CSE 439/510 Lecture Tue Oct 29 Fall 2024

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

Input: $M = pq$, when 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, ie. a is relatively prime to M ($a \in G_M$).

Goal: Compute the true period: least r such that $a^r \equiv 1$ modulo 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.

The test also plays fast-and-loose between r and the odd number r_0 obtained by dividing out all factors of 2 from r. Note this:

> IF $r = 2^k r_0$ and a has period r, then $a' = a^{2^k}$ has period r_0

Now a' is also relatively prime to M. So we could have picked it. To cover it when we pick a, we need only re-run the algorithm for all the guesses $a, a^2, a^4, a^8, \ldots a^{2^{2n-1}}$ (since $2^{2n} \approx M$). This involves only an $O(n)$ factor extra work $\rightarrow$ still poly(n) time. This suboptimal analysis allows us to presume $r_0 = r$, ie. that the true period is odd.

Since we have to worry about multiples of r anyway, in the optimal analysis, this comes out in the wash of Chapter 12. But the extra assumption that $r_0 = r$ makes Ch-11 easier to visualize.

Steps of the Quantum Part: (after guessing a but maybe considering all of $a, a^2, a^4, a^8 \ldots$ along with it)

(Q1) Fatten up the domain of $f_a(x) = a^x \bmod M$ to include all x up to $Q = 2^\ell$ where $\ell = \lceil \log_2(M^2) \rceil$ so Q is the least power of 2 above M^2. (We actually only need to guarantee $Q > rM$, noting that $r < |G_M| < M$.)
Then $\ell \approx 4n$ 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 bottom – a minor typo.)

(Q2) Prepare the state $\mathbf{a} = \frac{1}{\sqrt{Q}} \sum_{x<Q} |x\rangle|f_a(x)\rangle$.

(Q3) Apply QFT_ℓ (or its inverse) to the $|x\rangle$ part to get $\mathbf{b}$

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

BP2: We need there to exist an integer t such that $\left|x - \frac{tQ}{r}\right| \leq \frac{1}{2}$, 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 $\Omega\left(\frac{1}{\log n}\right)$. So we do under $\log n$ 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, i.e. rerunning quantum part

If fail n resamples – go all way back to BP1. (If that fails, n times you are insanely unlucky)

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

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

Let's not mention ⓓ 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 $\Omega\left(\frac{1}{\log\log r}\right) = \Omega\left(\frac{1}{\log n}\right)$ chance of success in any one go, and $\text{poly}(n)$ trials give almost certain final success.

Proof of ⓒ: Recall *good* means for some t relatively prime to the true period r, $\left|\frac{tQ}{r} - x\right| \le \frac{1}{2}$. Now any such t gives a good x because: Let us "re-center" the definition of "$y = c \bmod' d$" to give $-\lfloor \frac{d}{2} \rfloor \le c < \lceil \frac{d}{2} \rceil$ rather than $0 \le c < d$. Thus mod' 7 gives range -3 to $+3$ rather than 0 to 6, and mod' 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 $-\lfloor \frac{r}{2} \rfloor \le K < \lceil \frac{r}{2} \rceil$. This implies $tQ - xr = K$ when $-\frac{r}{2} \le K \le \frac{r}{2}$, so $|tQ - xr| \le \frac{r}{2}$, so $\left|\frac{tQ}{r} - x\right| \le \frac{1}{2}$. 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 $\Omega\left(\frac{r}{\log\log r}\right)$ 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 loglog factor, and that is "no biggie." So ⓒ is proved.

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

What that means is: there is only one lowest-terms fraction $\frac{r}{t}$ 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 "$@p_2$" from repeated trials of fa might make you rewind to B_1 with another a. The only way you get certainty 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).]

My simulator adopts 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.

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

$$b(x,y) = \frac{1}{\sqrt{Q}} \cdot \sum_{u \in \{0,1\}^\ell} \omega^{ux} a(u,y)$$

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

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

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

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

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

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

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

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 $f^{-1}(y) = \{u_0, u_0+r, \ldots, u_0+(T-1)r\}$. This enables us to group the sum as:

$$\sum_{u \in f_a^{-1}(y)} \omega^{xu} = \sum_{k=0}^{T-1} \omega^{x(u_0+kr)} = \omega^{xu_0} \sum_{k=0}^{T-1} \omega^{xrk}$$

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

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

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

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

$$= \frac{1}{Q^2} \underbrace{\omega^{xu_0} \overline{\omega}^{xu_0}}_{\text{unit, so } = 1} \cdot \frac{(\omega^{Txr}-1)(\overline{\omega}^{Txr}-1)}{(\omega^{xr}-1)(\overline{\omega}^{xr}-1)} = \frac{1}{Q^2} \left(\frac{1 - \omega^{Txr} + 1 - \overline{\omega^{Txr}}}{1 - \omega^{xr} + 1 - \overline{\omega^{xr}}} \right) = \frac{2 - 2\mathrm{Re}(\omega^{Txr})}{Q^2 (2 - 2\mathrm{Re}(\omega^{xr}))}$$

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

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

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

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

$$= \frac{1}{Q^2}\,\frac{\sin^2\left(\frac{\pi x r}{Q}T - T t\pi\right)}{\sin^2\left(\frac{\pi x r}{Q} - t\pi\right)} = \frac{1}{Q^2}\left|\frac{\sin^2\left(T\pi\left(\frac{xr-tQ}{Q}\right)\right)}{\sin^2\left(\pi\left(\frac{xr-tQ}{Q}\right)\right)}\right|$$

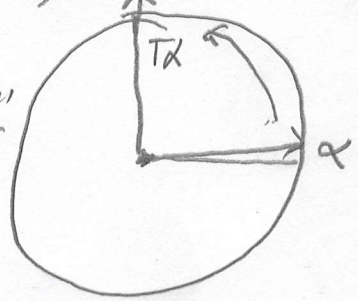
By goodness, the numerator $xr - tQ$ has absolute value at most $r/2$. Also, $\sin^2(-\theta) = \sin^2(\theta)$ for any θ. Thus we have

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

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

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

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



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

(← a little more than $\pi/2$)

Lemma (II.2) For all $T > 0$ and angles $\alpha > 0$ such that $T\alpha \le 1.581$,

$$\frac{\sin(T\alpha)}{\sin(\alpha)} \ge cT \quad \text{where } c = 0.63247 \text{ (chosen so that } c^2 \ge 0.4).$$ ⊠

So we finally get

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

This proves (b) ⊠