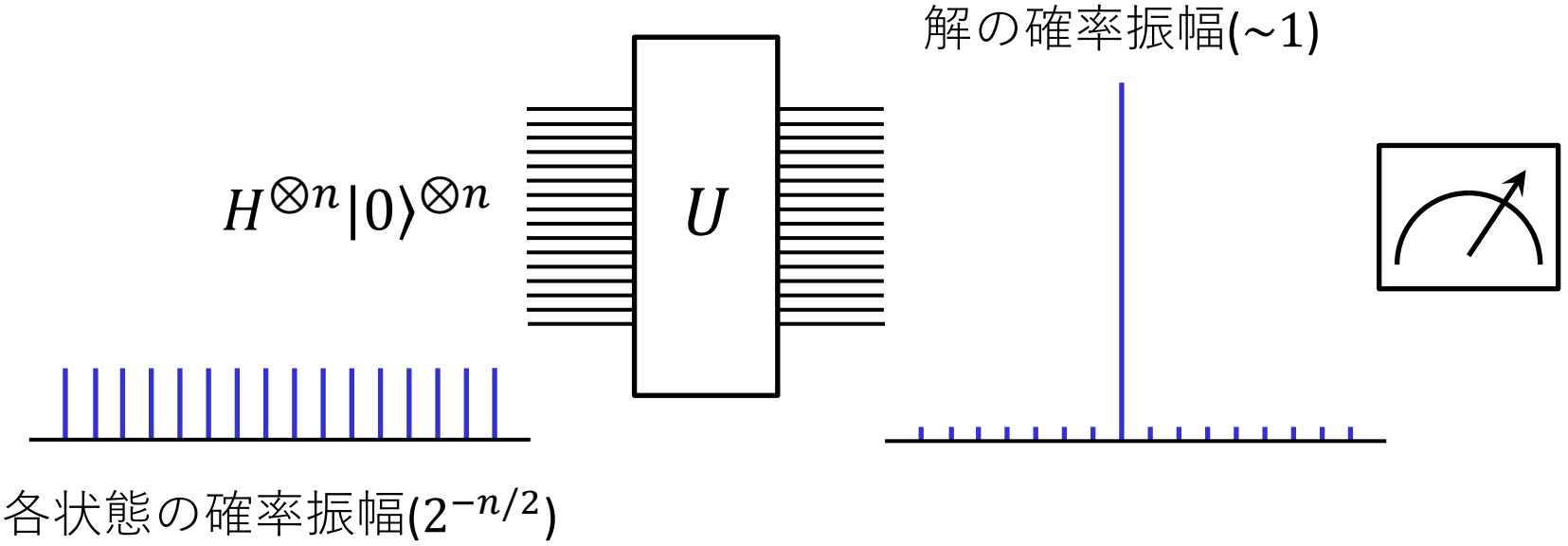
確率1/4でどれか1つの組の結果を知る

⇩

量子並列性にナイーブに期待される計算・情報処理の高速化は、
測定による状態の収縮によりキャンセルされそう

量子アルゴリズム

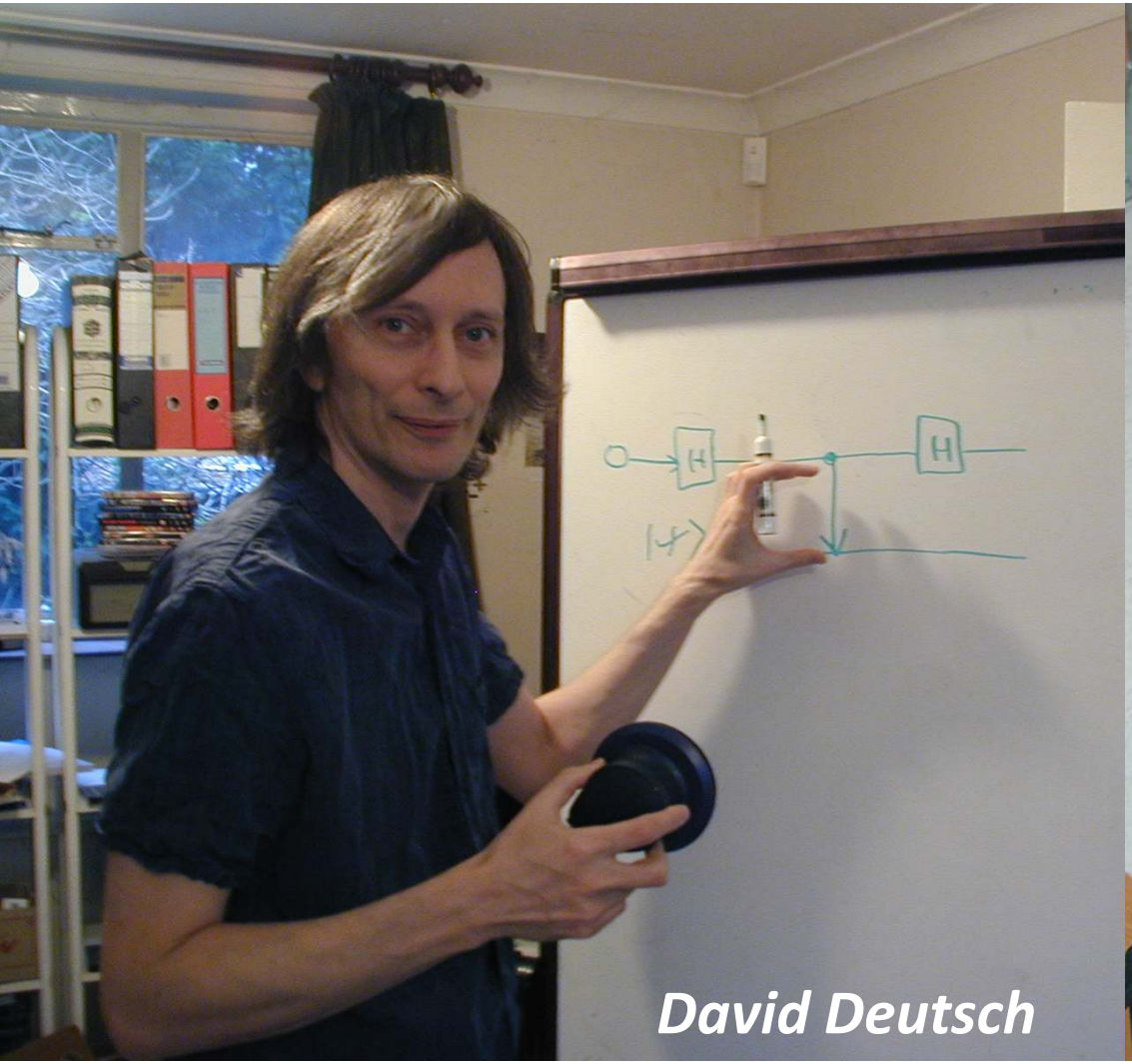
- 重ね合わせ状態(**量子並列性**)から始めて、解の状態の確率振幅が大きくなるよう(**量子干渉**)にユニタリ変換し、最後に**測定**
- **ドイチェ–ジョザ**、グローバー(データ検索)、ショア(素因数分解)...



講義内容

- 量子並列性
- **ドイチェ–ジョザのアルゴリズム**
- 量子フーリエ変換
- 位数発見アルゴリズム
- 素因数分解アルゴリズム

ドイチェ–ジョザのアルゴリズム



David Deutsch

Richard Jozsa

Proc. Royal. Soc. Lond. A **439**, 553 (1992) Deutsch & Jozsa

ドイチェの問題

定義: 2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)”**
- 半分が0、半分が1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

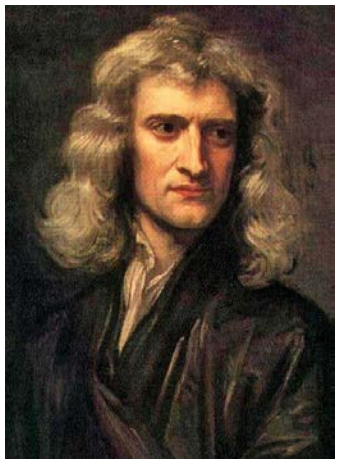
どちらでもない

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$f(x)$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



Isaac Newton
(1643–1727)

(From Wikipedia)

$x = 0$

$f(0) = 0$

$x = 1$

$f(1) = 0$

⋮

(最大$2^{n-1}+1$回)

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

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

$|\Psi\rangle$

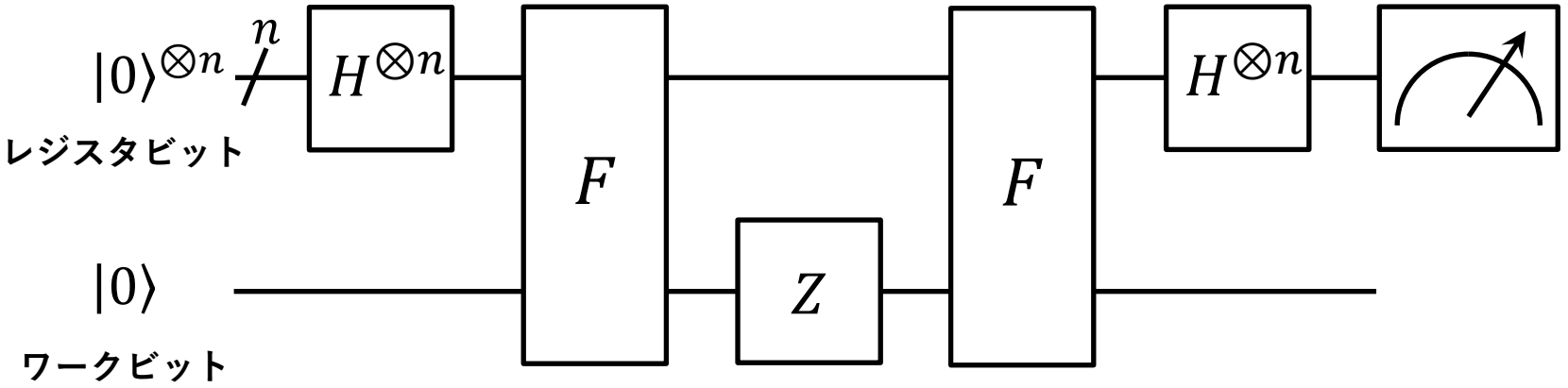
(常に1回)

“量子”問い合わせ

Erwin Schrödinger
(1887–1961)

©Nobel Foundation

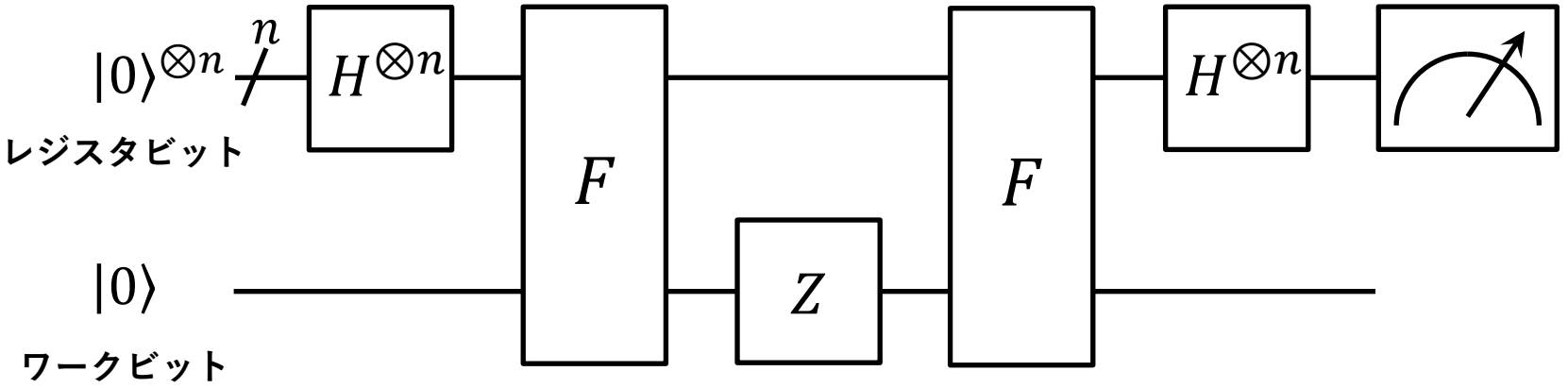
ドイチェ–ジョザのアルゴリズム



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

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

ドイチェ–ジョザのアルゴリズム

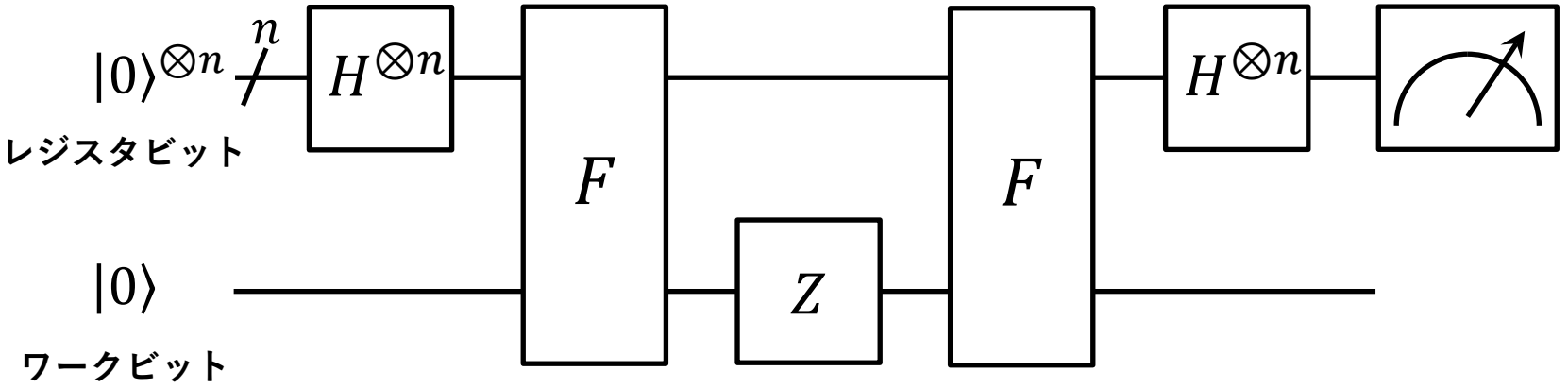


$$|0\rangle^{\otimes n}|0\rangle \xrightarrow{(H^{\otimes n})\otimes I} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle \xrightarrow{F} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle$$

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

$f(x)$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



$f(x)$の情報をワークビットから**消去**

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

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

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

ドイチェ–ジョザのアルゴリズム

レジスタビットが$|0\rangle^{\otimes n}$に戻る確率振幅

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

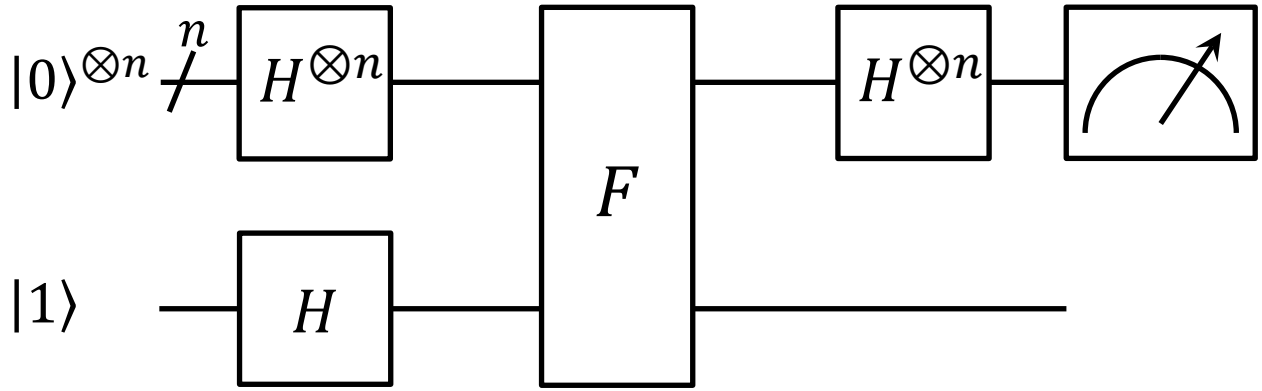
***n* = 2, 一定**　　干渉による強め合い

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

***n* = 2, 均等**　　干渉による弱め合い

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

改良版



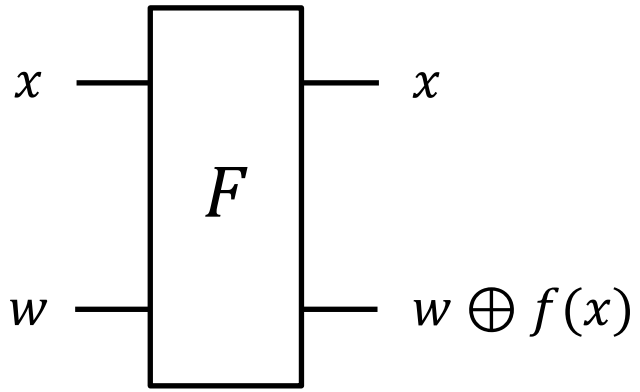
$$|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle)$$

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

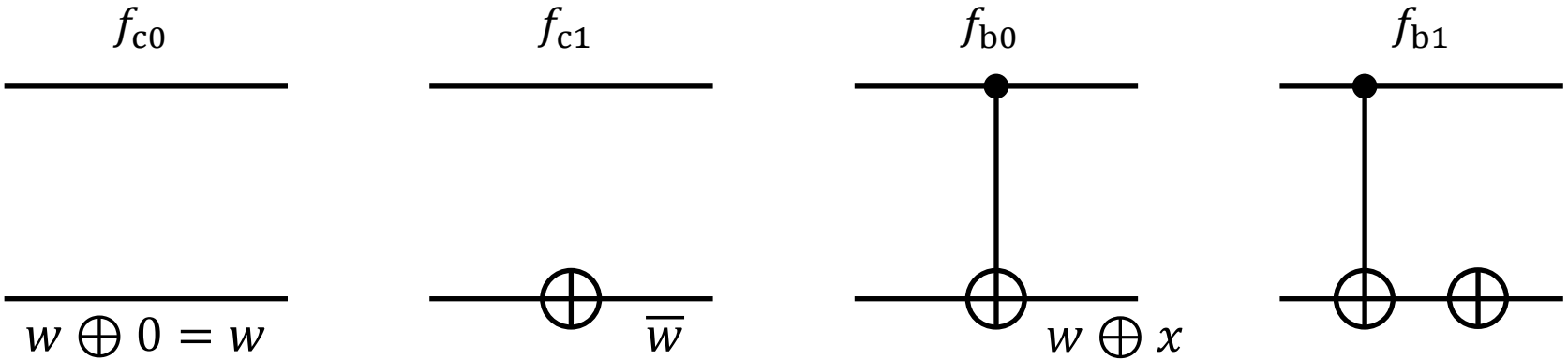
$$\xrightarrow{(H^{\otimes n})\otimes I} \sum_{x,y}\frac{(-1)^{f(x)+x\cdot y}}{2^n}|y\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

1ビットのFゲート

x	一定		均等	
	f_{c0}	f_{c1}	f_{b0}	f_{b1}
0	0	1	0	1
1	0	1	1	0

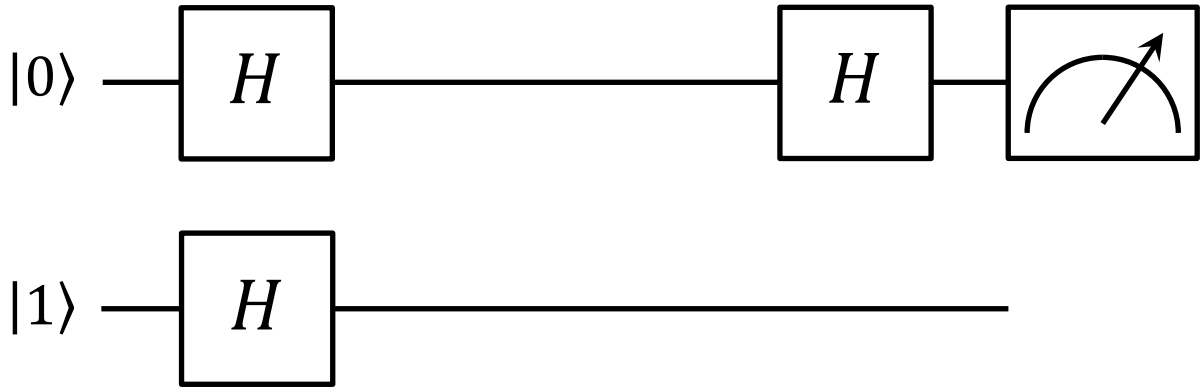


$$F|x\rangle|w\rangle = |x\rangle|w \oplus f(x)\rangle$$



NOTゲート　　制御NOTゲート

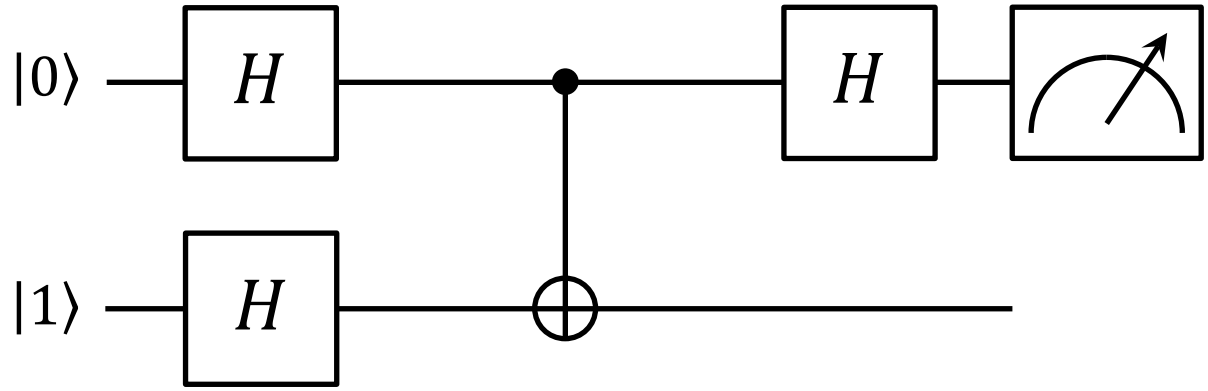
1ビットのDJ: f_{c0}(一定)



$$HH|0\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) = |0\rangle$$

干渉による強め合いと弱め合い

1ビットのDJ: f_{b0}(均等)



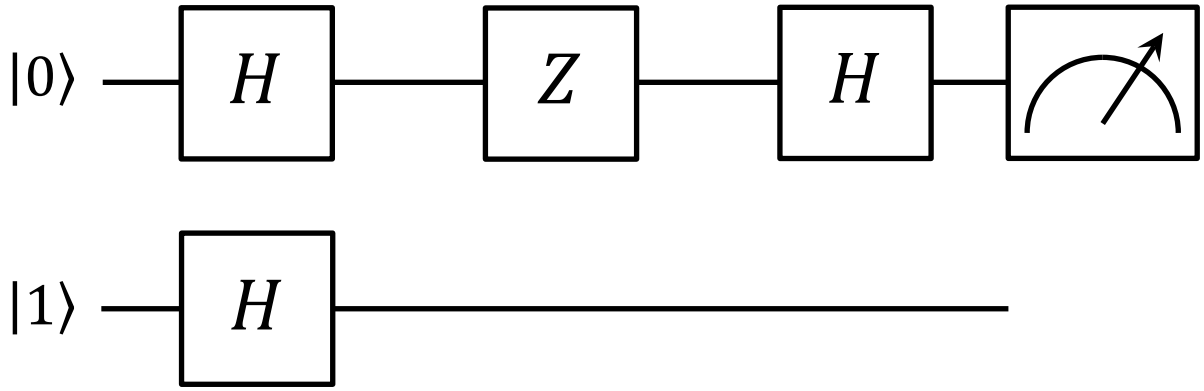
$$|0\rangle|1\rangle \xrightarrow{H^{\otimes 2}} \frac{1}{\sqrt{2}}\sum_{x=0}^{1}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$\xrightarrow{C_{\mathrm{rw}}} \frac{1}{\sqrt{2}}\sum_{x=0}^{1}(-1)^{x}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$(-1)^x$ ↓ レジスタへのZゲート

$$|0\oplus x\rangle-|1\oplus x\rangle=(-1)^{x}(|0\rangle-|1\rangle)$$

1ビットのDJ: f_{b0}(均等)



$$HZH|0\rangle = \frac{1}{2}(|1\rangle + |0\rangle + |1\rangle - |0\rangle) = |1\rangle$$

干渉による強め合いと弱め合い

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**位相コヒーレンス**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)

2ビットの$f(x)$

x	ab	一定		均等 ($_4C_2 = 6$)					
		f_{c0}	f_{c1}	f_{b0}	f_{b1}	f_{b2}	f_{b3}	f_{b4}	f_{b5}
0	00	0	1	0	0	0	1	1	1
1	01	0	1	0	1	1	1	0	0
2	10	0	1	1	0	1	0	1	0
3	11	0	1	1	1	0	0	0	1

$$f_{c0}(x) = 0$$

$$f_{c1}(x) = 1$$

$$f_{b0}(x) = a$$

$$f_{b1}(x) = b$$

$$f_{b2}(x) = a \oplus b$$

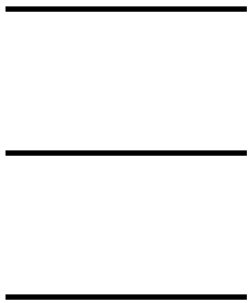
$$f_{b3}(x) = \bar{a}$$

$$f_{b4}(x) = \bar{b}$$

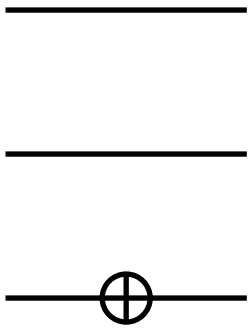
$$f_{b5}(x) = \overline{a \oplus b}$$

2ビットのFゲート

一定

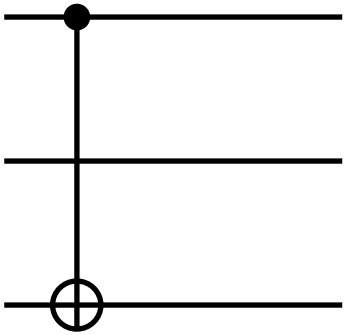


$f_{\mathrm{c}0}(x) = 0$

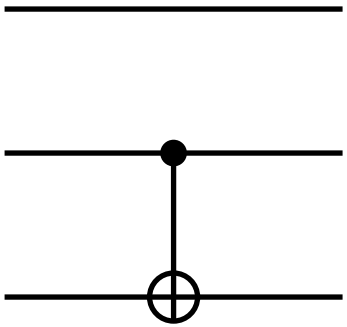


$f_{\mathrm{c}0}(x) = 1$

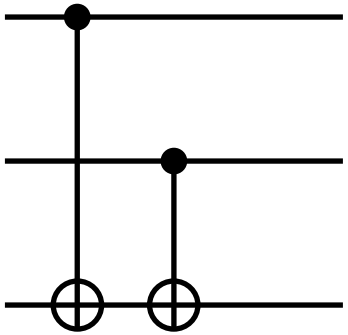
均等



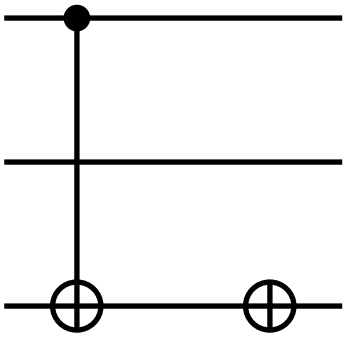
$f_{\mathrm{b}0}(x) = a$



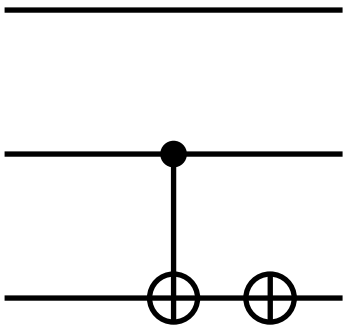
$f_{\mathrm{b}1}(x) = b$



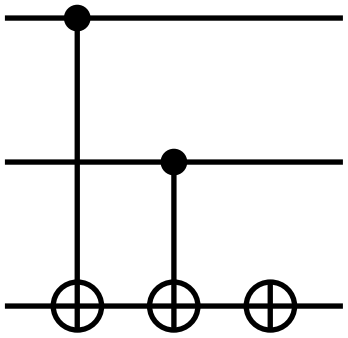
$f_{\mathrm{b}2}(x) = a \oplus b$



$f_{\mathrm{b}0}(x) = \bar{a}$



$f_{\mathrm{b}1}(x) = \bar{b}$



$f_{\mathrm{b}2}(x) = \overline{a \oplus b}$

3ビットの均等関数$f(x)$

可能な均等関数の数

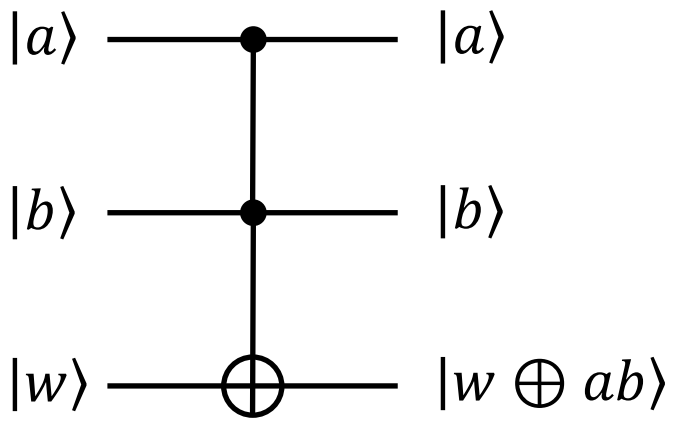
$$_8C_4 = 70$$

x	abc	f_{b0}	f_{b1}	f_{b2}	f_{b3}	f_{b4}	f_{b5}	f_{b6}	f_{b7}	f_{b8}	f_{b9}
0	000	0	0	0	0	0	0	0	0	0	0
1	001	0	0	1	1	1	1	0	0	0	0
2	010	0	1	1	0	0	1	0	1	0	1
3	011	0	1	0	1	1	0	1	0	1	0
4	100	1	1	1	0	1	1	1	1	0	1
5	101	1	1	0	1	0	0	1	1	1	0
6	110	1	0	0	1	0	1	0	1	1	1
7	111	1	0	1	0	1	0	1	0	1	1
均等関数の数		6	6	2	6	12	6	12	12	2	6

3ビットの均等関数$f(x)$

可能な均等関数の数

$$_8C_4 = 70$$



3ビットのFゲートの実装には
Toffoliゲートが有効

$f_{b0}(x) = a$ 他に$b, c, \bar{a}, \bar{b}, \bar{c}$

$f_{b1}(x) = a \oplus b$

$f_{b2}(x) = a \oplus b \oplus c$

$f_{b3}(x) = ab \oplus c$

$f_{b4}(x) = ab \oplus a \oplus c$

$f_{b5}(x) = ab \oplus a \oplus b \oplus c$

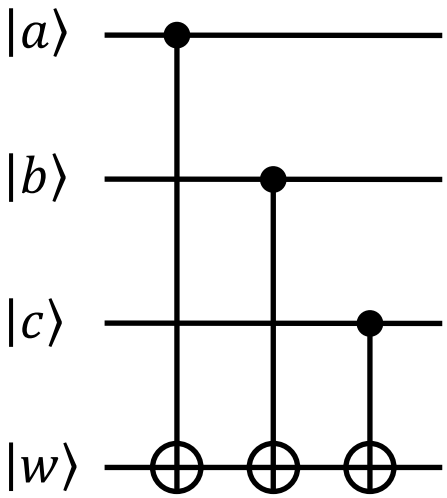
$f_{b6}(x) = ab \oplus bc \oplus a$

$f_{b7}(x) = ab \oplus bc \oplus a \oplus b$

$f_{b8}(x) = ab \oplus bc \oplus ca$

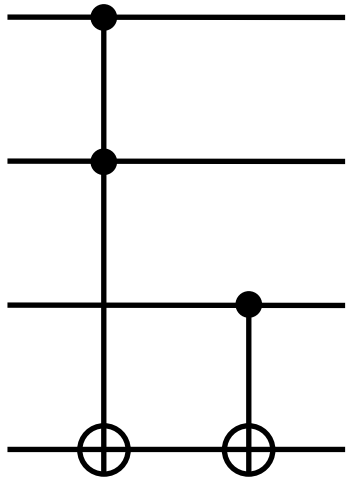
$f_{b9}(x) = ab \oplus bc \oplus ca \oplus a \oplus b$

3ビットのFゲートの例



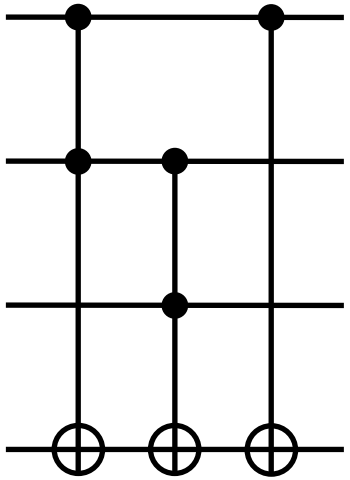
$f_{\mathrm{b2}} \oplus w =$

$a \oplus b \oplus c \oplus w$



$f_{\mathrm{b3}} \oplus w =$

$ab \oplus c \oplus w$



$f_{\mathrm{b6}} \oplus w =$

$ab \oplus bc \oplus a \oplus w$

レポート課題・第3問(12点)

f_{b9}に属する均等関数を全て示し、対応するFを
CNOT, Toffoli, NOTゲートを用いて構成せよ。

講義内容

- 量子並列性
- ドイチェ–ジョザのアルゴリズム
- **量子フーリエ変換**
- 位数発見アルゴリズム
- 素因数分解アルゴリズム

量子フーリエ変換

定義

$N = 2^n$とする

$$|j\rangle \xrightarrow{\mathrm{QFT}_N} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(2\pi i \frac{jk}{N}\right) |k\rangle$$

10進数表示　　10進数表示

例: $|5\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle$

$|6\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle$

例: $N = 2$

$$|j\rangle \xrightarrow{\mathrm{QFT}_2} \frac{1}{\sqrt{2}} \sum_{k=0}^{1} \exp(\pi i j k) |k\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{1} (-1)^{jk} |k\rangle$$

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

$$\exp(\pi i j k) = \begin{cases} 1 & (jk = 0) \\ -1 & (jk = 1) \end{cases}$$

QFT_2 = アダマールゲート

量子フーリエ変換

定義

$N = 2^n$とする

$$|j\rangle \xrightarrow{\mathrm{QFT}_N} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(2\pi i \frac{jk}{N}\right) |k\rangle$$

10進数表示　　10進数表示

例: $|5\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle$

$|6\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle$

レポート課題・第4問(5点)

$$|j\rangle \xrightarrow{\mathrm{QFT}_4} \frac{1}{2} \sum_{k=0}^{3} \exp\left(2\pi i \frac{jk}{4}\right) |k\rangle$$

QFT_4を4×4のユニタリ行列で表現せよ。

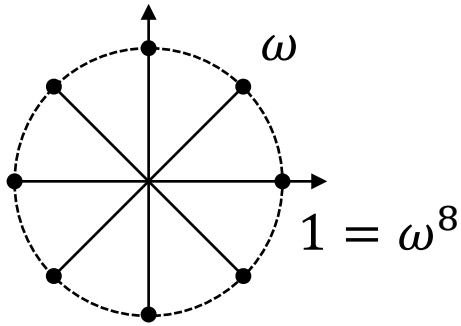
QFT_8

例: *N* = 8

$$|j\rangle \xrightarrow{\mathrm{QFT}_8} \frac{1}{\sqrt{8}}\sum_{k=0}^{7}\exp\left(2\pi i\frac{jk}{8}\right)|k\rangle = \frac{1}{\sqrt{8}}\sum_{k=0}^{7}\omega^{jk}|k\rangle$$

$$\omega \equiv \exp(2\pi i/8) = \sqrt{i}$$

$$\mathrm{QFT}_8 = \frac{1}{\sqrt{8}}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix}$$



$$\omega^l + \omega^{l+4} = 0$$

周期列の入力(QFT_8)

$$\sum_{j=0}^{7} \alpha_j |j\rangle \xrightarrow{\mathrm{QFT}_8} \sum_{k=0}^{7} \beta_k |k\rangle$$

r (周期)	入力列 $\{\alpha_j\}$									出力列 $\{\beta_k\}$								N/r
	0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7	
8	1	0	0	0	0	0	0	0	→	1	1	1	1	1	1	1	1	1
4	1	0	0	0	1	0	0	0	→	1	0	1	0	1	0	1	0	2
2	1	0	1	0	1	0	1	0	→	1	0	0	0	1	0	0	0	4
1	1	1	1	1	1	1	1	1	→	1	0	0	0	0	0	0	0	8

$$|0\rangle \longrightarrow |0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle$$

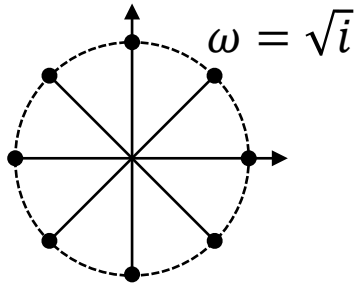
$$|0\rangle + |4\rangle \longrightarrow |0\rangle + |2\rangle + |4\rangle + |6\rangle$$

$$|0\rangle + |2\rangle + |4\rangle + |6\rangle \longrightarrow |0\rangle + |4\rangle$$

$$|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle \longrightarrow |0\rangle$$

周期列の入力(QFT_8)

r	入力列 $\{\alpha_j\}$									出力列 $\{\beta_k\}$								N/r
	0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7	
4	1	0	0	0	1	0	0	0	→	1	0	1	0	1	0	1	0	2



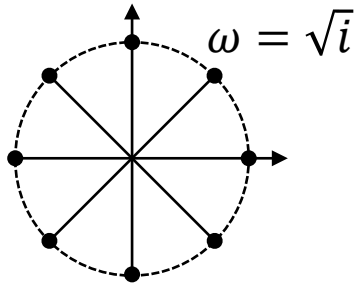
$$\omega^l + \omega^{l+4} = 0$$

$$\underbrace{|0\rangle + |4\rangle}_{} \qquad \underbrace{|0\rangle + |2\rangle + |4\rangle + |6\rangle}_{}$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1+\omega^4 \\ 2 \\ 1+\omega^4 \\ 2 \\ 1+\omega^4 \\ 2 \\ 1+\omega^4 \end{pmatrix} \approx \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

周期列の入力(QFT_8)

r	入力列 $\{\alpha_j\}$									出力列 $\{\beta_k\}$								N/r
	0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7	
2	1	0	1	0	1	0	1	0	→	1	0	0	0	1	0	0	0	4



$$\omega^l + \omega^{l+4} = 0$$

$$\underbrace{|0\rangle + |2\rangle + |4\rangle + |6\rangle}_{\text{}} \qquad \underbrace{|0\rangle + |4\rangle}_{\text{}}$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 1+\omega^2+\omega^4+\omega^6 \\ 1+\omega^4+1+\omega^4 \\ 1+\omega^6+\omega^4+\omega^2 \\ 4 \\ 1+\omega^2+\omega^4+\omega^6 \\ 1+\omega^4+1+\omega^4 \\ 1+\omega^6+\omega^4+\omega^2 \end{pmatrix} \approx \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

周期列の入力(QFT_8)

入力列 $\{\alpha_j\}$									出力列 $\{\beta_k\}$							
0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7
1	0	0	0	1	0	0	0	→	1	0	1	0	1	0	1	0
0	1	0	0	0	1	0	0	→	1	0	i	0	−1	0	$-i$	0
0	0	1	0	0	0	1	0	→	1	0	−1	0	1	0	−1	0
0	0	0	1	0	0	0	1	→	1	0	$-i$	0	−1	0	i	0

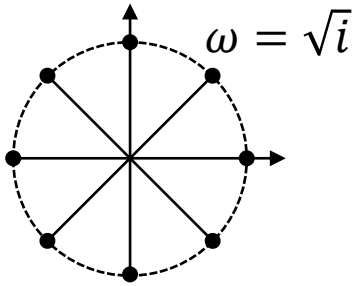
周期 *r* = 4

$$|0\rangle + |4\rangle \longrightarrow |0\rangle + |2\rangle + |4\rangle + |6\rangle$$
$$|1\rangle + |5\rangle \longrightarrow |0\rangle + i|2\rangle - |4\rangle - i|6\rangle$$
$$|2\rangle + |6\rangle \longrightarrow |0\rangle - |2\rangle + |4\rangle - |6\rangle$$
$$|3\rangle + |7\rangle \longrightarrow |0\rangle - i|2\rangle - |4\rangle + i|6\rangle$$

入力のオフセットは出力の位相因子に変換される(シフト不変)

周期列の入力(QFT_8)

r	入力列 $\{\alpha_j\}$									出力列 $\{\beta_k\}$								N/r
	0	1	2	3	4	5	6	7		0	1	2	3	4	5	6	7	
4	0	1	0	0	0	1	0	0	→	1	0	i	0	-1	0	i	0	2



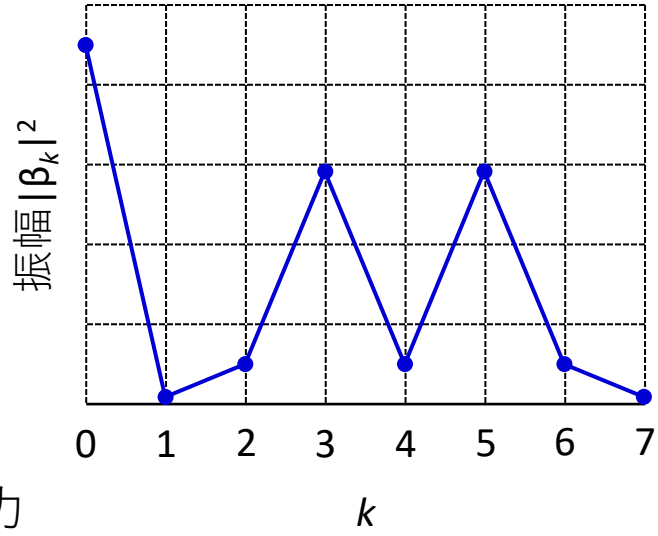
$$\omega^l + \omega^{l+4} = 0$$

$$\underbrace{|1\rangle + |5\rangle}_{} \qquad \underbrace{|0\rangle + i|2\rangle - |4\rangle - i|6\rangle}_{}$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ \omega^1 + \omega^5 \\ \omega^2 + \omega^2 \\ \omega^3 + \omega^7 \\ \omega^4 + \omega^4 \\ \omega^5 + \omega^1 \\ \omega^6 + \omega^6 \\ \omega^7 + \omega^3 \end{pmatrix} \approx \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \\ -1 \\ 0 \\ -i \\ 0 \end{pmatrix}$$

周期列の入力(QFT_8)

r	入力列 $\{\alpha_j\}$								N/r
	0	1	2	3	4	5	6	7	
3	1	0	0	1	0	0	1	0	2.7



周期 $r = 3$

Nがrで割り切れない場合は、近似的な周期を出力

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 1+\omega^3+\omega^6 \\ 1+\omega^6+\omega^4 \\ 1+\omega^1+\omega^2 \\ 2+\omega^4 \\ 1+\omega^7+\omega^6 \\ 1+\omega^2+\omega^4 \\ 1+\omega^5+\omega^2 \end{pmatrix}$$

周期列の入力(QFT_N)

$$\sqrt{\frac{r}{N}}\sum_{j=0}^{N/r-1}|jr+m\rangle \xrightarrow{\mathrm{QFT}_N} \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left(2\pi i\frac{mk}{r}\right)\left|\frac{N}{r}k\right\rangle$$

周期　オフセット　　位相　　周期の逆数

$$|j\rangle \to \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\exp\left(2\pi i\frac{jk}{N}\right)|k\rangle$$

証明(簡単のため*N*は*r*で割り切れると仮定)

$$\sqrt{\frac{r}{N}}\sum_{j=0}^{N/r-1}|jr+m\rangle \longrightarrow \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\sqrt{\frac{r}{N}}\sum_{j=0}^{N/r-1}\exp\left(2\pi i\frac{(jr+m)k}{N}\right)|k\rangle$$

$$\longrightarrow \frac{\sqrt{r}}{N}\sum_{k=0}^{N-1}\exp\left(2\pi i\frac{mk}{N}\right)\sum_{j=0}^{N/r-1}\exp\left(2\pi i\frac{jrk}{N}\right)|k\rangle$$

*N/r*が*k*で割り切れるかで場合分け

周期列の入力(QFT_N)

Case 1: $k = \frac{N}{r}k'$

$$\frac{\sqrt{r}}{N}\sum_{k=0}^{N-1}\exp\left(2\pi i\frac{mk}{N}\right)\underbrace{\sum_{j=0}^{N/r-1}\exp\left(2\pi i\frac{jrk}{N}\right)}|k\rangle$$

干渉による強め合い $\sum_{j=0}^{N/r-1}\exp(2\pi ijk') = \frac{N}{r}$

$\exp(2\pi ijk') = 1$

$$= \frac{\sqrt{r}}{N}\sum_{k'=0}^{r-1}\exp\left(2\pi i\frac{m}{N}\frac{N}{r}k'\right)\times\frac{N}{r}\times\left|\frac{N}{r}k'\right\rangle$$

$k: 0 \to N-1$
$k': 0 \to r-1$

$$= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left(2\pi i\frac{m}{r}k\right)\left|\frac{N}{r}k\right\rangle$$

周期列の入力(QFT_N)

Case 2: $k \neq \frac{N}{r}k'$

$$\frac{\sqrt{r}}{N}\sum_{k=0}^{N-1}\exp\left(2\pi i\frac{mk}{N}\right)\underbrace{\sum_{j=0}^{N/r-1}\exp\left(2\pi i\frac{jrk}{N}\right)}_{\sum_{j=0}^{N/r-1}\lambda^j=\frac{1-\lambda^{\frac{N}{r}}}{1-\lambda}=0}|k\rangle$$

干渉による弱め合い

$$\lambda \equiv \exp\left(2\pi i\frac{rk}{N}\right)$$

Case 1 & 2をまとめると

$$\sqrt{\frac{r}{N}}\sum_{j=0}^{N/r-1}|jr+m\rangle \xrightarrow{\mathrm{QFT}_N} \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left(2\pi i\frac{mk}{r}\right)\left|\frac{N}{r}k\right\rangle$$

量子干渉: 周期に一致した状態だけが生き残る

QFTの積表現

$|j_1 j_2 \cdots j_n\rangle$

$$\longrightarrow \frac{1}{\sqrt{2^n}}\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)$$

積表現を用いるとQFTの量子回路を見通しよく構成できる
(ユニタリ性も自動的に証明される)

記法

$$j = j_1 j_2 \cdots j_n = j_1 \cdot 2^{n-1} + j_2 \cdot 2^{n-2} + \cdots + j_n \cdot 2^0 = \sum_{k=1}^{n} j_k \cdot 2^{n-k}$$

$$0.j_1 j_2 \cdots j_n = j_1 \cdot 2^{-1} + j_2 \cdot 2^{-2} + \cdots + j_n \cdot 2^{-n} = \sum_{k=1}^{n} j_k \cdot 2^{-k}$$

QFTの積表現

$$|j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left(2\pi i \frac{jk}{2^n}\right) |k\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \exp\left(2\pi i \sum_{l=0}^{n} \frac{jk_l}{2^l}\right) |k_1 \cdots k_n\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} \exp\left(2\pi i \frac{jk_l}{2^l}\right) |k_l\rangle$$

$$= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} \exp\left(2\pi i \frac{jk_l}{2^l}\right) |k_l\rangle \right]$$

$$\frac{k}{2^n} = \frac{1}{2^n} \sum_{l=0}^{n} k_l 2^{n-l} = \sum_{l=0}^{n} k_l 2^{-l}$$

$$\exp(\alpha_1 + \alpha_2) |k_1\rangle \otimes |k_2\rangle = \left(e^{\alpha_1} |k_1\rangle\right) \otimes \left(e^{\alpha_2} |k_2\rangle\right)$$

$$\sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \left(e^{\alpha_1} |k_1\rangle \otimes e^{\alpha_2} |k_2\rangle\right) = \left(\sum_{k_1=0}^{1} e^{\alpha_1} |k_1\rangle \right) \otimes \left(\sum_{k_2=0}^{1} e^{\alpha_2} |k_2\rangle \right)$$

QFTの積表現

$$|j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} \exp\left(2\pi i \frac{jk_l}{2^l}\right) |k_l\rangle \right]$$

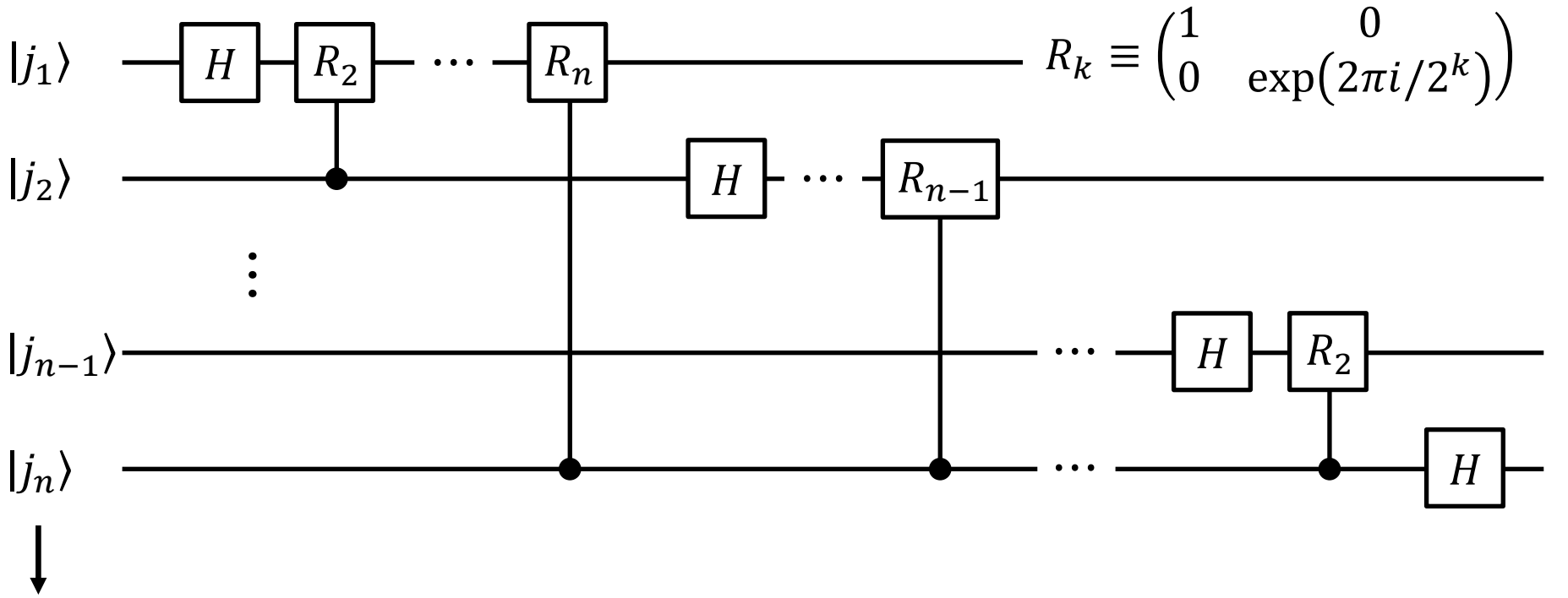
$$= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left[|0\rangle + \exp\left(2\pi i \frac{j}{2^l}\right) |1\rangle \right]$$

$$= \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)$$

$$\frac{j}{2^l} = \underbrace{\frac{1}{2^l}\left(j_1 \cdot 2^{n-1} + j_{n-l} \cdot 2^l + j_{n-l+1} \cdot 2^{l-1} \cdots + j_n \cdot 2^0\right)}$$

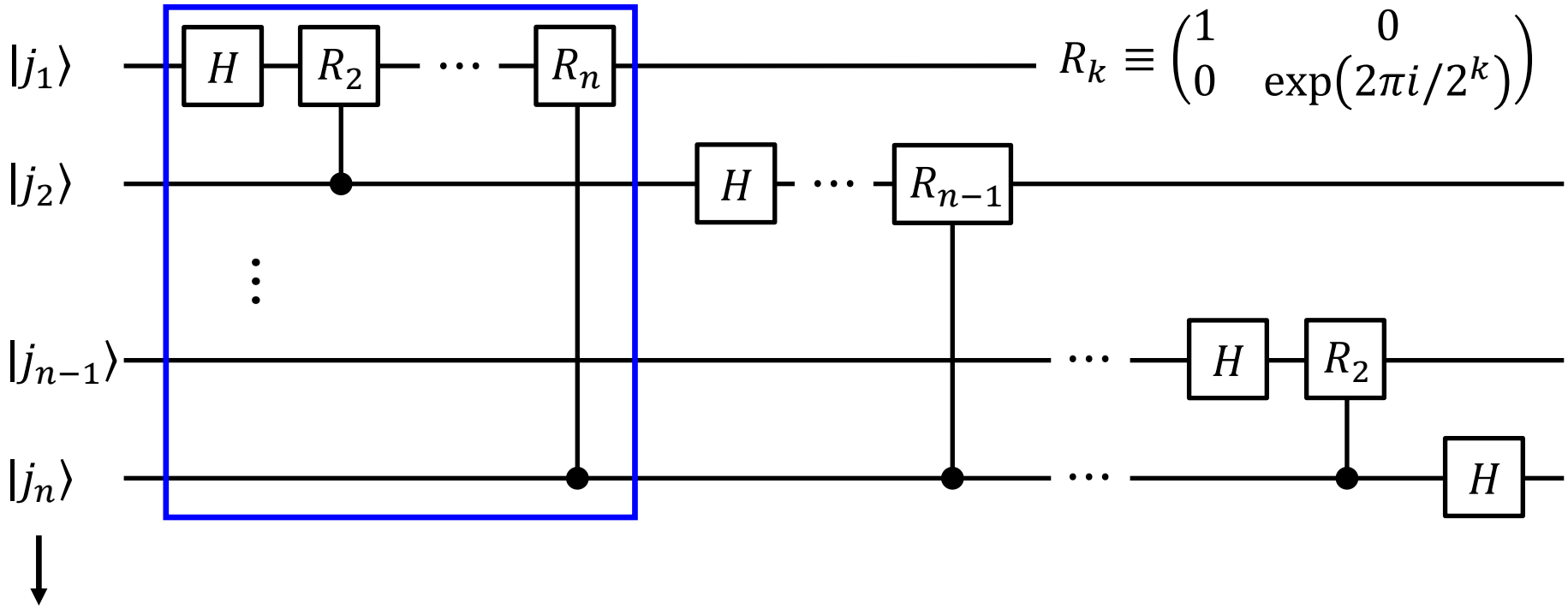
$$\exp(2\pi i j_1 \cdots j_{n-l}) = 1$$

QFTの量子回路



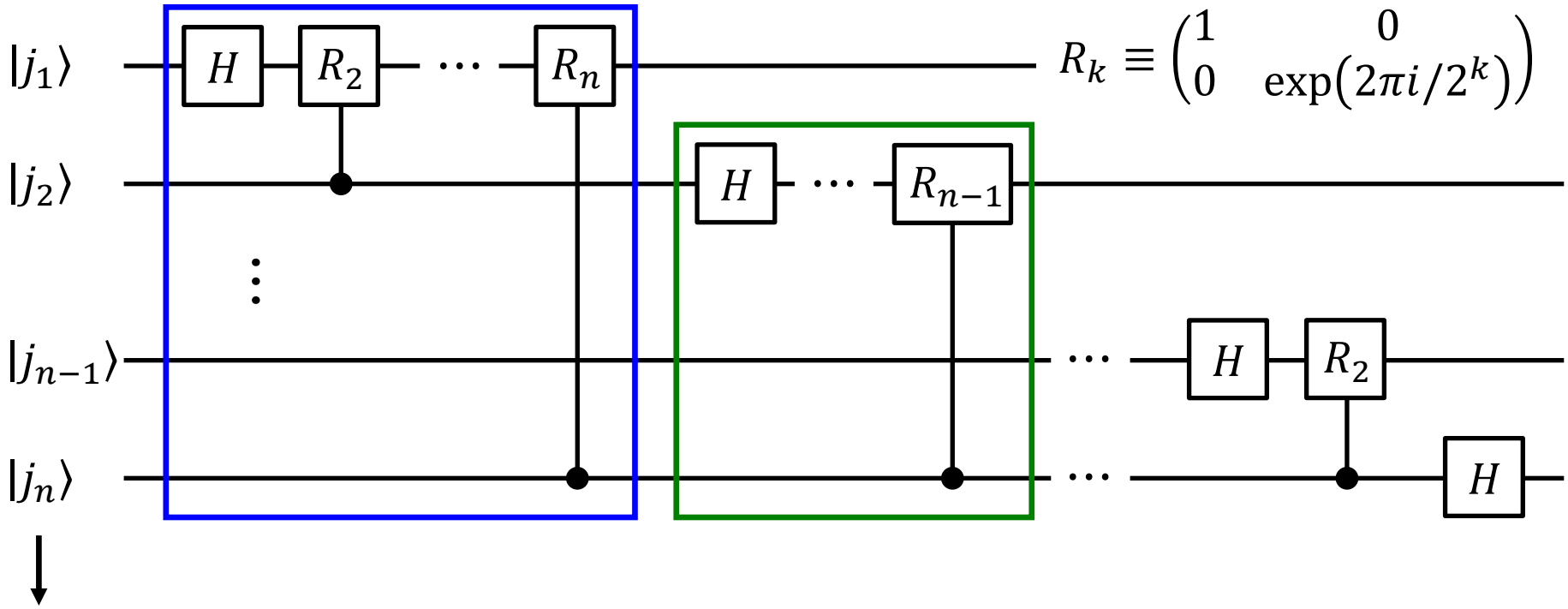
$$\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)$$

QFTの量子回路



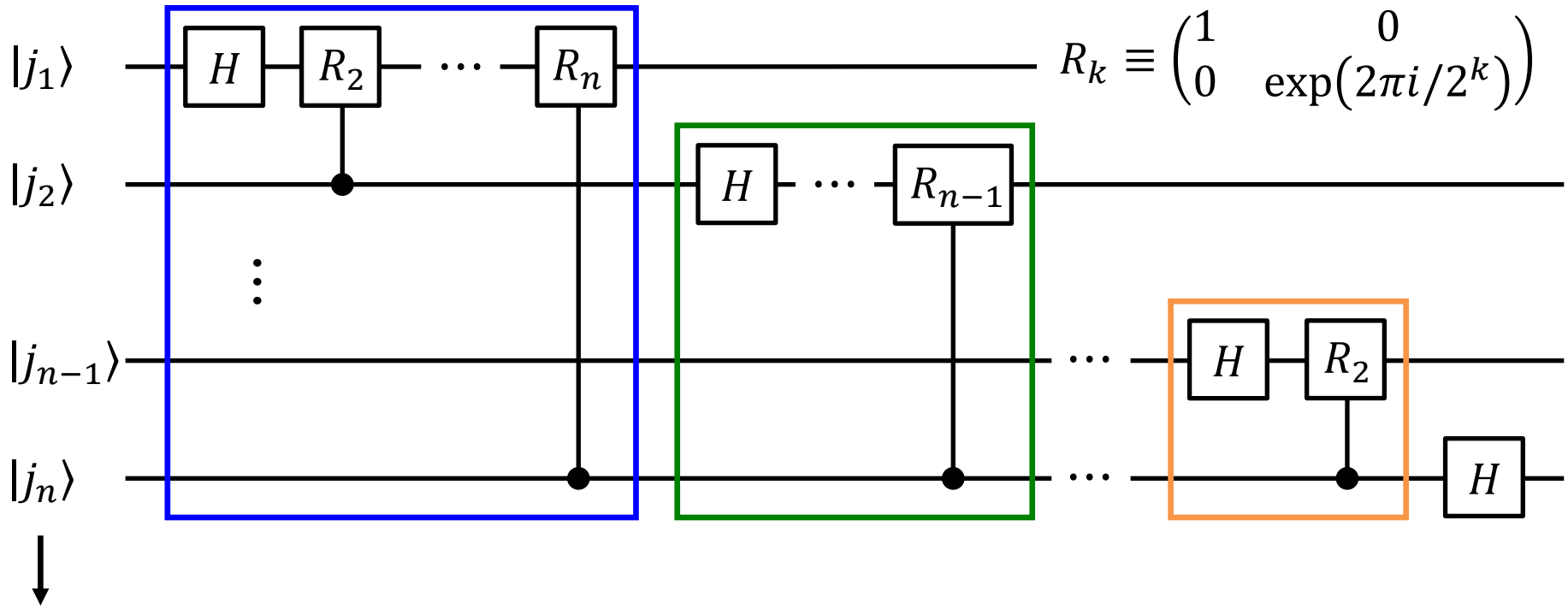
$$\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)$$

QFTの量子回路



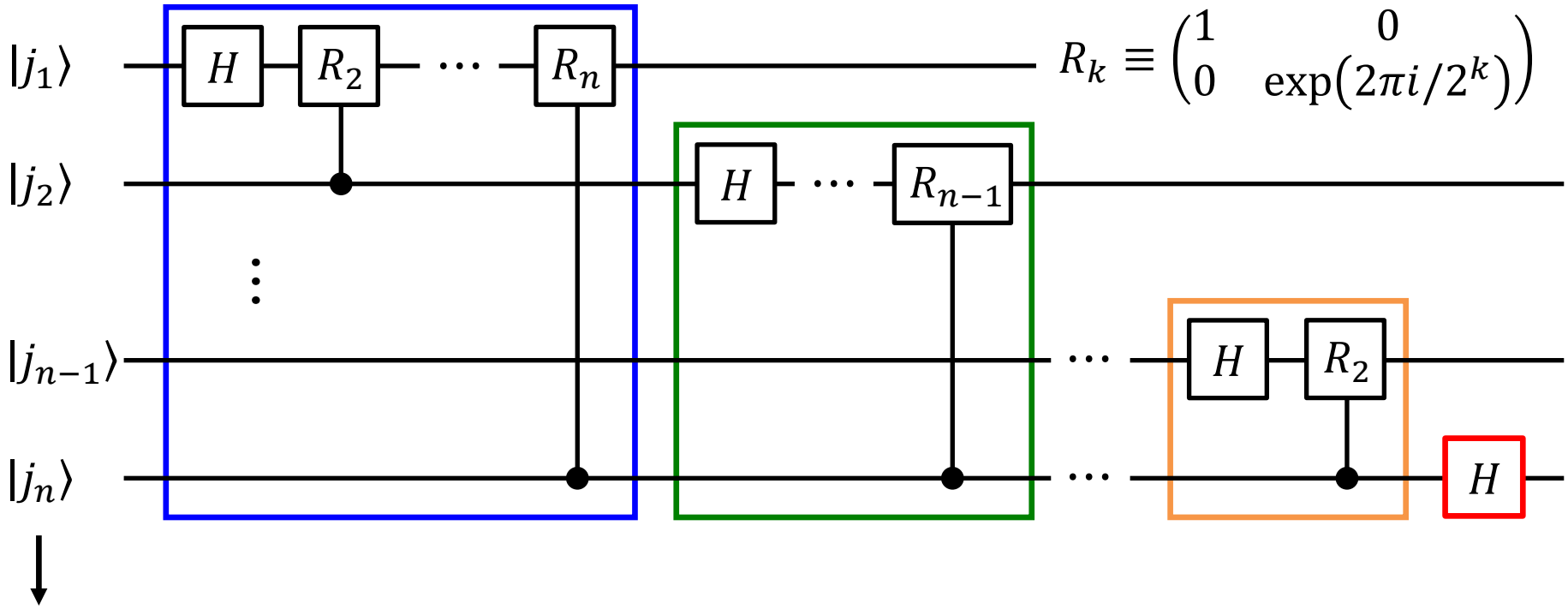
$$\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)$$

QFTの量子回路



$$\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)$$

QFTの量子回路

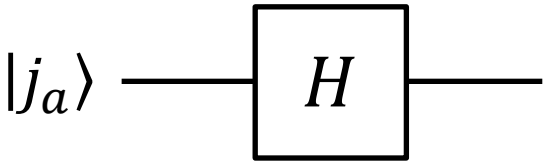


$$(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle) \cdots (|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)$$

SWAP

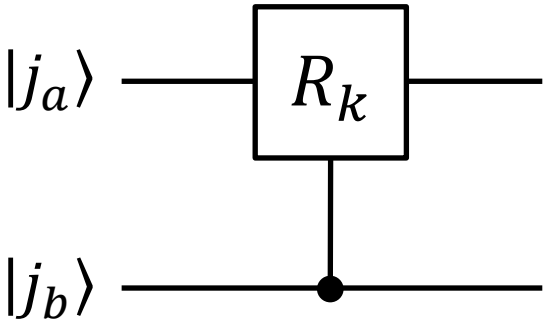
$$(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle) \cdots (|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle)$$

QFTの量子回路



$$\frac{|0\rangle + \exp(2\pi i 0.j_a)\,|1\rangle}{\sqrt{2}}$$

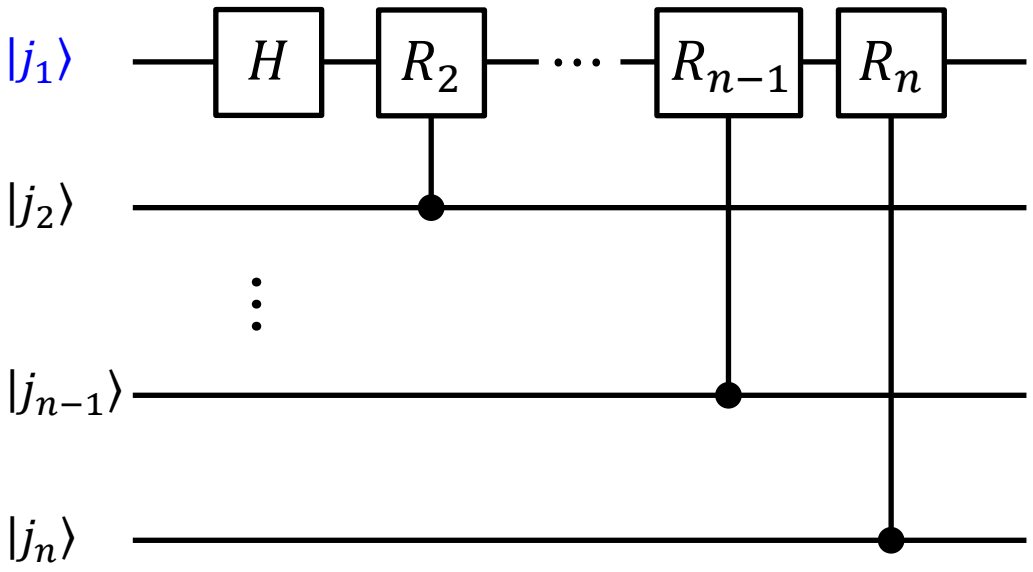
$$\exp(2\pi i 0.j_a) = \begin{cases} 1 & (j_a = 0) \\ -1 & (j_a = 1) \end{cases}$$



$$\exp(2\pi i \underbrace{0.0\cdots0j_b}_{k\text{桁}})\,|j_a\rangle \quad (j_a = 1, j_b = 1\text{のとき})$$

$$\exp(2\pi i 0.0\cdots0j_b) = \begin{cases} 1 & (j_b = 0) \\ \exp(2\pi i/2^k) & (j_b = 1) \end{cases}$$

QFTの量子回路

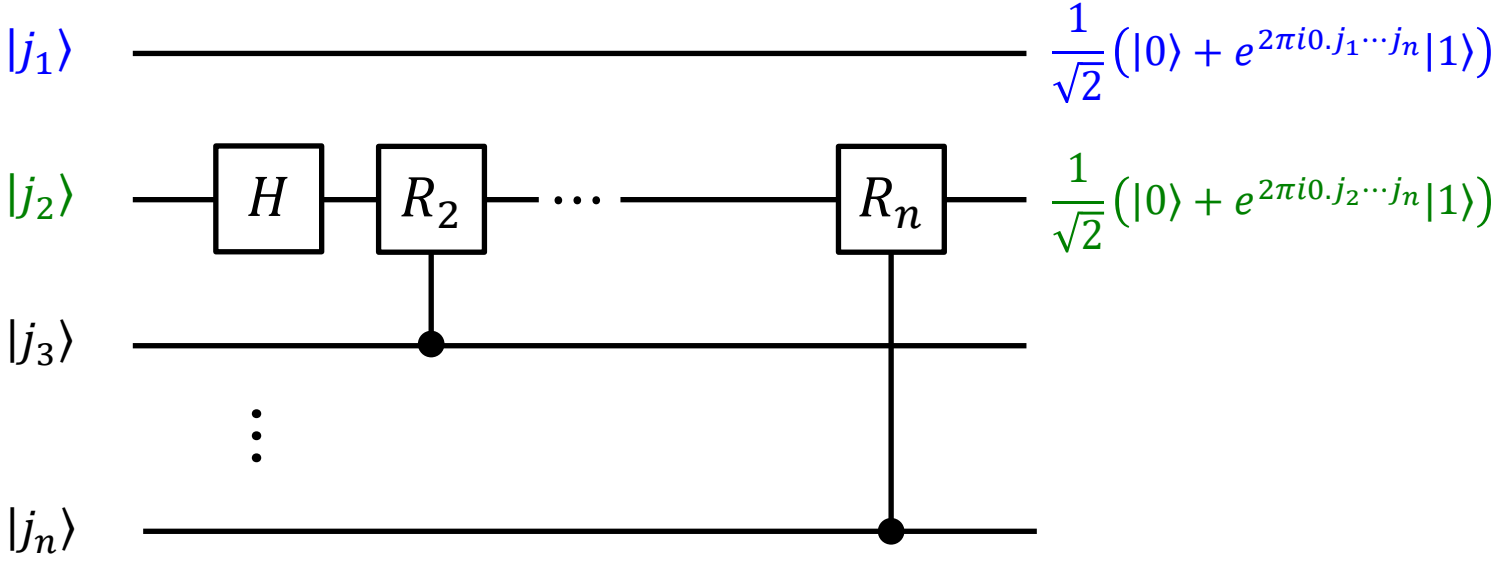


$$|j_1\rangle|j_2 \cdots j_n\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1}|1\rangle\right)|j_2 \cdots j_n\rangle$$

$$\xrightarrow{R_2} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle\right)|j_2 \cdots j_n\rangle$$

$$\cdots \xrightarrow{R_n} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)|j_2 \cdots j_n\rangle$$

QFTの量子回路

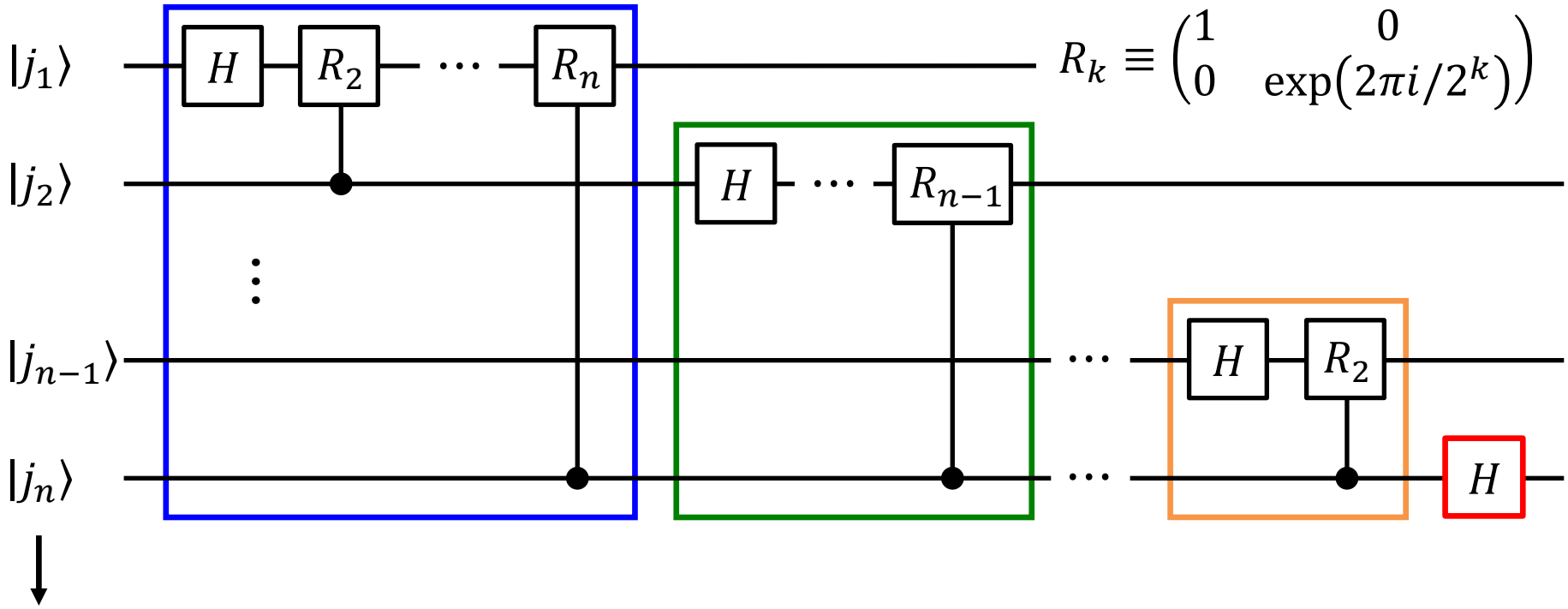


$$\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1\cdots j_n}|1\rangle)|j_2\rangle|j_3\cdots j_n\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_1\cdots j_n}|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i 0.j_2}|1\rangle)|j_3\cdots j_n\rangle$$

$$\xrightarrow{R_2} \frac{1}{2}(|0\rangle + e^{2\pi i 0.j_1\cdots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 j_3}|1\rangle)|j_3\cdots j_n\rangle$$

$$\cdots \xrightarrow{R_n} \frac{1}{2}(|0\rangle + e^{2\pi i 0.j_1\cdots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2\cdots j_n}|1\rangle)|j_3\cdots j_n\rangle$$

QFTの量子回路



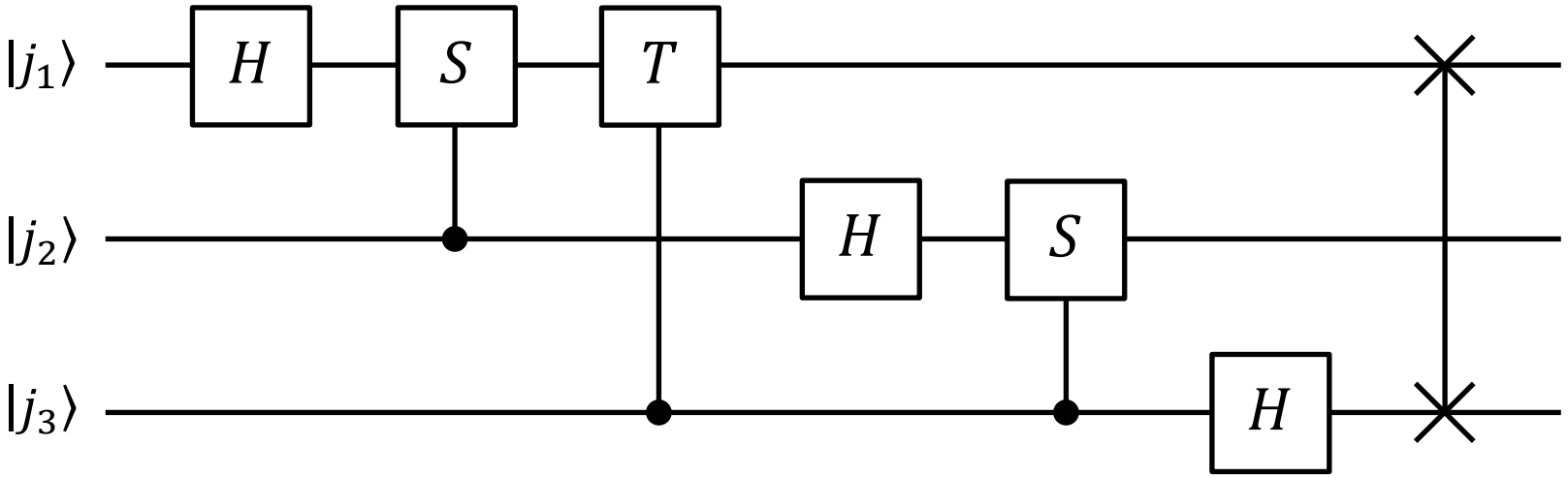
$$(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle) \cdots (|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)$$

SWAP

$$(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1} j_n}|1\rangle) \cdots (|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle)$$

QFT_8の量子回路

$$|j_1 j_2 j_3\rangle \xrightarrow{\mathrm{QFT}_8} \frac{1}{\sqrt{8}}\left(|0\rangle + e^{2\pi i 0.j_3}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 j_3}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.J_1 j_2 j_3}|1\rangle\right)$$



$$S = R_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad T = R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

講義内容

- 量子並列性
- ドイチェ–ジョザのアルゴリズム
- 量子フーリエ変換
- **位数発見アルゴリズム**
- 素因数分解アルゴリズム

置換の位数

例

y	$\pi(y)$
0	3
1	7
2	5
3	1
4	2
5	4
6	6
7	0

置換操作$\pi(y)$に対して

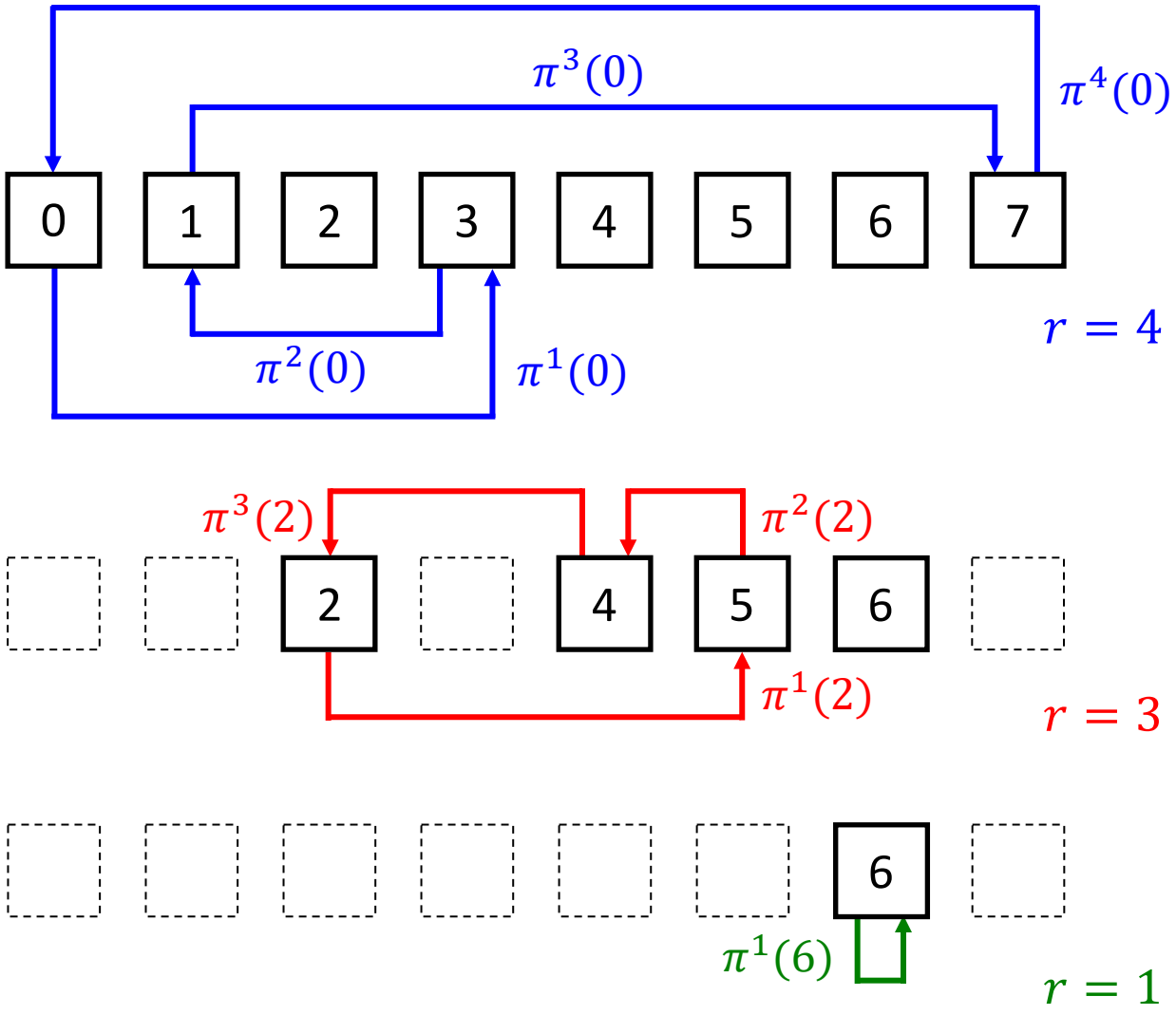
$$\pi^r(y_0) = y_0$$

を満たす**最小のr**を**位数(order)**と呼ぶ

一般に、rは入力y_0に依存

置換の位数

y	$\pi(y)$
0	3
1	7
2	5
3	1
4	2
5	4
6	6
7	0

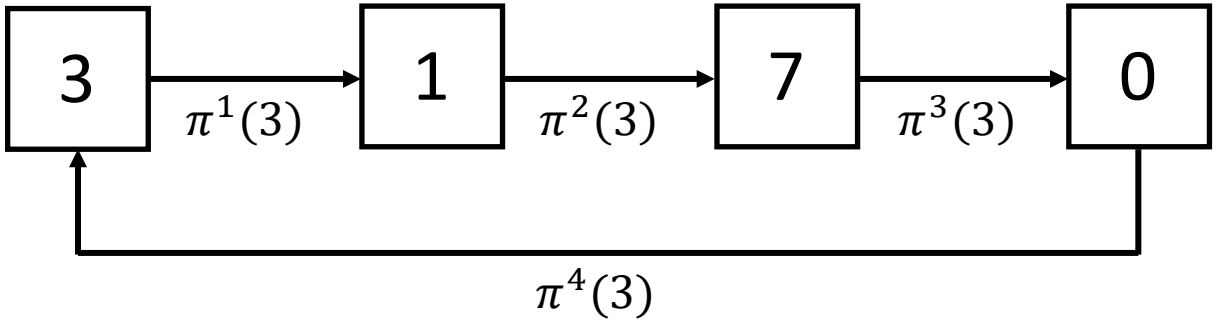


置換操作における周期性

$r = 4$

y	$\pi(y)$
0	**3**
1	**7**
2	5
3	**1**
4	2
5	4
6	6
7	**0**

量子計算でrを決定するには? → 周期性に着目



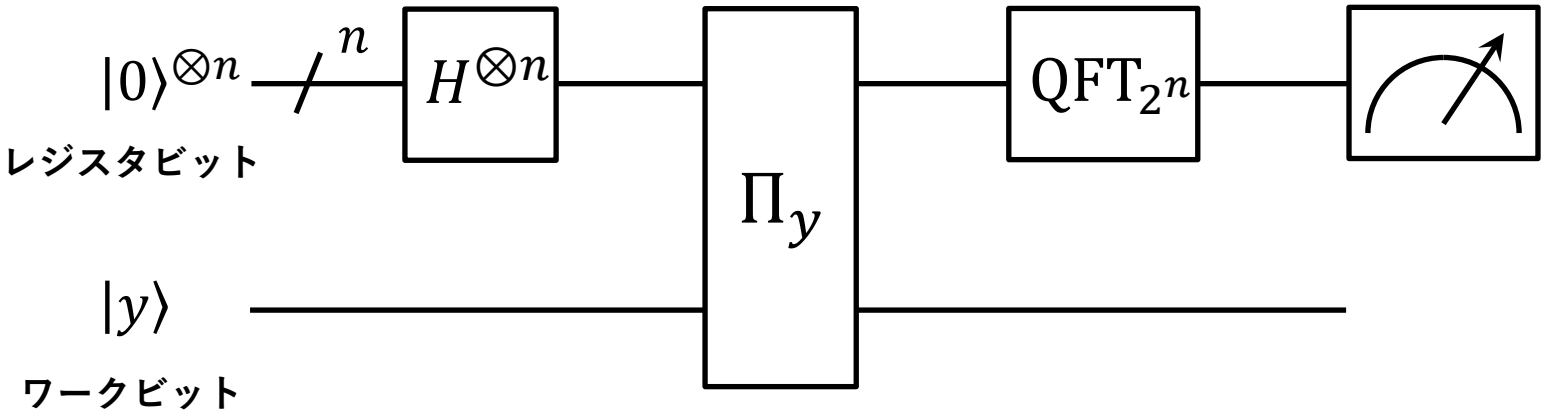
$$\pi^0(3) = \pi^4(3) = \pi^8(3) = \pi^{12}(3) = \cdots = 3$$

$$\pi^1(3) = \pi^5(3) = \pi^9(3) = \pi^{13}(3) = \cdots = 1$$

$$\pi^2(3) = \pi^6(3) = \pi^{10}(3) = \pi^{14}(3) = \cdots = 7$$

$$\pi^3(3) = \pi^7(3) = \pi^{11}(3) = \pi^{15}(3) = \cdots = 0$$

位数発見アルゴリズム



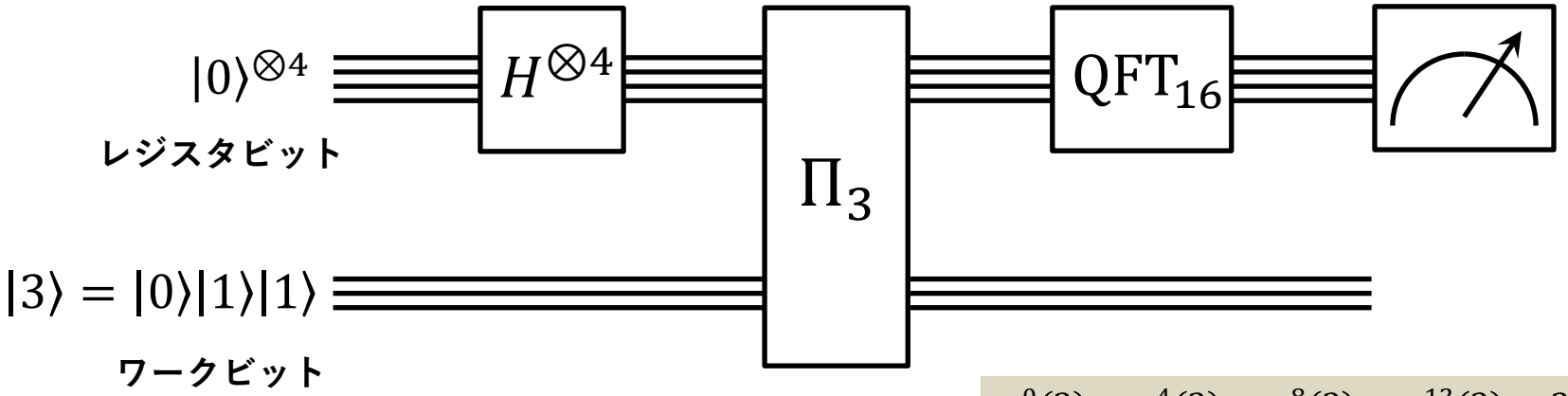
$$\Pi_y|x\rangle|y\rangle = |x\rangle|\pi^x(y)\rangle$$

疑問: 置換操作$\pi(y)$の内容を知らずにΠ_yを構成できるか?

ここでは、Π_yは**“オラクル(神託、ブラックボックス)”**として与えられているものとする

ドイチェの問題と似た状況を想定してもよい(ボブが$\pi(y)$を用意し、アリスがボブに問い合わせる)

位数発見アルゴリズム



レジスタビット

ワークビット

$$\pi^0(3) = \pi^4(3) = \pi^8(3) = \pi^{12}(3) = 3$$
$$\pi^1(3) = \pi^5(3) = \pi^9(3) = \pi^{13}(3) = 1$$
$$\pi^2(3) = \pi^6(3) = \pi^{10}(3) = \pi^{14}(3) = 7$$
$$\pi^3(3) = \pi^7(3) = \pi^{11}(3) = \pi^{15}(3) = 0$$

$$|0\rangle^{\otimes 4}|3\rangle \xrightarrow{H^{\otimes 4}} \frac{1}{4}\sum_{x=0}^{15}|x\rangle|3\rangle$$

$$\xrightarrow{\Pi_3} \frac{1}{4}\sum_{x=0}^{15}|x\rangle|\pi^x(3)\rangle \approx (|0\rangle + |4\rangle + |8\rangle + |12\rangle)|3\rangle$$
$$+(|1\rangle + |5\rangle + |9\rangle + |13\rangle)|1\rangle$$
$$+(|2\rangle + |6\rangle + |10\rangle + |14\rangle)|7\rangle$$
$$+(|3\rangle + |7\rangle + |11\rangle + |15\rangle)|0\rangle$$

位数発見アルゴリズム

$$\sqrt{\frac{r}{N}}\sum_{j=0}^{N/r-1}|jr+m\rangle \xrightarrow{\mathrm{QFT}_N} \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left(2\pi i\frac{mk}{r}\right)\left|\frac{N}{r}k\right\rangle$$

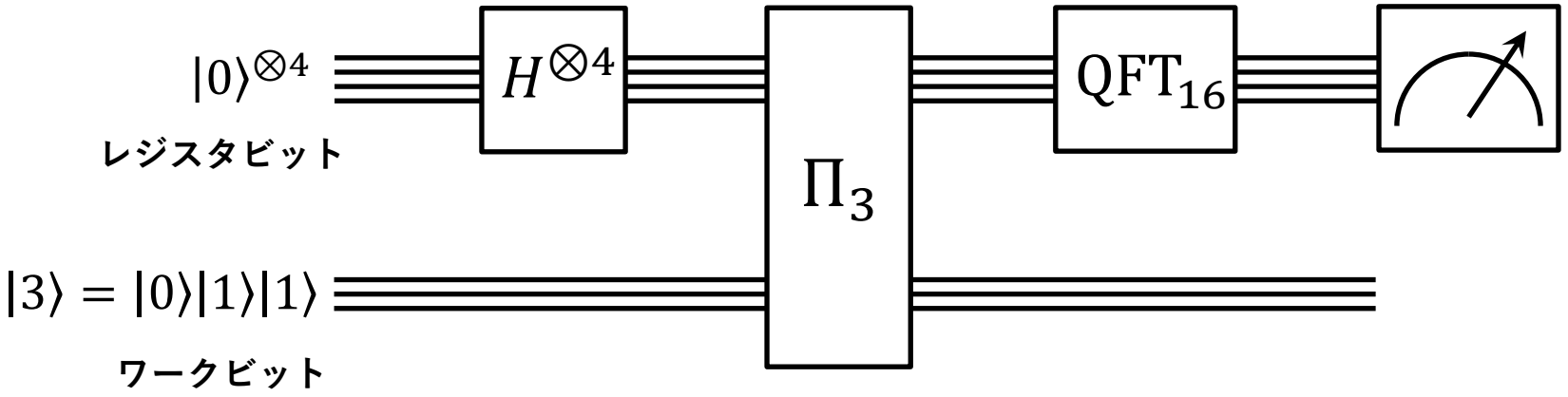
$N=2^4=16$
$r=4$
$N/r=4$

$$\frac{1}{4}\sum_{j=0}^{3}|4j+m\rangle \xrightarrow{\mathrm{QFT}_{16}} \frac{1}{2}\sum_{k=0}^{3}\exp\left(2\pi i\frac{mk}{4}\right)|4k\rangle$$

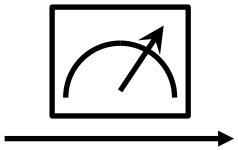
シフト不変

$$\begin{aligned}&(|0\rangle+|4\rangle+|8\rangle+|12\rangle)|3\rangle\\ &+(|1\rangle+|5\rangle+|9\rangle+|13\rangle)|1\rangle\\ &+(|2\rangle+|6\rangle+|10\rangle+|14\rangle)|7\rangle\\ &+(|3\rangle+|7\rangle+|11\rangle+|15\rangle)|0\rangle\end{aligned} \xrightarrow{\mathrm{QFT}_{16}} \begin{aligned}&(|0\rangle+|4\rangle+|8\rangle+|12\rangle)|3\rangle\\ &+(|0\rangle+i|4\rangle-|8\rangle-i|12\rangle)|1\rangle\\ &+(|0\rangle-|4\rangle+|8\rangle-|12\rangle)|7\rangle\\ &+(|0\rangle-i|4\rangle-|8\rangle+i|12\rangle)|0\rangle\end{aligned}$$

位数発見アルゴリズム



$$(|0\rangle + |4\rangle + |8\rangle + |12\rangle)|3\rangle$$
$$+(|0\rangle + i|4\rangle - |8\rangle - i|12\rangle)|1\rangle$$
$$+(|0\rangle - |4\rangle + |8\rangle - |12\rangle)|7\rangle$$
$$+(|0\rangle - i|4\rangle - |8\rangle + i|12\rangle)|0\rangle$$



0, 4, 8, 12のいずれかを等確率で出力

$$\rightarrow \frac{N}{r}k \quad (k = 0,1,2,3 < r)$$

rそのものが求まるわけではない

位数発見に関する疑問点

→ 素因数分解アルゴリズム

アルゴリズムに関して

- Π_yをどうやって構成するのか?
- “rを知らないと構成できない”あるいは“構成するのにrを知るのと同じ位手間が掛かる”だと、意味がない
  → 効率的に構成できる場合がある(素因数分解における位数発見問題)

位数の決定方法に関して

- 測定結果からrを求める方法は?
  → **連分数展開**(量子は関係ない)を用いると、rを推定できる
- それでも、“出力が0”のとき、“rとkが公約数をもつ”ときはうまくいかない
  → 素因数分解では解の候補が正しい解か確認することは容易
  → 失敗しても、やり直せばよいだけ(それでも十分早い)

講義内容

- 量子並列性
- ドイチェ–ジョザのアルゴリズム
- 量子フーリエ変換
- 位数発見アルゴリズム
- **素因数分解アルゴリズム**

講義内容

- **暗号と素因数分解**

- **素因数分解のための初等整数論**
  - ユークリッドの互除法
  - 中国剰余定理
  - 素因数分解と2次方程式
  - 剰余演算の位数

- **素因数分解アルゴリズム**
  - 位相発見と素因数分解の等価性
  - 冪剰余
  - 連分数展開

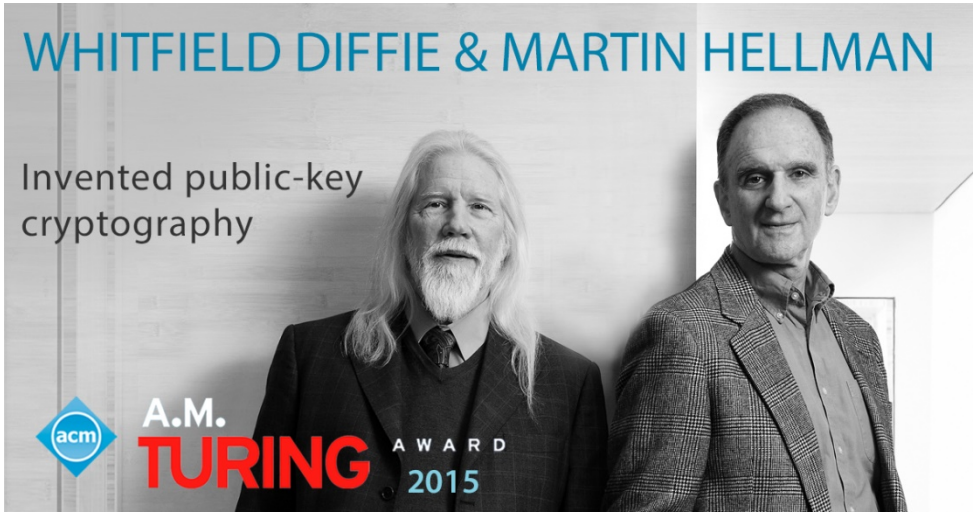
講義内容

- **暗号と素因数分解**

- **素因数分解のための初等整数論**
  - ユークリッドの互除法
  - 中国剰余定理
  - 素因数分解と2次方程式
  - 剰余演算の位数

- **素因数分解アルゴリズム**
  - 位相発見と素因数分解の等価性
  - 冪剰余
  - 連分数展開

公開鍵暗号、RSA暗号



ACM A.M. Turing Award
“Nobel Prize of Computing”

IEEE Trans. Inform. Theory **22**, 644 (1976)
W. Diffie & M. Hellman
“New directions in cryptography”

Commun. ACM **21**, 120 (1978)
R. Rivest, A. Shamir & L. Adleman
“A method for obtaining digital signatures and public-key cryptosystems”

RSA暗号

1. アリスは素数p, qからnとλを生成

$n = pq$ → nを公開(**公開鍵**)

$\lambda = (p-1)(q-1)$

2. アリスはλと互いに素となるeを生成

$e(= 2^{16} + 1 = 65537)$ → eを公開(**公開鍵**)

3. アリスはλ, eからdを生成

$de \equiv 1 \pmod{\lambda}$ → dは**秘密鍵**、p, q, λは破棄

4. ボブ(送信者)は公開鍵n, eを用いて送りたい平文mを暗号文cに暗号化

$c \equiv m^e \pmod{n}$ → cをアリスへ送信

5. アリスは秘密鍵dを用いて暗号文cを平文mに復号化

$c^d \equiv (m^e)^d \equiv m \pmod{n}$

オイラーの定理: $m^\lambda \equiv 1 \pmod{n}$

RSA暗号

秘匿性と安全性

公開鍵n, eを用いて平文mを暗号化することは容易だが
秘密鍵dを知らずに暗号文cを復号することは困難

$de \equiv 1 \pmod{(p-1)(q-1)}, n = pq$なので、公開鍵$n$を
素因数分解できれば、dを求めることができる

⇨ “素因数分解の難しさ”を利用した暗号方式

RSA-768 = 123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3

= 33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489

× 36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917

2009年に素因数分解された合成数 → シングルコアCPU(2.2 GHz AMD Opteron)で2000年掛かる

ショアの素因数分解アルゴリズム

©Aya Furuta

Nevanlinna Prize (1998)
“Fields Metal of Computer Science”

1982年から4年に1度、40歳以下の数学者に授与される(2018年までに受賞者10人)

Proceedings of the 35th Annual Symposium on Foundations of Computer Science P. 124–134 (1994)
“Algorithms for quantum computation: discrete logarithms and factoring”

SIAM J. Comput. **26**, 1484 (1997)
“Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”

講義内容

- **暗号と素因数分解**

- **素因数分解のための初等整数論**
  - ユークリッドの互除法
  - 中国剰余定理
  - 素因数分解と2次方程式
  - 剰余演算の位数

- **素因数分解アルゴリズム**
  - 位相発見と素因数分解の等価性
  - 冪剰余
  - 連分数展開

最大公約数

定義　整数a, bに共通の約数のうち最大のものを最大公約数(greatest common devisor)と呼び

$$\gcd(a, b)$$

と表す。$\gcd(a, b) = 1$のとき、“a, bは**互いに素**(coprime)”と言う。

例　$\gcd(9,6) = 3$　　$\gcd(5,3) = 1$

$\gcd(494,133) = ?$

ユークリッドの互除法

最大公約数を効率的に決定するアルゴリズム

例

$$\gcd(494,133) = 19$$

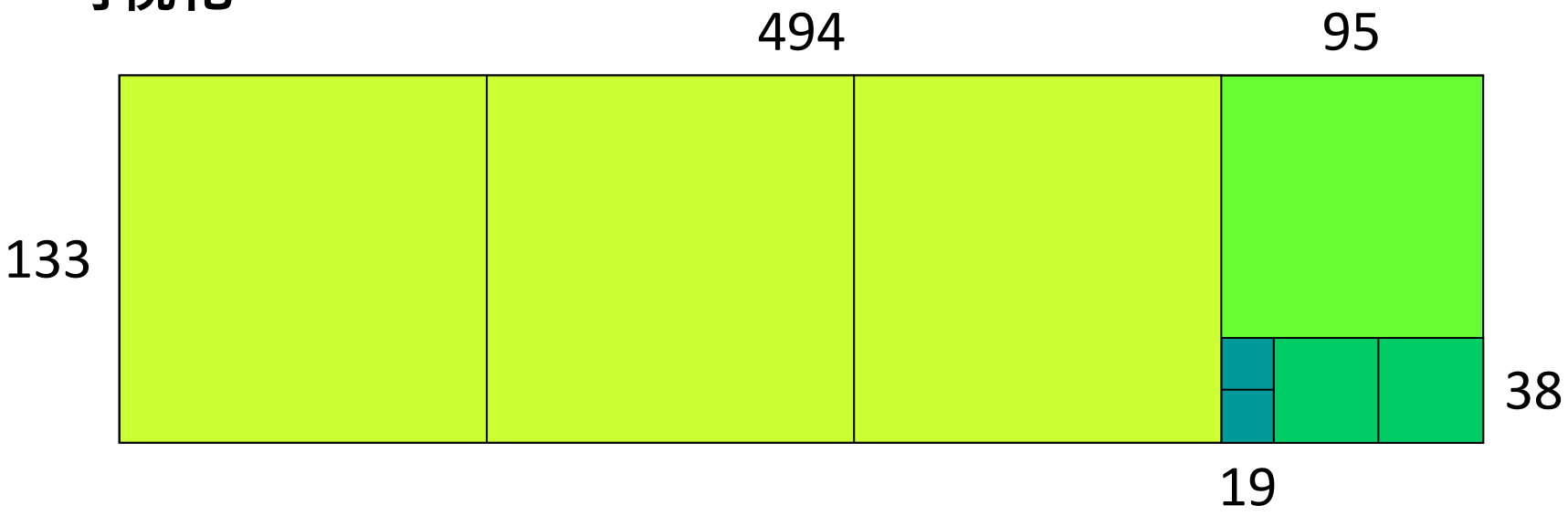
494 = **133** x 3 + **95**

133 = **95** x 1 + **38**

95 = **38** x 2 + **19**

38 = **19** x 2

可視化



中国剰余定理

(Chinese remainder theorem)

n_1, n_2は互いに素とする。すなわち

$$\gcd(n_1, n_2) = 1$$

p, qはそれぞれn_1, n_2で割った余り(剰余)とする。すなわち

$$0 \leq p \leq n_1 - 1$$
$$0 \leq q \leq n_2 - 1$$

このとき、以下を満たすsが**一意に存在**する。

$$1 \leq s \leq n_1 n_2$$
$$s \equiv p \pmod{n_1}$$
$$s \equiv q \pmod{n_2}$$

中国剰余定理

証明: 一意性　以下を満たす t が存在すると仮定。

$$t < s \qquad t \equiv p \pmod{n_1}$$
$$1 \leq t \leq n_1 n_2 \qquad t \equiv q \pmod{n_2}$$

⇨ $s - t \equiv 0 \pmod{n_1}$
$s - t \equiv 0 \pmod{n_2}$

⇨ $s - t \equiv 0 \pmod{n_1 n_2}$

n_1, n_2には公約数がないので
$s - t$はn_1の倍数かつn_2の倍数

⇨ $n_1 n_2 \leq s - t$　　**仮定と矛盾** (q.e.d)

中国剰余定理

証明: 存在　(p, q)の可能な組は$n_1 n_2$個あり、かつ
$s(1 \leq s \leq n_1 n_2)$は一意。

⇨　どの(p, q)にも対応するsが存在する。(q.e.d)

例　$n_1 = 3, n_2 = 5$

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
p	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
q	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0

与えれたsに対して対応する(p, q)を考える方が分かりやすい(かも)

素因数分解と2次方程式

n_1, n_2は互いに素、$L = n_1 n_2$とする。このとき、2次方程式

$$x^2 \equiv 1 \pmod{L}$$

には**非自明な解**

$$x \equiv \pm s \pmod{L} \qquad 1 < s < L - 1$$

が存在する。

↓

自明な解 $x \equiv \pm 1 \pmod{L}$

このため、$1, L-1, L$を非自明な解の候補から除いている

$\gcd(L, s+1), \gcd(L, s-1)$は$L$の**非自明な素因数**を与える。

素因数分解と2次方程式

証明　中国剰余定理より

$$\begin{cases} s \equiv 1 \pmod{n_1} \\ s \equiv -1 \pmod{n_2} \end{cases}$$

となる$s\ (1 < s < L-1)$が存在する。よって

$$\begin{cases} s^2 - 1 \equiv 0 \pmod{n_1} \\ s^2 - 1 \equiv 0 \pmod{n_2} \end{cases}$$

が成り立つ。 n_1, n_2は互いに素であるから

$$s^2 - 1 \equiv 0 \pmod{L}$$

よって

$$(s+1)(s-1) \equiv 0 \pmod{L}$$

素因数分解と2次方程式

証明(続き)　$1 < s < L - 1$ より

$$0 < s - 1 < s + 1 < L$$

よって、$\gcd(L, s+1)$, $\gcd(L, s-1)$はLの非自明な素因数である。

$$\begin{cases} s \equiv -1 \pmod{n_1} \\ s \equiv 1 \pmod{n_2} \end{cases}$$

についても同様。(q.e.d)

素因数分解と2次方程式

例 $n_1 = 3, n_2 = 5$

s	1	2	3	**4**	5	6	7	8	9	10	**11**	12	13	14	15
p	1	2	0	**1**	2	0	1	2	0	1	**2**	0	1	2	0
q	1	2	3	**4**	0	1	2	3	4	0	**1**	2	3	4	0

$$\begin{cases} 4 \equiv 1 \pmod 3 \\ 4 \equiv -1 \pmod 5 \end{cases} \qquad \begin{cases} 11 \equiv -1 \pmod 3 \\ 11 \equiv 1 \pmod 5 \end{cases}$$

$$\Rightarrow \begin{cases} \gcd(15, 4+1) = 5 \\ \gcd(15, 4-1) = 3 \end{cases} \qquad \Rightarrow \begin{cases} \gcd(15, 12) = 3 \\ \gcd(15, 10) = 5 \end{cases}$$

剰余演算の位数

定義　$1 \leq a \leq L-1$かつLと互いに素であるaに対して

$$a^r \equiv 1 \pmod{L}$$

を満たす最小のrを$a \pmod{L}$の**位数**と呼ぶ。

素因数分解との関係　偶数のrが見つかったとし

$$s \equiv a^{r/2} \pmod{L}$$

とおくと、sは

$$x^2 \equiv 1 \pmod{L}$$

の非自明な解の候補である。非自明な解であれば
Lの素因数が得られる。

例: $L = 15$

a	r	$a^{r/2} \pm 1$	$\gcd(a^{r/2} \pm 1, L)$
2	4	3, 5	3, 5
4	2	3, 5	3, 5
7	4	48, 50	3, 5
8	4	63, 65	3, 5
11	2	10, 15	5, 3
13	4	168, 170	3, 5

$2^4 = 16 \equiv 1$

$4^2 = 16 \equiv 1$

$7^4 = (49)^2 \equiv 4^2 \equiv 1$

$8^4 = (-7)^4 \equiv 1$

$11^2 = (-4)^2 \equiv 1$

$13^4 = (-2)^4 \equiv 1$

3, 5, 6, 9, 10, 12は15と公約数をもつので除外

1, 14は$x^2 \equiv 1$の自明な解と分かっているので除外

例: $L = 15$

a	r	$a^{r/2} \pm 1$	$\gcd(a^{r/2} \pm 1, L)$
2	4	3, 5	3, 5
4	2	3, 5	3, 5
7	4	48, 50	3, 5
8	4	63, 65	3, 5
11	2	10, 15	5, 3
13	4	168, 170	3, 5

$2^4 = 16 \equiv 1$

$4^2 = 16 \equiv 1$

$7^4 = (49)^2 \equiv 4^2 \equiv 1$

$8^4 = (-7)^4 \equiv 1$

$11^2 = (-4)^2 \equiv 1$

$13^4 = (-2)^4 \equiv 1$

レポート課題・第5問(5点)

$L = 21, a = 11$について、rを求め、 $a^{r/2} \pm 1$を計算せよ。
さらに、ユークリッドの互除法により $a^{r/2} \pm 1$とLの最大公約数を求めることでLの素因数を決定せよ。

講義内容

- **暗号と素因数分解**
- **素因数分解のための初等整数論**
  - ユークリッドの互除法
  - 中国剰余定理
  - 素因数分解と2次方程式
  - 剰余演算の位数
- **素因数分解アルゴリズム**
  - 位相発見と素因数分解の等価性
  - 冪剰余
  - 連分数展開

剰余演算と置換操作

$\pi(y) \equiv ay \pmod{L}$と定義すると$\pi(y)$は置換操作

$$\gcd(L, a) = 1$$
$$0 \leq y \leq L - 1$$

$0 \leq y' < y \leq L - 1$に対して
$ay \equiv ay' \pmod{L}$となることはない

例1　$L = 15, a = 7$

y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi(y)$	0	7	14	6	13	5	12	4	11	3	10	2	9	1	8

例2　$L = 15, a = 11$

y	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi(y)$	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4

位数発見と素因数分解の等価性

素因数分解では$a \pmod{L}$の偶数の位数rを見つけたい

$$a^r \equiv 1 \pmod{L}$$

⇩

一方、$\pi^k(y) \equiv \big(a \cdots (a(ay)\big) = a^k y \pmod{L}$なので

$$a^r \equiv 1 \pmod{L} \quad \Leftrightarrow \quad \pi^r(1) = 1$$

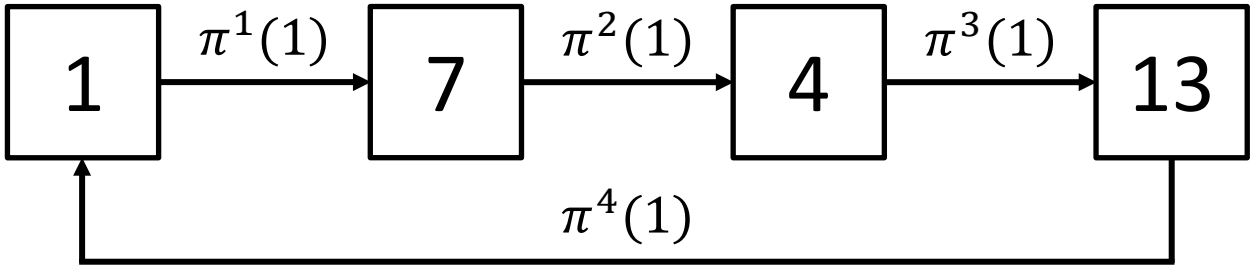
⇩

すなわち、置換$\pi(1)$の偶数の位数を求めることと等価

位数発見と素因数分解の等価性

例1 $L = 15, a = 7$

y	0	**1**	2	3	**4**	5	6	**7**	8	9	10	11	12	**13**	14
$\pi(y)$	0	**7**	14	6	**13**	5	12	**4**	11	3	10	2	9	**1**	8

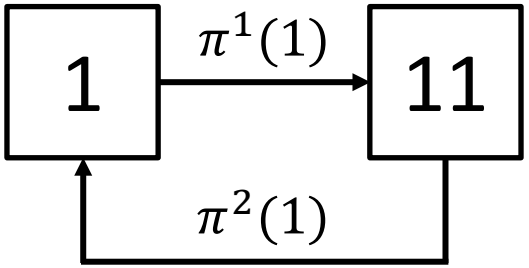


$r = 4$ ⇨ $7^{4/2} - 1 = 48$, $7^{4/2} + 1 = 50$ ⇨ $\gcd(15,48) = 3$, $\gcd(15,50) = 5$

位数発見と素因数分解の等価性

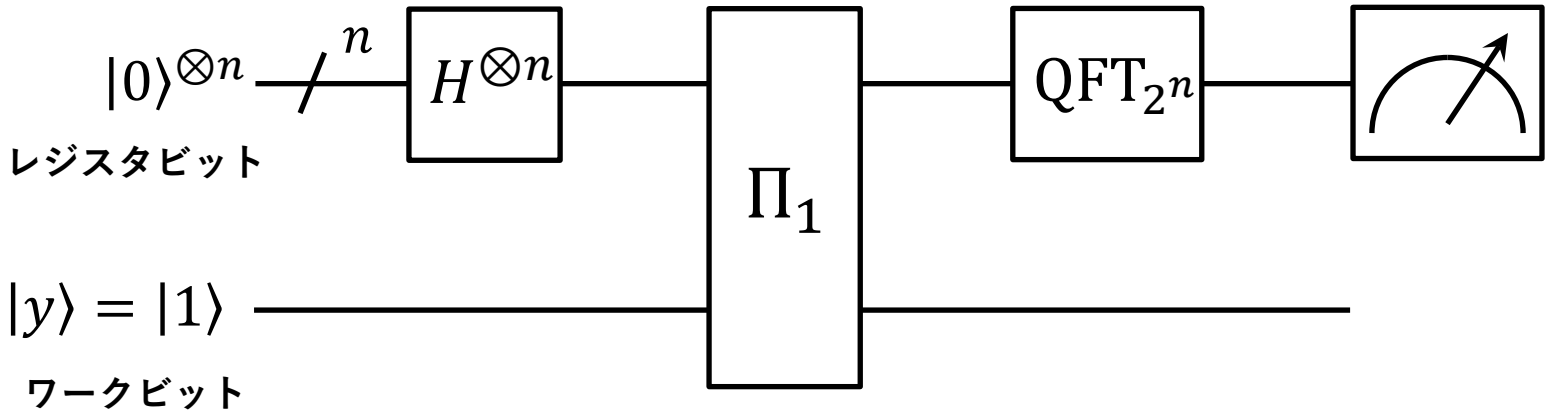
例2　$L = 15, a = 11$

y	0	**1**	2	3	4	5	6	7	8	9	10	**11**	12	13	14
$\pi(y)$	0	**11**	7	3	14	10	6	2	13	9	5	**1**	12	8	4



$r = 2$ ⇨ $11^{2/2} - 1 = 10$, $11^{2/2} + 1 = 12$ ⇨ $\gcd(15,10) = 5$, $\gcd(15,12) = 3$

位数発見アルゴリズム



$$\Pi_1|x\rangle|1\rangle = |x\rangle|\pi^x(1)\rangle$$

$$= |x\rangle|a^x \pmod{L}\rangle$$

回路的には何も変わっていない → Π_1ゲートをどのように構成するか

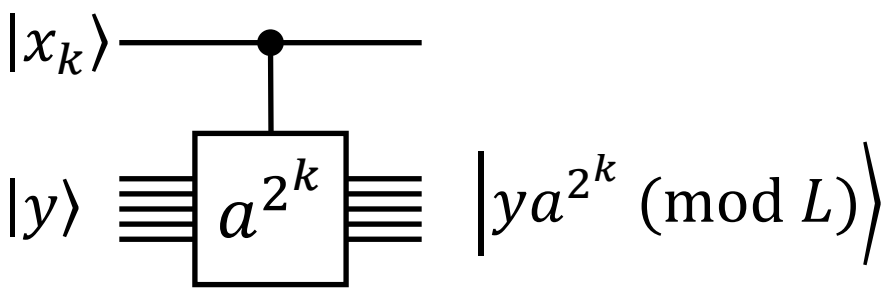
Π_1ゲート

$$\Pi_1|x\rangle|1\rangle = |x\rangle|a^x \pmod L\rangle$$

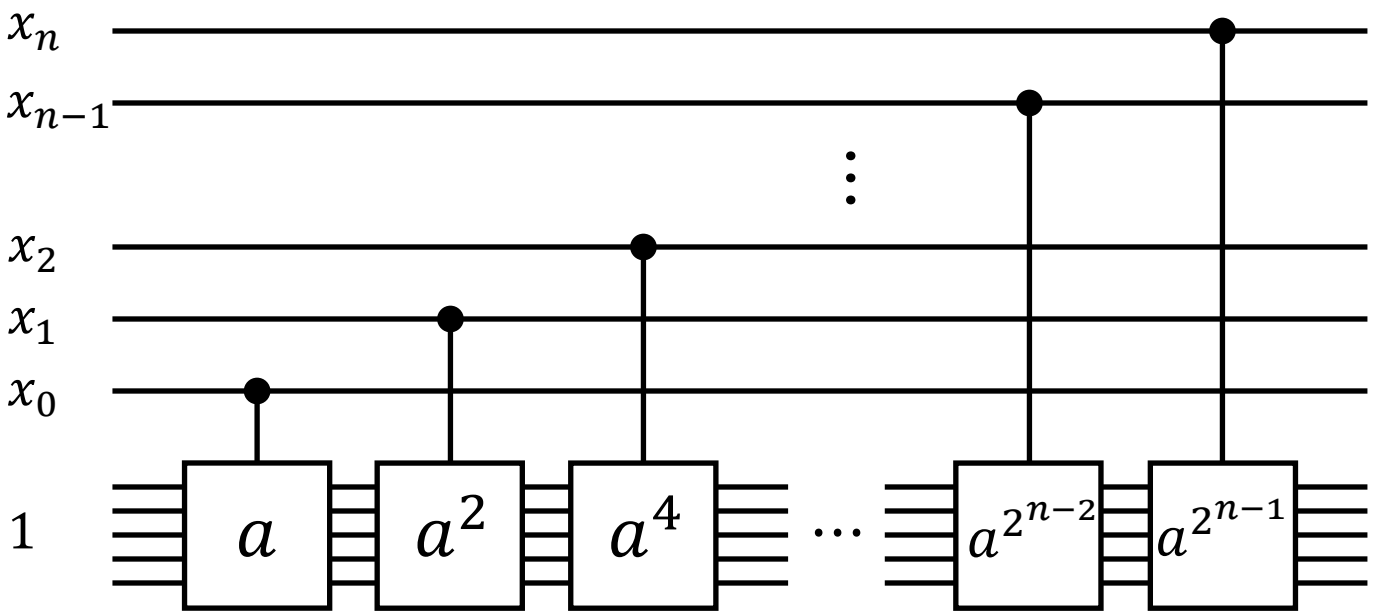
$$a^x \pmod L = a^{x_0+2x_1+\cdots+2^k x_k+\cdots+2^n x_n} \pmod L$$ 2進数展開($x_k = 0,1$)

$$= [a \pmod L]^{x_0} \cdots \left[a^{2^k} \pmod L\right]^{x_k} \cdots \left[a^{2^{n-1}} \pmod L\right]^{x_n=1}$$

$x_k = 1$のとき$a^{2^k} \pmod L$を実行

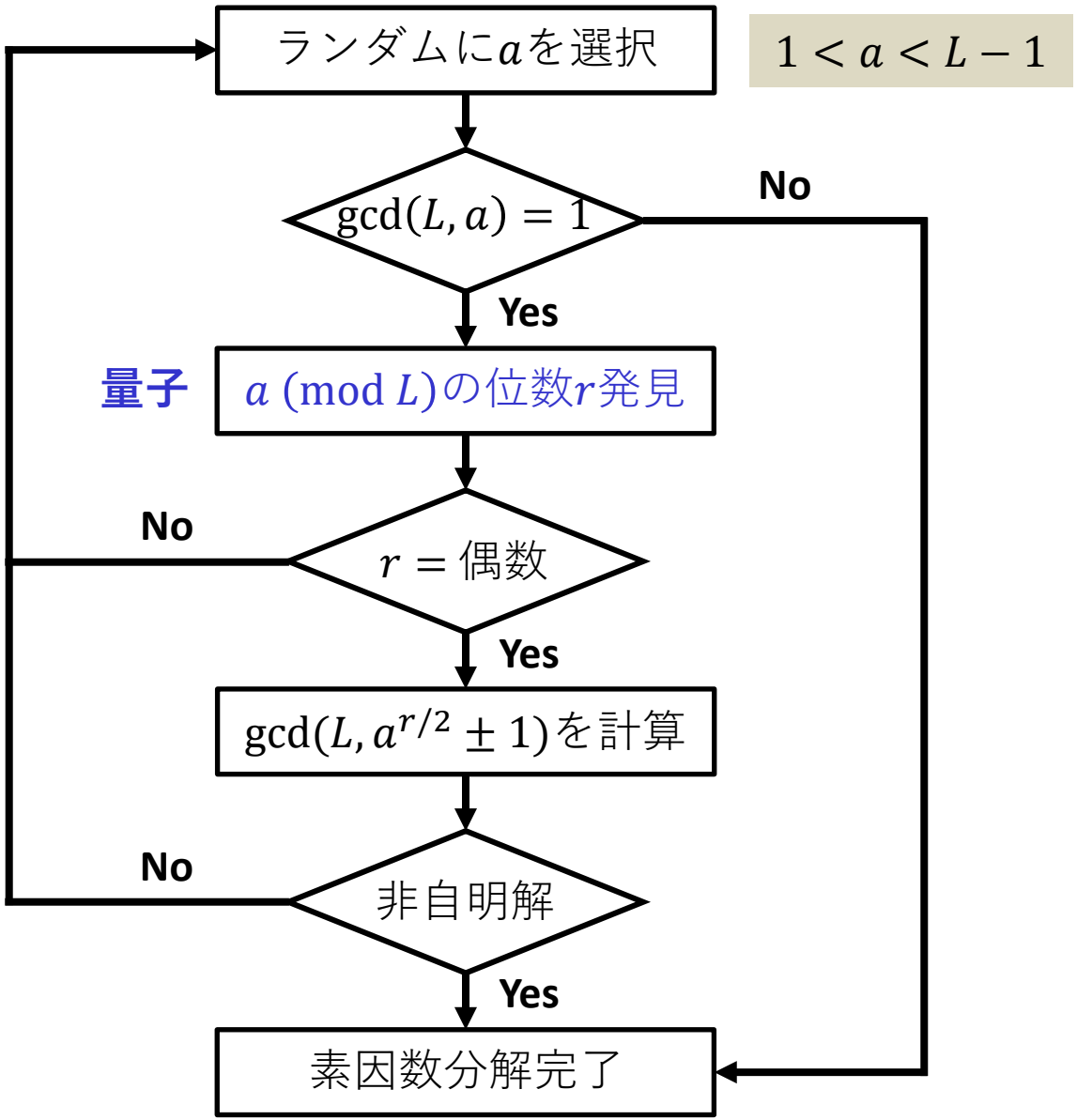


冪剰余



- 位数rそのものを知らなくても回路を構成できる
- $a^{2^k} \pmod{L}$の値は(古典コンピュータで)計算する必要があるが、$(a^{2^{k-1}})^2 = a^{2^k}$なので、一つ前の値から次の値を計算できる
- 具体的な回路は、a, Lの値に依存(この後$L = 15$の例を示す)

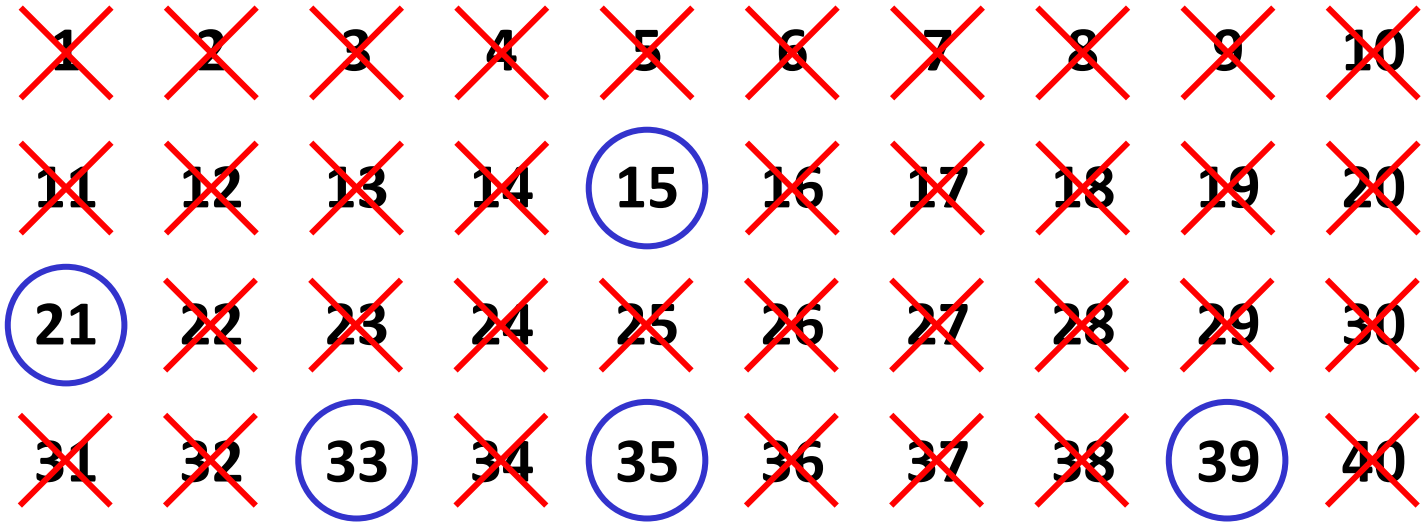
素因数分解アルゴリズム



素因数分解アルゴリズム

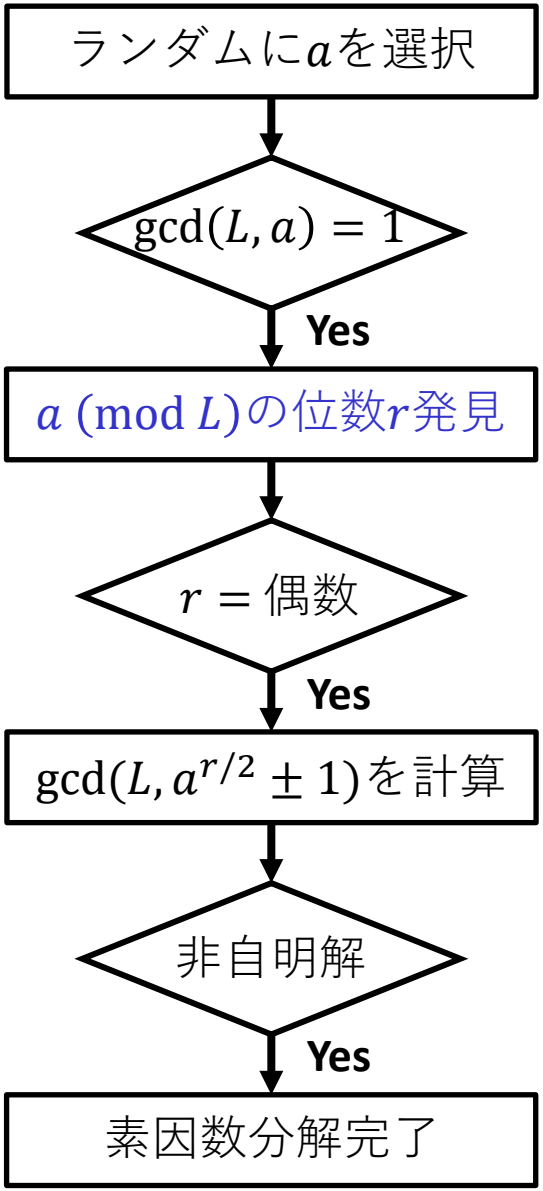
アルゴリズムが失敗するケース: Lが…

1. 素数
2. 偶数
3. 素数の冪乗



これらのケースは、素因数分解アルゴリズムを実行する前に
他の古典アルゴリズムで効率的にチェックできる

ケーススタディ：15の素因数分解



$a = 7$

⇩

$\gcd(15,7) = 1$

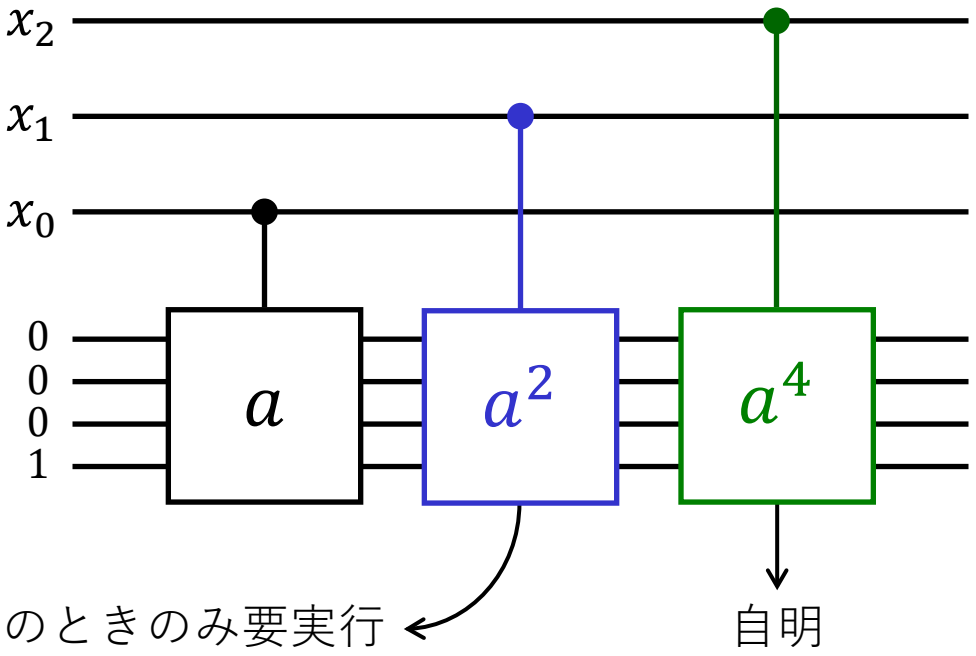
⇩

$7 \pmod{15}$の位数r発見

$a \pmod{15}$の位数r発見

a	a^2	a^4	r
2	4	1	4
4	1	1	2
7	4	1	4
8	4	1	4
11	1	1	2
13	4	1	4

$$a^{2^k}|y\rangle = \left|ya^{2^k} \pmod{L}\right\rangle$$



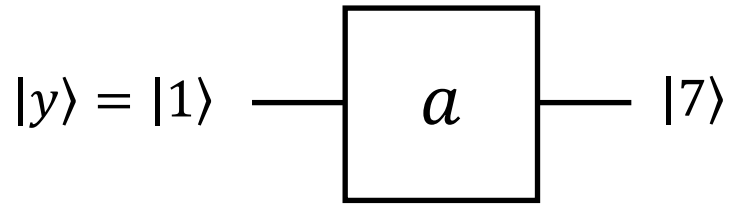
現実には、$r = a^{2^k} \pmod{L}$の形をしているときには、冪剰余を計算中に位数が分かってしまう(レアケース)

冪剰余の量子ゲート

$$7\ (\mathrm{mod}\ 15) = 1 + 2 \times 1 + 4 \times 1 + 8 \times 0\ (\mathrm{mod}\ 15)$$

2進数展開($y = y_0 + 2y_1 + 4y_2 + 8y_3$)

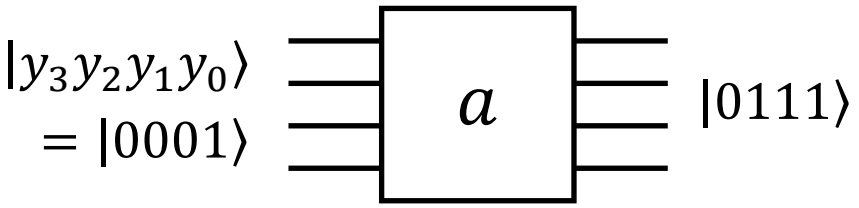
(10進数)



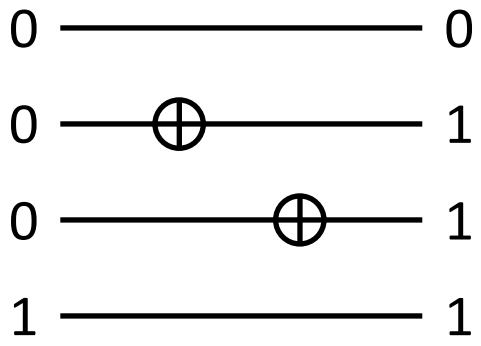
最初のゲートなので入力は必ず1

||

(2進数)



=



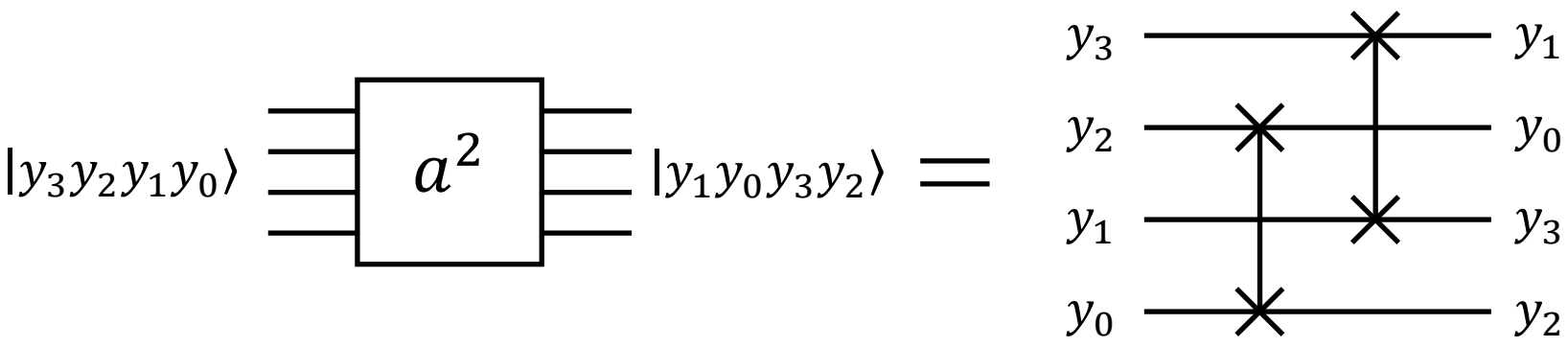
冪剰余の量子ゲート

$$
\begin{aligned}
& a^2 y \pmod{15} \\
\equiv\ & 4 \times (y_0 + 2y_1 + 4y_2 + 8y_3) \pmod{15} \\
=\ & 4y_0 + 8y_1 + 16y_2 + 32y_3 \pmod{15} \\
\equiv\ & 4y_0 + 8y_1 + y_2 + 2y_3 \pmod{15} \\
=\ & y_2 + 2y_3 + 4y_0 + 8y_1 \pmod{15}
\end{aligned}
$$

$a^2 \equiv 4 \pmod{15}$

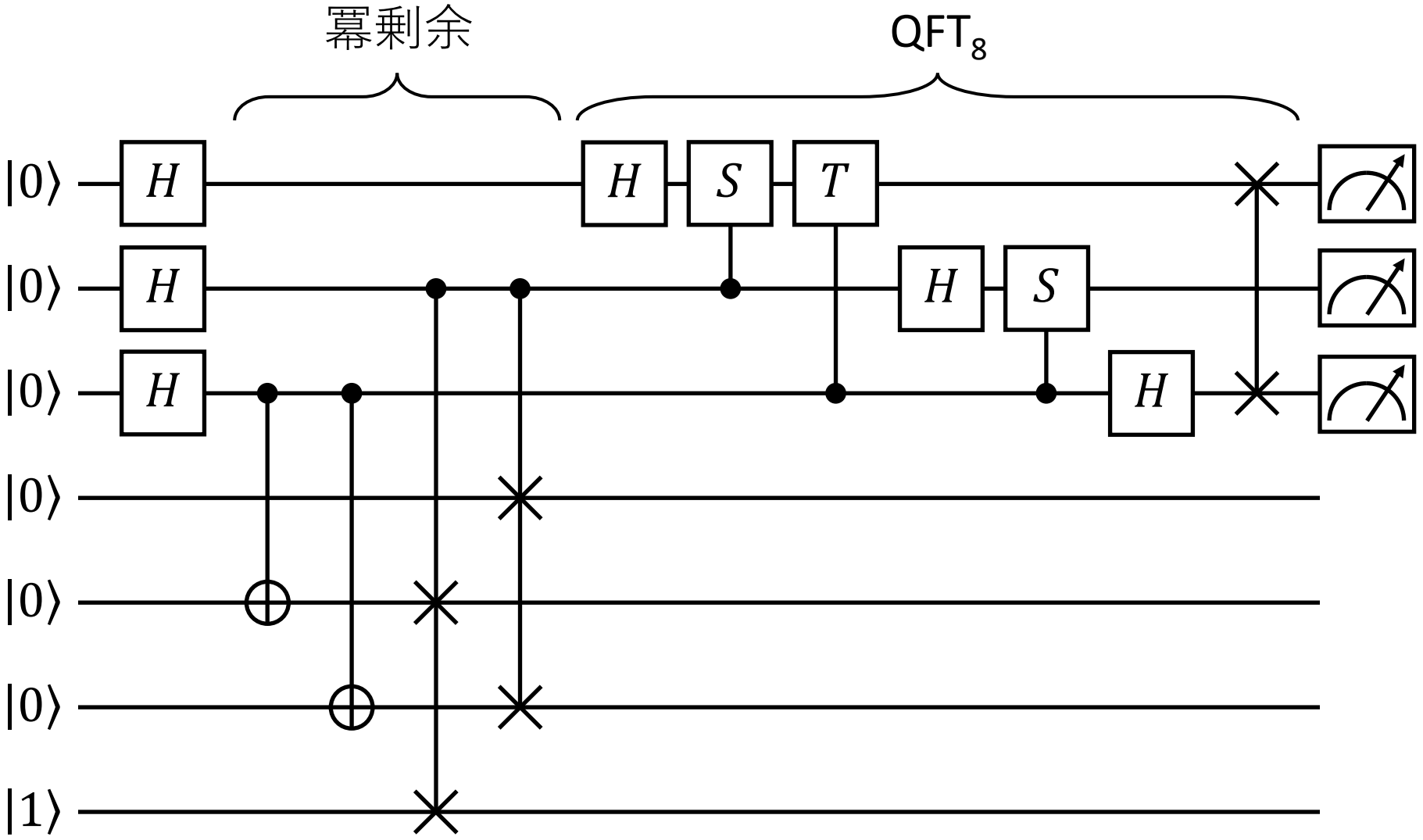
$32 \equiv 2 \pmod{15}$

$16 \equiv 1 \pmod{15}$



$a = 2,8,13$も同じ

15の素因数分解のための量子回路



位数発見に関する疑問点

→ 素因数分解アルゴリズム

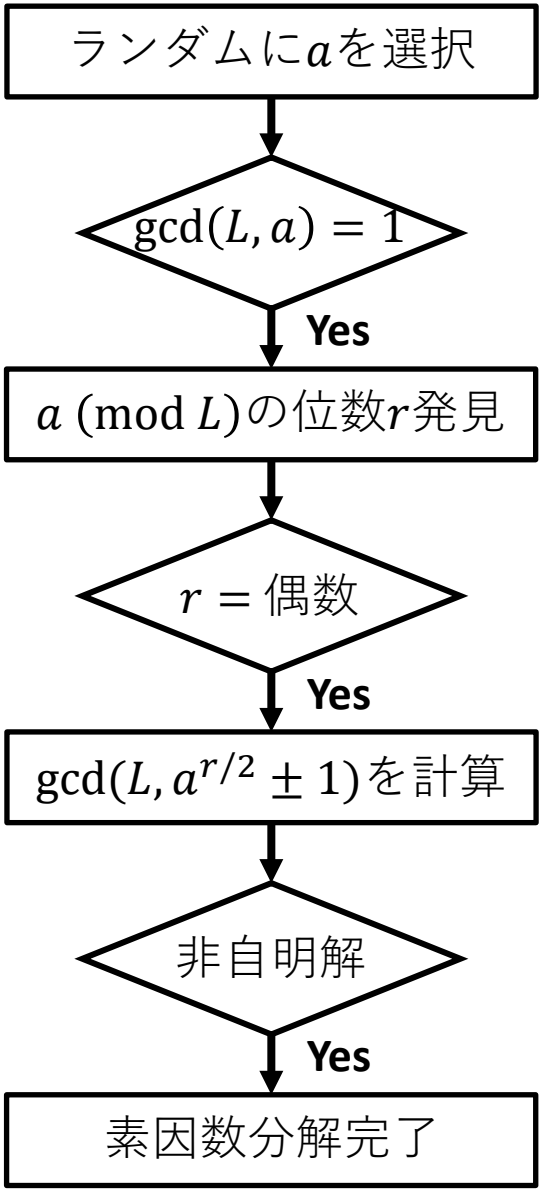
アルゴリズムに関して

- Π_yをどうやって構成するのか?
- “rを知らないと構成できない”あるいは“構成するのにrを知るのと同じ位手間が掛かる”だと、意味がない
  → 効率的に構成できる場合がある(素因数分解における位数発見問題)

位数の決定方法に関して

- 測定結果からrを求める方法は?
  → **連分数展開**(量子は関係ない)を用いると、rを推定できる
- それでも、“出力が0”のとき、“rとkが公約数をもつ”ときはうまくいかない
  → 素因数分解では解の候補が正しい解か確認することは容易
  → 失敗しても、やり直せばよいだけ(それでも十分早い)

ケーススタディ：15の素因数分解



$$a = 7$$

$$\gcd(15,7) = 1$$

$$r = 4$$

$$7^{4/2} - 1 = 48$$
$$7^{4/2} + 1 = 50$$

$$\gcd(15,48) = 3$$
$$\gcd(15,50) = 5$$

位数発見に関する疑問点

→ 素因数分解アルゴリズム

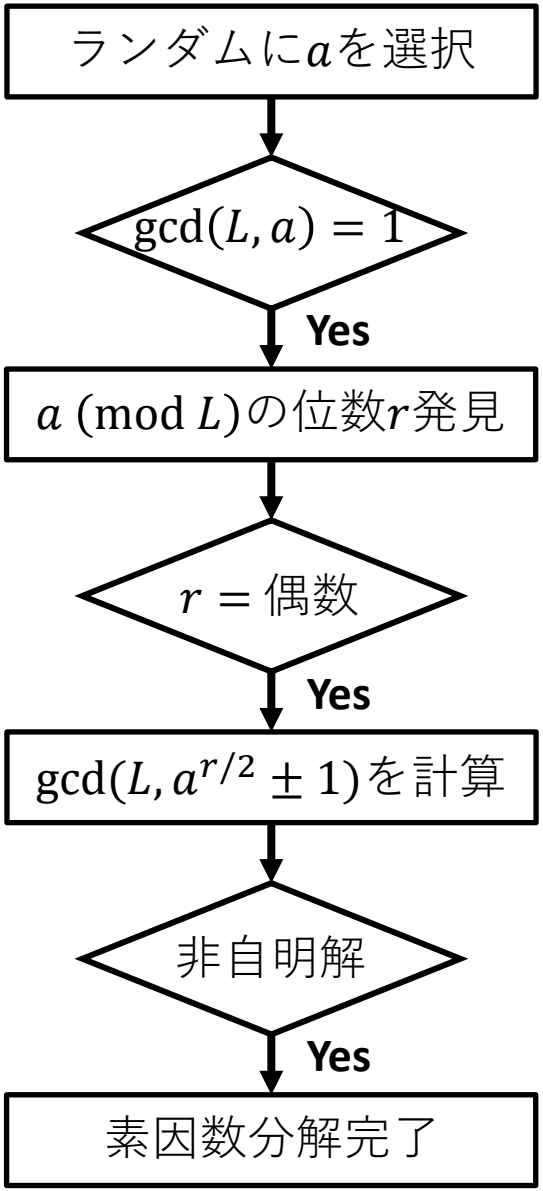
アルゴリズムに関して

- Π_yをどうやって構成するのか?
- “rを知らないと構成できない”あるいは“構成するのにrを知るのと同じ位手間が掛かる”だと、意味がない
  → 効率的に構成できる場合がある(素因数分解における位数発見問題)

位数の決定方法に関して

- 測定結果からrを求める方法は?
  → **連分数展開**(量子は関係ない)を用いると、rを推定できる
- それでも、“出力が0”のとき、“rとkが公約数をもつ”ときはうまくいかない
  → 素因数分解では解の候補が正しい解か確認することは容易
  → 失敗しても、やり直せばよいだけ(それでも十分早い)

ケーススタディ: 39の素因数分解



$a = 7$

⇩

$\gcd(39,7) = 1$

⇩

$7 \pmod{39}$の位数r発見

$7 \pmod{39}$の位数r発見

設定

$L = 39$

$a = 7$

$l = \lceil \log_2 L \rceil = 6$

$N = 2^{2l+1} = 8192$

$(r = 12)$

QFT & 測定

$$\approx \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi i \frac{mk}{r}} \left| \frac{N}{r} k \right\rangle \quad \xrightarrow{\text{測定}} \quad |\lambda\rangle \approx \left| \frac{N}{r} k \right\rangle$$

$k = 5$が選ばれたとすると

$\Rightarrow$ $\frac{Nk}{r} = \frac{8192 \cdot 5}{12} = 3413.\dot{3}$ より

$\lambda = 3413$を高確率で出力

計算結果からrを求めたい

$$\frac{\lambda}{N} \approx \frac{k}{r}$$

$$\frac{\lambda}{N} = \frac{3413}{8192} = 0.4166259 \ldots$$

$$\frac{k}{r} = \frac{5}{12} = 0.4166666 \ldots$$

$$\delta = \left| \frac{\lambda}{N} - \frac{k}{r} \right| = 0.0000407 \ldots$$

連分数展開

定義

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{m-1} + \cfrac{1}{a_m}}}}$$

$$\equiv [a_0, a_1, \cdots, a_m]$$

→ 実数を整数のみで表現できる

近似分数(convergent)

$$\frac{p_0}{q_0} = [a_0] = a_0$$

$$\frac{p_1}{q_1} = [a_0, a_1] = a_0 + \frac{1}{a_1}$$

$$\vdots$$

$$\frac{p_{m-1}}{q_{m-1}} = [a_0, a_1, \cdots, a_{m-1}]$$

$$\frac{p_m}{q_m} = [a_0, a_1, \cdots, a_m]$$

連分数展開

例	分割	反転	近似分数
$\alpha = \frac{31}{13}$	$= 2 + \frac{5}{13}$	$= 2 + \frac{1}{\frac{13}{5}}$	$\frac{p_0}{q_0} = [2]$
	$= 2 + \frac{1}{2 + \frac{3}{5}}$	$= 2 + \frac{1}{2 + \frac{1}{\frac{5}{3}}}$	$\frac{p_1}{q_1} = [2,2]$
	$= 2 + \frac{1}{2 + \frac{1}{1 + \frac{2}{3}}}$	$= 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}}$	$\frac{p_2}{q_2} = [2,2,1]$
	$= 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}$		$\frac{p_3}{q_3} = [2,2,1,1]$
			$\frac{p_4}{q_4} = [2,2,1,1,2]$

連分数アルゴリズム

$$\frac{p_0}{q_0} = [2] = 2$$

$$\frac{p_1}{q_1} = [2,2] = \frac{5}{2} = 2.5$$

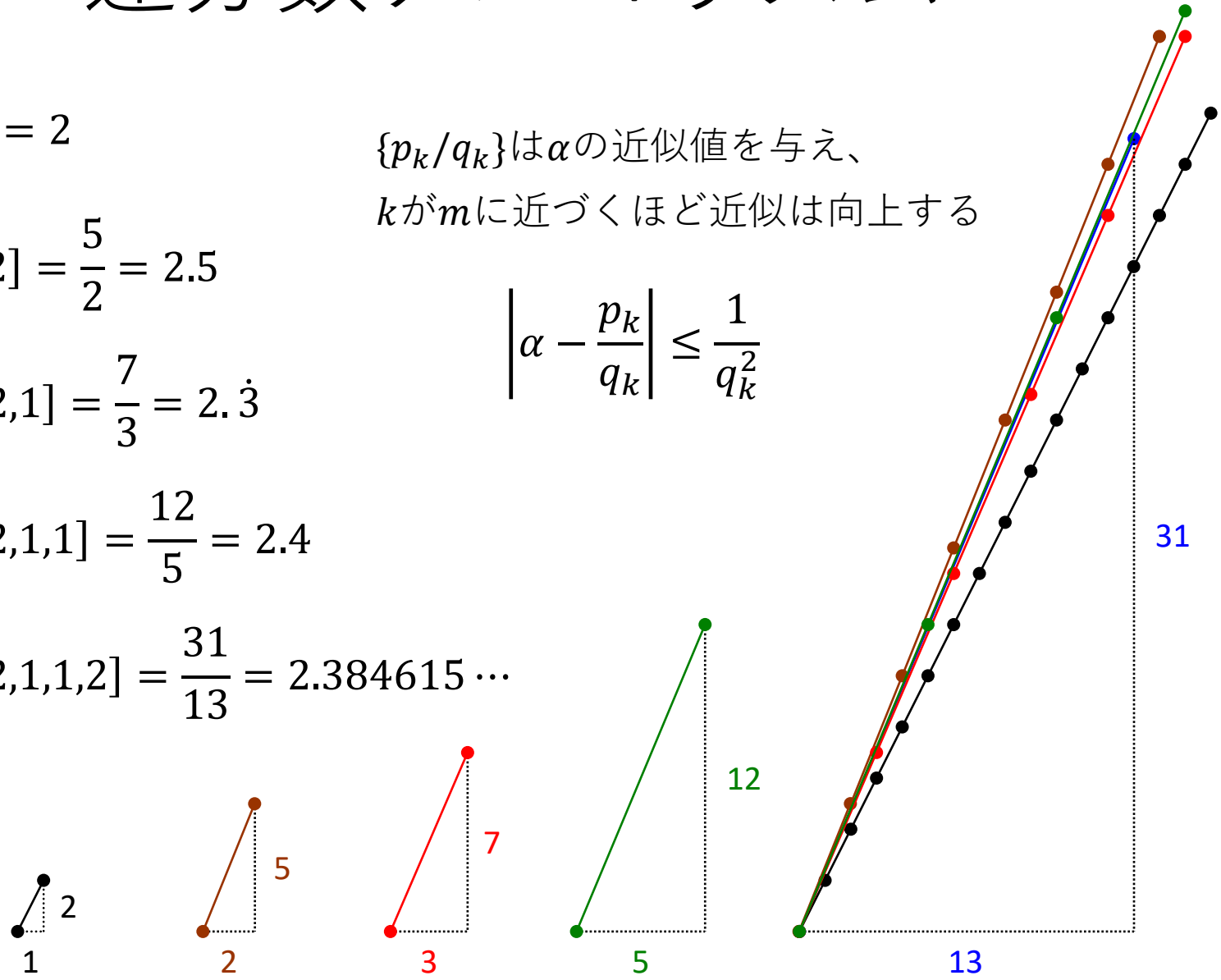
$$\frac{p_2}{q_2} = [2,2,1] = \frac{7}{3} = 2.\dot{3}$$

$$\frac{p_3}{q_3} = [2,2,1,1] = \frac{12}{5} = 2.4$$

$$\frac{p_4}{q_4} = [2,2,1,1,2] = \frac{31}{13} = 2.384615\cdots$$

$\{p_k/q_k\}$はαの近似値を与え、
kがmに近づくほど近似は向上する

$$\left|\alpha - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k^2}$$



連分数アルゴリズム

$\alpha = [a_0, a_1, \cdots, a_m]$の$n$次の近似分数は以下の漸化式で与えられる。

$$\begin{cases} p_n = a_n p_{n-1} + p_{n-2} \\ q_n = a_n q_{n-1} + q_{n-2} \end{cases} \quad \text{ただし} \quad \begin{cases} (p_{-2}, q_{-2}) = (0,1) \\ (p_{-1}, q_{-1}) = (1,0) \end{cases}$$

n	−2	−1	0	1	2	3	4
a_n	—	—	2	2	1	1	2
p_n	0	1	**2**	**5**	**7**	**12**	**31**
q_n	1	0	**1**	**2**	**3**	**5**	**13**

(p_n, q_nは互いに素となる)

連分数アルゴリズム

定理　有理数p/qと実数αに対して

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2^d} \leq \frac{1}{2q^2}$$

が成り立つとき、p/qはαのdビットの精度の近似分数となる

$$\delta = \left|\frac{\lambda}{N} - \frac{k}{r}\right| \leq \frac{1}{2^{2l+1}} \leq \frac{1}{2r^2}$$

$$\begin{cases} l \equiv \lceil \log_2 L \rceil \quad (2^{l-1} < L \leq 2^l) \\ 2^{2l+1} = 2\left(2^l\right)^2 \geq 2L^2 \geq 2r^2 \end{cases}$$

$0.0001220\ldots$　　$0.0034722\ldots$

⇨ $\delta = 0.0000407\ldots$なのでλ/Nの近似分数にk/rが含まれているはず

“出力が0”のとき、“rとkが公約数をもつ”ときはうまくいかない

→ 素因数分解では解の候補が正しい解か確認することは容易

→ 失敗しても、やり直せばよいだけ(それでも十分早い)

測定結果からrを求める

設定

$L = 39$

$a = 7$

$l = \lceil \log_2 L \rceil = 6$

$N = 2^{2l+1} = 8192$

$(r = 12)$

QFT & 測定

$$\approx \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{2\pi i \frac{mk}{r}} \left| \frac{N}{r} k \right\rangle \xrightarrow{\text{測定}} |\lambda\rangle \approx \left| \frac{N}{r} k \right\rangle$$

$k = 5$が選ばれたとすると

$\Rightarrow$ $\frac{Nk}{r} = \frac{8192 \cdot 5}{12} = 3413.\dot{3}$ より

$\lambda = 3413$を高確率で出力

λ/Nを連分数展開

$$\frac{\lambda}{N} = \frac{3413}{8192} = 0 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{170 + \frac{1}{4}}}}} = [0,2,2,2,170,4]$$

測定結果からrを求める

n	−2	−1	0	1	2	3	4	5
a_n	—	—	0	2	2	2	170	4
p_n	0	1	**0**	**1**	**2**	**5**	**852**	**3413**
q_n	1	0	**1**	**2**	**5**	**12**	**2045**	**8192**

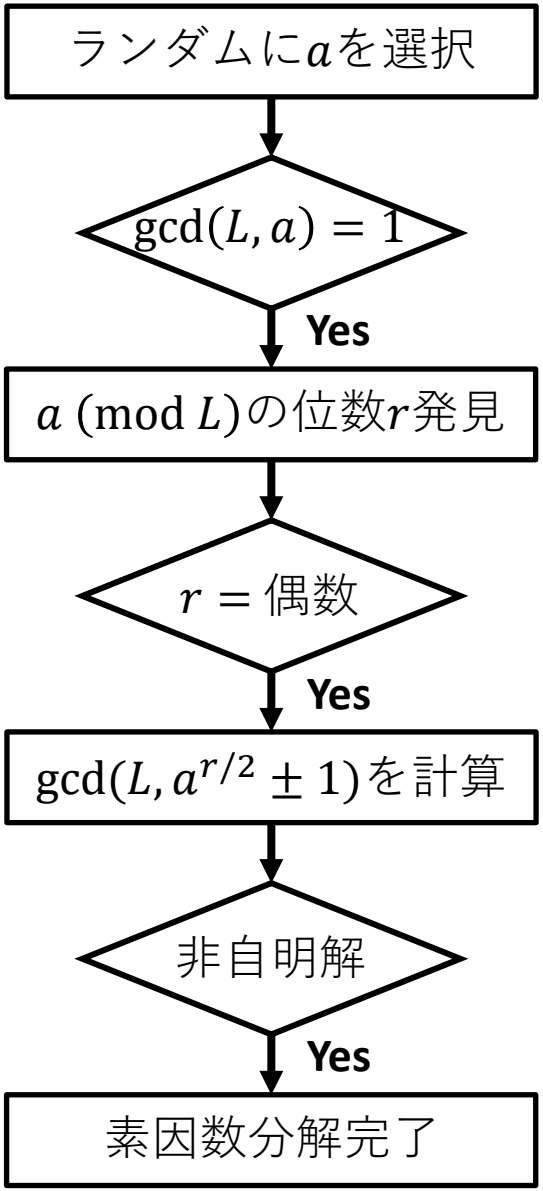
$$\frac{p_1}{q_1}=\frac{1}{2} \quad \frac{p_2}{q_2}=\frac{2}{5} \quad \frac{p_3}{q_3}=\frac{5}{12} \quad \frac{p_4}{q_4}=\frac{852}{2045} \quad \frac{p_5}{q_5}=\frac{3413}{8192}$$

k/rの候補

$p_n, q_n \geq L = 39$よりk/rの候補から外れる

⇨ 順次$a^{q_n} \pmod{L}$を計算し、$q_3 = 12$がrと求まる

ケーススタディ：39の素因数分解



$$a = 7$$

$$\gcd(39,7) = 1$$

$$r = 12$$

$$7^{12/2} - 1 \equiv 24 \pmod{39}$$
$$7^{12/2} + 1 \equiv 26 \pmod{39}$$

$$\gcd(39,24) = 3$$
$$\gcd(39,26) = 13$$

ケーススタディ：39の素因数分解

設定

$L = 39$

$a = 7$

$l = \lceil \log_2 L \rceil = 6$

$N = 2^{2l+1} = 8192$

$r = 12$

⇩

$k = 7$

$Nk/r = 4778.\dot{6}$

$\lambda = 4779$

レポート課題・第6問(10点)

λ/Nを連分数展開し、近似分数 p_n/q_nにk/rが含まれることを確認せよ。

$$\frac{\lambda}{N} = \frac{4779}{8192} = [a_0, a_1, a_2, a_3, a_4, a_5, a_6]$$

n	−2	−1	0	1	2	3	4	5	6
a_n	—	—							
p_n	0	1							4779
q_n	1	0							8192

$$\begin{cases} p_n = a_n p_{n-1} + p_{n-2} \\ q_n = a_n q_{n-1} + q_{n-2} \end{cases}$$