PHY682 Special Topics in Solid-State Physics: Quantum Information Science

Lecture time: 2:40-4:00PM Monday & Wednesday

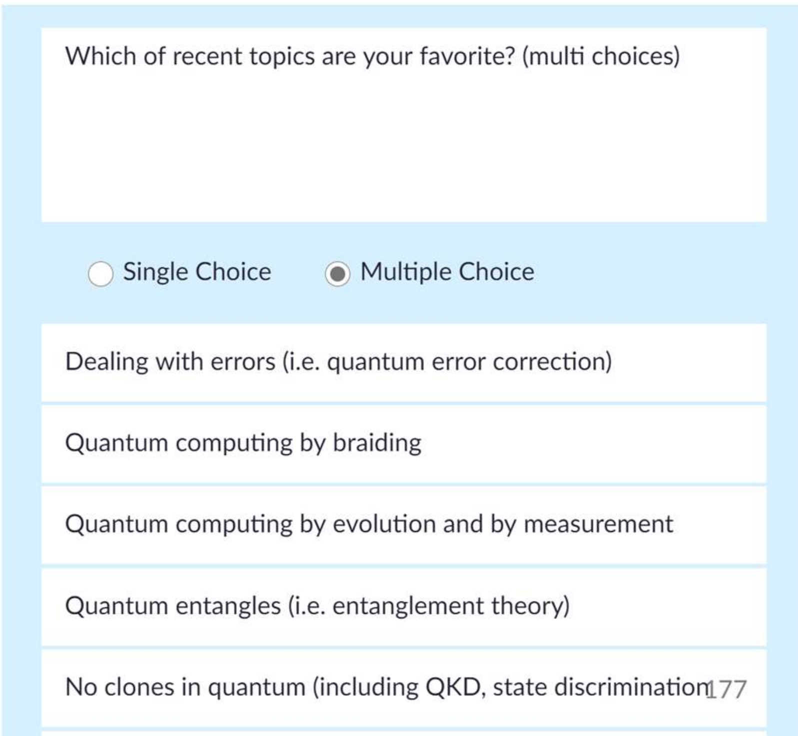
Today 11/11:

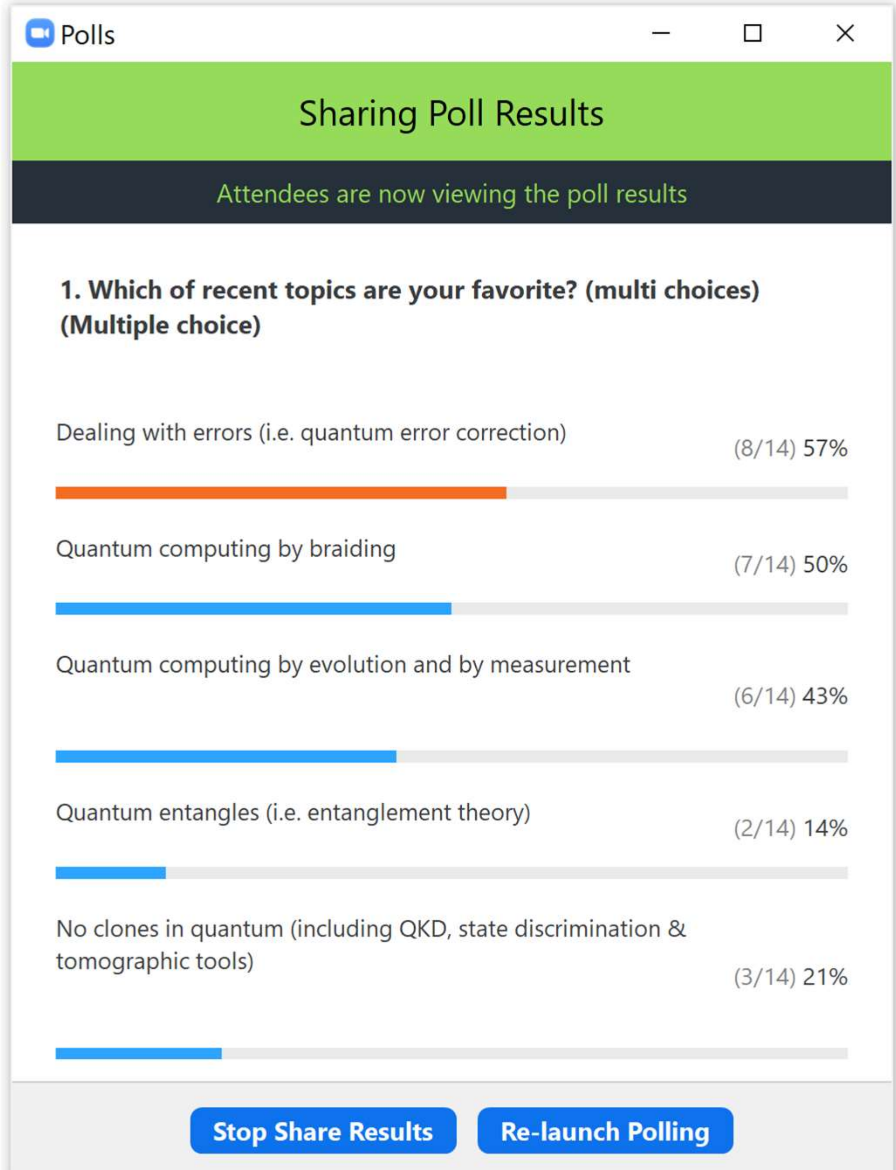
QIS syllabus

http://insti.physics.sunysb.edu/~twei/Courses/Fall2020/PHY682/

- ✓ (week 1) **The history of Q**: Overview and review of linear algebra, basics of quantum mechanics, quantum bits and mixed states.
- ✓ (week 2) **From foundation to science-fiction teleportation**: Bell inequality, teleportation of states and gates, entanglement swapping, remote state preparation, superdense coding, and superdense teleportation.
- ✓ (week 3) **Information is physical**---Physical systems for quantum information processing: Superconducting qubits, solid-state spin qubits, photons, trapped ions, and topological qubits
- ✓ (week 4) **Grinding gates in quantum computers**: Quantum gates and circuit model of quantum computation, introduction to IBM's Qiskit, Grover's quantum search algorithm, amplitude amplification.
- ✓ (week 5) **Programming through quantum clouds**: Computational complexity, Quantum programming on IBM's superconducting quantum computers, including VQE on quantum chemistry of molecules, QAOA for optimization, hybrid classical-quantum neural network.
- ✓ (week 6) **Dealing with errors**: Error models, Quantum error correction, topological stabilizer codes and topological phases (including fractons), error mitigations
- ✓ (week 7) **Quantum computing by braiding**: Kitaev's chain, Majorana fermions, anyons and topological quantum computation
- ✓ (week 8) **More topological please**: Topological quantum computation continued, surface code and magic state distillation
- ✓ (week 9) **Quantum computing by evolution and by measurement**: Other frameworks of quantum computation: adiabatic and measurement-based; D-Wave's quantum annealers
- ✓ (week 10) **Quantum entangles**: Entanglement of quantum states, entanglement of formation and distillation, entanglement entropy, Schmidt decomposition, majorization, quantum Shannon theory
- ✓ (week 11) **No clones in quantum**: No cloning of quantum states, non-orthogonal state discrimination, quantum tomographic tools, quantum cryptography: quantum key distribution from transmitting qubits and from shared entanglement
- (week 12) **Show me your 'phase', Mr. Unitary**: Quantum Fourier Transform, quantum phase estimation, Shor's factoring algorithm, and quantum linear system (such as the HHL algorithm) and programming with IBM Qiskit
- (week 13) **The quantum 'Matrix':** Quantum simulations and quantum sensing and metrology

Do poll


Which of recent topics are your favorite? (multi choices)
Single Choice
Multiple Choice
Dealing with errors (i.e. quantum error correction)
Quantum computing by braiding
Quantum computing by evolution and by measurement
Quantum entangles (i.e. entanglement theory)
No clones in quantum (including QKD, state discrimination


Polls
Sharing Poll Results
Attendees are now viewing the poll results
1. Which of recent topics are your favorite? (multi choices) (Multiple choice)
Dealing with errors (i.e. quantum error correction)
(8/14) 57%
Quantum computing by braiding
(7/14) 50%
Quantum computing by evolution and by measurement
(6/14) 43%
Quantum entangles (i.e. entanglement theory)
(2/14) 14%
No clones in quantum (including QKD, state discrimination & tomographic tools)
(3/14) 21%
Stop Share Results
Re-launch Polling

PHY682 Special Topics in Solid-State Physics: Quantum Information Science

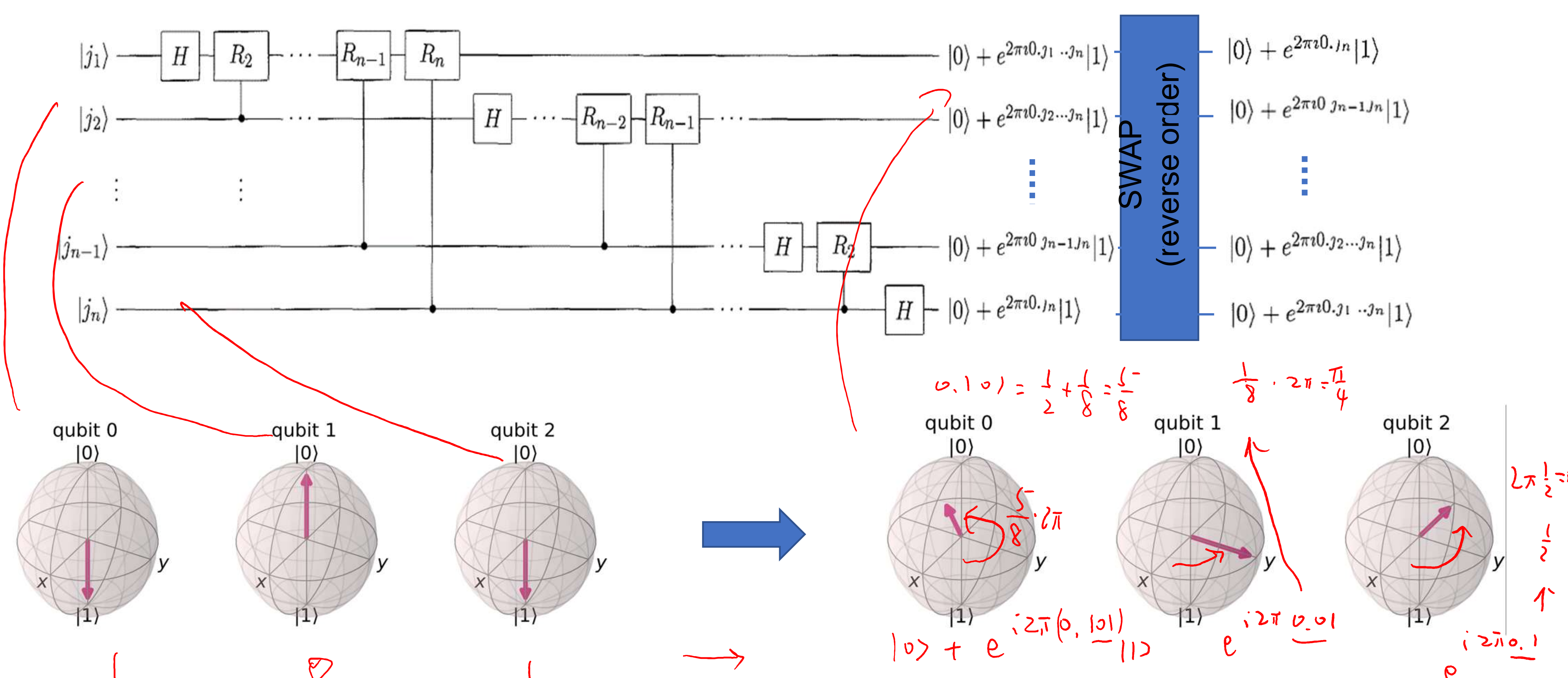
Lecture time: 2:40-4:00PM Monday & Wednesday

Today 11/11:

1. Final presentation selection and presentation outline
2. Review Quantum Fourier Transform and Quantum Phase Estimation
3. Finish Week 12's topics (quantum phase estimation and applications)

Prof. Steven M. Girvin on "**Progress and Prospects for the Second Quantum Revolution" (Physics and Astronomy Colloquium yesterday)**
http://www.physics.sunysb.edu/Physics/colloquium/2020/
Network stream: rtsp://www.physics.sunysb.edu:5554/girvin-111020

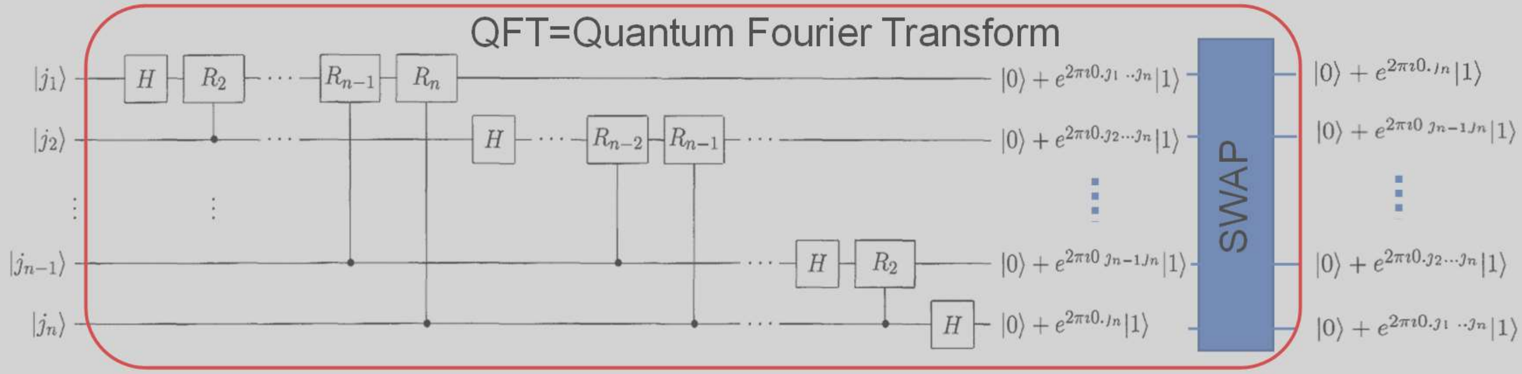
Quantum Fourier Transform and Bloch spheres

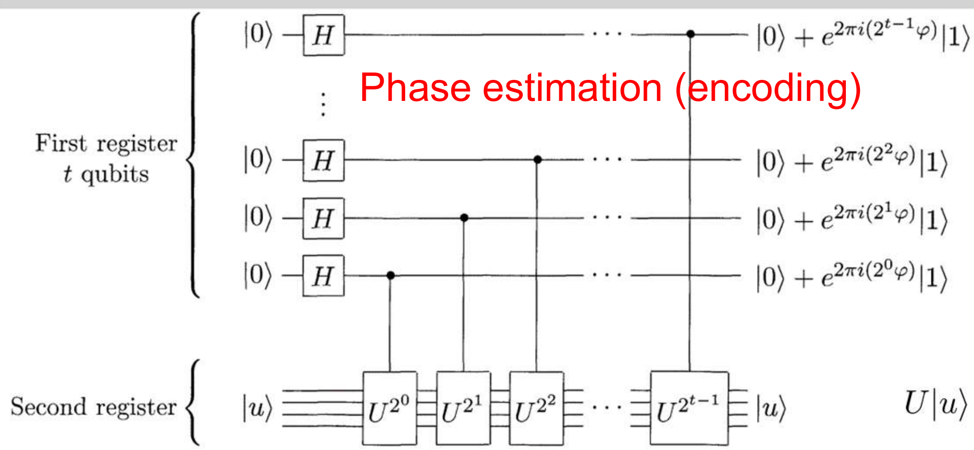


Ref: Qiskit notebook or Qiskit book

QFT and phase estimation

$$|j = j_1 j_2 \ldots j_n\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{i2\pi jk/2^n} |k = k_1 k_2 \ldots k_n\rangle \qquad R_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^n} \end{pmatrix}$$





[from Nielsen & Chuang]

Almost same structure
➔ Apply inverse QFT
to extract phase

$$U|u\rangle = e^{-iHt}|u\rangle = e^{i2\pi\phi}|u\rangle$$

$$\phi = 0.\phi_1\phi_2 \ldots \phi_t \ldots$$

Today: Application of QPE

- Approximate projection to eigenstates
- Order and period finding
- Shor's factoring algorithm
- Discrete logarithm $f(x_1, x_2) = a^{sx_1+x_2} \bmod N \qquad b = a^s \Longrightarrow s = ?$
  $f(x_1 + q, x_2 - q\, s) = f(x_1, x_2)$
- Hidden subgroup problem $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$
  f is constant on the cosets
  of a subgroup K ➔ find K
- Harrow-Hassidim-Lloyd (HHL) quantum linear system and related algorithms
- Quantum SVD

Projection to eigenstates

- Quantum Phase Estimation [Kitaev; Lloyd and ..]

$$U|u\rangle = e^{-iHt}|u\rangle = e^{i2\pi\phi}|u\rangle$$

$$\phi = 0.\phi_1\phi_2....\phi_t...$$

  - For eigenstate |u> of a unitary operator U, can extract eigenvalue via the phase φ

- But for a superposition can approximately project the system to some eigenstate |u>

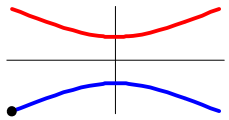
$|a_n|^2$

$$|\psi\rangle = \sum_n a_n|u_n\rangle \Longrightarrow$$ Obtain approximate φ_n with $P_n \approx |an|2$

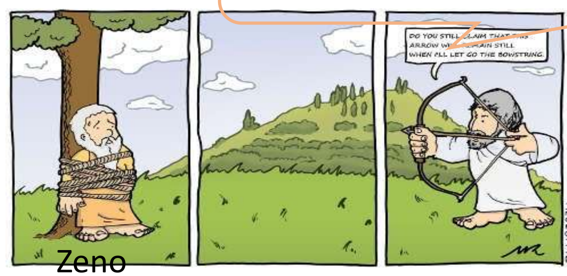
Recall: Adiabatic vs. "Zeno" approach

- ❑ **Adiabatic:**

$$H(t) = \left(1 - \frac{t}{T}\right) H_{\mathrm{initial}} + \frac{t}{T} H_{\mathrm{final}}$$



Do you still claim that this arrow will remain still ….

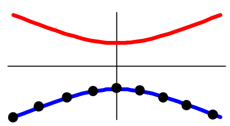


- ❑ It is also possible to use measurement, i.e. Zeno effect

- ❑ "Quantum simulations of classical annealing processes" by Somma, Boixo, Barnum and Knill [PRL101,130504 (2008)]

QPE is useful here

  - ➢ Measurement needs to **project to eigenstates of H(t)** [see e.g. Chen &Wei, PRA 101, 032339 (2020)]
  - ➢ Ground state at t=T can be arrived by such Zeno measurement on H(t) for a sequence of t=0,Δt, 2Δt, …, T



Order finding

- Given positive integers x and N ($x < N$) with no common factors, find the least integer r such that $x^r = 1 \,(\mathrm{mod}\, N)$

$x=2$. $N=5$

$\boxed{r=4}$

$2^1 = 2 \,(\mathrm{mod}\, 5)$

$2^2 = 4 \,(\mathrm{mod}\, 5)$

$2^3 = 8 = 3 \,(\mathrm{mod}\, 5)$

$2^4 = 16 = 1 \,(\mathrm{mod}\, 5)$

  - Apply phase estimation to the unitary operator:

$$U|y\rangle \equiv |xy \,(\mathrm{mod}\, N)\rangle \quad y \in \{0,1\}^L,\ y < N$$

$$U|y\rangle \equiv |y\rangle, \quad \text{for } N \le y < 2^L$$

  - We need to input an eigenstate? What are the eigenstates?

Eigenstates are (s in [0,r-1]): $|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-2\pi i s k}{r}} |x^k \mathrm{mod}\, N\rangle$

$$U|u_s\rangle = e^{\frac{2\pi i s}{r}} |u_s\rangle \quad \text{[check]}$$

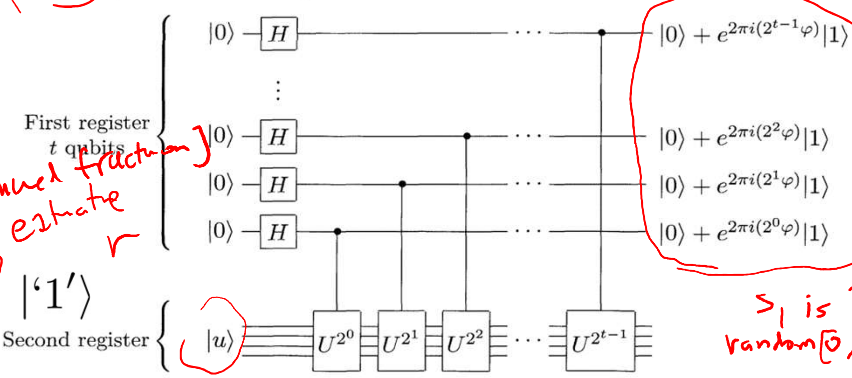
$\phi = \frac{s}{r}$

Their superposition gives |'1' = 0…01⟩:

$$\boxed{\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |\text{'}1\text{'}\rangle}$$

(continued fraction) estimate r

repeat $\left(\frac{s_1}{r}\right)$ $\left(\frac{s_2}{r}\right)$ … $\Rightarrow$ $|\text{'}1\text{'}\rangle$



QFT^{-1} $\Uparrow$ ϕ_r

$\Downarrow$ extract r $\Downarrow$

$\boxed{\left(\frac{\tilde{s}_1}{r}\right)}$

s_1 is random[0,r-1]

Order finding (cont'd)

- Given positive integers x and N ($x < N$) with no common factors, find the least integer r such that $x^r = 1 \pmod N$

$$U|u_s\rangle = e^{\frac{2\pi i s}{r}}|u_s\rangle \qquad \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |`1'\rangle$$

$\frac{\tilde{s}'}{r} \Rightarrow \frac{s_1''}{r} \quad \frac{s_2''}{r}$

$\Downarrow$

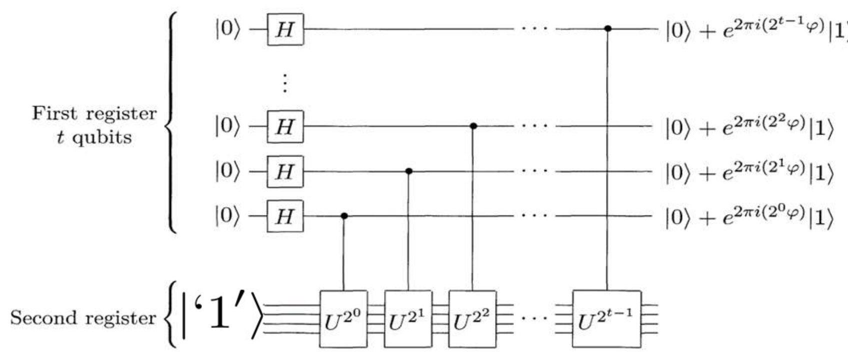
r

- Perform phase estimation with t qubits will randomly give estimated s/r

$$t = 2L + 1 + \log_2\left(2 + \frac{1}{2\epsilon}\right)$$

$$\text{accuracy: } 2^{-2L-1} < 1/(2r^2)$$

  - ✓ With above accuracy ➔ can deduce a 'r' and check whether it's a correct answer (repeat if necessary)



Order finding for Shor's factoring

order finding

- Given positive integers x and N ($x < N$) with no common factors, find the least integer r such that $x^r = 1 \pmod{N}$

- Note that: If $\gcd(x, N) = 1$, and period r of $F_{x,N}(a)$ is even,

$$F_{x,N}(a) := x^a \bmod N$$

if r is odd $\Rightarrow$ choose another x

Then (assume r is even)

$$\Longrightarrow (x^{r/2} + 1)(x^{r/2} - 1) = x^r - 1 = 0 \pmod{N}$$

$x^{r/2} + 1$

$x^{r/2} - 1$

may be nontrivial factors

N divides above expression ➔ obtain nontrivial factors of N

$\gcd(x^{r/2} \pm 1, N)$ factors of N

➔ Use quantum order finding as a subroutine of Shor's factoring algorithm

Factoring N

1. Randomly select x < N such that gcd(x,N)=1

   - X={ 2, 4, 7, 8, 11, 13,14} are coprime to 15

2. Find period r of $F_{x,N}(a) = x^a \bmod N$

   - R={ 4, 2, 4, 4, 2, 4, 2} are corresponding periods r

3. If r = even and z = $x^{r/2}$ (mod N) is not trivial
   Else start from step 1

4. Then gcd(z ±1, N) are factors of N

   $x^{r/2} \pm 1$ $11^{2/2}+1$ $11^{2/2}-1$

   - E.g. take x=11, z=11, gcd(11+1,15)=3, gcd(11-1,15)=5;
     15=3x5

     12 10

➔ Shor's quantum algorithm uses phase estimation for order/period finding on $U|y\rangle \equiv |xy(\bmod N)\rangle$

Quantum task: Shor factoring

→ exponential speedup

18070820886874048059516561644059055662781025167
69401349170127021450056662540244048387341127590
812303371781887966563182013214880557
=(????....?) x (????...?)

=(396859994595974542901611261628837
86067576449112810064832555157243)
x
(4553449864673597218840368689727440
8864356301263205069600999044599)

$\Sigma |u_s\rangle$; $|+\rangle|+\rangle|+\rangle$

superposition + unitary evolution + measurement

➔ Can break RSA (Rivest-Shamir-Aldeman) encryption exponentially faster than classical computers

RSA public key cryptography

$N =$
e.g. 15

1. Choose two different large prime numbers $\boldsymbol{p}$ and $\boldsymbol{q}$; $\boldsymbol{N} = \boldsymbol{pq}$
2. $\Phi = (\boldsymbol{p}-\mathbf{1})(\boldsymbol{q}-\mathbf{1})$ a number coprime with $\boldsymbol{N}$ and less than $\boldsymbol{N}$.

   $2 \cdot 4 = 8$ e.g. $e = 3$. $d = 3$
3. Choose $\boldsymbol{e}$ coprime with Φ and compute $\boldsymbol{d} = \boldsymbol{e}^{-1}$ (mod Φ) or $\boldsymbol{ed} = \mathbf{1}$ (mod $\boldsymbol{\Phi}$)
4. Broadcast public key $\boldsymbol{e}$ and number $\boldsymbol{N}$ (3, 15)

   e.g. $a = 2$
   $b = 2^3 = 8$
5. Other party encodes message $\boldsymbol{a}$ (assume coprime to $\boldsymbol{N}$) to be $\boldsymbol{b} = \boldsymbol{a}^{\boldsymbol{e}}$ (mod $\boldsymbol{N}$) and we can decode it by $\boldsymbol{b}$^$\boldsymbol{d} = \boldsymbol{a}$^$(\boldsymbol{ed}) = \boldsymbol{a}$^$(\boldsymbol{n}\,\Phi) = \boldsymbol{a}$ (mod $\boldsymbol{N}$), note $\boldsymbol{a}$^$\Phi = \mathbf{1}$ (mod $\boldsymbol{N}$)

   $b^d = 8^3 = 2$
6. We can identify ourselves by encoding our signature $\boldsymbol{s}$ to be $\boldsymbol{t} = \boldsymbol{s}$^$\boldsymbol{d}$ (mod $\boldsymbol{N}$), everyone can verify by decoding $\boldsymbol{t}$^$\boldsymbol{e} = \boldsymbol{s}$(mod **N**)

   e.g. $s = 4$. $t = 4^3 = 4$. $4^3 = 4$.

Performance: classical vs quantum

Assume to it takes 1 sec to a factor 30-digit number for both classical and quantum*

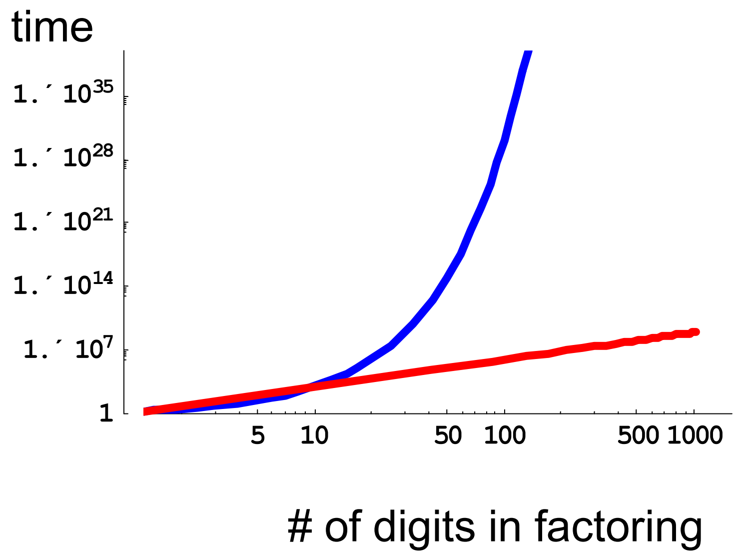
	Classical	Quantum
30-digit	1 sec	1 sec
50-digit	816 sec	4.6 sec
100-digit	9.4×10^{7} sec	37 sec
200-digit	4.6×10^{14} sec	296 sec
250-digit	1.8×10^{17} sec	578 sec

A year = 31536000 sec
= 3.2×10^{7}
Age of universe= 13.7 billion years
= 432 quadrillion sec
= 4.3×10^{17} sec

*actual number varies

Polynomial vs. Exponential

- What are tractable and intractable?
  - Tractable problems: can be solved in time polynomial of input size
  - Intractable problems: cannot be solved in time polynomial of input size



✓ Classical factoring: (almost) “exponential” time

✓ Shor’s factoring: Polynomial time

Summary of Shor's factoring algorithm

Procedure:

See e.g. [Nielsen&Chuang 5.3.2]

$(1 \cdots \sqrt{N})$ $e^{\frac{1}{2}\log_2 N}$

0. Check N is prime or not ~2000

Classical

1. If N is even, return the factor 2.

2. Determine whether $N = a^b$ for integers $a \geq 1$ and $b \geq 2$, and if so return the factor a (uses the classical algorithm of Exercise 5.17).

~~primality to be~~ easy (polynomial time)

3. Randomly choose x in the range 1 to $N-1$. If $\gcd(x, N) > 1$ then return the factor $\gcd(x, N)$.

Quantum

4. Use the order-finding subroutine to find the order r of x modulo N.

Classical

5. If r is even and $x^{r/2} \neq -1 (\text{mod } N)$ then compute $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$, and test to see if one of these is a non-trivial factor, returning that factor if so. Otherwise, the algorithm fails.

Quantum Linear System Algorithm

- Harrow-Hassidim-Lloyd (HHL) 2008
  - ✓ A : N x N matrix→ solve for vector x (encoded in quantum state)

$$A\vec{x} = \vec{b} \quad \Rightarrow \quad \vec{x} \; ?$$

$O(N^3)$

  - ✓ HHL complexity O(k^2 s^2 logN /ϵ)

    k: condition number = largest eigval/smallest,
    s: sparsity, ϵ: error

  - ✓ Classical algorithm complexity O(N^3)

- Potentially useful for some machine learning tasks

Quantum Linear System Algorithm: HHL

$$A\vec{x} = b$$

- Harrow-Hassidim-Lloyd 2008

$1 = \sum_i |b_i|^2$ normalized

$A' = \left(\begin{array}{c|c} 0 & A^\dagger \\ \hline A & 0 \end{array}\right)$ $A'^\dagger = A$

For simplicity, assume A: N x N Hermitian

$$A|u_j\rangle = \lambda_j|u_j\rangle \qquad |b\rangle = \sum_{i=1}^{N} b_i|i\rangle = \sum_{j=1}^{N} \beta_j|u_j\rangle$$

$A = \sum \lambda_j |u_j\rangle\langle u_j|$

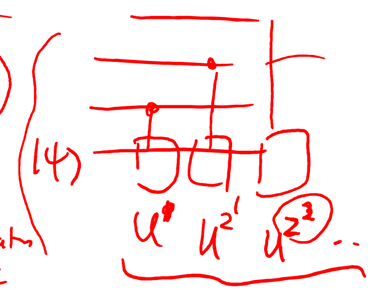
$j_1, j_2, \vdots$ $\Leftarrow QFT^{-1}$

- Prepare an initial state: $$|\Psi_0\rangle = \frac{1}{\sqrt{T}}\sum_{\tau=0}^{T}|\tau\rangle \otimes |b\rangle = |\text{all } \tau\rangle \otimes \sum_{j=1}^{N}\beta_j|u_j\rangle$$

C-A

- Define the "phase encoding" operator: $$\text{c} - \text{A} \equiv \sum_\tau |\tau\rangle\langle\tau| \otimes e^{iAt_0\tau}$$

Some normalization (unit of time)



$U = e^{iAt_0}$

Apply it to Ψ_0:

$$|\Psi_0\rangle \rightarrow |\Psi_1\rangle = \frac{1}{\sqrt{T}}\sum_{\tau=0}^{T}|\tau\rangle \otimes \sum_{j=1}^{N}\beta_j e^{i\lambda_j t_0\tau}|u_j\rangle$$

$\vec{x} = A^{-1}\vec{b}$

- Apply inverse QFT to first register for phase estimation: kicked back phase

$A^{-1}\sum_j \beta_j|u_j\rangle$

$= \sum_j \frac{1}{\lambda_j}|u_j\rangle\langle u_j|$ $\quad \frac{1}{\lambda_j}|u_j\rangle\langle u_j|$

$$|\Psi_1\rangle \rightarrow |\Psi_2\rangle = \sum_j \beta_j|\tilde{\lambda}_j\rangle \otimes |u_j\rangle$$

λ_j

$\Rightarrow$ "if we perform measurement" $\Downarrow$ collapse $\vec{b}$ to $|u_j\rangle$ $\tilde{\lambda}_j$

- How to apply inverse of A? divide above each term by λ_j ?

HHL Algorithm (cont'd)

$$A\vec{x} = b$$

- After phase estimation: $|\Psi_2\rangle = \frac{1}{\sqrt{T}} \sum_j \beta_j |\tilde{\lambda_j}\rangle \otimes |u_j\rangle$

  - Apply inverse of A? divide above each term by λ_j ?

$$\sum_j \beta_j/\lambda_j |\tilde{\lambda_j}\rangle \otimes |u_j\rangle \xrightarrow{\text{undo QPE}} |\text{all } \tau\rangle \otimes \sum_j \beta_j/\lambda_j |u_j\rangle?$$

- Application of inverse cannot be done with unit probability

$|C| \le |\lambda_j|$

  - Attach an ancillary qubit in $|0\rangle$, then apply a U gate controlled by first register:

[Note that $\left|\frac{C}{\lambda_j}\right| \le 1$

$$\sum_j \beta_j |\tilde{\lambda_j}\rangle \otimes |u_j\rangle \otimes |0\rangle \rightarrow \sum_j \beta_j |\tilde{\lambda_j}\rangle \otimes |u_j\rangle \otimes \left(\sqrt{1 - \frac{C^2}{\lambda_j^2}}|0\rangle + \frac{C}{\lambda_j}|1\rangle\right)$$

↑ what we want

back to starting pt
↑

$$\xrightarrow{\text{undo QPE}} \quad |\text{all } \tau\rangle \otimes \sum_j \beta_j |u_j\rangle \otimes \left(\sqrt{1 - \frac{C^2}{\lambda_j^2}}|0\rangle + \frac{C}{\lambda_j}|1\rangle\right)$$

if we get "0" $|\text{all } \tau\rangle \otimes \sum \beta_j |u_j\rangle \otimes |0\rangle$

- Inversion successful only when ancilla measurement gives 1

$$|\text{all } \tau\rangle \otimes \sum_j \beta_j \frac{C}{\lambda_j} |u_j\rangle \otimes |1\rangle = |\text{all } \tau\rangle \otimes A^{-1}|b\rangle \otimes |1\rangle$$

Qiskit implementation

1. Quantum Fourier Transform

2. Quantum Phase Estimation

3. HHL algorithm