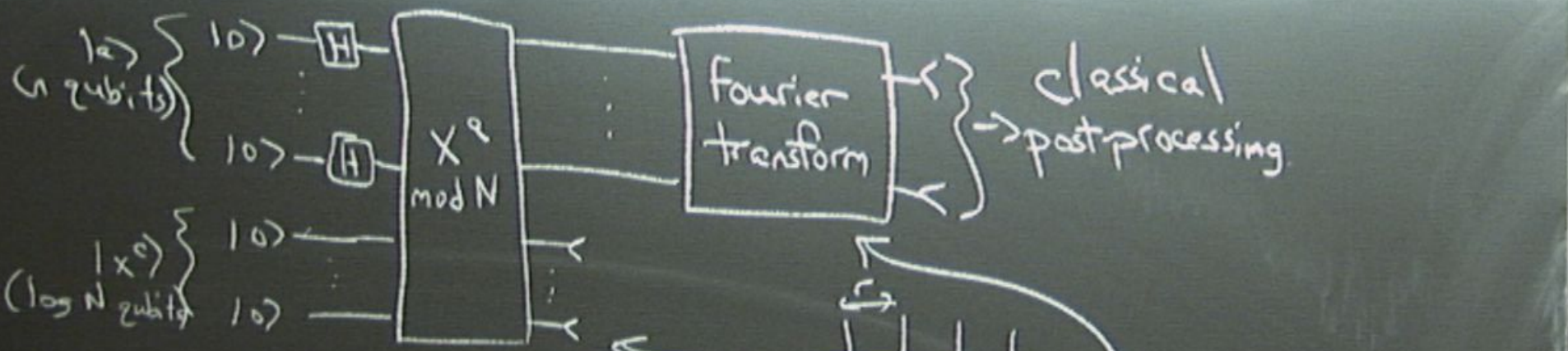
Title: Quantum Information Review - Lecture 8

Date: Feb 24, 2011 09:00 AM

URL: http://pirsa.org/11020043

Abstract:



$|a\rangle$ (n qubits)

$|x^a\rangle$ ($\log N$ qubits)

Find order of x (minimum $r > 0$ s.t. $x^r = 1 \bmod N$)

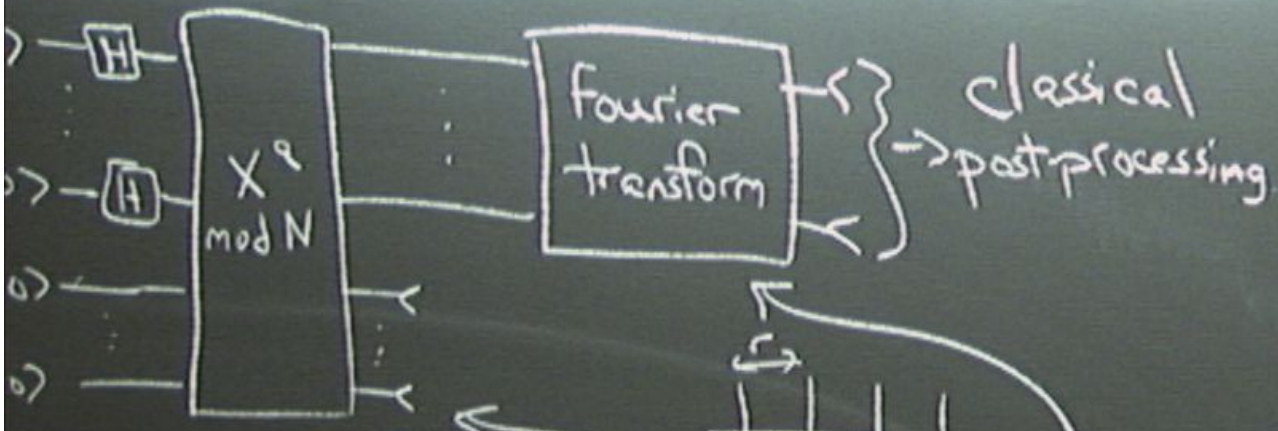
Ideal case: $r \mid 2^n$

$$\sum_a |a\rangle |x^a \bmod N\rangle$$

$$\left(\sum_j |a_0 + jr\rangle\right) |y\rangle$$

$$\sum_c \omega^{a_0 c 2^n/r} |c 2^n/r\rangle$$

Modular



der of x (minimum r : $x^r = 1 \bmod N$)

$\left(\sum_j |a_0 + jr\rangle\right)|y\rangle$

$\sum_c \omega^{a_0 c 2^n/r} |c 2^n/r\rangle$

case: $r \mid 2^n$

$\sum_a |a\rangle|\overbrace{x^a \bmod N}^{y}\rangle$

ourier transform: $\mathcal{F}: |a\rangle \mapsto \sum_b \omega^{ab}|b\rangle$, $\omega = e^{2\pi i/2^n}$

Modular exponentiation

$$|a\rangle|b\rangle \rightarrow |a\rangle|b \cdot x^a\rangle$$

Pre-calculate $x, x^2, x^4, x^8, \ldots, x^{2^{n-1}}$
by repeated squaring.

$$|a\rangle|b\rangle \rightarrow |a\rangle|b\rangle|x^{a_{n-1}}\rangle|(x^2)^{a_{n-2}}\rangle|(x^4)^{a_{n-3}}\rangle \cdots |(x^{2^{n-1}})^{a_0}\rangle$$

$$a = a_{n-1} + 2a_{n-2} + 4a_{n-3} + \cdots + 2^{n-1}a_0$$

Modular exponentiation

$|a\rangle|b\rangle \rightarrow |a\rangle|b \oplus x^a\rangle$

Pre-calculate $x, x^2, x^4, x^8, \ldots, x^{2^{n-1}}$
by repeated squaring.

$|a\rangle|b\rangle \rightarrow |a\rangle|b\rangle|x^{a_{n-1}}\rangle|(x^2)^{a_{n-2}}\rangle|(x^4)^{a_{n-3}}\rangle \ldots |(x^{2^{n-1}})^{a_0}\rangle$

$\rightarrow |a\rangle|b \oplus x^{a_{n-1}} x^{2a_{n-2}} x^{4a_{n-3}} \ldots x^{2^{n-1}a_0}\rangle|0\rangle \ldots |0\rangle = |a\rangle|b \oplus x^a\rangle|0\rangle \ldots |0\rangle$

$a = a_{n-1} + 2a_{n-2} + 4a_{n-3} + \ldots + 2^{n-1}a_0$

Modular exponentiation

$|a\rangle|b\rangle \rightarrow |a\rangle|b \oplus x^a\rangle$

Pre-calculate $x, x^2, x^4, x^8, \ldots, x^{2^{n-1}} \mod N$ each mult takes $(\log N)^2$
by repeated squaring.

$|a\rangle|b\rangle \rightarrow |a\rangle|b\rangle|x^{a_{n-1}}\rangle|(x^2)^{a_{n-2}}\rangle|(x^4)^{a_{n-3}}\rangle \ldots |(x^{2^{n-1}})^{a_0}\rangle$

$\rightarrow |a\rangle|b \oplus x^{a_{n-1}} x^{2a_{n-2}} x^{4a_{n-3}} \ldots x^{2^{n-1}a_0}\rangle|0\rangle \ldots |0\rangle = |a\rangle|b \oplus x^a\rangle|0\rangle \ldots |0\rangle$

$a = a_{n-1} + 2a_{n-2} + 4a_{n-3} + \ldots + 2^{n-1}a_0$

Modular exponentiation

$|a\rangle|b\rangle \to |a\rangle|b \oplus x^a\rangle$

Pre-calculate $x, x^2, x^4, x^8, \ldots, x^{2^{n-1}} \mod N$ by repeated squaring.

- each mult takes $O((\log N)^2)$
- n mult $\Rightarrow O(n(\log N)^2)$

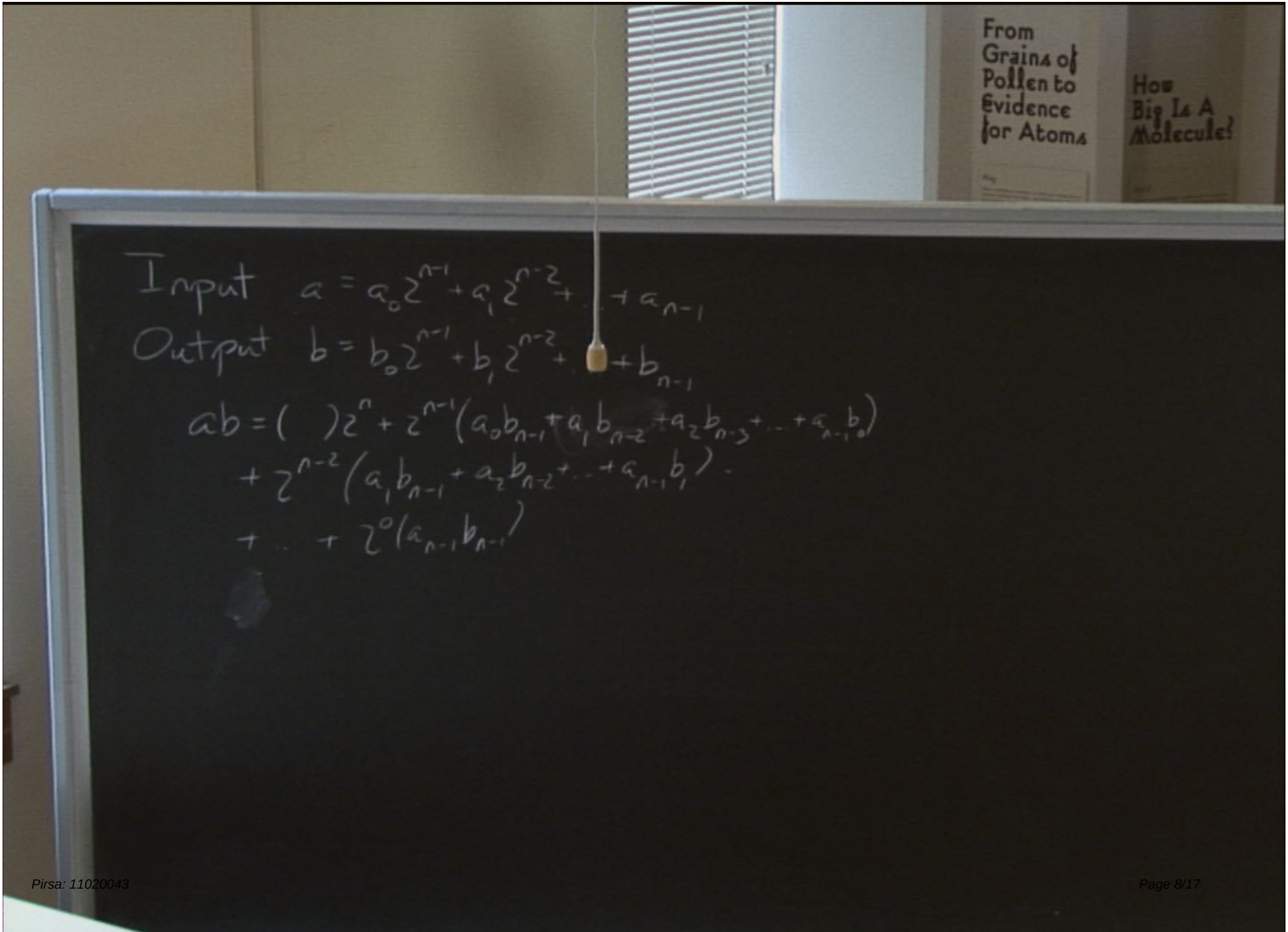
$|a\rangle|b\rangle \to |a\rangle|b\rangle|x^{a_{n-1}}\rangle|(x^2)^{a_{n-2}}\rangle|(x^4)^{a_{n-3}}\rangle \ldots |(x^{2^{n-1}})^{a_0}\rangle$

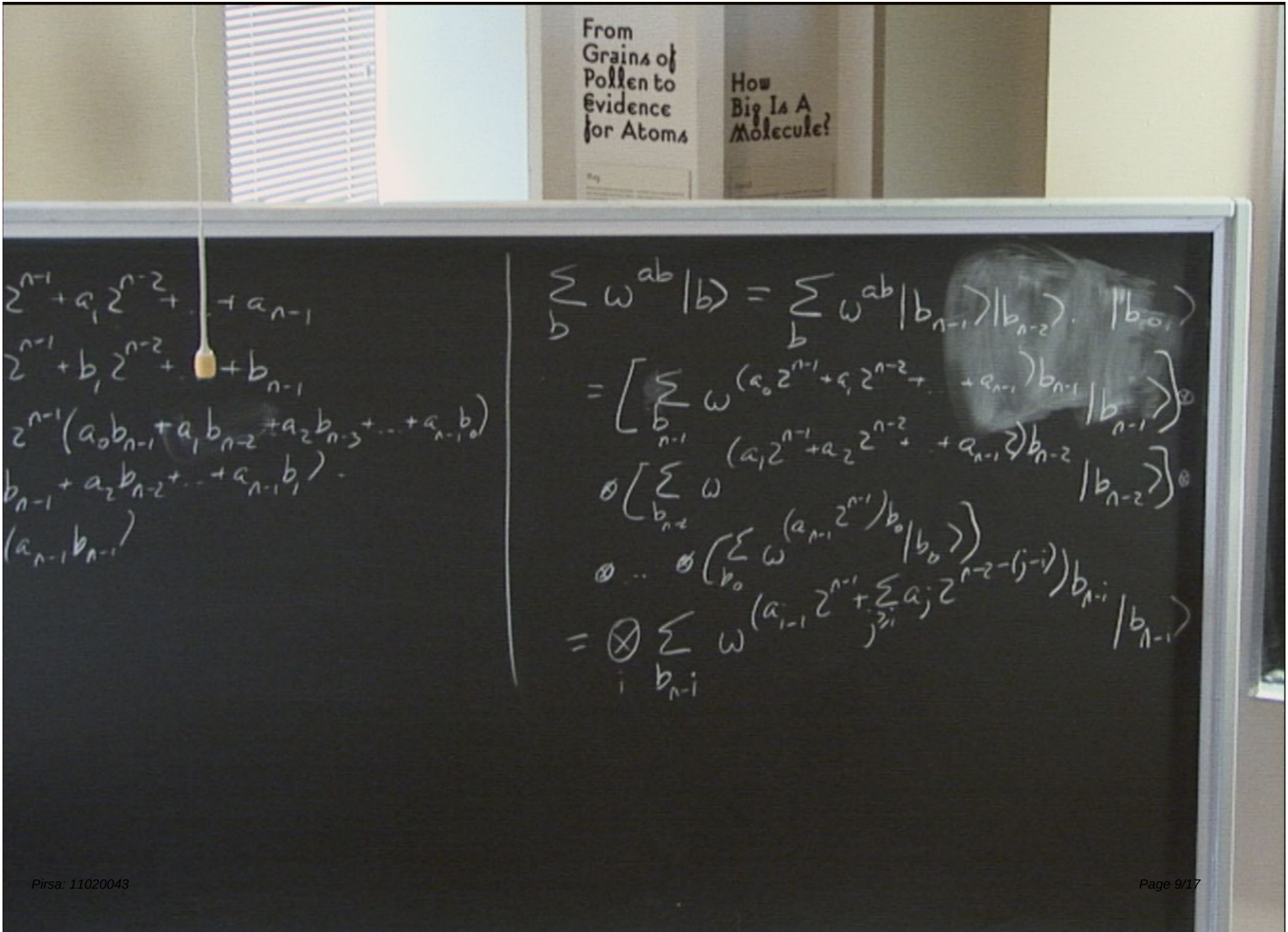
$\to |a\rangle|b \oplus x^{a_{n-1}} x^{2a_{n-2}} x^{4a_{n-3}} \ldots x^{2^{n-1}a_0}\rangle|0\rangle \ldots |0\rangle = |a\rangle|b \oplus x^a\rangle|0\rangle \ldots |0\rangle$

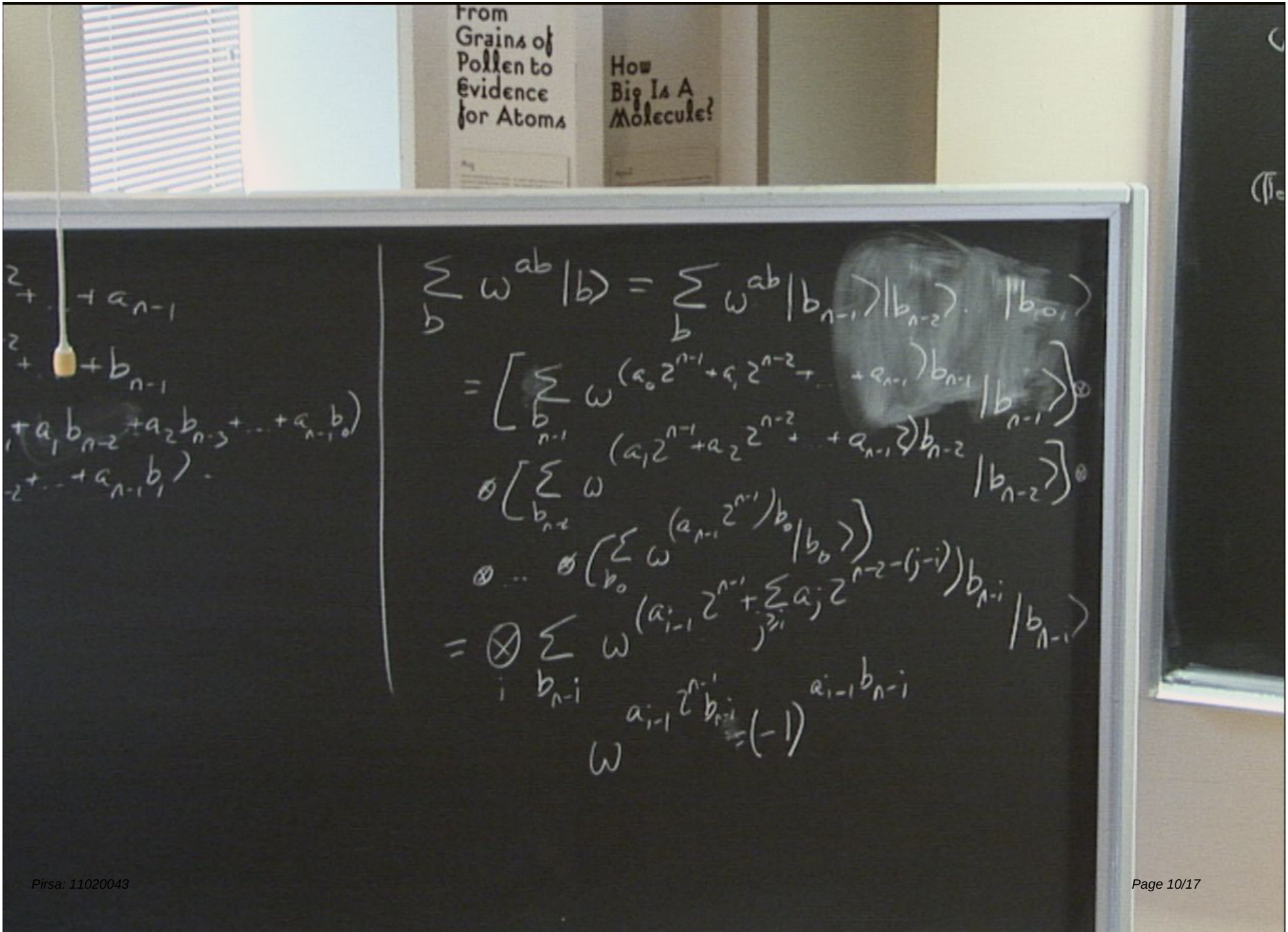
$a = a_{n-1} + 2a_{n-2} + 4a_{n-3} + \ldots + 2^{n-1}a_0$

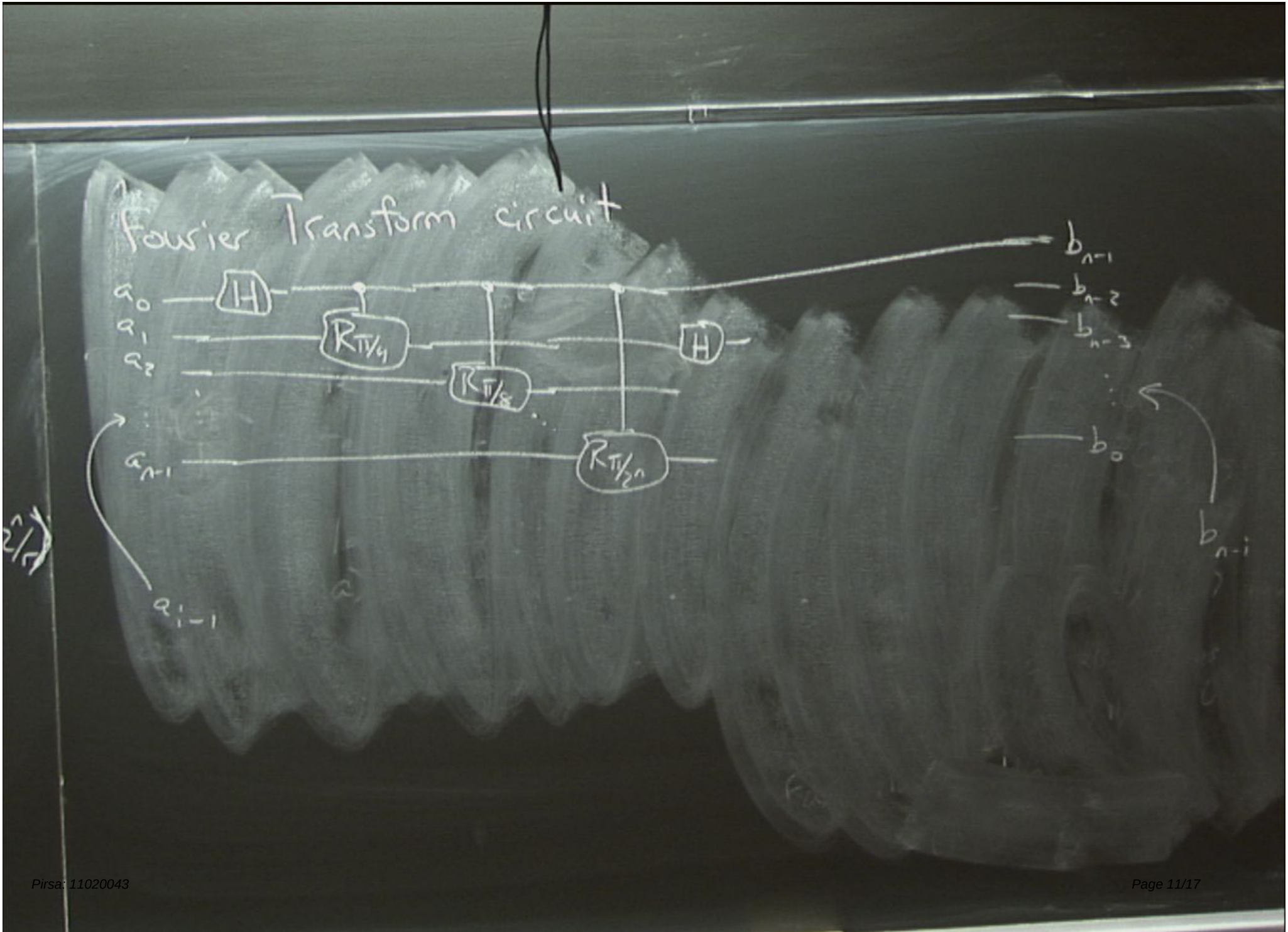
This step also takes $O(n(\log N)^2) \approx O(n^3)$

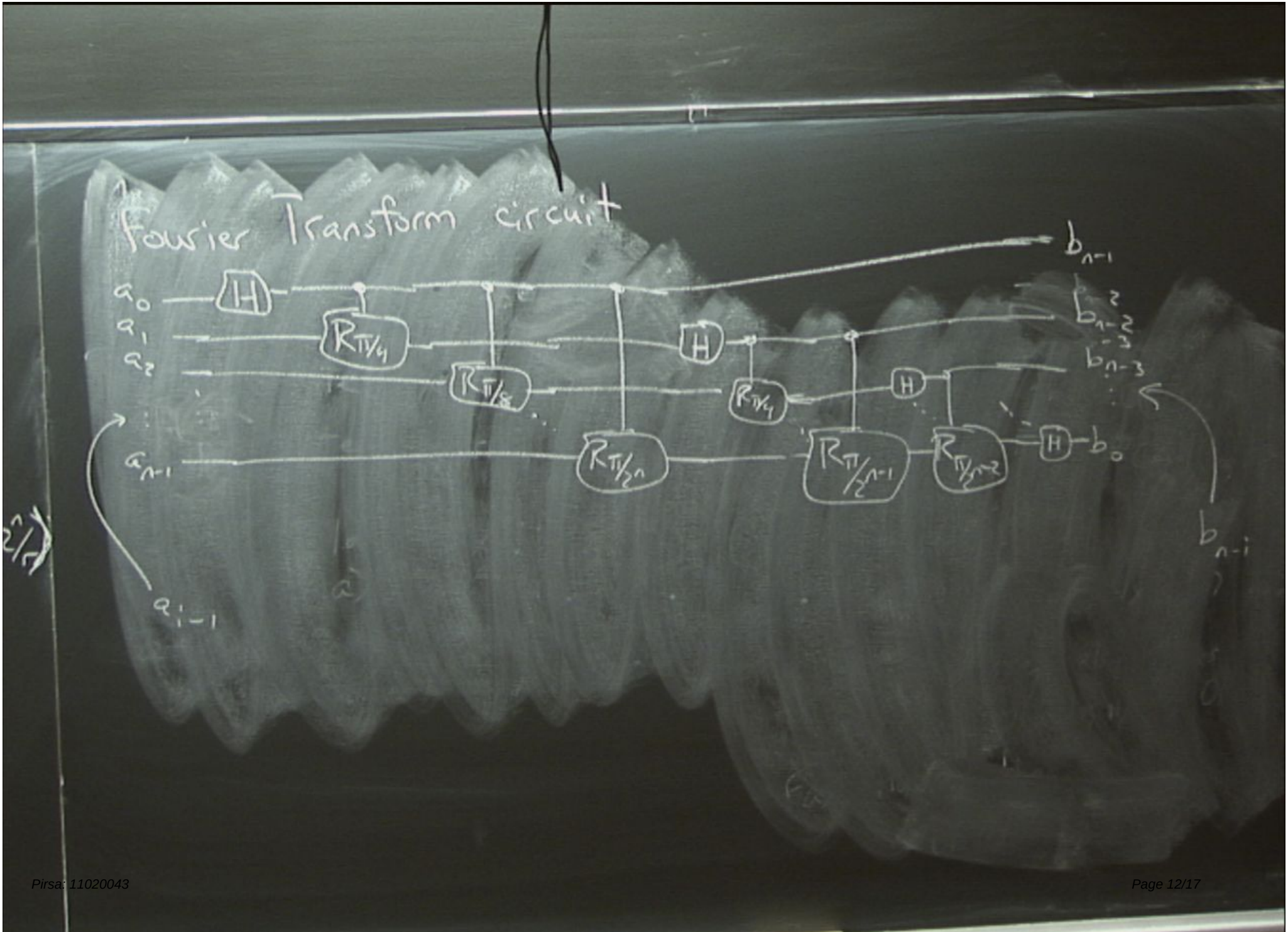
Fast multiplication $O(n^2 \log n \log\log n)$


From Grains of Pollen to Evidence for Atoms
How Big Is A Molecule?
Input $a = a_0 z^{n-1} + a_1 z^{n-2} + \dots + a_{n-1}$
Output $b = b_0 z^{n-1} + b_1 z^{n-2} + \dots + b_{n-1}$
$ab = (\ )z^n + z^{n-1}(a_0 b_{n-1} + a_1 b_{n-2} + a_2 b_{n-3} + \dots + a_{n-1} b_0)$
$+ z^{n-2}(a_1 b_{n-1} + a_2 b_{n-2} + \dots + a_{n-1} b_1)$
$+ \dots + z^0(a_{n-1} b_{n-1})$

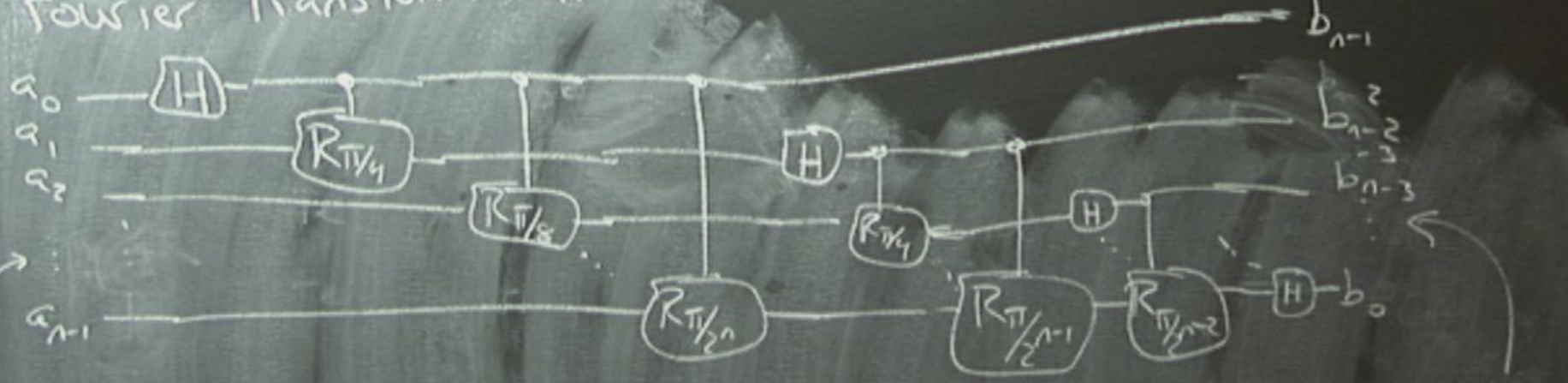

From Grains of Pollen to Evidence for Atoms
How Big Is A Molecule?
$z^{n-1} + a_1 z^{n-2} + \dots + a_{n-1}$
$z^{n-1} + b_1 z^{n-2} + \dots + b_{n-1}$
$z^{n-1}(a_0 b_{n-1} + a_1 b_{n-2} + a_2 b_{n-3} + \dots + a_{n-1} b_0)$
$b_{n-1} + a_2 b_{n-2} + \dots + a_{n-1} b_1)$
$(a_{n-1} b_{n-1})$
$\sum_b \omega^{ab} |b\rangle = \sum_b \omega^{ab} |b_{n-1}\rangle |b_{n-2}\rangle \dots |b_0\rangle$
$= \left[\sum_{b_{n-1}} \omega^{(a_0 z^{n-1} + a_1 z^{n-2} + \dots + a_{n-1}) b_{n-1}} |b_{n-1}\rangle \right] \otimes$
$\otimes \left[\sum_{b_{n-2}} \omega^{(a_1 z^{n-1} + a_2 z^{n-2} + \dots + a_{n-1} z) b_{n-2}} |b_{n-2}\rangle \right] \otimes$
$\otimes \dots \otimes \left(\sum_{b_0} \omega^{(a_{n-1} z^{n-1}) b_0} |b_0\rangle \right)$
$= \bigotimes_i \sum_{b_{n-i}} \omega^{(a_{i-1} z^{n-1} + \sum_{j \geq i} a_j z^{n-2-(j-i)}) b_{n-i}} |b_{n-i}\rangle$


From Grains of Pollen to Evidence for Atoms
How Big Is A Molecule?


Fourier Transform circuit
a_0
a_1
a_2
a_{n-1}
H
$R_{\pi/4}$
$R_{\pi/8}$
$R_{\pi/2^n}$
H
b_{n-1}
b_{n-2}
b_{n-3}
b_0
b_{n-i}
a_{i-1}


Fourier Transform circuit
a_0
a_1
a_2
a_{n-1}
a_{i-1}
H
$R_{\pi/4}$
$R_{\pi/8}$
$R_{\pi/2^n}$
$R_{\pi/2^{n-1}}$
$R_{\pi/2^{n-2}}$
b_{n-1}
b_{n-2}
b_{n-3}
b_0
b_{n-i}

Fourier Transform circuit



gates $= n + (n-1) + (n-2) + \ldots + 1 = \binom{n+1}{2}$

$= O(n^2)$

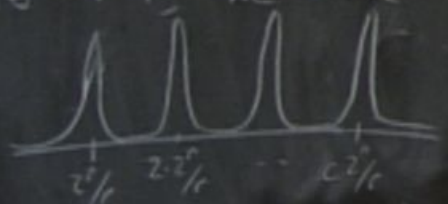
modular exponentiation $O(n^2 \log n \log\log n)$

From Grains of Pollen to Evidence for Atoms

How Big Is A Molecule?

Non-ideal $r \neq 2^n$

After FT we have



Peaks get narrow enough when $2^n \sim N^2 \Leftrightarrow n \approx 2 \log N$

Continued fractions:

$$\frac{c}{r} \approx \frac{b}{2^n} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cfrac{1}{\ddots + \cfrac{1}{c_s}}}}}$$

For rational $\frac{b}{2^n}$, finite # of terms

It turns out $\frac{c}{r}$ is given exactly as a partial sum

$$\frac{c}{r} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{\ddots + \cfrac{1}{c_r}}}}$$

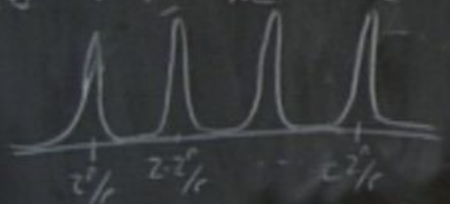
$m < l$

From Grains of Pollen to Evidence for Atoms

How Big Is A Molecule?

non-ideal $r \nmid 2^n$

After FT, we have



Peaks get narrow enough when $2^n \sim N^2 \Leftrightarrow n \approx 2 \log N$

Continued fractions:

$$\frac{c}{r} \approx \frac{b}{2^n} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots \frac{1}{c_s}}}}$$

For rational $\#$, finite $\#$ of terms

It turns out $\frac{c}{r}$ is given exactly as a partial sum

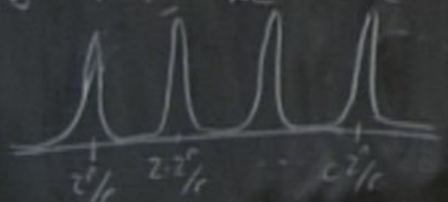
$$\frac{c}{r} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cdots \frac{1}{c_r}}}$$

From Grains of Pollen to Evidence for Atoms

How Big Is A Molecule?

non-ideal $r \nmid 2^n$

After FT we have



Peaks get narrow enough when $2^n \sim N^2 \Leftrightarrow n \approx 2 \log N$

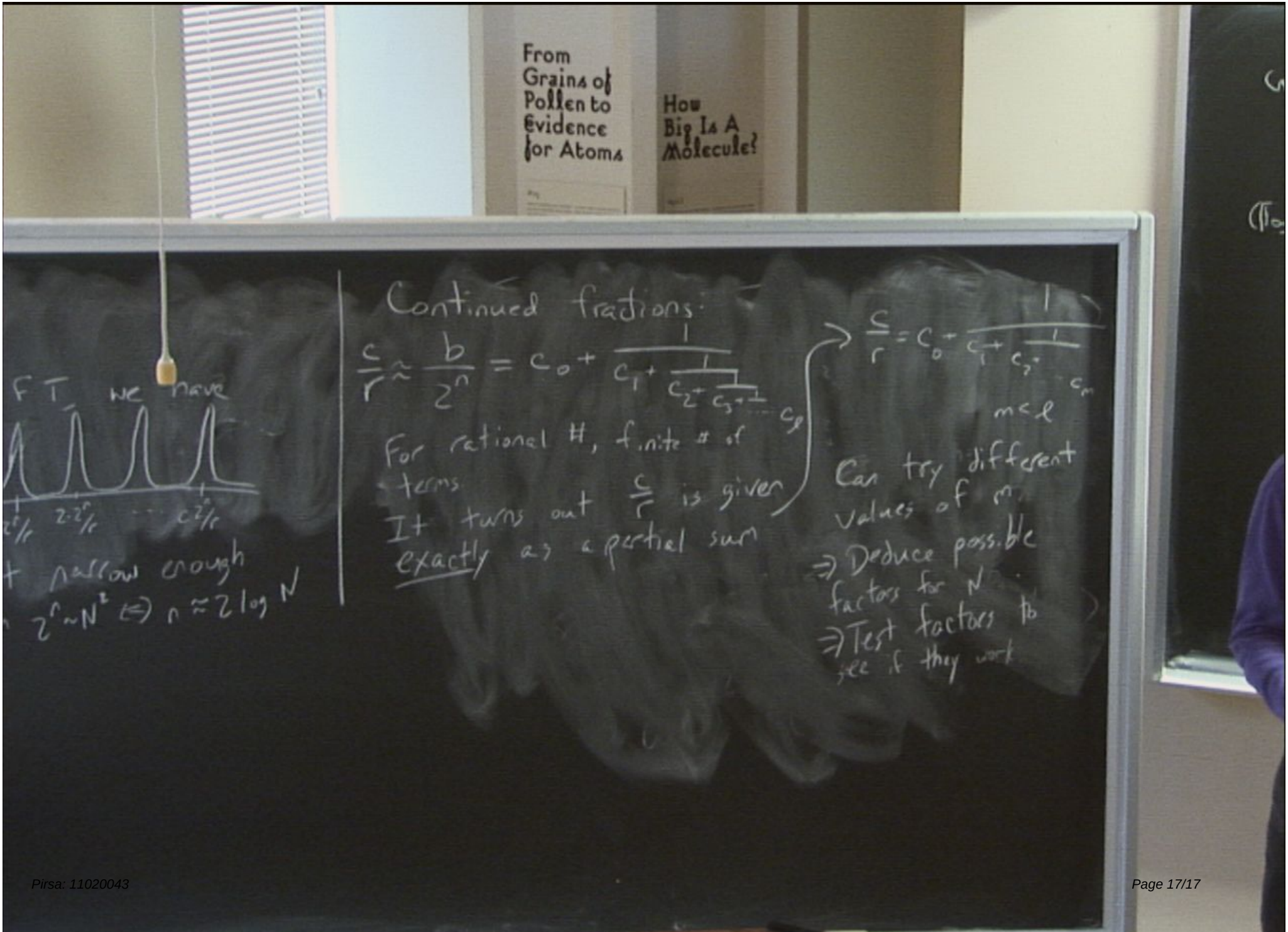
Continued fractions:

$$\frac{c}{r} \approx \frac{b}{2^n} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots \; c_s}}}$$

For rational $\#$, finite $\#$ of terms

It turns out $\frac{c}{r}$ is given exactly as a partial sum

$$\frac{c}{r} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cdots \; c_m}} \qquad m < \ell$$


From Grains of Pollen to Evidence for Atoms
How Big Is A Molecule?
FT we have
narrow enough
$2^n \sim N^2 \Leftrightarrow n \approx 2 \log N$
Continued fractions:
$\frac{c}{r} \approx \frac{b}{2^n} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots \frac{1}{c_\ell}}}}$
For rational θ, finite # of terms
It turns out $\frac{c}{r}$ is given exactly as a partial sum
$\frac{c}{r} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cdots \frac{1}{c_m}}}$
$m < \ell$
Can try different values of m.
⇒ Deduce possible factors for N
⇒ Test factors to see if they work