Period Finding

Overview

Last time:

Introduced the Fourier transform over $\mathbb{Z}_N$ and saw it can be implemented efficiently by a quantum circuit.

Today:

- Shor's period finding algorithm

  First we see a simple version, then what is needed for factoring.

- Integer Factorization = period finding + number theory

Period Finding

Like Simon's problem we are given a periodic function and the goal is to find its period.

Let $f : \mathbb{Z}_N \to [M]$ with the promise there is an s such that

1) $f(0), \ldots, f(s-1)$ are all distinct (injectivity assump.).

2) $f(x) = f(y)$ if $x - y = 0 \bmod s$

3) $s | N$

Conditions (2) and (3) mean $f(x) = f(x+s)$ for all $x \in \mathbb{Z}_N$

Oracle

- $f(x) = f(x+s)$ for all $x \in \mathbb{Z}_N$
- $f(0), \ldots, f(s-1)$ are all distinct (injectivity assumption).

We will again work in the query model.

We assume access to an oracle O_f

$$O_f|x\rangle|z\rangle = |x\rangle|z \oplus f(x)\rangle$$

$x \in \mathbb{Z}_N$

$z \in \{0,1\}^m$

where $z \in \{0,1\}^m$ and we think of $f(x)$ written as an m bit string.

Example

- $f(x) = f(x+s)$ for all $x \in \mathbb{Z}_N$
- $f(0), \ldots, f(s-1)$ are all distinct (injectivity assumption).

x	f(x)
0	red
1	blue
2	green
3	red
4	blue
5	green
6	red
7	blue
8	green

We will use this as a running example as we go over the algorithm.

$$N = 9, s = 3$$

Start of Algorithm

The period finding algorithm begins in a familiar fashion.

Step 1: Create uniform superposition on the first register.

$$|0\rangle|0^m\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle|0^m\rangle$$

Step 2: Apply the oracle O_f .

$$\frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle|f(x)\rangle$$

$$\frac{1}{3}\left(|0\rangle|\text{red}\rangle + |1\rangle|\text{blue}\rangle + |2\rangle|\text{green}\rangle + \cdots + |8\rangle|\text{green}\rangle\right)$$

Basis for periodic fn

$$\frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle |f(x)\rangle$$

As we did with Simon's algorithm, let's rewrite this state to group together x with the same value of $f(x)$.

$$\frac{1}{3}\left((|0\rangle + |3\rangle + |6\rangle)|\text{red}\rangle + (|1\rangle + |4\rangle + |7\rangle)|\text{blue}\rangle + (|2\rangle + |5\rangle + |8\rangle)|\text{green}\rangle\right)$$

$\{x : x \bmod s = 0\}$ $\{x : x \bmod s = 1\}$ $\{x : x \bmod s = 2\}$

To help with this in general, define

$$|g_t\rangle = \sqrt{\frac{s}{N}} \sum_{\substack{x \in \mathbb{Z}_N \\ x \bmod s = t}} |x\rangle$$

Basis for periodic fn

$$|g_t\rangle = \sqrt{\frac{s}{N}} \sum_{\substack{x \in \mathbb{Z}_N \\ x \bmod s = t}} |x\rangle$$

$$\frac{1}{3}\left((|0\rangle + |3\rangle + |6\rangle)|\text{red}\rangle + (|1\rangle + |4\rangle + |7\rangle)|\text{blue}\rangle + (|2\rangle + |5\rangle + |8\rangle)|\text{green}\rangle\right)$$

$$=$$

$$\frac{1}{\sqrt{3}}\left(|g_0\rangle|\text{red}\rangle + |g_1\rangle|\text{blue}\rangle + |g_2\rangle|\text{green}\rangle\right)$$

In general,

$$\frac{1}{\sqrt{N}} \sum_{z \in \mathbb{Z}_N} |x\rangle|f(x)\rangle = \frac{1}{\sqrt{s}} \sum_{t=0}^{s-1} |g_t\rangle|f(t)\rangle$$

$$\frac{1}{\sqrt{N}} \sum_{z \in \mathbb{Z}_N} |x\rangle |f(x)\rangle = \frac{1}{\sqrt{s}} \sum_{t=0}^{s-1} |g_t\rangle |f(t)\rangle$$

Step 2b: Measure the second register.

We see a random value of f. Say we see a such that $f(c) = a$ with $0 \leq c \leq s-1$.

Then we are left in the state $|g_c\rangle |f(c)\rangle$.

In our example, say we are in the state $|g_1\rangle |\text{blue}\rangle$.

Fourier Transform

$$|g_c\rangle|f(c)\rangle$$

Step 3: Apply the Fourier transform over $\mathbb{Z}_N$ to the first register.

Demo

Punchline

$$|g_t\rangle = \sqrt{\frac{s}{N}} \sum_{\substack{x \in \mathbb{Z}_N \\ x \bmod s = t}} |x\rangle$$

$$F_N |g_t\rangle = \frac{1}{\sqrt{s}} \sum_{\substack{y \in \mathbb{Z}_N \\ y \bmod \frac{N}{s} = 0}} \omega^{-yt} |y\rangle$$

- All nonzero entries of $F_N|g_t\rangle$ have the same magnitude.
- The zero/nonzero pattern is periodic with period $\frac{N}{s}$.
- The zero/nonzero pattern is independent of t.

Finishing the algorithm

$$F_N|g_t\rangle = \frac{1}{\sqrt{s}} \sum_{\substack{y\in\mathbb{Z}_N \\ y \bmod \frac{N}{s}=0}} \omega^{-yt}|y\rangle$$

Measure $F_N|g_c\rangle$.

We see an index $\frac{kN}{s}$ for $k \in \{0,\ldots,s-1\}$ uniformly at random.

As long as $k \neq 0$ we learn something about s .

We can classically compute s from a few of these samples.

Bad case

Let's quickly handle the bad case of seeing $k = 0$.

We can check if $s \leq 5$ by querying $f(0), \ldots, f(5)$.

From now on assume $s \geq 6$. Then the probability we see $k = 0$ is at most $1/s \leq 1/6$.

We can repeat the whole procedure 5 times to get 3 non-zero values of k with probability at least 95% .

Classical reconstruction

Say we obtained $\frac{k_1 N}{s}, \frac{k_2 N}{s}, \frac{k_3 N}{s}$ all nonzero.

We compute the greatest common divisor of these three numbers. This can be done classically in $O(\log N)$ time.

This will be $\frac{N}{s}$ if $\gcd(k_1, k_2, k_3) = 1$.

What is the probability this will happen?

This will be $\dfrac{N}{s}$ if $\gcd(k_1, k_2, k_3) = 1$.

What is the probability this will happen?

The probability a prime p divides all of k_1, k_2, k_3 when they are chosen independently at random is $1/p^3$.

$$\sum_{p \text{ prime}} \frac{1}{p^3} \leq \frac{1}{8} + \frac{1}{27} + \frac{1}{125} + \frac{1}{343} + \sum_{\substack{t \in \mathbb{N} \\ t \geq 11}} \frac{1}{t^3}$$

$$\leq \frac{2}{11} + \int_{10}^{\infty} \frac{dx}{x^3}$$

$$\leq \frac{1}{5} \ .$$

Summary

First query $f(0), \ldots, f(5)$. If no collision repeat the quantum procedure 5 times. Total queries 11.

Each quantum procedure requires two applications of the Fourier transform, thus can be done by a quantum circuit with $O(\log(N)^2)$ gates.

Classical reconstruction $O(\log(N))$ time.

Success probability 75%.

Proof of Punchline

$$|g_t\rangle = \sqrt{\frac{s}{N}} \sum_{\substack{x \in \mathbb{Z}_N \\ x \bmod s = t}} |x\rangle$$

$$F_N|g_t\rangle = \frac{1}{\sqrt{s}} \sum_{\substack{y \in \mathbb{Z}_N \\ y \bmod \frac{N}{s} = 0}} \omega^{-yt}|y\rangle$$

$$F_N|g_t\rangle = \sqrt{\frac{s}{N}} \sum_{\substack{x \in \mathbb{Z}_N \\ x \bmod s = t}} F_N|x\rangle$$

$$\omega = e^{2\pi \mathrm{i}/N}$$

$$= \frac{\sqrt{s}}{N} \sum_{\substack{x \in \mathbb{Z}_N \\ x \bmod s = t}} \sum_{y \in \mathbb{Z}_N} \omega^{-xy}|y\rangle$$

$$= \frac{\sqrt{s}}{N} \sum_{k=0}^{N/s-1} \sum_{y \in \mathbb{Z}_N} \omega^{-(ks+t)y}|y\rangle$$

Proof of Punchline

$$F_N|g_t\rangle = \frac{\sqrt{s}}{N} \sum_{k=0}^{N/s-1} \sum_{y \in \mathbb{Z}_N} \omega^{-(ks+t)y} |y\rangle$$

$$= \frac{\sqrt{s}}{N} \sum_{y \in \mathbb{Z}_N} \omega^{-ty} |y\rangle \left(\sum_{k=0}^{N/s-1} \omega^{-ksy} \right)$$

$$= \frac{\sqrt{s}}{N} \sum_{y \in \mathbb{Z}_N} \omega^{-ty} |y\rangle \left(\sum_{\substack{a \in \mathbb{Z}_N \\ a \bmod s = 0}} \omega^{-ay} \right)$$

Recall the "key property" of characters from last lecture.

Proof of Punchline

$$F_N|g_t\rangle = \frac{\sqrt{s}}{N} \sum_{y \in \mathbb{Z}_N} \omega^{-ty}|y\rangle \left(\sum_{\substack{a \in \mathbb{Z}_N \\ a \bmod s = 0}} \omega^{-ay} \right)$$

Recall the "key property" of characters from last lecture.

If $\omega^{-ys} \neq 1$ then $\sum_{\substack{a \in \mathbb{Z}_N \\ a \bmod s = 0}} \omega^{-ay} = 0$. Otherwise it is N/s.

$$F_N|g_t\rangle = \frac{1}{\sqrt{s}} \sum_{\substack{y \in \mathbb{Z}_N \\ y \bmod \frac{N}{s} = 0}} \omega^{-yt}|y\rangle$$

Activity

Period finding with weaker assumptions

More general period finding

For the application to factoring we need to solve a more general version of the period finding problem.

Now $f : \mathbb{Z}_N \to [M]$ and we are promised there is an s such that

1) $f(0), \ldots, f(s-1)$ are all distinct (injectivity assump.).

2) $f(x) = f(y)$ if $x - y = 0 \bmod s$

3') $N > M^2/2$

Note $s \leq M$

Condition (3') ensures we see at least $s/2$ many periods.

New difficulties (1)

x	f(x)
0	red
1	blue
2	green
3	red
4	blue
5	green
6	red

$f(x) = f(y)$ **iff** $x - y = 0 \bmod s$.

We refer to these as almost-periodic functions.

Some output values occur $\lfloor N/s \rfloor + 1$ times and some occur $\lfloor N/s \rfloor$ times.

There are $\ell_t = 1 + \left\lfloor \frac{N-1-t}{s} \right\rfloor$ many $x \in \mathbb{Z}_N$ with $x \bmod s = t$.

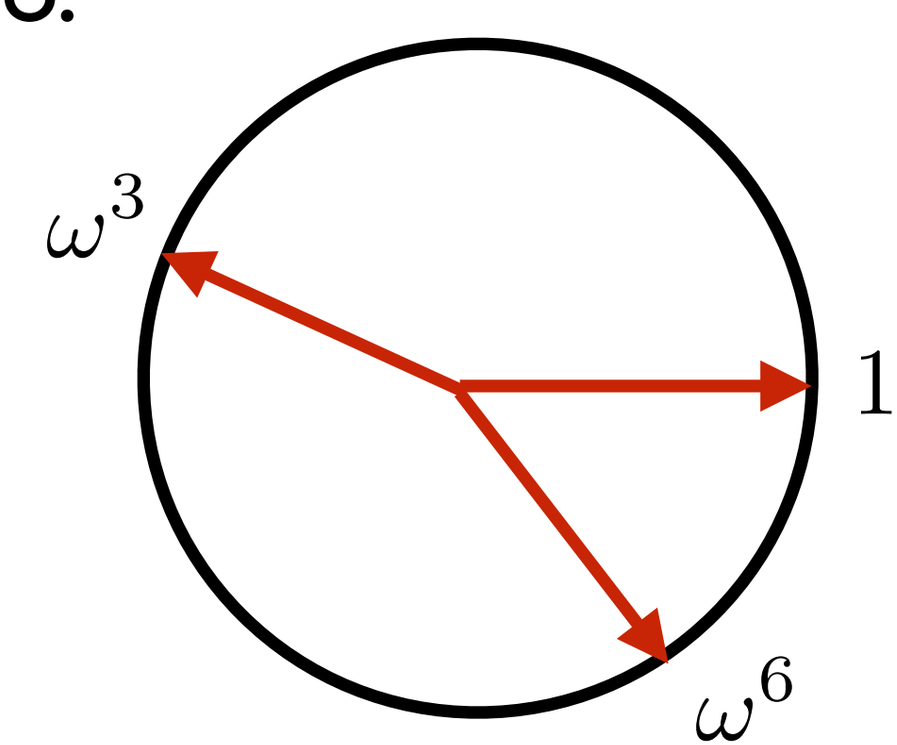
New difficulties (2)

x	f(x)
0	red
1	blue
2	green
3	red
4	blue
5	green
6	red

$$f(x) = f(y) \text{ iff } x - y = 0 \bmod s.$$

$$\omega = e^{2\pi i/7}$$

The vectors $1, \omega^3, \omega^6$ no longer sum to zero.



This difficulty is harder to deal with.

Algorithm

The algorithm is the same as before:

Step 1: Create uniform superposition on the first register.

$$|0\rangle|0^m\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle|0^m\rangle$$

Step 2: Apply the oracle O_f .

$$\frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle|f(x)\rangle$$

Algorithm

Step 2: Apply the oracle O_f .

$$\frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle |f(x)\rangle$$

Let us again group together by $f(x)$ value.

$$\frac{1}{\sqrt{7}} (|0\rangle|\text{red}\rangle + |1\rangle|\text{blue}\rangle + |2\rangle|\text{green}\rangle + \cdots + |6\rangle|\text{red}\rangle)$$

$$=$$

$$\frac{1}{\sqrt{7}} ((|0\rangle + |3\rangle + |6\rangle)|\text{red}\rangle + (|1\rangle + |4\rangle)|\text{blue}\rangle + (|2\rangle + |5\rangle)|\text{green}\rangle)$$

Basis for almost periodic fn

To do this in general define

$$|g_t\rangle = \frac{1}{\sqrt{\ell_t}} \sum_{\substack{x \in \mathbb{Z}_N \\ x \bmod s = t}} |x\rangle$$

Then

$$\frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle |f(x)\rangle = \frac{1}{\sqrt{N}} \left(\sum_{t=0}^{s-1} \sqrt{\ell_t} |g_t\rangle |f(t)\rangle \right)$$

Measure 2nd register

$$\frac{1}{\sqrt{N}}\left(\sum_{t=0}^{s-1}\sqrt{\ell_t}|g_t\rangle|f(t)\rangle\right)$$

Step 2b: Measure the second register.

We see $f(t)$ with probability $\frac{\ell_t}{N} \approx \frac{1}{s}$.

Say we see value a such that $f(c) = a$ with $c \in \{0, \ldots, s-1\}$.

Then our state is $\frac{1}{\sqrt{\ell_t}}|g_c\rangle|f(c)\rangle$.

$$\frac{1}{\sqrt{\ell_t}}|g_c\rangle|f(c)\rangle$$

Step 3: Apply F_N to the first register and measure.

In the periodic case, $F_N|g_c\rangle$ only had nonzero amplitude on $|y\rangle$ where

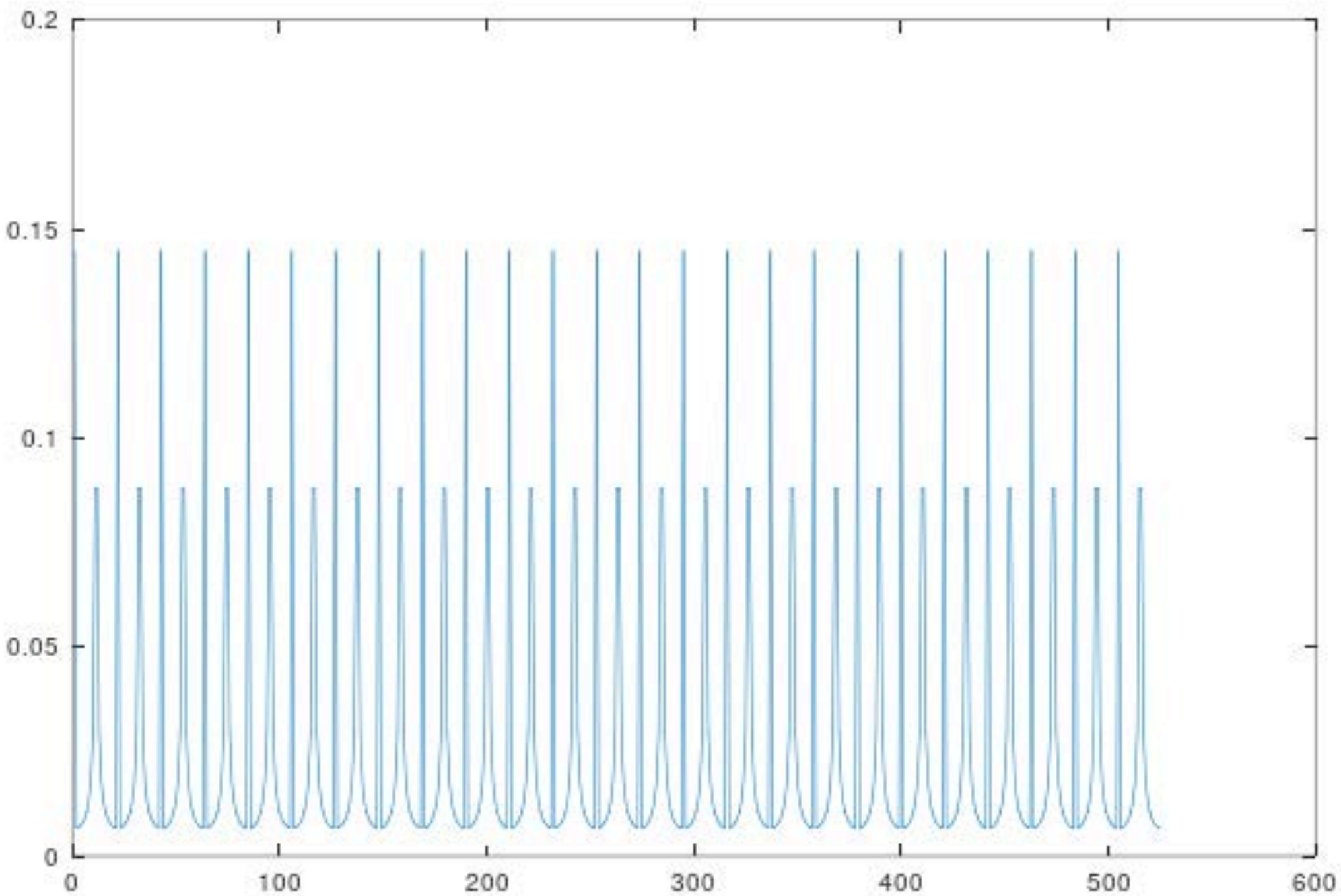
$$y = \frac{kN}{s}$$

for $k \in \{0, \ldots, s-1\}$.

This is no longer true in the almost-periodic case.

But with good prob. we will get a y close to $\frac{kN}{s}$.

Here is a plot of the magnitude of the coefficients of $F_N|g_0\rangle$ with $N = 525, s = 50$.



Overview

Formally, we will argue that $|\langle b|F_N|g_0\rangle|^2$ is large when

$$-\frac{s}{2} \leq bs - kN \leq \frac{s}{2}$$

This gets technical and we postpone it for now.

Let's first see why this still suffices to learn s.

Good b's

Call $b \in [N]$ good if $\exists k \in \mathbb{N}$ with $\gcd(s,k) = 1$ s.t.

$$-\frac{s}{2} \leq bs - kN \leq \frac{s}{2}$$

If we measure and see a good b then we claim we can compute s classically in polynomial time.

Dividing by sN we see $\left|\frac{b}{N} - \frac{k}{s}\right| \leq \frac{1}{2N}$.

Dividing by sN we see $\left|\frac{b}{N} - \frac{k}{s}\right| \leq \frac{1}{2N}$

and $\frac{k}{s}$ is in lowest terms as $\gcd(s,k) = 1$.

We claim that k/s is the unique rational number with denominator $\leq M$ that is this close to b/N.

$$\left|\frac{k}{s} - \frac{k'}{s'}\right| = \left|\frac{ks' - k's}{ss'}\right| \geq \frac{1}{ss'} \geq \frac{1}{M^2}$$

This is bigger than $1/(2N)$ by Condition 3' which says $N > M^2/2$.

Dividing by sN we see $\left|\frac{b}{N} - \frac{k}{s}\right| \leq \frac{1}{2N}$

Plan: Given b we find the rational number with denominator $\leq M$ that is $1/(2N)$-close to b/N.

Expressing this rational number in lowest terms it must be k/s and thus we learn s .

Find: $k', s' \in \mathbb{N}$ such that

$$\begin{aligned} s' &\leq M \\ bs' - k'N &\leq s'/2 \\ bs' - k'N &\geq -s'/2 \end{aligned}$$

Integer linear program

Find: $k', s' \in \mathbb{N}$ such that

$$
\begin{aligned}
s' &\leq M \\
bs' - k'N &\leq s'/2 \\
bs' - k'N &\geq -s'/2
\end{aligned}
$$

This is an integer linear program in two variables and can be solved classically in $O(\log(N))$ time.

This particular case can also be solved efficiently via continued fraction expansion, covered in problem set 2.

Prob. of good b

We have now shown if we find a good b we are done.

Lemma: On measuring $F_N|g_t\rangle$ we find a good b with probability at least $1/(100 \log \log s)$.

This means after repeating the whole process $O(\log \log(s))$ times we will solve the period finding problem.

I will prove this lemma in a separate video.

Summary

Let $f : \mathbb{Z}_N \to [M]$ with the promise there is an s such that

1) $f(0), \ldots, f(s-1)$ are all distinct (injectivity assump.).

2) $f(x) = f(y)$ if $x - y = 0 \bmod s$

3') $N > M^2/2$

There is a quantum algorithm that finds s with const. probability after $O(\log(N)^2 \log\log(N))$ operations and $O(\log\log(N))$ queries to the function f.

Integer Factorization

Integer Factorization

We now apply the period finding algorithm to the problem of finding the factors of an integer M.

This remains the premier example of a potential quantum speedup.

- Best known classical algorithms run in time roughly $\exp(\log(M)^{1/3})$ heuristically or $\exp(\log(M)^{1/2})$ rigorously.

- Shor gives an $\tilde{O}(\log(M)^2)$ time quantum algorithm to find a nontrivial factor of M.

Order Finding

What remains for Shor's factorization algorithm is a purely classical reduction from integer factorization to order finding.

The multiplicative group of integers modulo M is the set $\{x \in [M] : \gcd(x, M) = 1\}$ under the operation of multiplication modulo M.

This group is denoted $\mathbb{Z}_M^*$.

For $x \in \mathbb{Z}_M^*$ its order $\mathrm{ord}_M(x)$ is the least positive s s.t.

$$x^s = 1 \bmod M$$

Order Finding

Order finding: Given x, M with $\gcd(x, M) = 1$ compute $\mathrm{ord}_M(x)$.

Example: $x = 2, M = 21$

$$2^1 = 2 \bmod 21$$
$$2^2 = 4 \bmod 21$$
$$2^3 = 8 \bmod 21$$
$$2^4 = 16 \bmod 21$$
$$2^5 = 11 \bmod 21$$
$$2^6 = 1 \bmod 21$$

Thus $\mathrm{ord}_{21}(2) = 6$.

Order Finding

To map this back to period finding, let

$$f : [M^2] \to [M] \qquad\qquad f(a) = x^a \bmod M$$

Say that $\mathrm{ord}_M(x) = s$.

1) $x^{a_1} = x^{a_1+a_2} \bmod M \implies 1 = x^{a_2} \bmod M$

This implies that $f(0), \ldots, f(s-1)$ are all distinct.

2) $x^{a+s} = x^a \bmod M$ so f is almost periodic.

3) By design there are at least $M \geq s$ periods.

Complexity

Thus we satisfy the conditions to apply the period finding algorithm.

What is the complexity of computing f ?

Using the "square-and-multiply" method and fast modular multiplication we can do this in

$$O((\log(M))^2 \log\log(M) \log\log\log(M))$$

steps. This is the bottleneck of Shor's algorithm!

Reduction

Let's see how to factor if you can do order finding.

The key idea is to find a number x such that

$$x^2 = 1 \bmod M$$

and $x \neq \pm 1 \bmod M$.

Then $(x+1)(x-1) = 0 \bmod M$ and
$x+1, x-1 \neq 0 \bmod M$.

Taking $\gcd(x+1, M)$ gives a nontrivial factor of M.

Example

To go back to our example with $M = 21$

$$8^2 = 1 \bmod 21$$

$$8 \neq \pm 1 \bmod M$$

Thus 8 is a nontrivial square root of $1 \bmod M$.

Can you think of another one?

Example

To go back to our example with $M = 21$

$$8^2 = 1 \bmod 21$$

$$8 \neq \pm 1 \bmod M$$

So

$$(8+1)(8-1) = 0 \bmod 21$$

and each of $7, 9$ share a common factor with 21.

Finding a nontrivial sqrt

Thus it suffices to find a nontrivial square root of $1 \bmod M$.

We will do this via order finding.

Let us look at our example again.

$$2^6 = 1 \bmod 21$$

The order is even! Thus $(2^3)^2 = 1 \bmod 21$ and we have found a square root of $1 \bmod 21$.

Example

The order is even! Thus $(2^3)^2 = 1 \bmod 21$ and we have found a square root of $1 \bmod 21$.

We are guaranteed that $2^3 \neq 1 \bmod 21$ since $\mathrm{ord}_{21}(2) = 6$.

We are lucky in that $2^3 \neq -1 \bmod 21$ thus we have found a nontrivial square root of $1 \bmod 21$.

The next lemma says this is not so unusual.

Lemma: Let M be odd with

$$M = \prod_{i=1}^{k} p_i^{\alpha_i} .$$

If we pick $x \in \mathbb{Z}_M^*$ uniformly at random then with probability at least $1 - 1/2^{k-1}$

1) $s = \mathrm{ord}_M(x)$ will be even.

2) $x^{s/2} \neq \pm 1 \bmod M$

Note: We have to handle the case of prime powers separately.

Reduction

Step 1: Check if M is even or a prime power.

Step 2: Choose a random $0 < x < M$ and compute $\gcd(x, M)$. If this is not 1 then we are done, else continue.

Step 3: Compute the order s of x in $\mathbb{Z}_M^*$.

With prob at least $1/2$ we find a nontrivial square root of $1 \bmod M$ from which we get a factor.

We can repeat (2) and (3) to boost the success probability.

Total running time is $\tilde{O}(\log(M)^2)$.

Proving the "good" lemma

Good Lemma

Now we prove the "good lemma" that we skipped in the presentation of Shor's period finding algorithm.

$$|g_t\rangle = \frac{1}{\sqrt{\ell_t}} \sum_{\substack{x \in \mathbb{Z}_N \\ x \bmod s = t}} |x\rangle$$

Call $b \in [N]$ **good** if $\exists k \in \mathbb{N}$ with $\gcd(s,k) = 1$ s.t.

$$-\frac{s}{2} \leq bs - kN \leq \frac{s}{2}$$

Lemma: On measuring $F_N|g_t\rangle$ we find a good b with probability at least $1/(100 \log\log s)$.

Number of good b

$b \in [N]$ is good if $\exists k \in \mathbb{N}$ with $\gcd(s,k) = 1$ and

$$-\frac{s}{2} \leq bs - kN \leq \frac{s}{2}$$

Let us lower bound the number of good b.

The key idea is instead to count "good" $k \in [s]$.

Claim: The number of good b is at least the number of $k \in [s]$ with $\gcd(k,s) = 1$.

Number of good b

Claim: The number of good b is at least the number of $k \in [s]$ with $\gcd(k, s) = 1$.

Such a k obviously satisfies the gcd condition.

Next we can always write $kN = as + c$ for $c \in \{0, 1, \ldots, s-1\}$.

Then either a or $a+1$ will be good.

The good elements we obtain in this way are distinct, giving the claim.

Number of good b

Claim: The number of good b is at least the number of $k \in [s]$ with $\gcd(k, s) = 1$.

The Euler totient function $\phi(z)$ is the number of integers in $[1, z]$ that are relatively prime to z .

It is known that $\phi(z) \geq \dfrac{z}{4 \log \log(z)}$ for any $z \geq 16$.

Thus the number of good b is at least $\dfrac{s}{4 \log \log(s)}$.

Prob. of seeing good b

Claim: Let b be good. Then

$$|\langle b|F_N|g_t\rangle|^2 \geq \frac{1}{25s} \ .$$

Note: This holds for every $t \in [s]$.

As there are $s/(4\log\log(s))$ many good b overall, this implies the lemma that the prob. of seeing a good b is at least $1/(100\log\log s)$.

Proving the claim

Claim: Let b be good. Then

$$|\langle b|F_N|g_t\rangle|^2 \geq \frac{1}{25s} \ .$$

For this claim the important thing is that

$$-\frac{s}{2} \leq bs - kN \leq \frac{s}{2}$$

for some integer k .

$$\langle b|F_N|g_t\rangle = \frac{1}{\sqrt{N\ell_t}} \sum_{\substack{y\in\mathbb{Z}_N \\ y \bmod s = t}} \omega^{-by}$$

$$= \frac{1}{\sqrt{N\ell_t}} \sum_{j=0}^{\ell_t-1} \omega^{-b(js+t)}$$

$$= \frac{\omega^{-bt}}{\sqrt{N\ell_t}} \sum_{j=0}^{\ell_t-1} \omega^{-bjs}$$

$$= \begin{cases} \omega^{-bt}\sqrt{\frac{\ell_t}{N}} & \text{if } \omega^{-bs} = 1 \\ \frac{\omega^{-bt}}{\sqrt{N\ell_t}} \frac{1-\omega^{-bs\ell_t}}{1-\omega^{-bs}} & \text{otherwise} \end{cases}$$

We are interested in the squared magnitude of this.

Sampling probability

Let's focus on the case where $\omega^{-bs} \neq 1$.

$$\langle b|F_N|g_t\rangle = \frac{\omega^{-bt}}{\sqrt{N\ell_t}} \frac{1-\omega^{-bs\ell_t}}{1-\omega^{-bs}}$$

We have
$$\begin{aligned} |1-\omega^{-q}|^2 &= (1-\omega^{-q})(1-\omega^{q}) \\ &= 2-\omega^{-q}-\omega^{q} \\ &= 2(1-\cos(2\pi q/N)) \end{aligned}$$

Now use the half-angle formula $1-\cos(\theta) = 2\sin^2(\theta/2)$.

$$|1-\omega^{-q}|^2 = (2\sin(\pi q/N))^2$$

Sampling probability

Let's focus on the case where $\omega^{-bs} \neq 1$.

$$\langle b|F_N|g_t\rangle = \frac{\omega^{-bt}}{\sqrt{N\ell_t}} \frac{1-\omega^{-bs\ell_t}}{1-\omega^{-bs}}$$

$$|1-\omega^{-q}|^2 = (2\sin(\pi q/N))^2$$

This gives $|\langle b|F_N|g_t\rangle|^2 = \frac{1}{N\ell_t} \frac{\sin^2(\pi bs\ell_t/N)}{\sin^2(\pi bs/N)}$.

Overview

$$|\langle b|F_N|g_t\rangle|^2 = \frac{1}{N\ell_t}\frac{\sin^2(\pi bs\ell_t/N)}{\sin^2(\pi bs/N)}$$

- Dependence on t is minor.
- Before magnitude was only nonzero when $b = \frac{kN}{s}$.
- Now we want to show magnitude is large when $\exists k \in \mathbb{N}$

$$-\frac{s}{2} \leq bs - kN \leq \frac{s}{2}$$

$$|\langle b|F_N|g_t\rangle|^2 = \frac{1}{N\ell_t}\frac{\sin^2(\pi bs\ell_t/N)}{\sin^2(\pi bs/N)}$$

Now we want to show magnitude is large when $\exists k \in \mathbb{N}$

$$-\frac{s}{2} \leq bs - kN \leq \frac{s}{2}$$

Say $bs = kN + d$ for $-\frac{s}{2} \leq d \leq \frac{s}{2}$.

$$|\sin(\pi bs/N)| = |\sin(\pi(kN+d)/N)| = |\sin(\pi d/N)|$$

$$|\langle b|F_N|g_t\rangle|^2 = \frac{1}{N\ell_t}\frac{\sin^2(\pi bs\ell_t/N)}{\sin^2(\pi bs/N)}$$

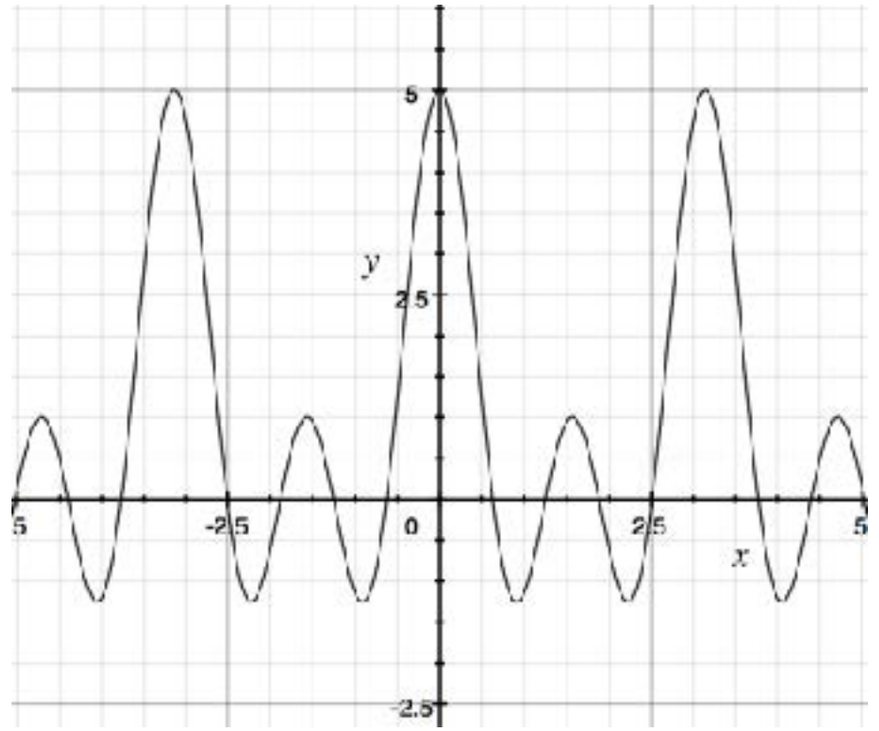
Say $bs = kN + d$ for $-\frac{s}{2} \leq d \leq \frac{s}{2}$.

$$|\langle b|F_N|g_t\rangle|^2 = \frac{1}{N\ell_t}\frac{\sin^2(\pi d\ell_t/N)}{\sin^2(\pi d/N)}$$

Let us lower bound $\frac{\sin(\ell\theta)}{\sin(\theta)}$ for $0 < \theta \leq \frac{3\pi}{4\ell}$.

Bounding the magnitude

$$\lim_{\theta \to 0} \frac{\sin(\ell\theta)}{\sin(\theta)} = \ell \qquad \frac{\sin(\pi)}{\sin(\pi/\ell)} = 0$$



$\frac{\sin(\ell\theta)}{\sin(\theta)}$ **is decreasing for** $\theta \in (0, \pi/\ell)$.

On the interval $(0, 3\pi/(4\ell)]$ **it is minimized at** $\theta = \frac{3\pi}{4\ell}$.

$$\frac{\sin(\ell\theta)}{\sin(\theta)} \geq \frac{\sin(3\pi/4)}{\sin(3\pi/(4\ell))} \geq \frac{\sqrt{2}}{2}\frac{4\ell}{3\pi}$$

using $\sin(x) \leq x$ **for** $x \geq 0$.

Bounding the magnitude

$$|\langle b|F_N|g_t\rangle|^2 = \frac{1}{N\ell_t}\frac{\sin^2(\pi d\ell_t/N)}{\sin^2(\pi d/N)}$$

$$\frac{\pi d\ell_t}{N} \leq \frac{\pi s}{2N}\left(\frac{N}{s}+1\right) = \frac{\pi}{2}+\frac{\pi s}{2N}$$

So for $s \leq \frac{N}{2}$ this will be at most $\frac{3\pi}{4}$.

Applying bound from the previous slide gives

$$|\langle b|F_N|g_t\rangle|^2 \geq \frac{8}{9\pi^2}\frac{\ell_t}{N}$$

$$\geq \frac{8}{9\pi^2}\frac{1}{2s} \geq \frac{1}{25s}$$