CSE439/510 Fall 2025 Week 10: Details of Shor's Algorithm

CSE 439/510 Lecture Tue Oct 29 Fall 2024

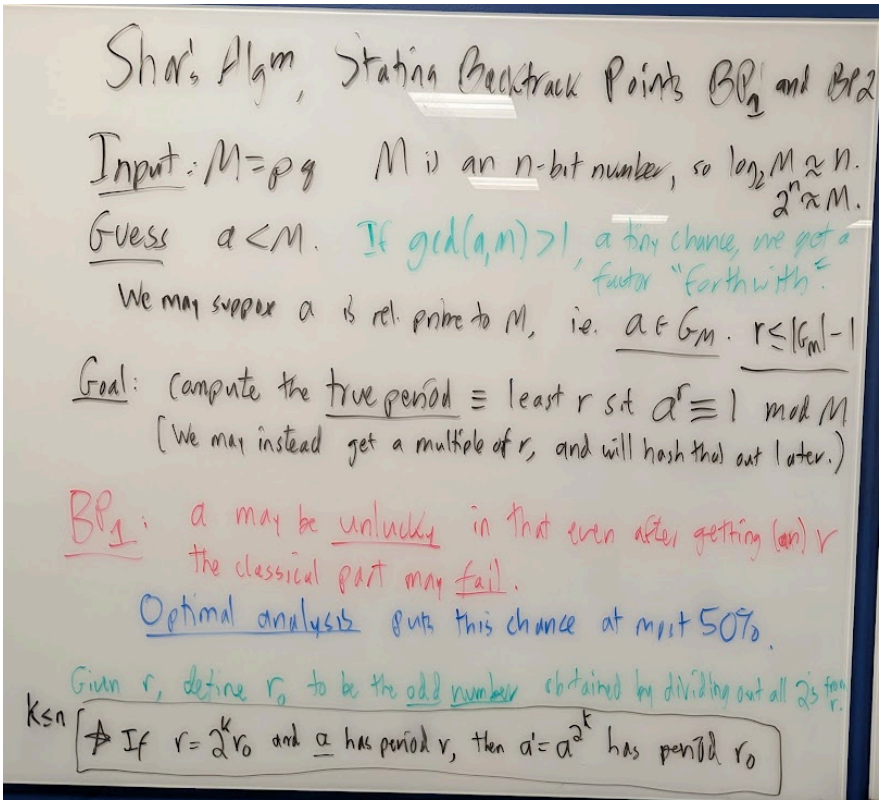
Shor's Algorithm, Stating Its Backtrack Points BP1 & BP2

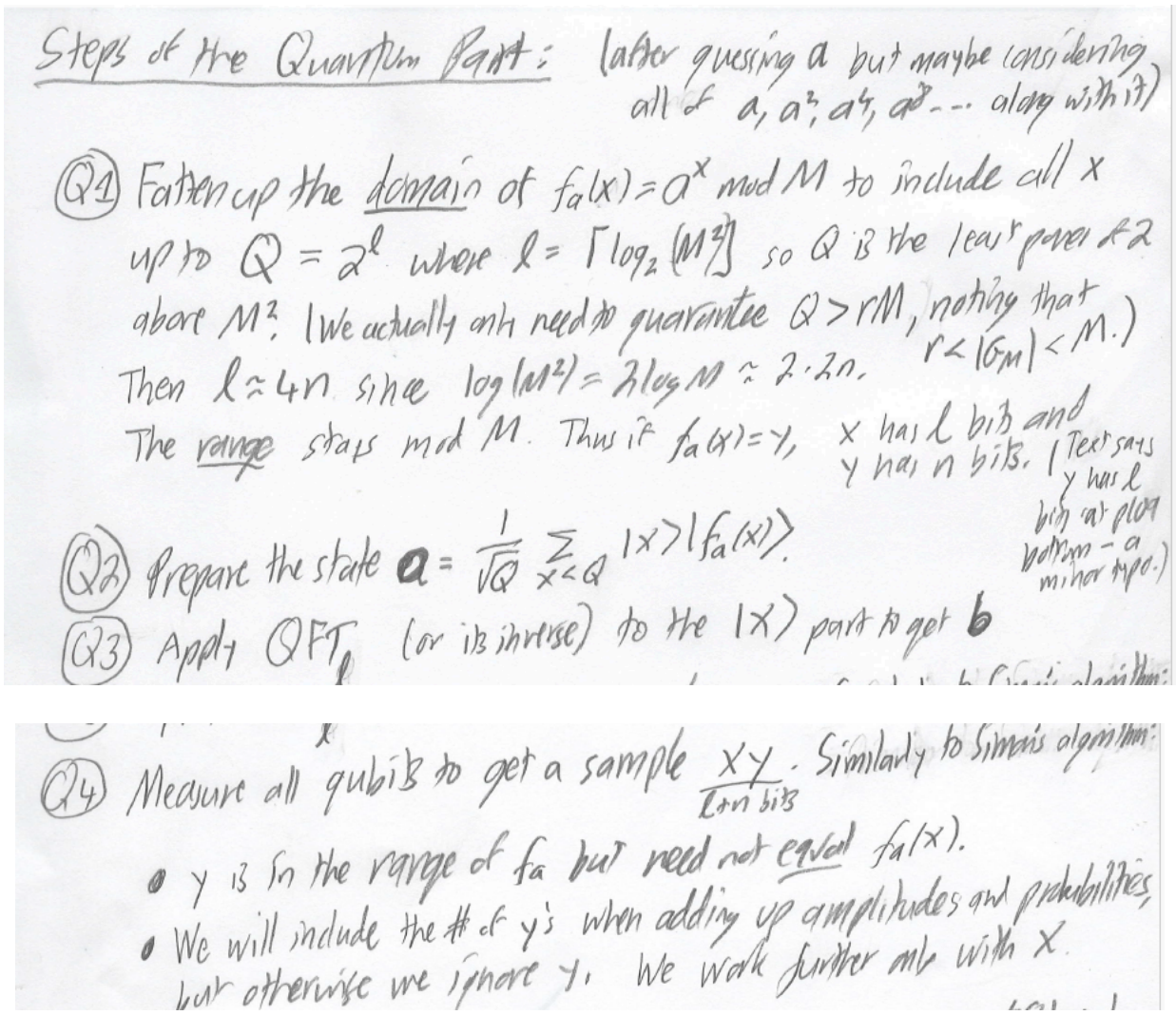
Input: $M = pq$, where p, q are n-bit primes. So $\log_2 M \approx 2n$.

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 ($a \in G_M$).

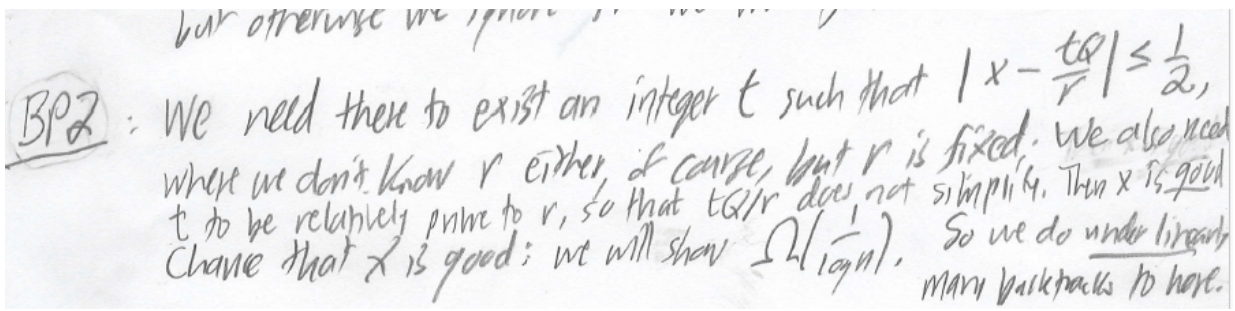
Goal: Compute the true period: least r such that $a^r \equiv 1$ modulo M.
Note: multiples of r are also periods, and we may get them instead.

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 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 $f_a(x) = a^x \bmod M$.

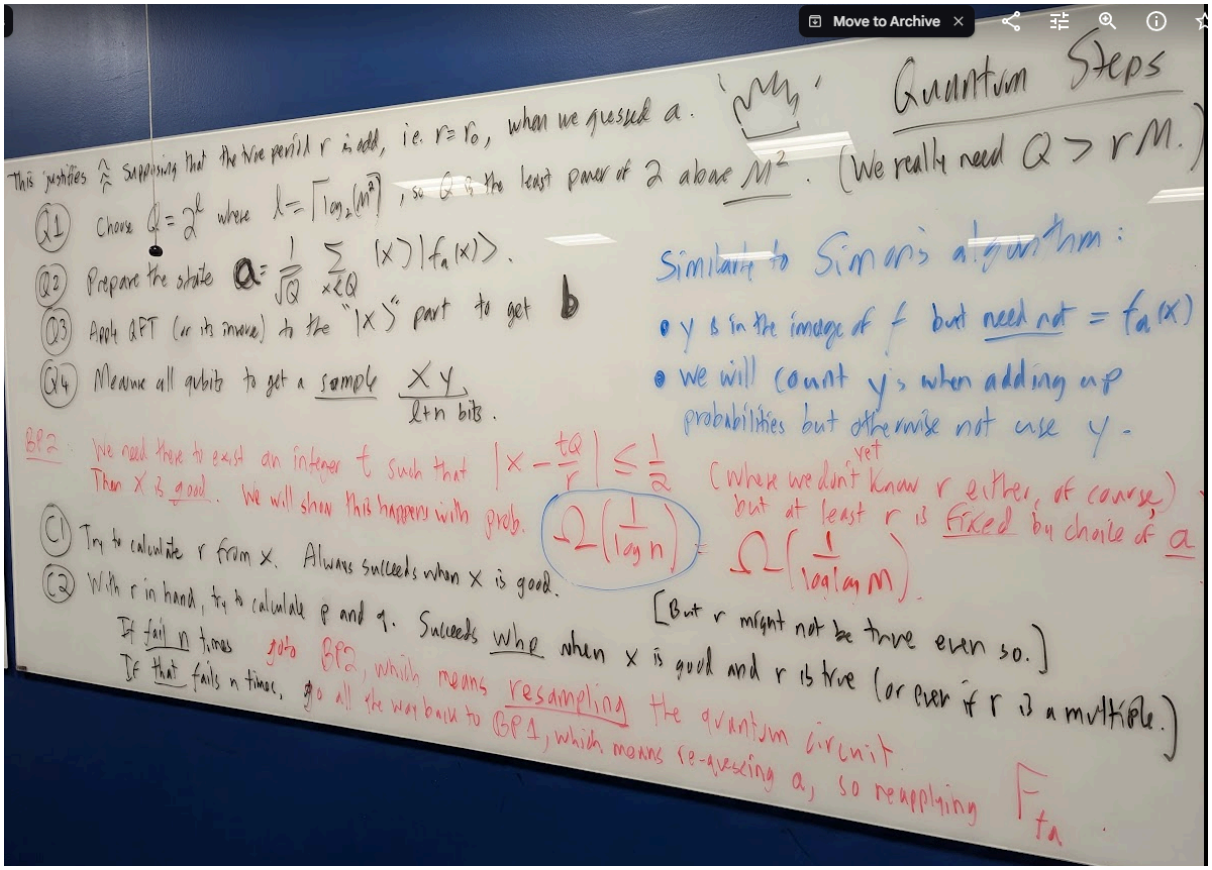


(C1) Try to calculate r from x. This always succeeds when x is good.

(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 insanely unlucky)



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

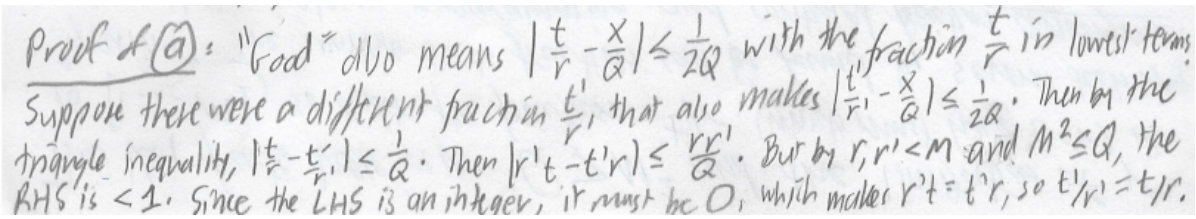
(a) If the measurement gives a good x, then we get the true period r.
(b) The probability of an individual good x and $y \in \text{Ran}(f)$ is $\Omega\left(\frac{1}{r^2}\right)$
(c) There are $\Omega\left(\frac{r}{\log\log r}\right)$ good x's, times $|\text{Ran}(f)| = r$ many y's. Thus any one run and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

Let's not mention (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 (at "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.

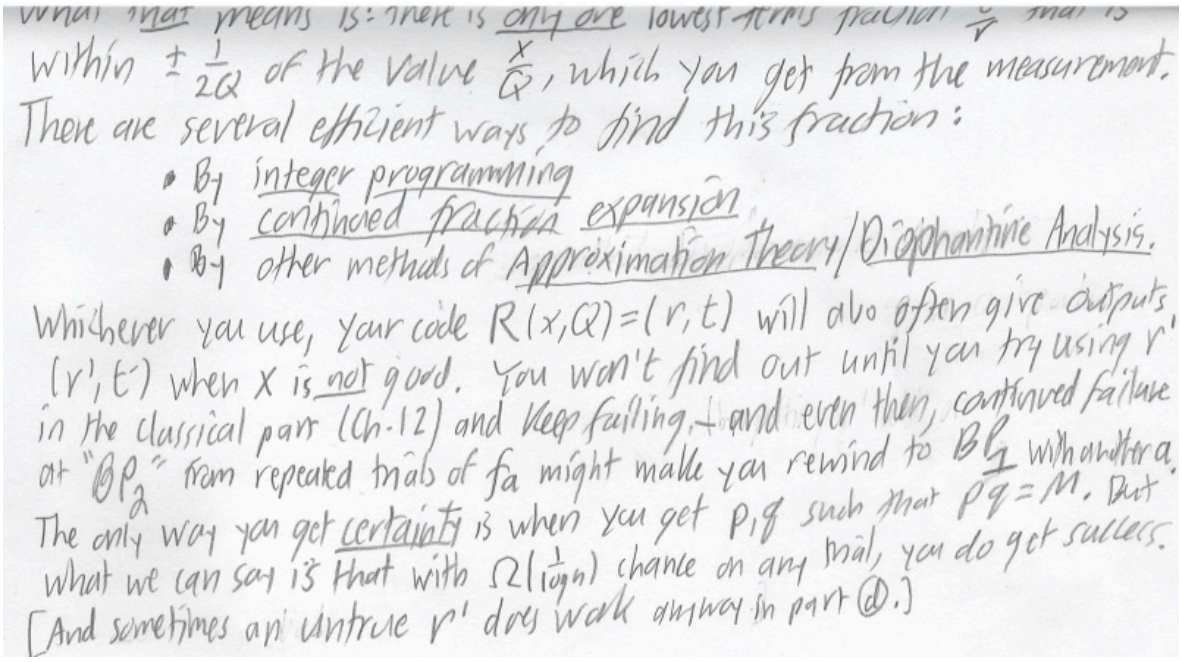
Proof of (c): Recall good means for some t relatively prime to the true period r, $\left|\frac{tQ}{r} - x\right| \leq \frac{1}{2}$. Now any such t gives a good x because: Let us "re-center" the definition of "$y = c \bmod' d$" to give $-\lfloor \frac{d}{2} \rfloor \leq c < \lceil \frac{d}{2} \rceil$ rather than $0 \leq c < d$. 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 $-\lfloor \frac{r}{2} \rfloor \leq K < \lceil \frac{r}{2} \rceil$. This implies $tQ - Xr = K$ where $-\frac{r}{2} \leq K \leq \frac{r}{2}$, so $|tQ - Xr| \leq \frac{r}{2}$, so $\left|\frac{tQ}{r} - X\right| \leq \frac{1}{2}$. 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 $\Omega\left(\frac{r}{\log\log r}\right)$ 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 (c) is proved.



Proof of (a): "Good" also means $\left|\frac{t}{r} - \frac{x}{Q}\right| \leq \frac{1}{2Q}$ with the fraction $\frac{t}{r}$ in lowest terms. Suppose there were a different fraction $\frac{t'}{r'}$ that also makes $\left|\frac{t'}{r'} - \frac{x}{Q}\right| \leq \frac{1}{2Q}$. Then by the triangle inequality, $\left|\frac{t}{r} - \frac{t'}{r'}\right| \leq \frac{1}{Q}$. 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 $t'/r' = t/r$.

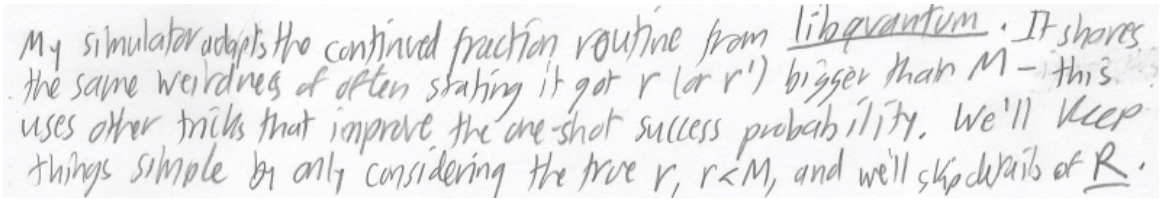


What that means is: there is only one lowest-terms fraction $\frac{t}{r}$ that is within $\pm \frac{1}{2Q}$ of the value $\frac{x}{Q}$, which you get from the measurement. There are several efficient ways to find this fraction:

- 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 "BP_2" from repeated trials of f_a 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 $\Omega\left(\frac{1}{\log n}\right)$ chance on any trial, you do get success. [And sometimes an untrue r' does work anyway in part (d).]

Footnote:



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.

Now to set up the main quantum analysis:

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 EXACTLY wisest 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 $\omega = e^{2\pi i/Q} = e^{2\pi i/2^{\ell}}$ has the property that $\omega^Q = 1$ but no smaller power is 1 — so it is a principal complex Qth root of unity.

[The Tuesday 10/28 lecture ended here.]

"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 $y \notin \text{Ran}(f_a)$ then the amplitude $b(x,y) = 0$ for all x. For any one $y \in \text{Ran}(f_a)$, 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 $f^{-1}(y) = \{u_0, u_0+r, \dots, u_0+(T-1)r\}$. This enables us to group the sum as:

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

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

So: $b(x,y) = \frac{1}{Q} w^{xu_0} \sum_{k=0}^{T-1} (w^{xr})^k$ 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.

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

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

$$= \frac{1}{Q^2} \frac{1 - \mathrm{Re}(e^{2\pi i Txr/Q})}{1 - \mathrm{Re}(e^{2\pi i xr/Q})} = \frac{1}{Q^2} \left(\frac{1 - \cos\left(\frac{2\pi Txr}{Q}\right)}{1 - \cos\left(\frac{2\pi xr}{Q}\right)} \right)$$

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

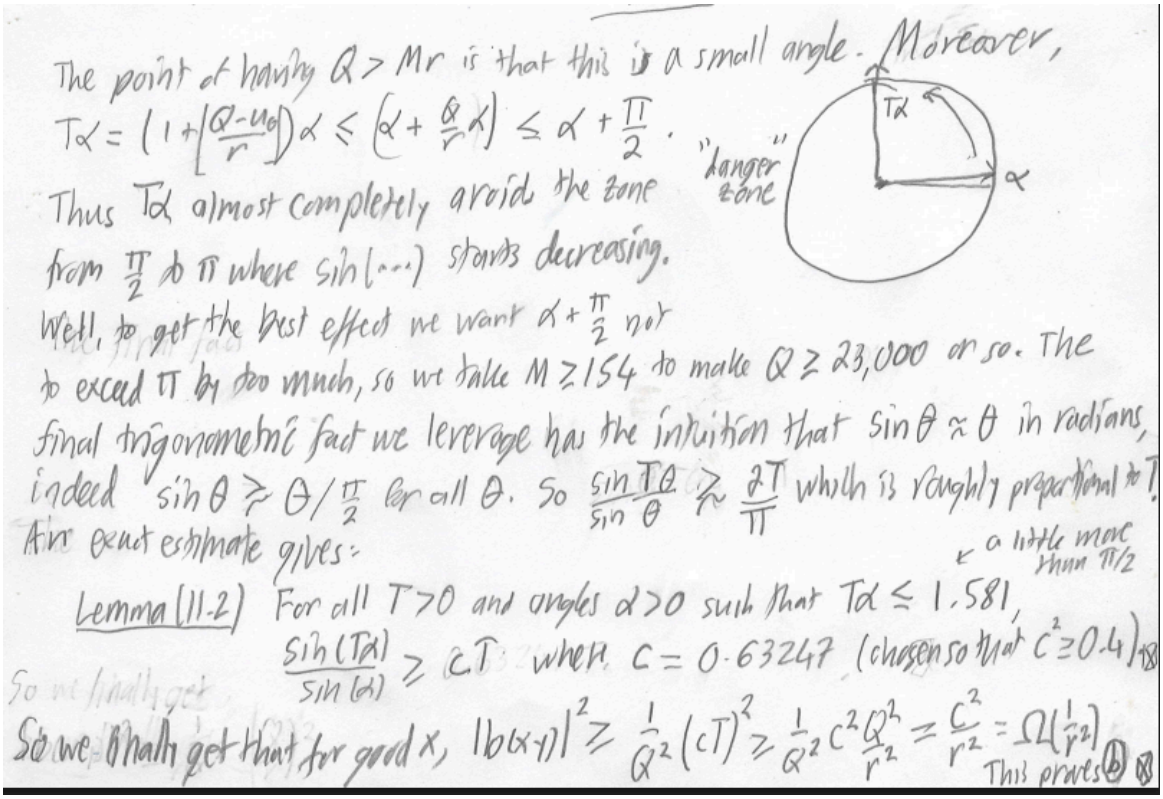
$$= \frac{1}{Q^2} \frac{\sin^2\left(\frac{\pi xr}{Q} T\right)}{\sin^2\left(\frac{\pi xr}{Q}\right)}$$

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

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

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

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



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 is not $\equiv 1$ or $\equiv -1$ 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: $21 = 3*7$. 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 $77 = 7*11$. Then $(p-1)(q-1) = 60$. "Helpful" means the period is a multiple of 6 or of 10. Note: $34^2 = 1156 = 77*15 + 1$ is a nontrivial square root of 1 and $43^2 = 1849 = 77*24 + 1$ 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*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).