Shor's Algorithm

수학문제연구회 2024S Seminar

36기 한승우

KAIST 수학문제연구회

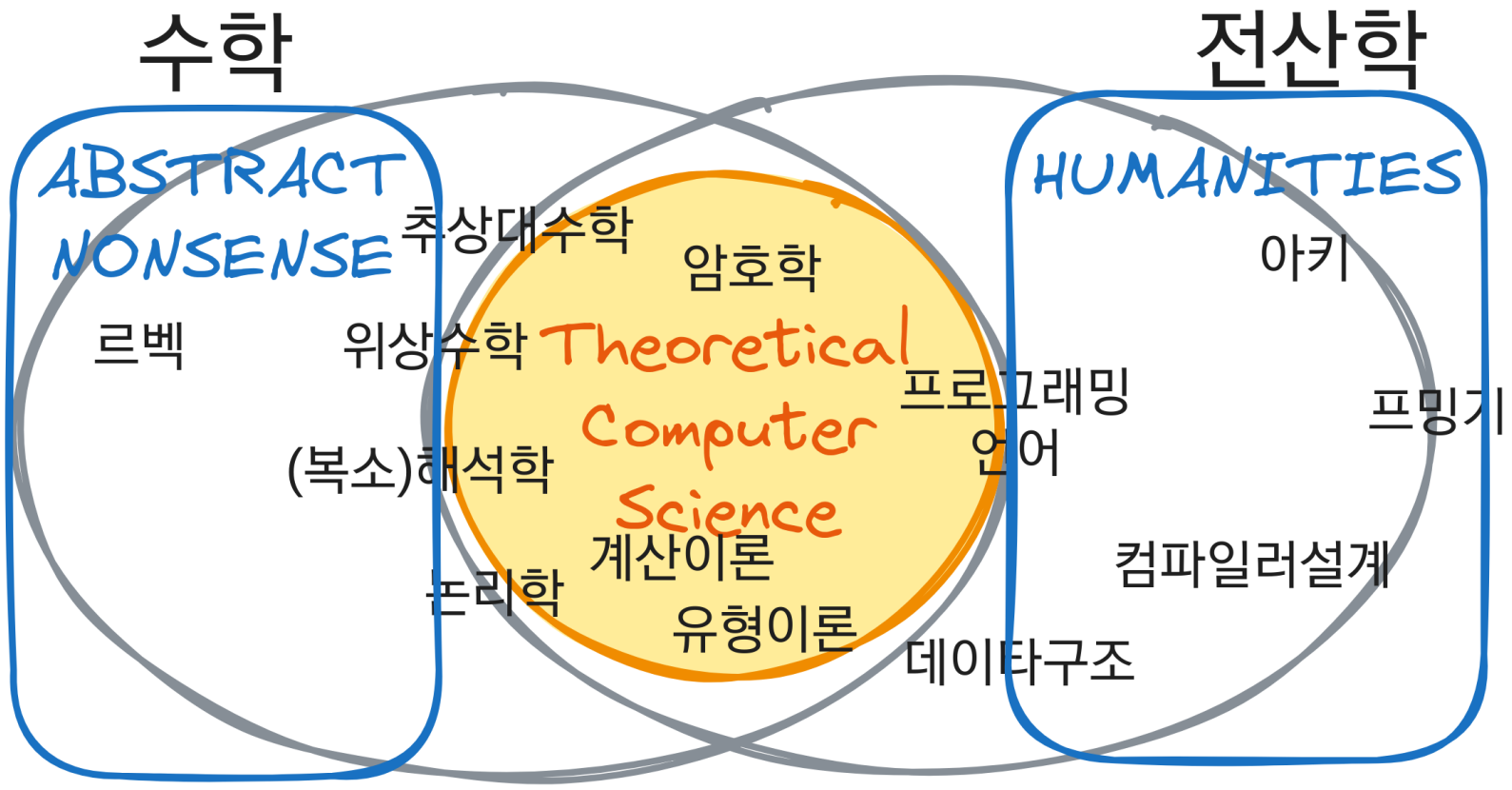
2024년 5월 13일

Theoretical Computer Science

Theoretical computer science is a subfield of computer science and mathematics that focuses on the abstract and mathematical foundations of computation, such as the theory of computation, formal language theory, the lambda calculus and type theory.

Theoretical computer science, Wikipedia.

Theoretical Computer Science



Two Different Perspectives

$\gcd(a, b)$를 바라보는 두 가지 시각

MATH MAN

smallest positive integer that divides both a and b

존재성, 유일성, 정의에서 오는 여러 정리...

CS MAN

1. how to "compute" it
2. how much time it needs to compute

효율적으로 "계산"할 수 없으면 다른 유용한 것을 계산하는 데 사용할 수 없음

오늘 세미나를 CS Man의 시각에서 보면 더 재미있을 것임!

RSA Cryptosystem

Euler's Theorem

If $\gcd(x, N) = 1$, then $x^{\phi(N)} \equiv 1 \pmod{N}$.

RSA Cryptosystem

1. 천지원이 최푸른하늘한테 메시지 $m \in \mathbb{N}$을 보내고 싶어 함.
2. 최푸른하늘은 큰 소수 p, q를 골라서 $N = pq$를 계산함.
3. 최푸른하늘은 또 $\phi(N) = (p-1)(q-1)$과 서로소인 적당한 e를 골라서 $ed \equiv 1 \pmod{\phi(N)}$인 d를 계산함
4. 최푸른하늘은 모두에게 N과 e를 공개함.
5. 천지원은 $c = x^e \bmod N$을 계산해서 모두에게 공개함
6. 최푸른하늘은 $m = c^d \bmod N$을 계산할 수 있음
7. 다른 사람은 d을 계산할 수 없기 때문에 최푸른하늘만 m을 해독할 수 있음

RSA Cryptosystem: Calculation

정수에 대한 Time Complexity

어떤 문제에 대한 input이 정수 N 일 때는 input의 크기를 $\log N$ 으로 봄. (N 을 표현하는 데 $\log N$ 개의 글자가 필요해서) 예를 들어 시간 복잡도가 $O(N)$ 이면 poly-time이 아니라 $O(2^{\log N})$, 즉 exponential time임.

Modular Exponentiation

$x^e \mod N$ 을 어떻게 계산할까? Time complexity는?

Factorization

Problem "Factoring"

Given $n \in \mathbb{N}_{>1}$, find a non-trivial divisor d of n if n is composite.

Unsolved Question

이 문제가 고전적인 컴퓨터에서 poly-time안에 해결 가능할까? 즉, 이 문제는 P에 속할까?

Current Best: General Number Field Sieve

$$\exp\left(\left(\left(\frac{64}{9}\right)^{1/3} + o(1)\right)(\log n)^{1/3}(\log\log n)^{2/3}\right)$$

Shor's Algorithm

Randomized quantum computing으로 poly-time안에 해결 가능. 즉, "Factoring"은 BQP에 속함.

Shor's Algorithm: Overview

Given $n \in \mathbb{N}_{>1}$, find a non-trivial divisor d of n if n is composite.

Procedure of Shor's Algorithm

Input: $n \in \mathbb{N}_{>1}$

1. If n is even or is a prime power, then done.
2. Pick a random integer $1 < x < n$ and loop.
   1. If $\gcd(x, n) > 1$, then done.
   2. Calculate $r = \mathrm{ord}_n x$. ▷ where we need quantum computing
   3. If r is even and $x^{r/2} \not\equiv_n -1$, break the loop.
3. $\gcd(x^{r/2} + 1, n)$ and $\gcd(x^{r/2} - 1, n)$ are non-trivial divisors.

Quantum computing은 order를 계산하는 데에만 쓰임!

Correctness: Part 1

Theorem

If $b \in \mathbb{Z}$ satisfies $b^2 \equiv 1 \pmod{n}$ and $b \not\equiv_n \pm 1$, then

$$1 < \gcd(b-1, n), \gcd(b+1, n) < n.$$

Proof

Set $d = \gcd(b-1, n)$ and use Bézout's identity. □

Corollary

If $r = \operatorname{ord}_n x$ is even and $x^{r/2} \not\equiv -1 \pmod{n}$, then

$$1 < \gcd(x^{r/2}-1, n), \gcd(x^{r/2}+1, n) < n.$$

위 보조정리에 의해 Shor's algorithm (3)의 정확성은 보여졌다!

Correctness: Part 2

이제 (2) Loop가 무한 루프가 아니라는 걸 보이자!

Definition

소수 p와 자연수 n에 대해

$$u(p,n) = \max\{\, k \in \mathbb{Z}_{\geq 0} \mid p^k \text{ divides } n \,\}$$

라고 정의하자.

Example

- $u(2,24) = 3,\ u(3,24) = 1.$
- $u(2,30) = u(3,30) = u(5,30) = 1,\ u(7,30) = 0.$

Correctness: Part 2

Lemma

소수 p와 자연수 n, 음이 아닌 정수 α에 대해,

$$\left|\left\{k \in [n] \;\middle|\; u\big(p, \gcd(k,n)\big) = \alpha\right\}\right| = \begin{cases} \dfrac{p-1}{p^{\alpha+1}} n, & 0 \le \alpha < u(p,n) \\ \dfrac{1}{p^{\alpha}} n, & \alpha = u(p,n) \\ 0 & \alpha > u(p,n) \end{cases}$$

이다.

Lemma

n이 짝수이면 $\left|\left\{k \in [n] \;\middle|\; u\left(2, \dfrac{n}{\gcd(k,n)}\right) = \alpha\right\}\right| \le \dfrac{n}{2}$.

Correctness: Part 2

Theorem

n이 odd prime power이면 모든 자연수 α에 대해

$$\Pr_{x \in \mathbb{Z}_n^*}\left[u(2, \operatorname{ord}_n x) = \alpha\right] \leq \frac{1}{2}$$

이다. $(\mathbb{Z}_n^* = \{\, m \in [n] \mid \gcd(m, n) = 1 \,\})$

Proof

n이 odd prime power이므로 n의 primitive root g가 존재한다. 그러면, 각각의 $x \in \mathbb{Z}_n^*$에 대해 $x \equiv g^k \pmod{n}$인 k가 존재하고 따라서

$$\operatorname{ord}_n x = \frac{\operatorname{ord}_n g}{\gcd(k, \operatorname{ord}_n g)} = \frac{\phi(n)}{\gcd(k, \phi(n))}$$

이다. 이제 전 슬라이드의 lemma를 적용한다. □

Correctness: Part 2

Theorem

$n = p_1^{a_1} \cdots p_k^{a_k}$ 를 n의 소인수분해라고 하자. $\gcd(x, n) = 1$인 x를 하나 고르자. $r = \mathrm{ord}_n x$, $r_i = \mathrm{ord}_{p_i^{a_i}} x$라고 하자. $r = \mathrm{ord}_n$가 짝수라면,

$$x^{r/2} \equiv -1 \pmod{n} \iff u(2, r_1) = \cdots = u(2, r_k) > 0\text{이다.}$$

Proof

$r = \mathrm{lcm}(r_1, \cdots, r_k)$이다. r을 r_i로 나눈 몫을 s_i라고 하자.

$$x^{r/2} \equiv -1 \pmod{n} \iff \forall i \in [n],\ x^{r_i s_i/2} = x^{r/2} \equiv -1 \pmod{p_i^{a_i}}$$

만약 어느 s_i가 짝수라면 $x^{r_i s_i/2} \equiv 1 \pmod{p_i^{a_i}}$가 되므로, 모든 s_i는 홀수이고, 따라서 모든 r_i는 짝수이다.

Continued...

Correctness: Part 2

모순을 보이기 위해 $u(2, r_1) > u(2, r_2)$라고 가정하자. $r_1 = 2^{\alpha_1} t_1$, $r_2 = 2^{\alpha_2} t_2$로 쓰자. (t_1, t_2는 홀수.) 그러면 $\alpha_1 > \alpha_2$이므로

$$2^{\alpha_1} \mid r = r_2 s_2 = 2^{\alpha_2} t_2 s_2$$

이고, t_2와 s_2 모두 홀수이므로 이는 불가능하다.

반대로, $u(2, r_1) = \cdots = u(2, r_k) > 0$을 가정하면 모든 i에 대해 $2 \nmid s_i$이고, 따라서 $x^{r/2} = (x^{r_i/2})^{s_i} \equiv (-1)^{s_i} = -1 \pmod{p_i^{s_i}}$이다. □

Correctness: Part 2

Lemma

$$\Pr_{x \in \mathbb{Z}_n^*}[\mathrm{ord}_n\, x \text{ is even}] \geq \frac{1}{2}$$

Proof

일대일 함수

$$f : \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_n^*$$
$$x \longmapsto -x$$

는 order가 odd인 원소를 order가 even인 원소로 보낸다. □

Correctness: Part 2

Theorem

n이 합성수이면,

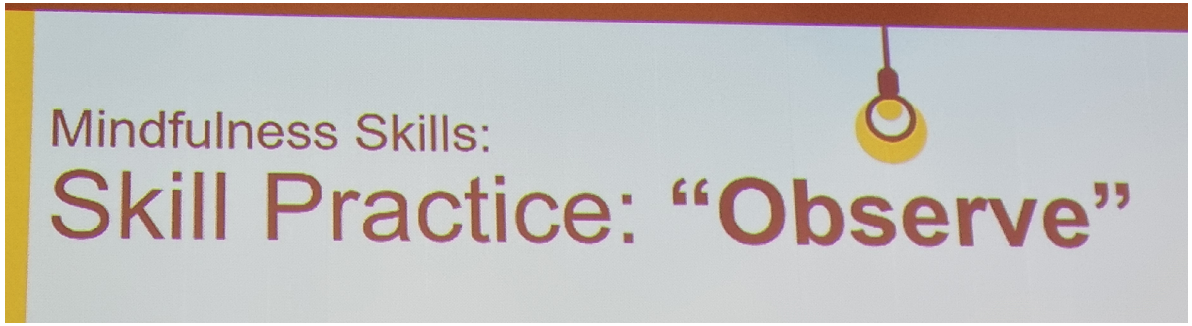
$$\Pr_{x \in \mathbb{Z}_n^*} \left[\operatorname{ord}_n x \text{ is even and } x^{(\operatorname{ord}_n x)/2} \not\equiv -1 \pmod{n} \right] \geq \frac{1}{4}.$$

이제 Shor's algorithm (2)의 loop가 평균적으로 $O(1)$ 안에 끝난다는 사실을 알았음!

Quantum Computing

Quantum State

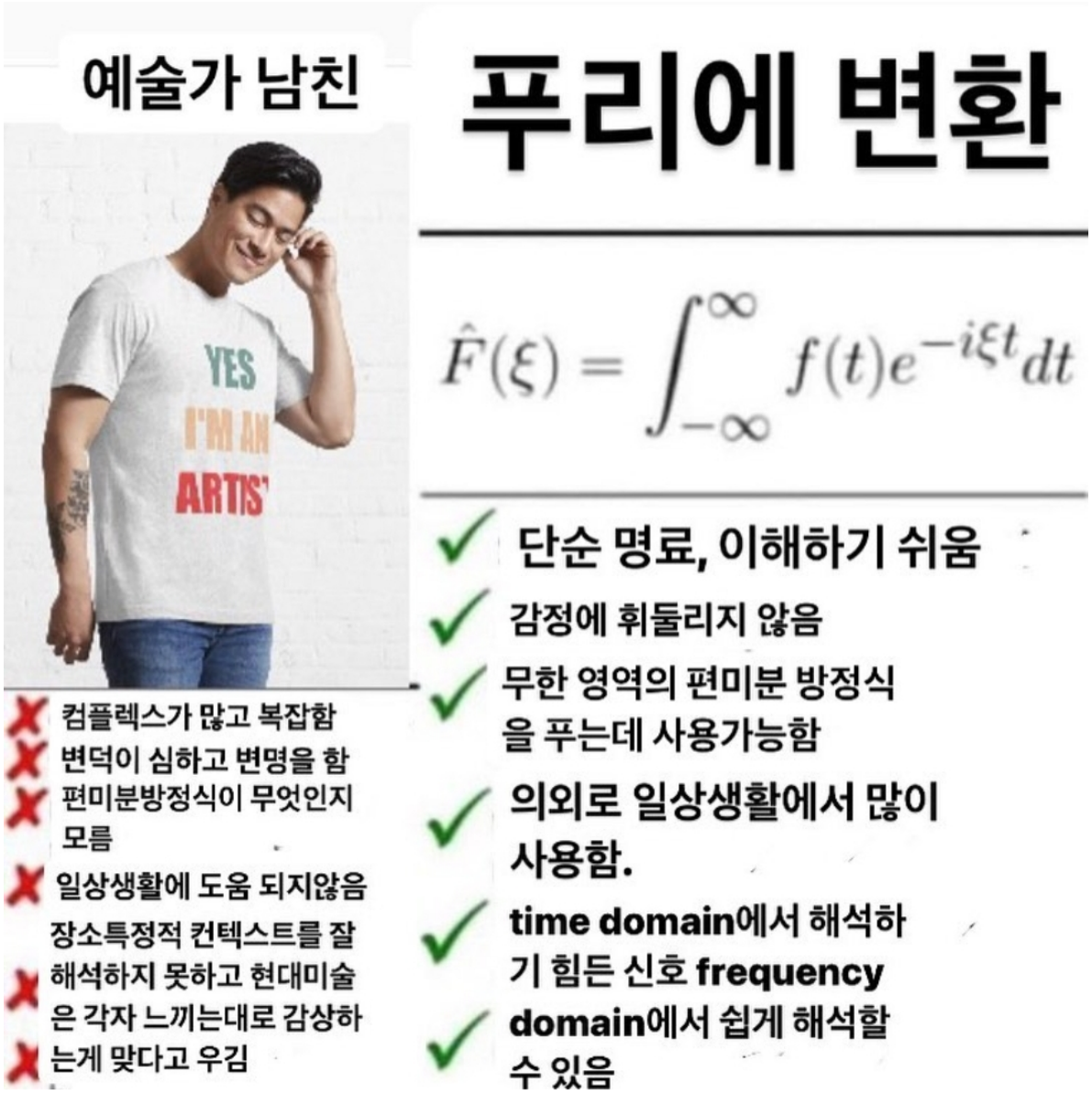
A *quantum state* is a unit-length vector in an N-dimensional complex vector space.



Observation

If $v = \sum_{i=0}^{N-1} a_i |b_i\rangle$ where $|b_i\rangle$'s are basis vectors (also called *pure states*), v를 "관측"하면 $|b_i\rangle$ 중 하나를 보게 되는데, $|b_i\rangle$을 관측할 확률은 각각 $|a_i|^2$임.

Quantum Fourier Transform



Quantum Fourier Transform

$$\omega = e^{2\pi i/N}$$

Quantum Fourier Transform

Quantum Fourier transform은 basis vector $|b_i\rangle$를

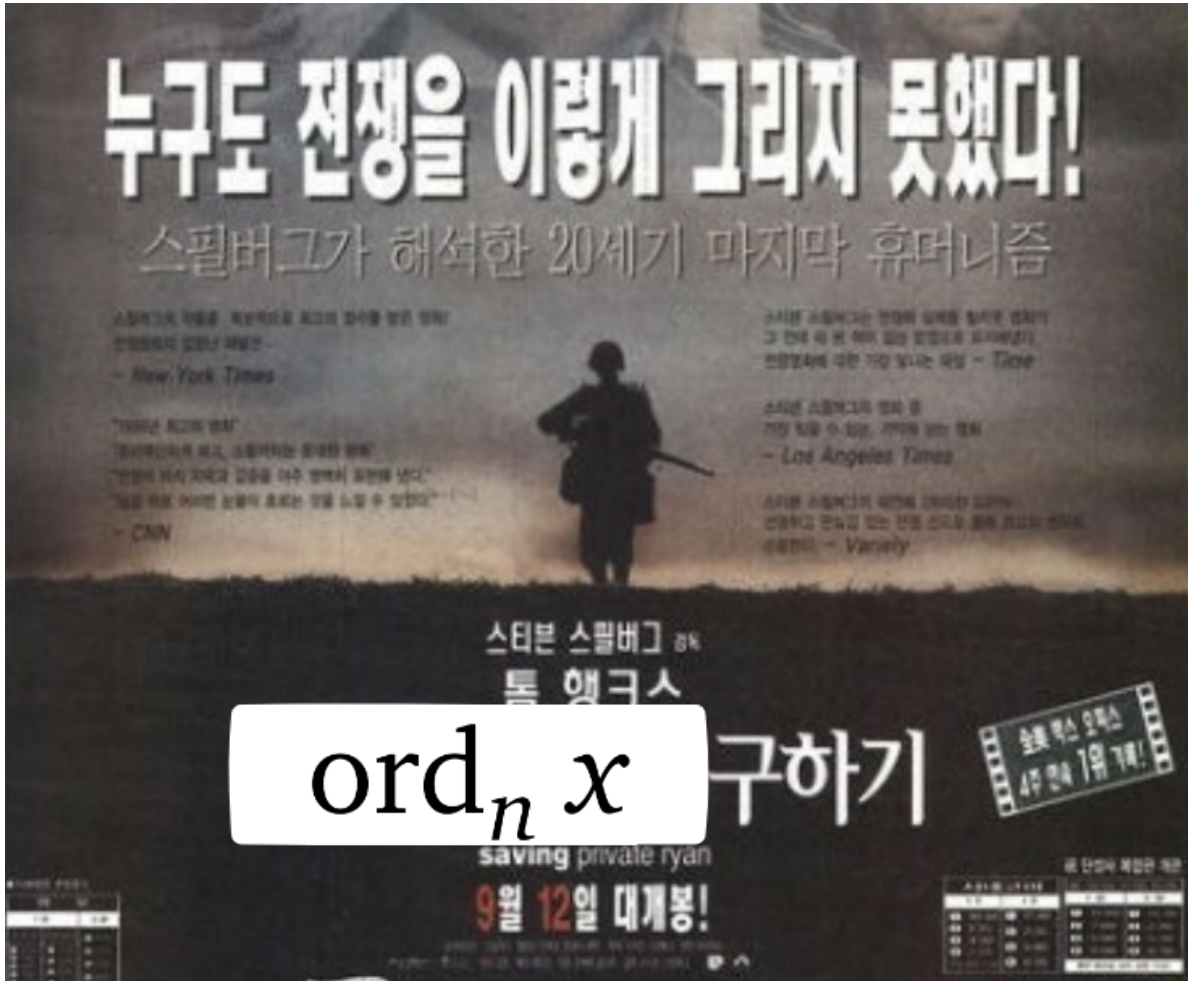
$$|b_i\rangle \longmapsto \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{ij} |b_j\rangle$$

로 보내는 linear map이다.

Blackbox

임의의 N-dimensional quantum state에 대한 QFT를 $O((\log N)^2)$ 시간 안에 계산 가능하다.

Calculating the Order: Overview



$$\operatorname{ord}_n x$$

Calculating the Order: Overview

Calculating the Order

목표: Fixed x, n에 대해 $\mathrm{ord}_n x$를 찾기.

1. $N = 2^\ell$, $n^2 < N < 2n^2$인 N 찾기. (Easy!)
2. Nn-dimensional quantum state를 다음으로 초기화.

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i, x^i \bmod n\rangle$$

   (Basis vector들을 $|a, b\rangle$, $0 \le a < N$, $0 \le b < n$ 꼴로 나타냄.)
3. 위 quantum state의 first register에 대해 quantum fourier transform 적용. (디테일은 뒤에서)
4. 관찰. $|j, x^i \bmod n\rangle$을 관찰했다고 하자.
5. 운이 좋으면 j/N의 convergent (continued fraction)의 분모 중 $\mathrm{ord}_n x$가 등장함! (확률 $\in \Omega(1/\log \ell)$)

Calculating the Order: Initialization

Initialization Step (2)

1. Quantum state를

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i, 0\rangle$$

으로 초기화

2. $|i, 0\rangle \mapsto |i, x^i \bmod n\rangle$으로 보내는 linear map 을 계산.[1]

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i, x^i \bmod n\rangle$$

---

[1] time complexity: $O(\ell^2 \log \ell)$

Calculating the Order: QFT

Quantum Fourier Transform (3)

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i, x^i \bmod n\rangle$$

의 QFT를 $O(\ell^2)$ blackbox algorithm으로 계산:

$$\frac{1}{N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \omega^{ij} |j, x^i \bmod n\rangle$$

Calculating the Order: Observation

$$\frac{1}{N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\omega^{ij}|j, x^i \bmod n\rangle$$

Observation (3)

Basis vector $|j, x^i \bmod n\rangle$ $(0 \le j < N, 0 \le i < \mathrm{ord}_n x)$을 관측할 확률은?

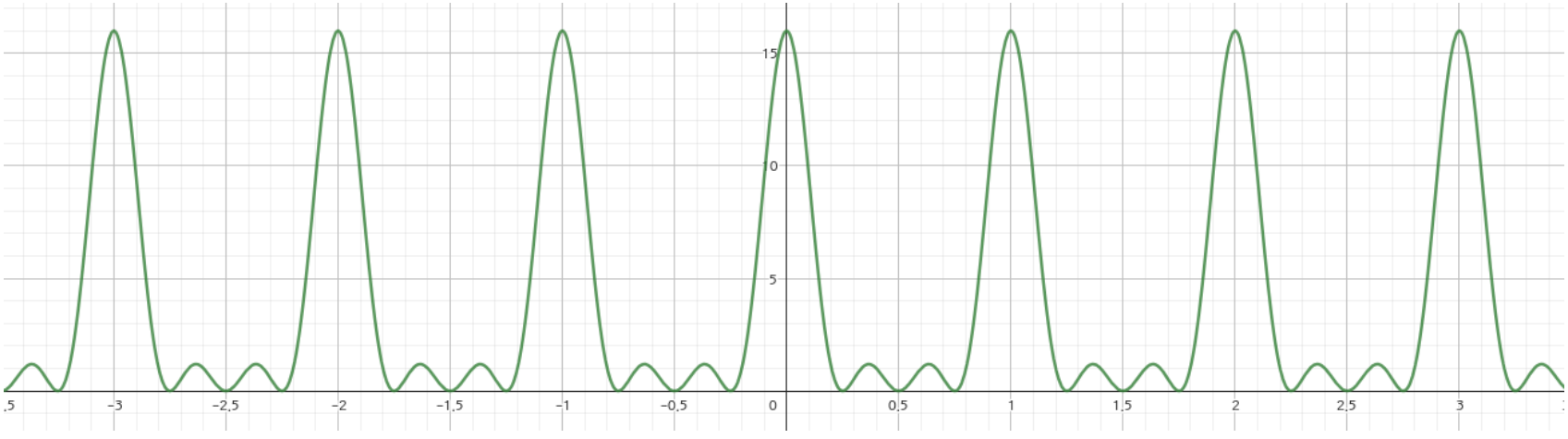
Note that $x^i \equiv x^{i+r} \equiv x^{i+2r} \equiv \cdots \pmod n$ where $r = \mathrm{ord}_n x$!

$$\left|\frac{1}{N}\sum_{b=0}^{m-1}\omega^{rjb}\right|^2 = \frac{1}{N^2}\cdot\frac{\sin^2(\pi mrj/N)}{\sin^2(\pi rj/N)}$$

where $m = \lfloor (N-i-1)/r \rfloor + 1 \approx N/r$.

Calculating the Order: Observation

$$\Pr\left[\text{observing } |j, x^i \bmod n\rangle\right] = \frac{1}{N^2} \cdot \frac{\sin^2(\pi m r j/N)}{\sin^2(\pi r j/N)}$$



$\frac{rj}{N}$ 이 정수에 가까운 j를 관찰할 확률이 크다!

즉, $\frac{j}{N}$ 이 r을 분모로 갖는 유리수와 가까울 확률이 크다!

Calculating the Order: Observation

Lemma

$\frac{rj}{N}$과 가장 가까운 정수 사이의 거리 $\leq \frac{r}{2N}$이면

$$\Pr\left[\text{observing } |j, x^i \bmod n\rangle\right] \geq \frac{c}{r^2}$$

for some constant $c > 0$. (c is independent from $x, N, \cdots$.)

Proof

Left to readers. (Hint: start by filling the details omitted in the slides.)

Note that:

$$(\text{거리}) \leq \frac{r}{2N} \iff \exists d \in \mathbb{N},\ \left|\frac{j}{N} - \frac{d}{r}\right| \leq \frac{1}{2N}.$$

Calculating the Order: Continued Fraction

$$\exists d \in \mathbb{N},\ \left|\frac{j}{N} - \frac{d}{r}\right| \leq \frac{1}{2N} \text{이면 (관측 확률)} \in \Omega\left(\frac{1}{r^2}\right)$$

Theorem (Legendre, 1798)

If $\alpha \in \mathbb{N}$ and $p, q \in \mathbb{N}$ satisfy

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2},$$

then p/q is a convergent of α.

Note that $N > n^2 > r^2$.

만약 $\left|\frac{j}{N} - \frac{d}{r}\right| \leq \frac{1}{2N}$ 이라면 $\frac{d}{r}$ 은 $\frac{j}{N}$ 의 convergent!

Calculating the Order: Continued Fraction

$$\left|\frac{j}{N}-\frac{d}{r}\right| \le \frac{1}{2N} \text{ 이면 } \frac{d}{r} \text{ 은 } \frac{j}{N} \text{ 의 convergent}$$

- Convergent는 약분된 꼴로 구할 수 있으므로 적어도 $\gcd(d,r)=1$ 일 때 r 을 구할 수 있음.
- 각각의 $d \in \mathbb{Z}_r^*$ 에 대해 $|j/N - d/r| \le 1/2N$ 인 j 는 unique하고, 서로 다름.
- 따라서, ($\phi(r)$ 개의 j 값) $\times$ (r 개의 $x^i \bmod n$ 값) $= r\phi(r)$ 개 중 하나를 관측하면 r 을 계산할 수 있음! (실패하면 처음부터)
- $r\phi(r)$ 개 중 하나를 관측할 확률은

$$r\phi(r)\cdot\Omega\left(\frac{1}{r^2}\right)=\Omega\left(\frac{\phi(r)}{r}\right).$$

Calculating the Order: Continued Fraction

$$\text{성공 확률} = r\phi(r) \cdot \Omega\left(\frac{1}{r^2}\right) = \Omega\left(\frac{\phi(r)}{r}\right)$$

Theorem (Rosser, 1980)

For each natural number n greater than 2,

$$\frac{\phi(n)}{n} > \frac{1}{e^{\gamma} \ln\ln n + \frac{3}{\ln\ln n}}$$

where γ is the Euler's constant.

$$\text{성공 확률} \in \Omega\left(\frac{1}{\log\log r}\right) \subseteq \Omega\left(\frac{1}{\log \ell}\right)$$

Calculating the Order: Recap

목표: Fixed x, n에 대해 $\mathrm{ord}_n x$를 찾기.

1. $N = 2^\ell$, $n^2 < N < 2n^2$인 N 찾기.
2. $(N+n)$-dimensional quantum state를 다음으로 초기화.

$$\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i, x^i \bmod n\rangle$$

3. 위 quantum state의 first register에 대해 quantum fourier transform 적용.
4. 관찰. $|j, x^i \bmod n\rangle$을 관찰했다고 하자.
5. $\Omega(1/\log \ell)$의 확률로 j/N의 convergent (continued fraction)의 분모 중 $\mathrm{ord}_n x$가 등장함

References

- Shor, P.W. (1994). "Algorithms for quantum computation: Discrete logarithms and factoring". *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press. pp. 124–134.
- Burton, David M. *Elementary Number Theory*. 2nd ed, Wm. C. Brown, 1989.

Q&A

질문 받습니다.