Lec 16, 27 Oct 2020

$2^n/r$ not necessarily an integer
- only when $r = 2^k$

$f(x) = b^x \bmod N$ $N = pq$
period r divides $|G_{pq}| = (p-1)(q-1)$

If $p = 2^a + 1$ $q = 2^b + 1$
Then $(p-1)(q-1) = 2^{a+b}$
$\Rightarrow r = 2^k$

when is $2^\ell + 1$ = prime?
"Fermat prime" $\ell = 2^m$ $m = 0, 1, 2, 3, 4$
5 known, perhaps no more, $p, 2 = 3, 5, 17, 257, 65537$
up to $2^{2048} + 1$ factored

(not relevant) Mersenne prime $2^p - 1$, p prime]
47 of these

Easy case, factor 15

"Cheats": if pick b s.t. $b^2 \bmod N = 1$

$r = 2$

$u^4 = u^6 = \ldots = 1$

"precompiled" knowing r in advance

$G_{15} = (1, 2, 4, 7, 8, 11, 13, 14)$

$f(x) = 7^x \bmod 15 \quad r = 4 \quad n_0 = 4$

$$U_f H^{\otimes n} |0\rangle_n |0\rangle_{n_0} = \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} |x\rangle_n |f(x)\rangle_{n_0}$$

For $(2^1+1)(2^2+1)$, can use $n = n_0 = 4$

Then for $f(x) = 7^x \bmod 15$ wave function is

$$\frac{1}{4}\left(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + \ldots + |15\rangle|13\rangle\right)$$

measure output as $|13\rangle = |f(x_0)\rangle$

Then wave function collapses to

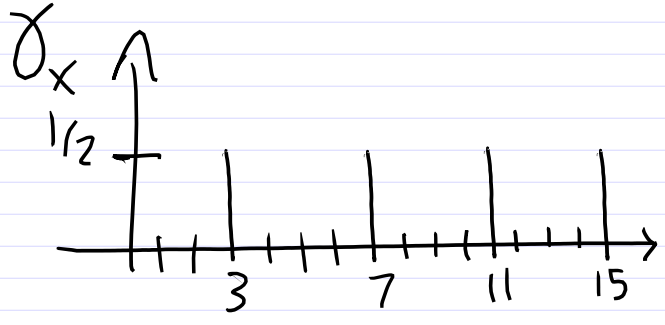
$$\rightarrow \frac{1}{2}\left(|3\rangle + |7\rangle + |11\rangle + |15\rangle\right)|13\rangle$$

(of the form $\frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle$ with $r = 4$, $x_0 = 3$, $m = 4$)

$$|\Psi\rangle = \sum_x \left(\gamma_x |x\rangle\right)|13\rangle$$

where

$$\gamma_x = \frac{1}{2}\,\delta_{x,\,4k+3}$$



Want period of γ_x

$$\tilde{\gamma}_y = \frac{1}{2^{n/2}} \sum_{0 \le x < 2^n} e^{2\pi i xy/2^n} \gamma_x = \frac{1}{4} \sum_{0 \le x < 16} e^{2\pi i xy/2^4} \gamma_x$$

$x = 3 \bmod 4$

$\gamma_x = \frac{1}{2} \delta_{x, 4k+3}$

$$= \frac{1}{8} e^{2\pi i 3y/16} \sum_{k=0}^{3} e^{2\pi i 4ky/16}$$

non-zero only when $4y/16 = j$

$y/4 = j$ or $y = 0, 4, 8, 12$

Suppose measure $y = 12$

$12 = j \frac{16}{r}$ r is an (integer) multiple of $4/3$ so

first possibility is $r = 4$

To factor 15, use (see next page)

$(7^4 - 1) = (7^2 - 1)(7^2 + 1) = 0 \bmod 15$

Then run Euclidean alg. $(48, 15) \to 3$

on the two factors: $(50, 15) \to 5$

how to factor N knowing $b^r \bmod N = 1$

Two conditions: need r even

and $b^{r/2} \bmod N \neq -1$

$\not\Rightarrow (b^{r/2} - 1)(b^{r/2} + 1) = 0 \bmod N$

p must be a factor of one, and q of the other

run Euclidean algorithm on $(b^{r/2} \pm 1, N)$

Simple example, factor $5 \cdot 7 = 35$

Use $4^6 = 1 \bmod 35$

$(4^3 - 1)(4^3 + 1) = 0 \bmod 35$

$(63, 35) \to (35, 28) \to (28, 7) \to (7, 0)$

$(65, 35) \to (35, 30) \to (30, 5) \to (5, 0)$

Continued fraction,

write any number as $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}$

$= [a_0; a_1, a_2, a_3 \dots]$

$\pi = 3.14159265358\dots$

$\frac{1}{.14159\dots} = 7.06251330542\dots$

$\frac{1}{.0625\dots} = 15.9965945\dots$

$\frac{1}{.9965\dots} = 1.003417099\dots$

$\frac{1}{.003\dots} = 292.64\dots$

$\pi = (3; 7, 15, 1, 292, \dots)$

$3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \dots}}}$

partial sums =

$3, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \dots$

$\frac{355}{113} = 3.14159292\dots$

known in 5th C. A.D. to Chinese (Tsu)

Some continued fractions

Golden mean:

$$\varphi = \frac{1+\sqrt{2}}{2} = 1.618\ldots = [1; \overline{1}]$$

$$\sqrt{2} = [1; \overline{2}]$$

$$\sqrt{3} = [1; \overline{1,2}]$$

$$e = [2; 1,2,1,1,4,1,1,6,1,1,8,\ldots]$$

...

φ satisfies $\varphi - 1 = \frac{1}{\varphi}$

$\sqrt{2}$ satisfies $x - 1 = \frac{1}{1+x}$

...

Thm: If x estimates j/r and $|x - j/r| < \frac{1}{2r^2}$ then j/r appears as one of the partial sums of x

Example: $r < 2^7$, measure $y = 11490$ within $1/2$ of $\frac{2^{14}}{r} j$ $(n = 14)$

$$\left| \frac{11490}{2^{14}} - \frac{j}{r} \right| < \frac{1}{2 \cdot 2^{14}}$$

$$\frac{11490}{2^{14}} = .7012939453\ldots = \cfrac{1}{1 + \cfrac{1}{2 + \cdots}}$$

$$= [0; 1, 2, 2, 1, 7, 35, \ldots]$$

$$= 54/77 = j/r$$

$$\Rightarrow r = 77$$

(Confirm: $2^{14} \frac{54}{77} = 11490.079\ldots$ within $1/2$ of $y = 11490$)

small phases?

$$V_k = e^{i\pi/2^k}$$

If factoring number with hundreds of digits, then $2^k \gtrsim 10^{100}$

Not experimentally feasible.

Resolution: accurate phases affect probability, but not precision of y once measured.

$$P_\varphi(y) = \frac{1}{2^n m}\left| \sum_{k=0}^{m-1} e^{2\pi i k r y/2^n}\, e^{i\varphi_k(y)} \right|^2$$

to leading order in small φ:

$$|p(y) - p_\varphi(y)| \lesssim 2\varphi \quad (\text{all } |\varphi_k| < |\varphi|)$$

$$\lesssim .4\,\frac{1}{100} \quad (< 1\%\ \text{effect})$$

$$\Rightarrow \varphi \lesssim \frac{1}{500}$$

want max $\varphi = n\pi/2^k < \frac{1}{500}$

so can ignore phases $e^{\pi i/2^k}$

with $2^k > 500n\pi$

For $n \approx 3000$ ($N \approx 10^{500}$, 500 digit number)

$\Rightarrow$ Can ignore all $k \gtrsim 22$

QFT grows only linearly in n!

(to desired probability)

Quantum Physics

[Submitted on 23 May 2019 (v1), last revised 5 Dec 2019 (this version, v2)]

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney, Martin Ekerå

We significantly reduce the cost of factoring integers and computing discrete logarithms in finite fields on a quantum computer by combining techniques from Shor 1994, Griffiths–Niu 1996, Zalka 2006, Fowler 2012, Ekerå–Håstad 2017, Ekerå 2017, Ekerå 2018, Gidney–Fowler 2019, Gidney 2019. We estimate the approximate cost of our construction using plausible physical assumptions for large-scale superconducting qubit platforms: a planar grid of qubits with nearest-neighbor connectivity, a characteristic physical gate error rate of 10^{-3}, a surface code cycle time of 1 microsecond, and a reaction time of 10 microseconds. We account for factors that are normally ignored such as noise, the need to make repeated attempts, and the spacetime layout of the computation. When factoring 2048 bit RSA integers, our construction's spacetime volume is a hundredfold less than comparable estimates from earlier works (Fowler et al. 2012, Gheorghiu et al. 2019). In the abstract circuit model (which ignores overheads from distillation, routing, and error correction) our construction uses $3n + 0.002n \lg n$ logical qubits, $0.3n^3 + 0.0005n^3 \lg n$ Toffolis, and $500n^2 + n^2 \lg n$ measurement depth to factor n-bit RSA integers. We quantify the cryptographic implications of our work, both for RSA and for schemes based on the DLP in finite fields.

Dec 2009: 768 bits, 2000 core years

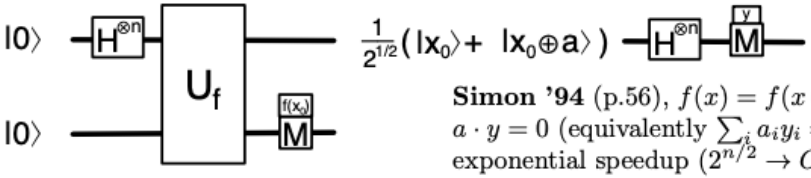
better algorithms:

Dec 2019: 795 bits took 900 core years

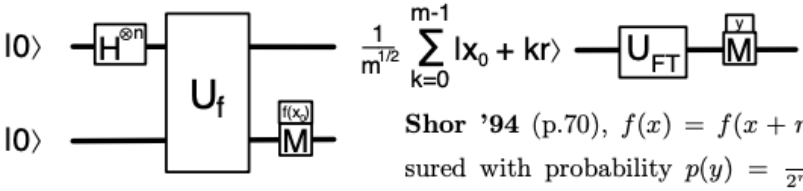
[Intel Xeon Gold 2.1 GHz CPUs]

Feb 2020: 829 bits took 2700 core years

⟹ 2048 bits would take $>10^{10}$ x more

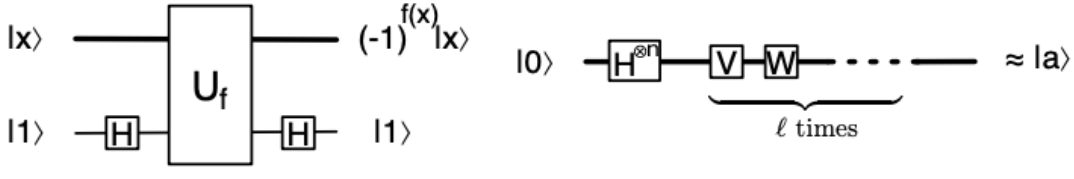


Simon '94 (p.56), $f(x) = f(x \oplus a)$, measured y has $a \cdot y = 0$ (equivalently $\sum_i a_i y_i = 0 \bmod 2$), exponential speedup ($2^{n/2} \to O(n)$) to determine a



Shor '94 (p.70), $f(x) = f(x + r)$, resulting y is measured with probability $p(y) = \frac{1}{2^n m}\left|\sum_{k=0}^{m-1} e^{2\pi i k r y/2^n}\right|^2$, gives $|y - 2^n/r| < 1/2$ with $p > .4$, sufficient to determine period r via partial fraction expansion, exponential speedup ($n2^n, \exp(n^{1/3}) \to O(n^3)$).
(Note: replaces $\mathbf{H}^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{0 \le y < 2^n} e^{i\pi x \cdot y}|y\rangle$ with $\mathbf{U}_{\rm FT}|x\rangle = \frac{1}{2^{n/2}} \sum_{0 \le y < 2^n} e^{2\pi i x y/2^n}|y\rangle$.)

Practical application is $f(x) \equiv b^x \bmod N$, where $b \equiv a^c \bmod N$ is an encrypted message, from which d', satisfying $cd' \equiv 1 \bmod r$, can be calculated, and d' recovers unencrypted message $a \equiv b^{d'} \bmod N$ (in contrast to using d, with $cd = 1 \bmod (p-1)(q-1)$, where $N = pq$ and r divides $(p-1)(q-1) = |G_{pq}|$).



Grover '96 (p.90), $f(x) = 1$ only for (m) marked value(s) $x = a$, uses "phase kickback" to express $\mathbf{U}_f$ in terms of $\mathbf{V} = \mathbf{1} - 2|a\rangle\langle a|$, and $\mathbf{W} = 2|\phi\rangle\langle\phi| - \mathbf{1} = \mathbf{H}^{\otimes n}\big(2|0\rangle\langle 0| - \mathbf{1}\big)\mathbf{H}^{\otimes n}$ is easily constructed. Applying $\ell \approx \frac{\pi}{4}\frac{2^{n/2}}{\sqrt{m}}$ times gives probability $p(a) \approx 1 - O(m/2^n)$, for square-root speedup ($2^n/m \to \sqrt{2^n/m}$).