Shor‘s Algorithm for Factoring Large Integers
ー量子コンピュータと暗号解読ー

Journal Club, 2017/06/09, T.Yoshie

Shor's Algorithm for Factoring Large Integers
C. Lavor, L.R.U. Manssur, R. Portugal, **arXiv:quant-ph/0303175**
Comments: 25 pages, 14 figures, **introductory review**

Polynomial-time Algorithms for Prime Factorization and discrete logarithms on Quantum Computer
P. W. Shor, **SIAM J. COMPUT., 26 (1997) 1484**

共通鍵暗号と公開鍵暗号

- 暗号
  - 平文を特定のアルゴリズムと鍵を使って、鍵を持つ人しか復号できない形に変形すること
  - 平文は符号化で数値の列に　(e.g. A:1 B:2 … z:26)
  - e.g. シーザー暗号 :
    yoshie -> 25,15,19,08,09,05 --> 2,18,21,11,12,08
    3文字右に(cyclic)にシフト、鍵:3、Alg.:右シフト
- 共通鍵暗号
  - 暗号化と復号に、同じ鍵（とAlg.）が必要
  - 通信に暗号を用いる際に、鍵を秘密裡にやり取りしなければならないので、(原理的に)安全ではない

- 公開鍵暗号
  - 2つの鍵(秘密鍵(S-key)と公開鍵(P-key))を使う
    一方の鍵で暗号化したメッセージは他方の鍵でしか復号できない
  - AさんはBさんから秘密のメッセージを受け取たい

Aさん

Bさん

一度だけ

1) 鍵ペア (S-key, P-key) を生成し、
2) P-key をBさんに平文で送る

3) メッセージを P-key で暗号化しAさんに送る

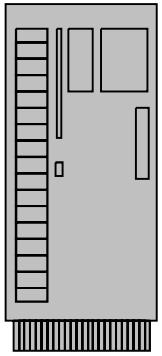
4) S-key で復号

  - 復号に必要な鍵(S-key)は誰にも渡す必要がない

- 公開鍵暗号と認証
  - 公開鍵暗号方式は認証にも使われる
  - Aさんはコンピュータにログインしようとしている
    本人である事をどう証明するか

ユーザー
登録時に

Aさん



コンピュータ

1) 鍵ペア (S-key, P-key) を生成し、
2) P-key をコンピュータに平文で送る

3) 適当なメッセージを平文で送る

4) S-key で暗号化して送り返す

5) P-keyで復号して元のメッセージと比較

  - 正しく暗号化できる鍵(S-key)はAさんしか持っていない
  - (ユーザー登録時のなりすましは防げない、要公的認証)

RSA 暗号(1977)

- RSA暗号
  - 初の公開鍵方式の暗号
  - 現在も(もっともよく)使われている, e.g. ssh
  - 安全性は、『大きな数の素因子分解が極めて困難（既知アルゴリズムでは膨大な計算時間が必要』である事により保証されている
- 概要
  - 大きな素数 p,q の積 N=pq を法とした演算を使用
  - 平文(数列)の各項をべき乗して暗号文を作る。暗号文の各項をべき乗して復号する。

$$N = pq \ (p, q \text{ large prime numbers})$$

$$x_0 x_1 \ldots x_n \ldots \Rightarrow \ y_0 y_1 \ldots y_n \ldots \Rightarrow \ z_0 z_1 \ldots z_n \ldots$$

$$y_n = x_n^E \mod N, \quad z_n = y_n^D = x_n^{ED} \mod N = x_n$$

$$ED = mLCM(p-1, q-1) + 1 \ \Rightarrow x^{ED} = x \mod N$$

– c.f. フェルマーの小定理

$$x^p = x \mod p$$

– *E* (公開鍵), *D*(秘密鍵) (暗号化の場合)

– *p,q* から *N* と *E,D* pair を生成、*p,q* は破棄

– *N*と*E*を公開しても、*p,q* が求まらなければ *D* は求められない。

量子計算

- qubit $q = \alpha|0\rangle + \beta|1\rangle \in H$
- register $|\psi\rangle \in H \otimes H .... \otimes H = H^{\otimes n}$

$$e.g.\ |\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$
$$= \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle + \delta|3\rangle$$

数値に対応させる

entangled/ non-entangled

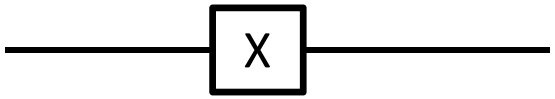
$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$$

- quantum computation: unitary transformation
- measurement: qubit の値を読む。確率的に 0か1が得られる。

量子回路

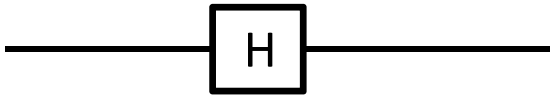
- gate

NOT



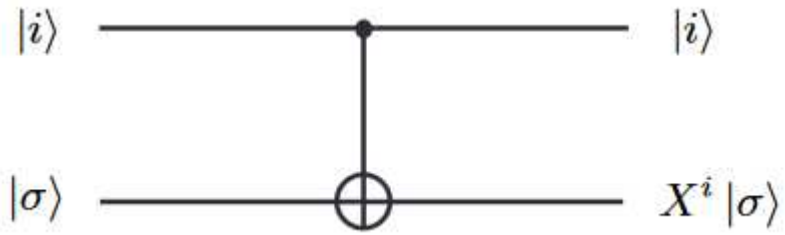
$$X|0\rangle = |1\rangle \quad X|1\rangle = |0\rangle$$

Hadamard



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

CNOT



$$|i,\sigma\rangle \rightarrow |i, i \oplus \sigma\rangle$$

- these gates are universal, i.e., any other gate can be written a compositions and direct products of these gates

素因子分解とオーダー計算

- 数 N の素因子を求める
  - 『適当な』数 x ($<N$)のオーダー r を求める

$$x^r = 1 \mod N \quad \text{smallest } r$$

$$\mathrm{GCD}(N, x) = 1, \qquad r \text{ is even}$$

$$y = x^{r/2} \qquad y^2 = 1 \quad (y-1)(y+1) = 0 \mod N$$

$$1 < y < N-1 \qquad 1 < y-1 < y+1 < N$$

  - GCD(y-1,N) と GCD(y+1,N) は、N の素因子

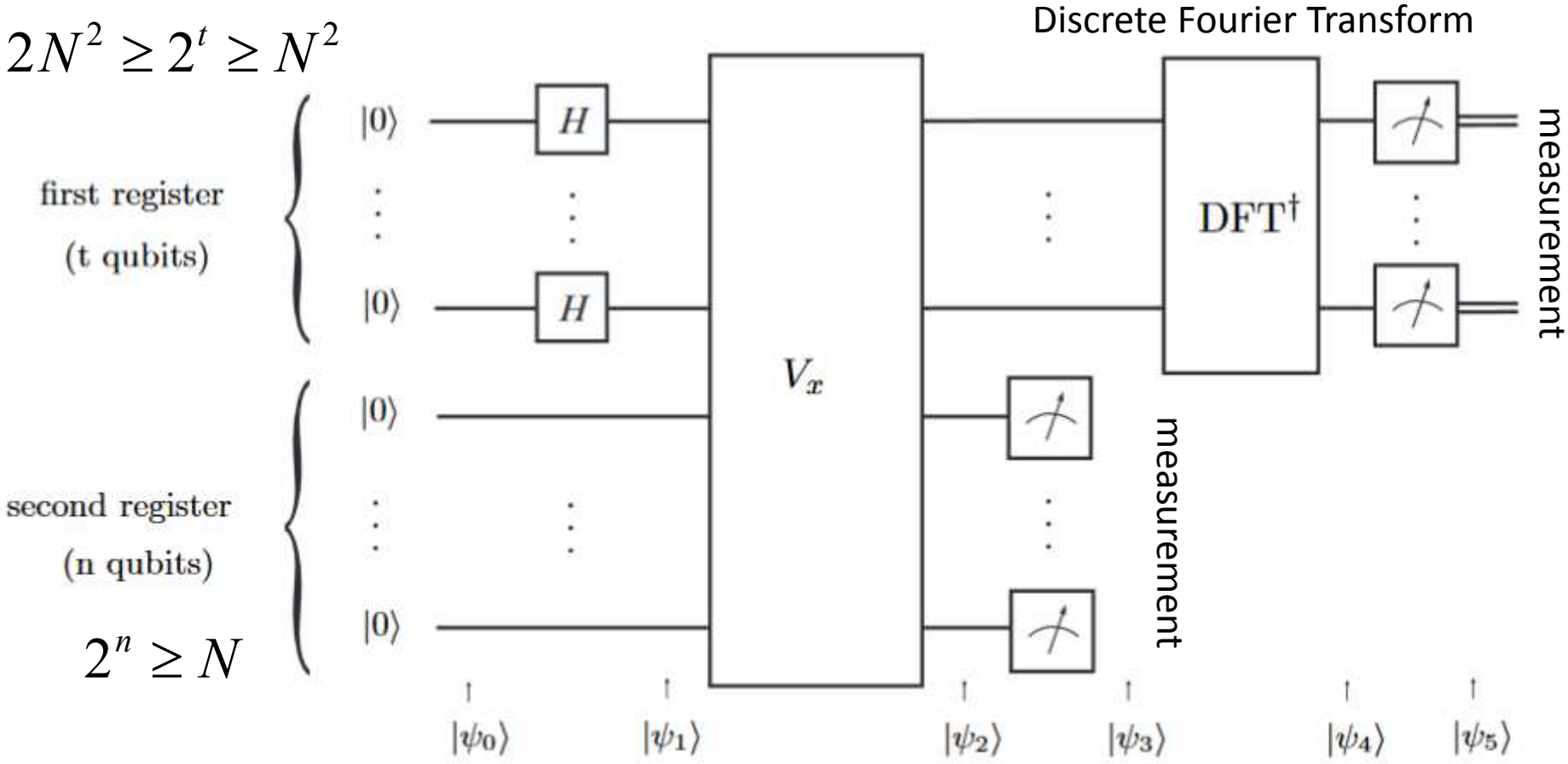
$$N = 21 \quad x = 2 \quad 2^4 = 16 \quad 2^5 = 11 \quad 2^6 = 1 \quad r = 6$$

$$y = 8 \quad y-1 = 7 \quad y+1 = 9 = 3^2$$

  - xがこの条件を満たす確率: $1-1/2^{k-1} > 1/2$ k=#factor

オーダーの計算アルゴリズム

$2N^2 \geq 2^t \geq N^2$



consider $r = 2^s$ case

$t = n$

$|\psi\rangle = |j\rangle|k\rangle \qquad V_x(|j\rangle|k\rangle) = |j\rangle|k + x^j\rangle$

(V_x : linear unitary op. i.e. quantum circit)

$$|\psi_0\rangle = |0\rangle|0\rangle = |00\ldots0\rangle|00\ldots0\rangle$$

$$|\psi_1\rangle = (H^{\otimes t}|0\rangle)|0\rangle = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|0\rangle$$

$$|\psi_2\rangle = V_x|\psi_1\rangle = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|x^j\rangle$$

全ての *j* に対して *x* の *j* 乗が 1回の演算でできる
(quantum parallelism)
古典計算機では、$x \to x^2 \to x^3 .... \to x^r = 1$ sequential

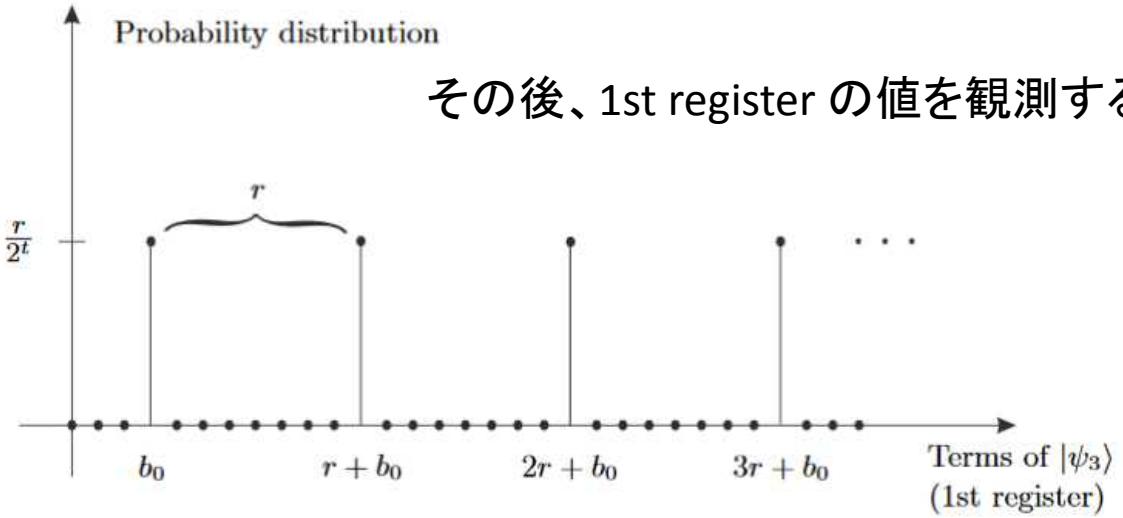
波動関数は *x* の order *r* (*x^r=1*) の情報も持っているが、(classical な)観測によって、order を取り出せるか、が肝。この段階で 観測したら、*(j, x^j)*が等確率で観測されるだけ

x^j は order *r* の周期関数 $1 \to x \to x^2 \to x^3 .... \to x^r = 1 \to x \to x^2 \to x^3 .... \to x^r = 1$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^t}}\sum_{b=0}^{r-1}\sum_{a=0}^{2^t/r-1}|ar+b\rangle|x^b\rangle$$

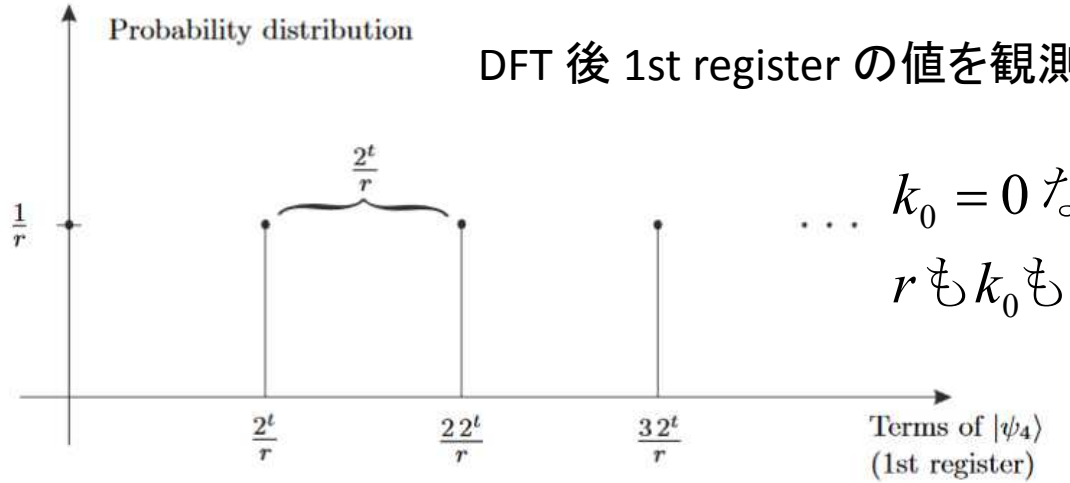
$$|\psi_3\rangle = \frac{\sqrt{r}}{\sqrt{2^t}}\sum_{a=0}^{2^t/r-1}|ar+b_0\rangle|x^{b_0}\rangle$$

second register の値を観測



その後、1st register の値を観測すると $ar + b_0$ が求まる

$$\mathrm{DFT}(|k\rangle) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp(2\pi i jk / N) |j\rangle \qquad |\psi_4\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp(-2\pi i \frac{k}{r} b_0) \left| \frac{k2^t}{r} \right\rangle |x^{b_0}\rangle$$



DFT 後 1st register の値を観測すると $k_0 / r \in [0,1)$ が求まる

$k_0 = 0$ ならやり直し

r も k_0 も unkown, ratio k_0 / r のみ

$$q = \left(\frac{k_0}{r}\right) = \frac{k_1}{r_1} \quad GCD(k_1, r_1) = 1 \Rightarrow r_1 \text{ is a factor of } r$$

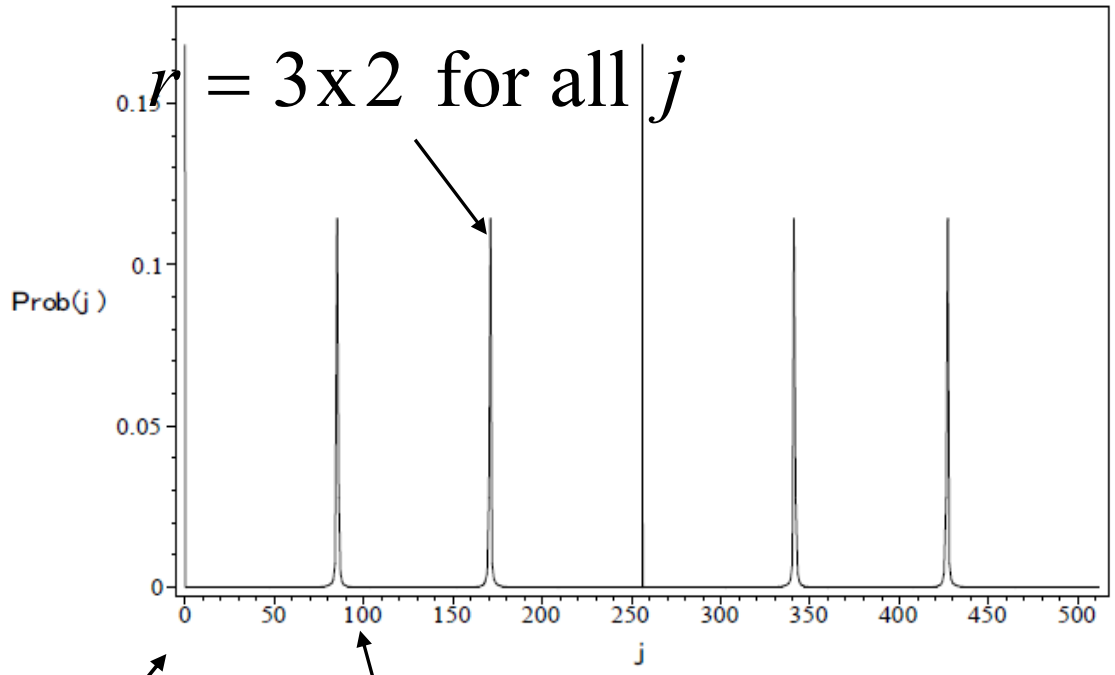
i.e. $r = r_1 r_2 \quad 1 = x^r = (x^{r_1})^{r_2}$ repeat quantum circuit for new $x = x^{r_1}$ to find r_2

recursive procedure stops at most $\log_2 r$ steps

$r \neq 2^s$ case

$N = 21 \quad x = 2 \quad r = 6$

$t = 9 \quad 2^t = 512 \qquad \frac{k_0}{r} = \frac{j}{512}$



retry $r = 6$ for all j

分布が広がる
得られた 1st reg の値(有理数)
から order r を求める方法
連分数による近似列

DFTとV_xの量子回路について

- DFT: 古典計算機ではコストが大きい計算

$$\mathrm{DFT}(|j\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp(2\pi i j k / N) |k\rangle \qquad \text{cost } O(N^2) = O(2^{2n})$$

$$|k\rangle = |k_1\rangle |k_2\rangle \ldots |k\rangle \qquad \sum_{k_1=0}^{1} \qquad k = \sum_{l=1}^{n} k_l 2^{n-l}$$

$$\mathrm{DFT}(|j\rangle) = \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \ldots \sum_{k_n=0}^{1} \exp(2\pi i j \sum_{l=1}^{n} \frac{k_l}{2^i})$$

$$= \frac{1}{\sqrt{2^n}} \prod_{l=1}^{n} \sum_{k_l=0}^{1} \exp(2\pi i j \sum_{l=1}^{n} \frac{k_l}{2^i}) \qquad \text{cost} \quad O(Nn) = O(n2^n)$$

- 量子計算: quantum parallelism for j cost $O(n^2)$
  - 量子回路 (基本gateの組み合わせで表した) 有

- べき乗計算　$V_x(|j\rangle|0\rangle) \exists |j\rangle|x^j\rangle$
  - 古典回路のgateを量子gateに置き換えて実現可能
  - x^{2^l}をhard codingし、$j = \sum_{l=0}^{n-1} j_l\, 2^l$として、$l$の loop で積の繰り返しで実現

$power := 1$
for $l = 0$ to $n-1$
  if $(j_l == 1)$ then
    $power := power \times x^{2^l} \pmod N$
  endif
endif

  - 4行目: $b = bc$ も、“同様に”和の繰り返しで実現
  - gate array の構造は、N と x に依存
  - どの程度一般化できるかは不明

実装例

- non-trivial な最小の N=15 の実装は幾つか
  - L.M.K. Vandersypen, et al., Nature 414 , 883-887 (2001), NMR
  - C.-Y. Lu, et al., Phys. Rev. Lett. 99 250504 (2007), Photonic Qubits.
  - B.P. Lanyon, et al.,Phys. Rev. Lett.99 , 250505 (2007). Photonic Chip
  - A. Politi, et al., Science 325, , 1221 (2009), Photonic Chip
  - T. Monz, et al., arXiv:1507.08852, ion-trap Q.C.
- N=21 が一つ
  - E. Martin-Lopez, et.al. Nature Photonics 6, 773(2012) Photonic Chip