Portland State U

F, 05/01/2020

S′20 CS 410/510

Intro to quantum computing

Fang Song

Week 5

- Modular arithmetic
- Order finding
- Prime factorization

Credit: based on slides by Richard Cleve

Exercise

1. Compute the product of the numbers below
   - Example. $3 \times 5 = 15$
   - $19 \times 31 =$
   - $244176193 \times 176944583 =$
2. Find the prime factorization of the numbers below.
   - Example. $15 = 3 \times 5$
   - $21 =$
   - $247 =$
   - $205027 =$
   - $55514685797288803 =$
3. How many bits do we need to write an integer $x \in \mathbb{Z}$ in binary?

A round of applause

- Exponential quantum speedup
  - Nice, but query-model, "artificial" problems …

Black-box problem	Deterministic	Randomized	Quantum
Deutsch	2 (queries)	2 (queries)	1 (query)
Deutsch-Josza	$2^{n-1}+1$	$\Omega(n)$	1 (Exact)
Simon	$2^{n-1}+1$	$\Omega(\sqrt{2^n})$	$O(n)$

- Today: quantum (exponential) speedup on a "real-life" hard problem

Integer factorization

Input. Positive integer $N (= pq, p, q\ prime)$

Goal. Find p, q

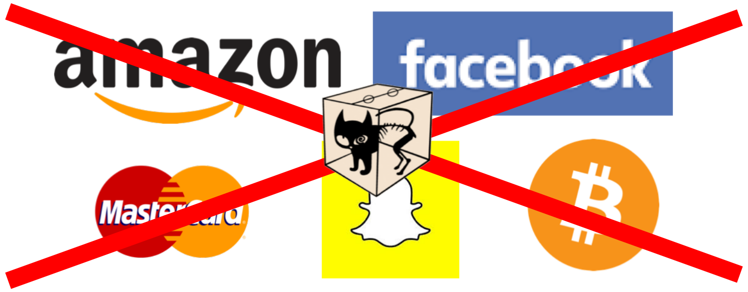
- Classical efficient algorithm NOT known
  - Number field sieve ~ $2^{O((\log N)^{\frac{1}{3}} (\log \log N)^{\frac{2}{3}})}$

Efficient = poly-time in input size
Ex. N has n bits. Runtime $O(n^5)$

- Efficient quantum algorithm $O((\log N)^3)$ [Shor94, Kitaev94]
  - Generalization of Simon's algorithm

An inconvenient consequence in cybersecurity

- RSA cryptosystem relies on hardness of factorization
  - Foundation of modern cryptography and Internet security



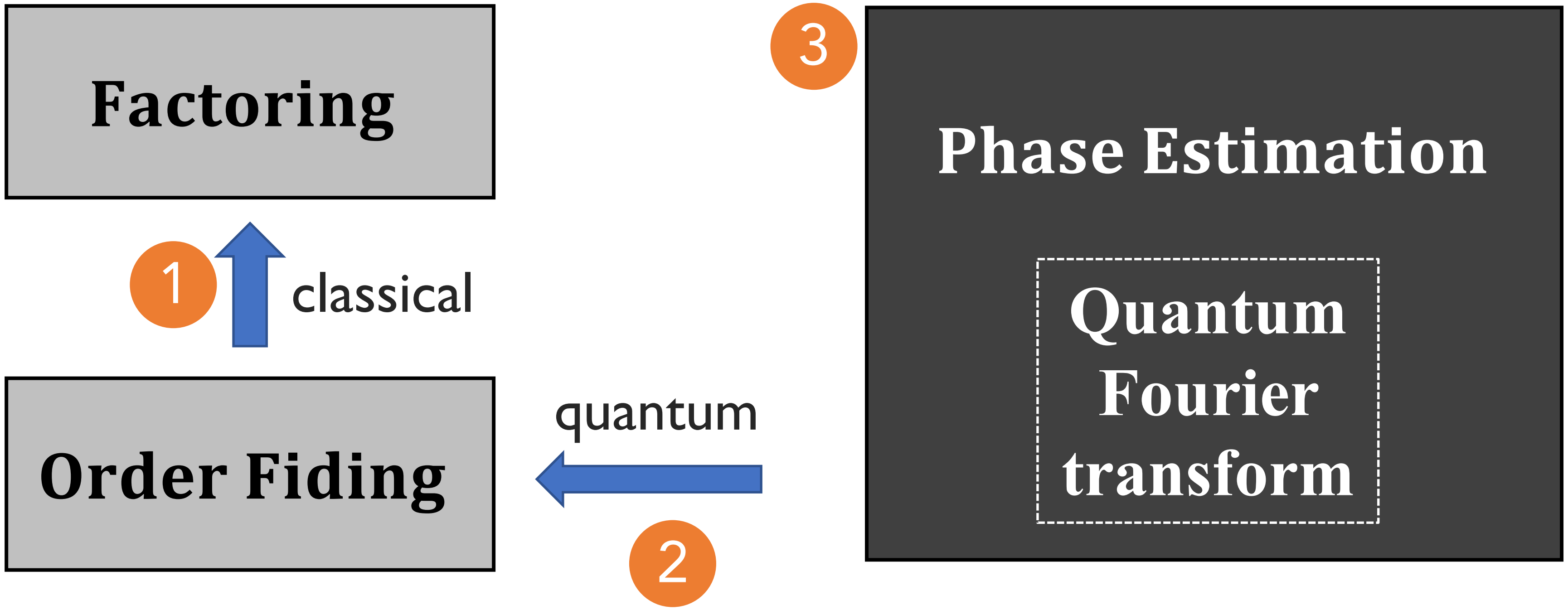
Will be broken by a quantum computer

- RSA Factoring Challenge

Feb 28, 2020: RSA-250 (250 decimal digits = 829 bits) factored!
Total computation time ~ 2700 core-years (Intel Xeon Gold 6130)

RSA-250 = 641352894770715802787901901705773890848250147429434472081168596320245323446302386235987526683477087376619255856946397988533367 ×
3337202759497815655622601060535511422794076034476755466678452098702384172921
0037080257448673296881877565718986258036932062711

Roadmap to quantum factorization algorithm



- Today: 1 & 2 (treating PE as black-box)
- Next time: 3 open up PE and QFT

Review: arithmetic/number theory

Modular arithmetic

$$a, b, N \in \mathbb{Z}, N \geq 1$$

- $a \equiv b \bmod N \Leftrightarrow N \mid (a - b)$
- $\gcd(a, b) = \max\{c: c|a \text{ and } c|b\}$
  - a, b coprime, if $\gcd(a, b) = 1$
- $\mathbb{Z}_N := \{0,1, \dots, N-1\}$
- $\mathbb{Z}_N^* := \{a \in \mathbb{Z}_N: \gcd(a, N) = 1\}$
  - Euler φ function $\varphi(N) := |\mathbb{Z}_N^*|$
- Fact. $\forall\, a \in \mathbb{Z}_N^*, \exists!$ (unique) $b \in \mathbb{Z}_N^*\ s.t.\ ab \equiv 1 \bmod N$
  - Call b the inverse of a, and write it $a^{-1} \bmod N$
  - $\mathbb{Z}_N^*$ under multiplication mod N form a group.

Order

$$\mathbb{Z}_N^* := \{a \in \mathbb{Z}_N : \gcd(a, N) = 1\}, \varphi(N) = |\mathbb{Z}_N^*|$$

- Def (order mod N). Given $a \in \mathbb{Z}_N^*$, $\mathrm{ord}_\mathrm{N}(\mathrm{a}) := \min\{r : a^r \equiv 1 \bmod N\}$
- Fact (Euler's Theorem). $\forall\, a \in \mathbb{Z}_N^*, a^{\varphi(N)} \equiv 1 \bmod N$

  →$\mathrm{ord}_N(a)$ is well-defined

  →$\mathrm{ord}_N(a) \mid \varphi(N)$

Exercises

- Show that $\mathrm{ord}_N(a) \mid \varphi(N)$ always holds.
- Let $a = 4, N = 35$
  - $\mathbb{Z}_{35}^* =$
  - $\mathrm{ord}_{35}(4) =$

Order finding

Order finding

Input. Positive integer $N \geq 2, a \in \mathbb{Z}_N^*$

Goal. Compute $\mathrm{ord}_N(a)$

- Theorm. Factorization $\equiv$ Order finding
  - We can solve one efficiently iff. we can solve the other efficiently.

  → Best classical algorithm takes exponential time

- Theorm. ∃ poly-time quantum algorithm for order finding (hence factorization too)

Reducing factoring to order finding

Input. $N (= pq)$
Goal. Find p, q

Factoring

$a \longrightarrow$ **Order Fiding** $\longrightarrow ord_N(a)$

- Idea: Pick random $a \in \mathbb{Z}_N^*$, compute $r = ord_N(a)$

$$a^r \equiv 1 \; mod \; N \Leftrightarrow N |\; a^r - 1$$

- If r happens to be even, $a^r - 1 = (a^{\frac{r}{2}}+1)(a^{\frac{r}{2}}-1)$

$$N|(a^{\frac{r}{2}}+1)(a^{\frac{r}{2}}-1)$$

  - can $N|(a^{\frac{r}{2}}-1)$?
  - What if $N \nmid (a^{\frac{r}{2}}+1)$?

Reducing factoring to order finding cont'd

Input: an odd, composite integer N that is not a prime power.

Repeat

  Randomly choose $a \in \{2, \ldots, N-1\}$.

  Compute $d = \gcd(a, N)$.

  If $d \geq 2$ then /* We've been incredibly lucky. */

    Return $u = d$ and $v = N/d$.

  Else /* Now we know $a \in \mathbb{Z}_N^*$. */

    Let r be the order of a in $\mathbb{Z}_N^*$. /* Requires the order finding algorithm. */

    If r is even then

      Compute $x = a^{r/2} - 1 \pmod{N}$.

      Compute $d = \gcd(x, N)$.

      If $d \geq 2$ then

        Return $u = d$ and $v = N/d$. /* Answer is found. */

Until answer is found (or you get tired).

- Bad a
  - $ord_N(a)$ is odd
  - $N | (a^{\frac{r}{2}} + 1)$
- Fact. $\Pr_{a \leftarrow \mathbb{Z}_N^*}[a \text{ BAD}] \leq \frac{1}{2}$

➔Succeed in k iterations with prob. $\geq 1 - \frac{1}{2^k}$.

- Runtime = $O(k \cdot \text{Order-finding})$

Exercise

Let $\omega_r \coloneqq e^{2\pi i \frac{1}{r}}$ be the r^{th} root of unity

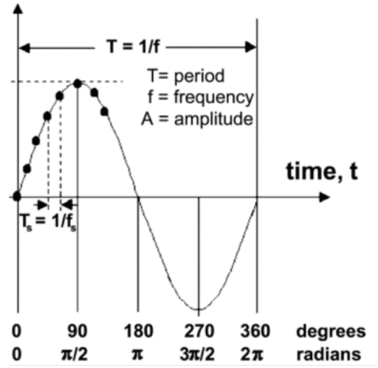
1. Show that $\omega_r^r = 1$.

2. Show that $\sum_{j=0}^{r-1} \omega_r^j = 0$.

Phase estimation

Meaning of "phase"

- Phase transition
  - Solid → liquid → gas , plasma
  - https://en.wikipedia.org/wiki/Phase_transition
- Phase in periodic function (waves)
  - Location with a single wave length
  - https://en.wikipedia.org/wiki/Phase_(waves)



- Phase factor $e^{i\theta}$
  - Global phase: $e^{i\theta}|\psi\rangle$ vs. $|\psi\rangle$ same statistics under measurements
  - Relative phase: $|0\rangle + e^{i\theta}|1\rangle$
    - $|0\rangle + |1\rangle$ vs. $|0\rangle - |1\rangle$: Measurement statistics differ

Phase estimation (a.k.a. eigenvalue est.)

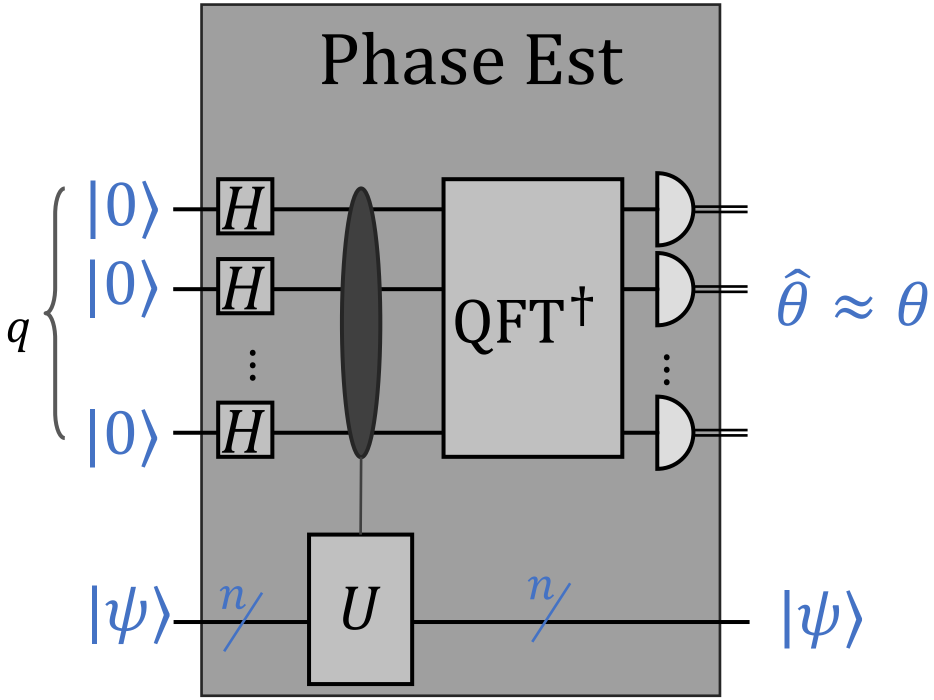
Input:

- Unitary operation U (described by a quantum circuit).
- A quantum state $|\psi\rangle$ that is an eigenvector of U: $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$.

Output: An approximation to $\theta \in [0, 1)$.

- Fact (HW4): Unitary U on n qubits has a complete set of orthonormal eigenvectors $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle\}, N = 2^n$
  - $\langle\psi_j|\psi_k\rangle = \begin{cases} 1, j = k \\ 0, j \neq k \end{cases}$
  - $U|\psi_j\rangle = e^{2\pi i\theta}|\psi_j\rangle$

Kitaev's quantum phase estimation algorithm



- Theorem. PE produces $\hat{\theta}$ with
  - precision $|\hat{\theta} - \theta| \leq \delta$ and
  - failure probability $\leq \varepsilon$

whenever $t = \Omega(\log \frac{1}{\delta \cdot \varepsilon})$.

- Proof (Next time)

- Theorem. PE produces $\hat{\theta}$ with

Solving order finding by phase estimation

Reducing order finding to phase estimation

Given $a \in \mathbb{Z}_N^*$, find $r := ord_N(a)$.

[$n \sim \log N$: # bits to encode elements of $\mathbb{Z}_N^*$]

- Wishful thinking:
  - A unitary operation U easy to implement
  - An eigenvector $|\psi\rangle$ whose eigenvalue reveals r. (Ex. $U\,|\psi\rangle = e^{2\pi i\theta}|\psi\rangle, \theta = 1/r$)
  - Plug into Phase Estimation and done!

A proper unitary and eigenvec for order finding

Given $a \in \mathbb{Z}_N^*$, find $r \coloneqq ord_N(a)$.

$[n \sim \log N$: # bits to encode elements of $\mathbb{Z}_N^*]$

- Unitary $M_a \colon |x\rangle \mapsto |ax \bmod N\rangle$

$\omega_r \coloneqq e^{2\pi i \frac{1}{r}}$ (r^{th} root of unity)

$\omega_r^r \coloneqq e^{2\pi i \frac{r}{r}} = 1$

- Eigenvector: $|\psi\rangle \coloneqq \frac{1}{\sqrt{r}}(|1\rangle + \omega_r^{-1}|a\rangle + \omega_r^{-2}|a^2\rangle + \cdots + \omega_r^{-(r-1)}|a^{r-1}\rangle)$

- What is missing?

Live with a set of eigenvectors

- Unitary M_a: $|x\rangle \mapsto |ax \bmod N\rangle$

$\omega_r := e^{2\pi i \frac{1}{r}}$

- Eigenvector: $|\psi\rangle := \frac{1}{\sqrt{r}}(|1\rangle + \omega_r^{-1}|a\rangle + \omega_r^{-2}|a^2\rangle + \cdots + \omega_r^{-(r-1)}|a^{r-1}\rangle)$

$$|\psi_0\rangle = 1/\sqrt{r}(|1\rangle + |a\rangle + |a^2\rangle + \cdots + |a^{r-1}\rangle)$$

$$|\psi_1\rangle = 1/\sqrt{r}(|1\rangle + \omega_r^{-1}|a\rangle + \omega_r^{-2}|a^2\rangle + \cdots + \omega_r^{-(r-1)}|a^{r-1}\rangle) = |\psi\rangle$$

$$\vdots$$

$$|\psi_j\rangle = \frac{1}{\sqrt{r}}(|1\rangle + \omega_r^{-j}|a\rangle + \omega_r^{-2j}|a^2\rangle + \cdots + \omega_r^{-(r-1)j}|a^{r-1}\rangle)$$

$$\vdots$$

$$|\psi_{r-1}\rangle = 1/\sqrt{r}\left(|1\rangle + \omega_r^{-(r-1)}\middle|a\right\rangle + \omega_r^{-2(r-1)}|a^2\rangle + \cdots + \omega_r^{-(r-1)(r-1)}|a^{r-1}\rangle)$$

Live with a set of eigenvectors cont'd

- Unitary $M_a: |x\rangle \mapsto |ax \bmod N\rangle$

$\omega_r := e^{2\pi i \frac{1}{r}}$

- Eigenvector: $|\psi\rangle := \frac{1}{\sqrt{r}}\left(|1\rangle + \omega_r^{-1}|a\rangle + \omega_r^{-2}|a^2\rangle + \cdots + \omega_r^{-(r-1)}|a^{r-1}\rangle\right)$

$$|\psi_0\rangle = \frac{1}{\sqrt{r}}\left(|1\rangle + |a\rangle + |a^2\rangle + \cdots + |a^{r-1}\rangle\right)$$

$$M_a|\psi_0\rangle =$$

Live with a set of eigenvectors cont'd

- Unitary $M_a: |x\rangle \mapsto |ax \bmod N\rangle$

$$\omega_r := e^{2\pi i \frac{1}{r}}$$

- Eigenvector: $|\psi\rangle := \frac{1}{\sqrt{r}}\left(|1\rangle + \omega_r^{-1}|a\rangle + \omega_r^{-2}|a^2\rangle + \cdots + \omega_r^{-(r-1)}|a^{r-1}\rangle\right)$

$$|\psi_j\rangle = \frac{1}{\sqrt{r}}\left(|1\rangle + \omega_r^{-j}|a\rangle + \omega_r^{-2j}|a^2\rangle + \cdots + \omega_r^{-(r-1)j}|a^{r-1}\rangle\right)$$

$$M_a|\psi_j\rangle =$$

Live with a set of eigenvectors cont'd

$\omega_r := e^{2\pi i \frac{1}{r}}$

- Unitary $M_a: |x\rangle \mapsto |ax \bmod N\rangle$
- Eigenvector: $|\psi\rangle := \frac{1}{\sqrt{r}}(|1\rangle + \omega_r^{-1}|a\rangle + \omega_r^{-2}|a^2\rangle + \cdots + \omega_r^{-(r-1)}|a^{r-1}\rangle)$

$$|\psi_0\rangle = 1/\sqrt{r}(|1\rangle + |a\rangle + |a^2\rangle + \cdots + |a^{r-1}\rangle)$$

$$\vdots$$

$$|\psi_j\rangle = 1/\sqrt{r}(|1\rangle + \omega_r^{-j}|a\rangle + \omega_r^{-2j}|a^2\rangle + \cdots + \omega_r^{-(r-1)j}|a^{r-1}\rangle)$$

$$\vdots$$

$$|\psi_{r-1}\rangle = 1/\sqrt{r}(|1\rangle + \omega_r^{-(r-1)}|a\rangle + \omega_r^{-2(r-1)}|a^2\rangle + \cdots + \omega_r^{-(r-1)(r-1)}|a^{r-1}\rangle)$$

$$\sum_{j=0}^{r-1}|\psi_j\rangle =$$

Quantum order finding algorithm

$$|1\rangle = \frac{1}{\sqrt{r}}\sum_j |\psi_j\rangle \,, M_a|\psi_j\rangle = e^{2\pi i \frac{j}{r}}$$

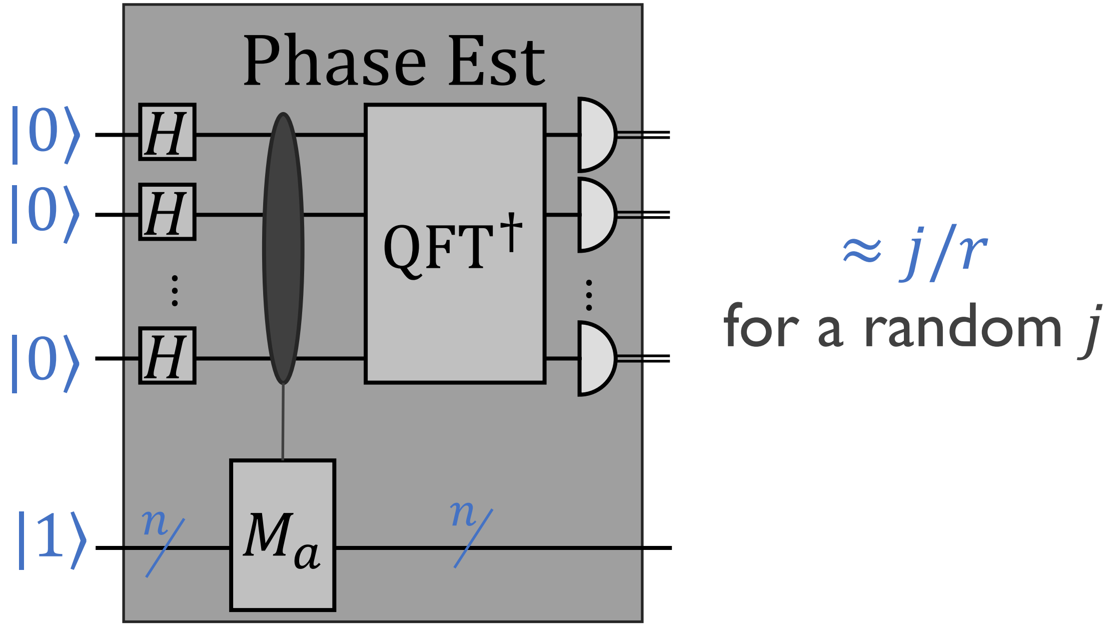
- Observation: $|\psi_j\rangle$ orthonormal

$$\langle \psi_j | \psi_k \rangle = \delta_{jk}$$

➔ PE with input $|1\rangle$

$\equiv$ PE with $|\psi_j\rangle$ for a random j

- Post-processing to recover r

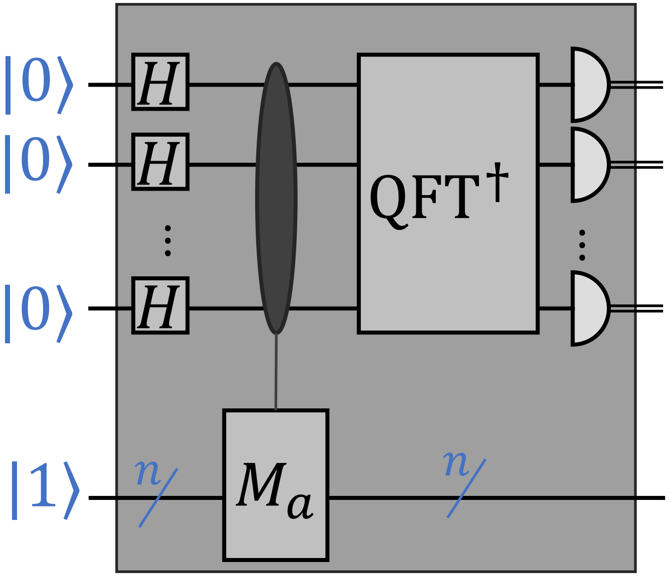


Quantum order-finding algorithm

Summary

$$N|(a^{\frac{r}{2}}+1)(a^{\frac{r}{2}}-1)$$

- What's next?
  - Phase estimation algorithm
  - Complexity of quantum order finding (implementing controlled M_a)



Quantum order-finding algorithm

Logistics

- Proposal due Sunday May 3rd , 11:59pm AoE
  - Submit as a group via Gradescope
  - No group? Submit a proposal and I will coordinate
  - 1-2 pages: consisting of 1) the topic, background, context, and motivation; 2) identify a few core references; and 3) a goal you intend to achieve and a plan.
- Talk by Silverman in Math department
  - Cryptography and quantum computing
  - See campuswire for details. Register by May 6
- IBM Qiskit competition

Scratch