

CSE 439/510

Lecture Tue Oct 29

Fall 2024

Shor's Algorithm, Stating Its Backtrack Points BP1 & BP2

Input: $M = pq$, where p, q are n -bit primes. So $\log_2 M \approx 2n$.Guess $a < M$. If $\gcd(a, M) > 1$ (a tiny chance) we get a factor right away.
So suppose $\gcd$ is 1, i.e. a is relatively prime to M ($a \in G_M$).Goal: Compute the true period: least r such that $a^r \equiv 1 \pmod{M}$.
Note: multiples of r are also periods, and we may get them instead.BP1: a may be unlucky in that even after getting (an) r , it is not true or otherwise the classically randomized part fails. Optimal analysis makes it so this is at most a 50-50 chance of backtracking all the way here where you have to guess a different a .Shor's Alg^m, Stating Backtrack Points BP₁ and BP₂Input: $M = pq$ M is an n -bit number, so $\log_2 M \approx n$.
 $2^n \approx M$.Guess $a < M$. If $\gcd(a, M) > 1$, a tiny chance, we get a factor "forthwith".We may suppose a is rel. prime to M , i.e. $a \in G_M$. $r \leq |G_M| - 1$ Goal: compute the true period $\equiv$ least r s.t. $a^r \equiv 1 \pmod{M}$
(We may instead get a multiple of r , and will hash that out later.)BP₁: a may be unlucky in that even after getting (an) r the classical part may fail.Optimal analysis puts this chance at most 50%.Given r , define r_0 to be the odd number obtained by dividing out all 2's from r .
Ksn $\left[\text{If } r = 2^k r_0 \text{ and } a \text{ has period } r, \text{ then } a' = a^{2^k} \text{ has period } r_0 \right]$

Steps of the Quantum Part: (after guessing a but maybe considering all of $a, a^2, a^3, a^4, \dots$ along with it)

(Q1) Fatten up the domain of $f_a(x) = a^x \bmod M$ to include all x up to $Q = 2^l$ where $l = \lceil \log_2(M^2) \rceil$ so Q is the least power of 2 above M^2 . (We actually only need to guarantee $Q > rM$, noting that $r < \log M < M$.) Then $l \approx 4n$ since $\log(M^2) = 2\log M \approx 2 \cdot 2n$.
The range stays mod M . Thus if $f_a(x) = y$, x has l bits and y has n bits. (Text says y has l bits at plot bottom - a minor typo.)

(Q2) Prepare the state $\alpha = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |f_a(x)\rangle$.

(Q3) Apply QFT (or its inverse) to the $|x\rangle$ part to get b .

(Q4) Measure all qubits to get a sample $\frac{xy}{\text{len bits}}$. Similarly to Simon's algorithm:
 • y is in the range of f_a but need not equal $f_a(x)$.
 • We will include the # of y 's when adding up amplitudes and probabilities, but otherwise we ignore y . We work further only with x .

The second backtrack point comes after the measurement. A quantum technote: Because the measurement "collapses" the quantum state b , in the actual quantum algorithm, backtracking here requires rebuilding the whole functional superposition---i.e., redoing the whole circuit. But in my brute-force quantum simulator, it can do another sample without having to re-create all the Boolean formulas that simulate the superposed applications of $f_a(x) = a^x \bmod M$.

BP2: We need there to exist an integer t such that $|x - \frac{tQ}{r}| \leq \frac{1}{2}$, where we don't know r either, of course, but r is fixed. We also need t to be relatively prime to r , so that tQ/r does not simplify. Then x is good. Chance that x is good: we will show $\Omega(\frac{1}{\log n})$. So we do under linear many backtracks to here.

- (C1) Try to calculate r from x . This always succeeds when x is good.
- (C2) With true r in hand, calculate p and q (at least $\frac{1}{2}$ success each shot).
 If fail n times — go to BP2, which means resampling,
 ie. rerunning quantum part.
 If fail n resamples — go all way back to BP1. (If that fails, n times
 you are thousands unlikely)

Quantum Steps

This justifies $\hat{r}$ Supposing that the true period r is odd, ie. $r = r_0$, when we guessed a . 'mystery'

(Q1) Choose $Q = 2^L$ where $L = \lceil \log_2(M^2) \rceil$, so Q is the least power of 2 above M^2 . (We really need $Q > rM$.)

(Q2) Prepare the state $\frac{1}{\sqrt{Q}} \sum_{x \in \mathbb{Z}_Q} |x\rangle |f_a(x)\rangle$.

(Q3) Apply QFT (or its inverse) to the " $|x\rangle$ " part to get b .

(Q4) Measure all qubits to get a sample $\frac{xy}{L+n \text{ bits}}$.

Similarly to Simon's algorithm:

- y is in the image of f but need not $= f_a(x)$
- We will count y 's when adding up probabilities but otherwise not use y .

BP2: We need there to exist an integer t such that $|x - \frac{ta}{r}| \leq \frac{1}{2}$ (where we don't know r either, of course) but at least r is fixed by choice of a . Then x is good. We will show this happens with prob. $\Omega(\frac{1}{\log n}) = \Omega(\frac{1}{\log \log M})$.

(C1) Try to calculate r from x . Always succeeds when x is good. [But r might not be true even so.]

(C2) With r in hand, try to calculate p and q . Succeeds whp when x is good and r is true (or even if r is a multiple.)

If fail n times goto BP2, which means resampling the quantum circuit.

If that fails n times, go all the way back to BP1, which means re-guessing a , so reapplying F_a .

Analysis of the Quantum Part: (In a different order from the text!)

- (a) If the measurement gives a good x , then we get the true period r .
- (b) The probability of an individual good x and $y \in \text{Ran}(f)$ is $\Omega(1/r^2)$.
- (c) There are $\Omega(1/\log^2 r)$ good x 's, times $|\text{Ran}(f)| = r$ many y 's. Thus any one run and measurement has an $\Omega(1/\log^2 r)$ chance of getting a good x .

Let's not mention (d) that at least half the guessed $a < M$ enable factoring $M = pq$ when you obtain the true period r of $f_a(x) = a^x \bmod M$. The at worst roughly $1/2$ chance of failure and forced restart (or "BP1") still leaves $\Omega(1/\log^2 r) = \Omega(1/\log^2 n)$ chance of success in any one go, and $\text{poly}(n)$ trials give almost certain final success.

Proof of (c): Recall good means for some t relatively prime to the true period r , $|tQ/r - x| \leq \frac{1}{2}$. Now any such t gives a good x because: Let us "re-center" the definition of " $y = c \bmod d$ " to give $-\lfloor \frac{d}{2} \rfloor \leq c < \lfloor \frac{d}{2} \rfloor$ rather than $0 \leq c < d$. Thus $\bmod' 7$ gives range -3 to $+3$ rather than 0 to 6 , and $\bmod' 8$ means -4 to 3 . Then we simply let $K = tQ \bmod' r$. This means there is a multiple Xr of r such that $tQ = K + Xr$ with $-\lfloor \frac{r}{2} \rfloor \leq K < \lfloor \frac{r}{2} \rfloor$. This implies $tQ - Xr = K$ where $-\frac{r}{2} \leq K \leq \frac{r}{2}$, so $|tQ - Xr| \leq \frac{r}{2}$, so $|\frac{tQ}{r} - x| \leq \frac{1}{2}$. Thus x is good. Moreover, if $t_1 \neq t_2$ and we thus get $t_1 Q = K_1 + X_1 r$ and $t_2 Q = K_2 + X_2 r$, then $x_1 \neq x_2$ because the difference on the left is at least Q whereas the difference between K_1 and K_2 can be at most r which is $< Q$. So:

- The number of good x 's equals the number of t 's that are relatively prime to r .
- That number is $\Omega(1/\log^2 r)$ by a theorem of Leonhard Euler in the 1700s.

Note that r can be general and have lots of factors, unlike the case $M = pq$ where $|G_M| = (p-1)(q-1)$, which is $\sim M$. We don't have $|G_r| \sim r$, but it's off by only a $\log \log$ factor, and that is "no biggie". So (c) is proved.

Proof of (a): "Good" also means $|\frac{t}{r} - \frac{x}{Q}| \leq \frac{1}{2Q}$ with the fraction $\frac{t}{r}$ in lowest terms. Suppose there were a different fraction $\frac{t'}{r'}$ that also makes $|\frac{t'}{r'} - \frac{x}{Q}| \leq \frac{1}{2Q}$. Then by the triangle inequality, $|\frac{t}{r} - \frac{t'}{r'}| \leq \frac{1}{Q}$. Then $|r't - t'r| \leq \frac{rr'}{Q}$. But by $r, r' < M$ and $M^2 \leq Q$, the RHS is < 1 . Since the LHS is an integer, it must be 0, which makes $r't = t'r$, so $\frac{t'}{r'} = \frac{t}{r}$.

What that means is: there is only one lowest terms fraction $\frac{t}{r}$ that is within $\pm \frac{1}{2Q}$ of the value $\frac{x}{Q}$, which you get from the measurement. There are several efficient ways to find this fraction:

- By integer programming
- By continued fraction expansion
- By other methods of Approximation Theory/Diophantine Analysis.

Whichever you use, your code $R(x, Q) = (r, t)$ will also often give outputs (r', t') when x is not good. You won't find out until you try using r' in the classical part (Ch-12) and keep failing, and even then, continued failure at " ΘP_2 " from repeated trials of fa might make you remind to B_1 with another. The only way you get certainly is when you get p, q such that $pq = M$. But what we can say is that with $\Omega(\frac{1}{\log n})$ chance on any trial, you do get success. [And sometimes an untrue r' does work anyway in part (d).]

Footnote:

My simulator adapts the continued fraction routine from libquantum. It shares the same weirdness of often stating it got r (or r') bigger than M - this uses other tricks that improve the one-shot success probability. We'll keep things simple by only considering the true $r, r < M$, and we'll skip details of R.

Now to set up the main quantum analysis:

Proof of (b): This is the true "quantum analysis". Given a quantum state a of $l+n$ qubits, its Fourier transform on the first l qubits gives the quantum state b whose definition is RNHO nicest with the text, indexing notation:

$$b(xy) = \frac{1}{\sqrt{Q}} \sum_{u \in \{0,1\}^l} \omega^{ux} a(uy)$$

Here x and u do double-duty as l -bit strings and as integers in the range $[0 \dots Q-1]$ where $Q = 2^l$. So xu means numerical multiplication, not concatenation of strings — but xy and uy are concatenations with the n -bit string y . And $\omega = e^{2\pi i/Q} = e^{2\pi i/2^l} = e^{2\pi i/2^{l-1}}$ has the property that $\omega^Q = 1$ but no smaller power is 1 — so it is a principal complex Q th root of unity.

[The Tuesday 10/28 lecture ended here.]

"The" Quantum Analysis: We apply QFT to the functional superposition

$$a(uy) = \frac{1}{\sqrt{Q}} \text{ if } y = f_a(u), \text{ 0 otherwise. So}$$

$$b(xy) = \frac{1}{Q} \sum_{u: y=f_a(u)} \omega^{xu} = \frac{1}{Q} \sum_{u \in f_a^{-1}(y)} \omega^{xu}$$

(not $\sqrt{Q}$ — we had $\frac{1}{\sqrt{Q}}$)

We can instantly infer that if $y \notin \text{Ran}(f_a)$ then the amplitude $b(xy) = 0$ for all x . For any one $y \in \text{Ran}(f_a)$, let u_0 be the least element in $[0 \dots Q-1]$ such that $f_a(u_0) = y$. Then

$$f_a(u_0) = f_a(u_0+r) = f_a(u_0+2r) = f_a(u_0+3r) = \dots$$

by the periodicity of f_a , stopping only when $u_0 + Tr$ exceeds $Q-1$.

This makes $T = 1 + \left\lfloor \frac{Q-u_0}{r} \right\rfloor$. By the injectivity condition again, these are the only arguments that go to y , so $f^{-1}(y) = \{u_0, u_0+r, \dots, u_0+(T-1)r\}$. This enables us to group the sum as:

$$\sum_{u \in f^{-1}(y)} w^{xu} = \sum_{k=0}^{T-1} w^{x(u_0+kr)} = w^{xu_0} \sum_{k=0}^{T-1} w^{xkr}$$

It may look weird to see u_0 outside the sum, but it depends only on y .

So: $b(x, y) = \frac{1}{Q} w^{xu_0} \sum_{k=0}^{T-1} (w^{xr})^k$ This is a classic finite geometric series: $\sum_{k=0}^{T-1} z^k = \frac{z^T - 1}{z - 1}$.

So: $b(x, y) = \frac{1}{Q} w^{xu_0} \left(\frac{w^{Txr} - 1}{w^{xr} - 1} \right)$. That we only need the probability helps simplify this further - and we haven't used the property of x being good yet.

$$|b(x, y)|^2 = b(x, y) \overline{b(x, y)}$$

$$= \frac{1}{Q^2} \underbrace{w^{xu_0} \overline{w^{xu_0}}}_{\text{unit, so } = 1} \frac{(w^{Txr} - 1)(\overline{w^{Txr} - 1})}{(w^{xr} - 1)(\overline{w^{xr} - 1})} = \frac{1}{Q^2} \frac{(1 - w^{Txr} + 1 - \overline{w^{Txr}})}{(1 - w^{xr} + 1 - \overline{w^{xr}})} = \frac{2 - 2\operatorname{Re}(w^{Txr})}{Q^2(2 - 2\operatorname{Re}(w^{xr}))}$$

$$= \frac{1}{Q^2} \frac{1 - \operatorname{Re}(e^{2\pi i T x r / Q})}{1 - \operatorname{Re}(e^{2\pi i x r / Q})} = \frac{1}{Q^2} \frac{(1 - \cos(\frac{2\pi T x r}{Q}))}{(1 - \cos(\frac{2\pi x r}{Q}))}$$

Now by trig identities, $1 - \cos(2\alpha) = 2\sin^2(\alpha)$ and cancelling the outer 2s, we get

$$= \frac{1}{Q^2} \frac{\sin^2(\frac{\pi T x r}{Q})}{\sin^2(\frac{\pi x r}{Q})}$$

$$= \frac{1}{Q^2} \frac{\sin^2(\frac{\pi T x r}{Q} - T\pi)}{\sin^2(\frac{\pi x r}{Q} - t\pi)}$$

$$= \frac{1}{Q^2} \frac{\sin^2(T\pi(\frac{xr-tQ}{Q}))}{\sin^2(\pi(\frac{xr-tQ}{Q}))}$$

$$= \frac{1}{Q^2} \frac{\sin^2(T\alpha)}{\sin^2(\alpha)} \text{ where } \alpha = \pi \left| \frac{xr-tQ}{Q} \right| \leq \frac{\pi r}{2Q}.$$

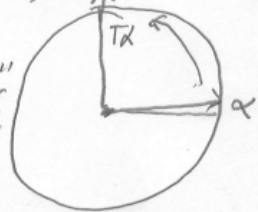
Now for the black magic of periodicity and the definition of x being good. We can add or subtract any integer multiple of π from the argument of $\sin^2(\dots)$ and the value does not change. So:

By goodness, the numerator $xr-tQ$ has absolute value at most $r/2$. Also, $\sin^2(-\theta) \leq \sin^2(\theta)$ for any θ . Thus we have

The point of having $Q > Mr$ is that this is a small angle. Moreover,

$$T\alpha = \left(1 + \left|\frac{Q-u_0}{r}\right|\right)\alpha \leq \left(\alpha + \frac{Q}{r}\alpha\right) \leq \alpha + \frac{\pi}{2}.$$

Thus $T\alpha$ almost completely avoids the zone from $\frac{\pi}{2}$ to π where $\sin(\dots)$ starts decreasing. "danger zone"



Well, to get the best effect we want $\alpha + \frac{\pi}{2}$ not to exceed π by too much, so we take $M \geq 154$ to make $Q \geq 23,000$ or so. The final trigonometric fact we leverage has the intuition that $\sin \theta \approx \theta$ in radians, indeed $\sin \theta \geq \theta / \frac{\pi}{2}$ for all θ . So $\frac{\sin T\alpha}{\sin \alpha} \gtrsim \frac{2T}{\pi}$ which is roughly proportional to T . A more exact estimate gives:

Lemma (11.2) For all $T > 0$ and angles $\alpha > 0$ such that $T\alpha \leq 1.581$, $\frac{\sin(T\alpha)}{\sin \alpha} \geq cT$ where $c = 0.63247$ (chosen so that $c^2 \geq 0.4$). a little more than $\pi/2$

So we finally get:

$$|b(x+1)|^2 \geq \frac{1}{Q^2} (cT)^2 \geq \frac{1}{Q^2} c^2 \frac{Q^2}{r^2} = \frac{c^2}{r^2} = \Omega\left(\frac{1}{r^2}\right)$$

So we shall get that for good x , $|b(x+1)|^2 \geq \frac{1}{Q^2} (cT)^2 \geq \frac{1}{Q^2} c^2 \frac{Q^2}{r^2} = \frac{c^2}{r^2} = \Omega\left(\frac{1}{r^2}\right)$. This proves (11.2)

And that completes the proof that the one-shot success probability of getting the *actual true period* r is $\Omega\left(\frac{1}{\log \log r}\right)$. (Individual runs of the algorithm may give you multiples of r , and those may work fine.

Even non-good x results in the measurement will sometimes work. But we get a bedrock minimum probability from the cases where x is good and the r we get is minimum.]

Classical Part of Shor's Algorithm (skim coverage of chapter 12)

The top-down goal is to find a number X such that $X^2 \equiv 1$ modulo M but $X \not\equiv 1$ or $X \not\equiv -1$ modulo M . Then $X^2 - 1 = (X - 1)(X + 1)$ is a multiple of M but neither factor is zero. When $M = pq$ with p, q prime, this means p and q each divide one or both factors. We need to split them across the factors, so that $\gcd(X - 1, M)$ and/or $\gcd(X + 1, M)$ will find p and q as opposed to just giving M back again. Thus we want to guess a such that:

1. The period r of a is even, so that $r/2$ is defined;
2. $X = a^{r/2} \not\equiv M - 1$ modulo M .
3. Either $X - 1$ or $X + 1$ is a multiple of one of p, q **but not both**.

If our value of a fails any of these ("unlucky"), we just try again from the start of guessing another $a < M$.

Our treatment ([blog post](#) and chapter 12) also desires r to be a multiple of $p - 1$ or $q - 1$. It can be shown that many a give this "helpful" property, which requires $r \geq \sqrt{(p-1)(q-1)} \approx \sqrt{M}$.

(This comes out of the wash of the above requirements, together with the "important fact" noted earlier about periods of a and $a2^k$, so that most a have large enough periods. It uses arguments modulo p and modulo q separately that might not be clear in the chapter. It could be an exercise: Consider numbers r that divide a product mn of two nearly-equal composite numbers. Conditioned on $r \geq \min\{m, n\}$, give a lower bound for the proportion that are a multiple of m or a multiple of n . Note that m and n need not be themselves relatively prime; $p - 1$ and $q - 1$ are both even, for instance. It would still need to be argued that most a give such an r . But I am also not sure that the "helpful" property is needed after all--most other treatments just omit it. But also incidentally, the closer r is to $\sqrt{M}$ as opposed to being order-of M , the more challenging for a potential classical simulation of Shor's algorithm.)

Chapter 12 does handle the argument in property 3, given that r is "helpful"---which also subsumes issue 1 since $p - 1$ and $q - 1$ are even. Item 2 is handled by a random argument. We will skim over these and instead focus on examples of the particular numerical properties.

One thing to observe is that when M is a **Blum integer**, meaning that p and q are both congruent to 3 modulo 4, then $(p - 1)(q - 1)$ is divisible by 4 but no higher even number. There are always four square roots of 1 modulo $M = pq$, so we need to argue that the a 's such that $a^{r/2}$ is one of the good ones are as plentiful as the bad ones. (Note that r depends only on a .) Here is an example for the smallest Blum integer: $21 = 3 \cdot 7$. The **quadratic residues** are:

Mod 7: 1, 4, 2

Mod 3: 1

Eligible numbers: 2, 10, 11, 13

Quadratic residues modulo 21:

1:1, 2:4, 3:9, 4:16, 5:4, 6:15, 7:7, 8:1, 9:18, 10:16,
20:1, 19:4, 18:9, 17:16, 16:4, 15:15, 14:7, 13:1, 12:18, 11:16

Now $(p - 1)(q - 1) = 12$. The numbers $Y = 8 - 1, 8 + 1, 13 + 1$, and $13 - 1$ all give a factor via $\gcd(21, Y)$.

$a = 1$: $r = 1$; of course doesn't work.

$a = 2$: 2, 4, 8, 16, 11, 1. Works

$a = 4$: 4, 16, 1 (period 3 is odd)

$a = 5$: 5, 4, 20, 16, 17, 1; doesn't work because $20 \equiv -1$.

$a = 8$: $8^2 \equiv 1$. Period $r = 2$ is "helpful" with regard to $p = 3$, and $8^{r/2} = 8$ is not -1 . So works.

$a = 10$: 10, 16, 13, 4, 19, 1. Works

$a = 11$: 11, 16, 13, 4, 19, 1. **Works**

$a = 13$: 13, 1

The other values are mirror images.

A more interesting Blum integer IMHO is $77 = 7 \cdot 11$. Then $(p-1)(q-1) = 60$. "Helpful" means the period is a multiple of 6 or of 10. Note: $34^2 = 1156 = 77 \cdot 15 + 1$ is a nontrivial square root of 1 and $43^2 = 1849 = 77 \cdot 24 + 1$ is the other one. Does 2 work?

2: 4, 8, 16, 32, 64, 51, 25, 50, 23, 46, 15, 30, 60, 43, 9, 18, 36, 72, 67, 57, 37, 74, etc.: **yes**.

Let's try the Blum integer $33 = 3 \cdot 11$. Then $(p-1)(q-1) = 20$. Whenever 3 is a factor, every even period length r is "helpful." Let's see what we get:

$a = 2$: 2, 4, 8, 16, 32 --- which $\equiv -1$ modulo 33, so we can already tell this "shouldn't" work.

$a = 4$: 4, 16, 31, 25, 1 --- which has an odd period (but maybe we can tweak it to work).

$a = 5$: 5, 25, 26, 31, 23, 16, 14, 4, 20, 1. **Works**. (Note relation to reverse of $a = 4$ series.)

$a = 7$: 7, 16, 13, 25, 10, 4, 28, 31, 19, 1. **Works**.

$a = 8$: 8, 31, 17, 4, 32 --- Cannot work.

$a = 10$: 10, 1. **This counts as working**.

$a = 13$: 13, 4, 19, 16, 10, 31, 7, 25, 28, 1. **Works**.

$a = 14$: 14, 31, 5, 4, 23, 25, 20, 16, 26, 1. **Works**.

$a = 16$: 16, 25, 4, 31, 1. Odd period, should not work (but might with tricks).