Title: PSI 2018/2019 - Quantum Information Review - Lecture 9

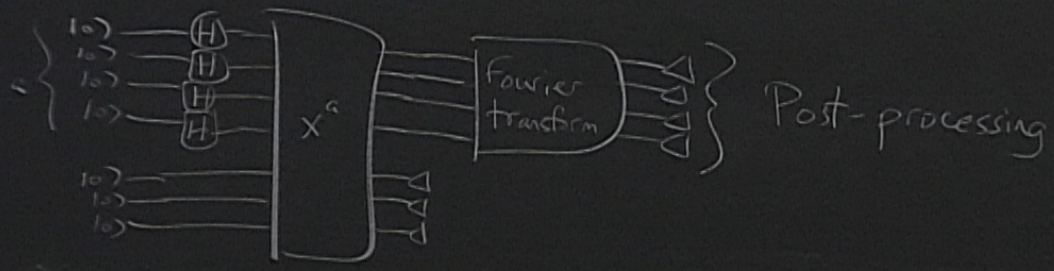
Speakers: Daniel Gottesman

Collection: PSI 2018/2019 - Quantum Information Review (Gottesman)

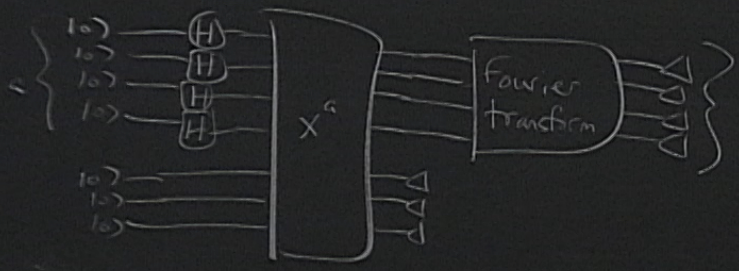
Date: March 14, 2019 - 11:30 AM

URL: http://pirsa.org/19030046

Shor's algorithm:



Shor's algorithm.

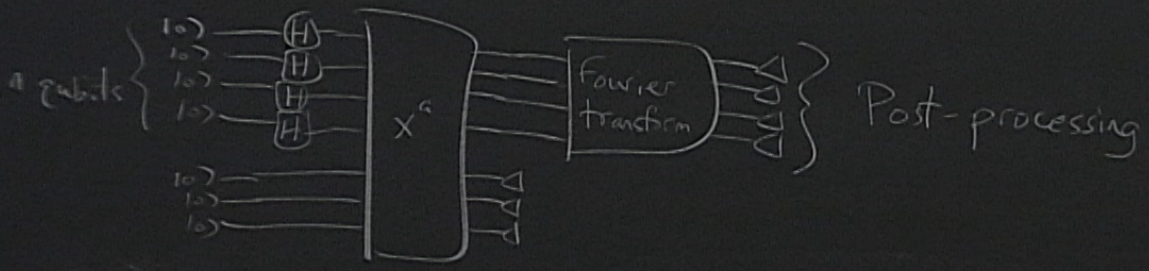



Post-processing

Find order $r$ of $x$, i.e

minimum $r$ s.t. $x^r = 1 \bmod N$.

# Shor's algorithm.




Find order $r$ of $x$, i.e

minimum $r$ s.t. $x^r = 1 \bmod N$.

$$a = \sum_i a_i 2^{n-1-i}$$

Classically pre-compute $x, x^2, x^4, x^8, \ldots x^{2^{n-1}} \pmod N$

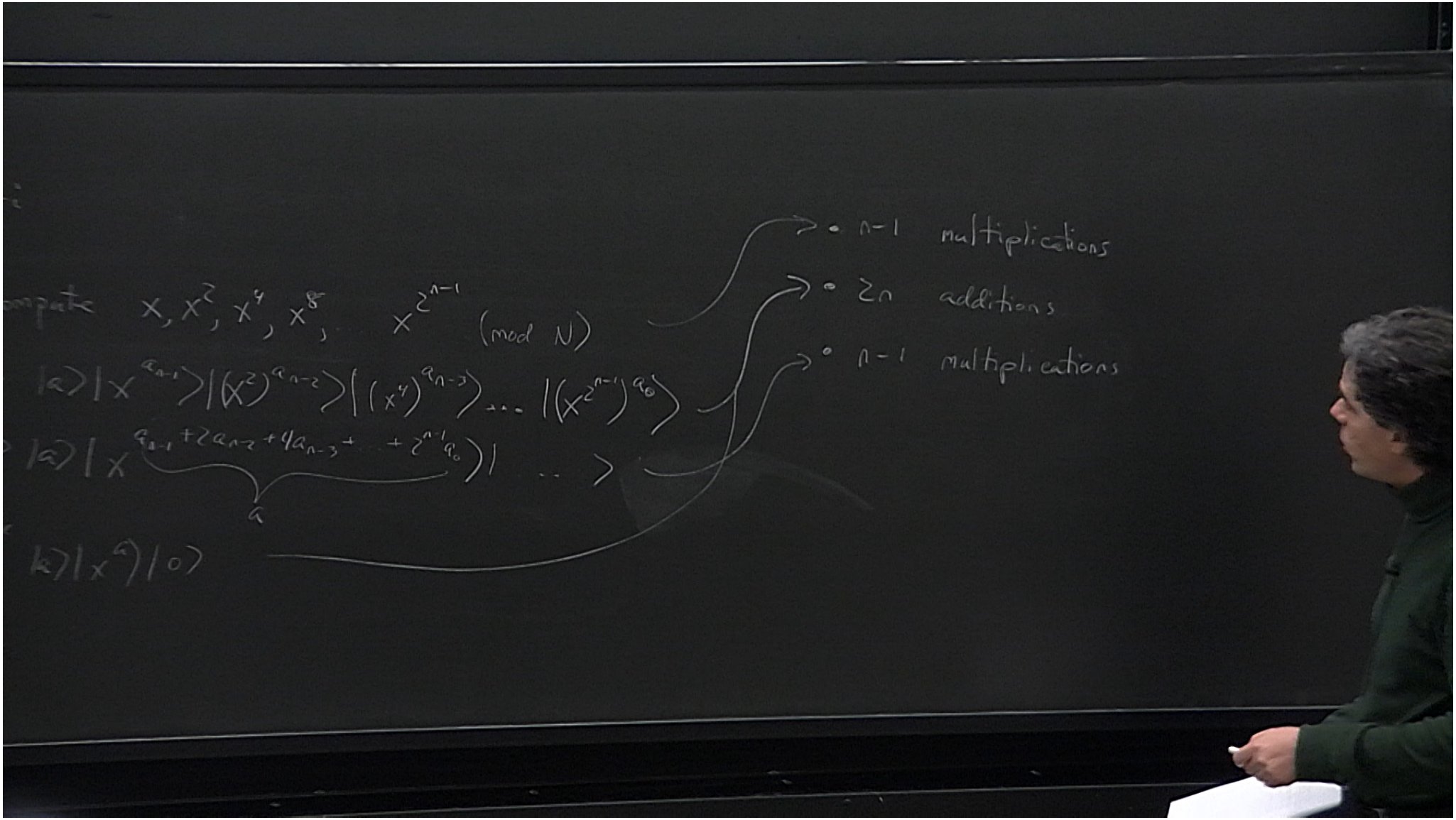
$$|a\rangle|0\rangle \longmapsto |a\rangle|x^{a_{n-1}}\rangle|(x^2)^{a_{n-2}}\rangle|(x^4)^{a_{n-3}}\rangle \cdots |(x^{2^{n-1}})^{a_0}\rangle$$

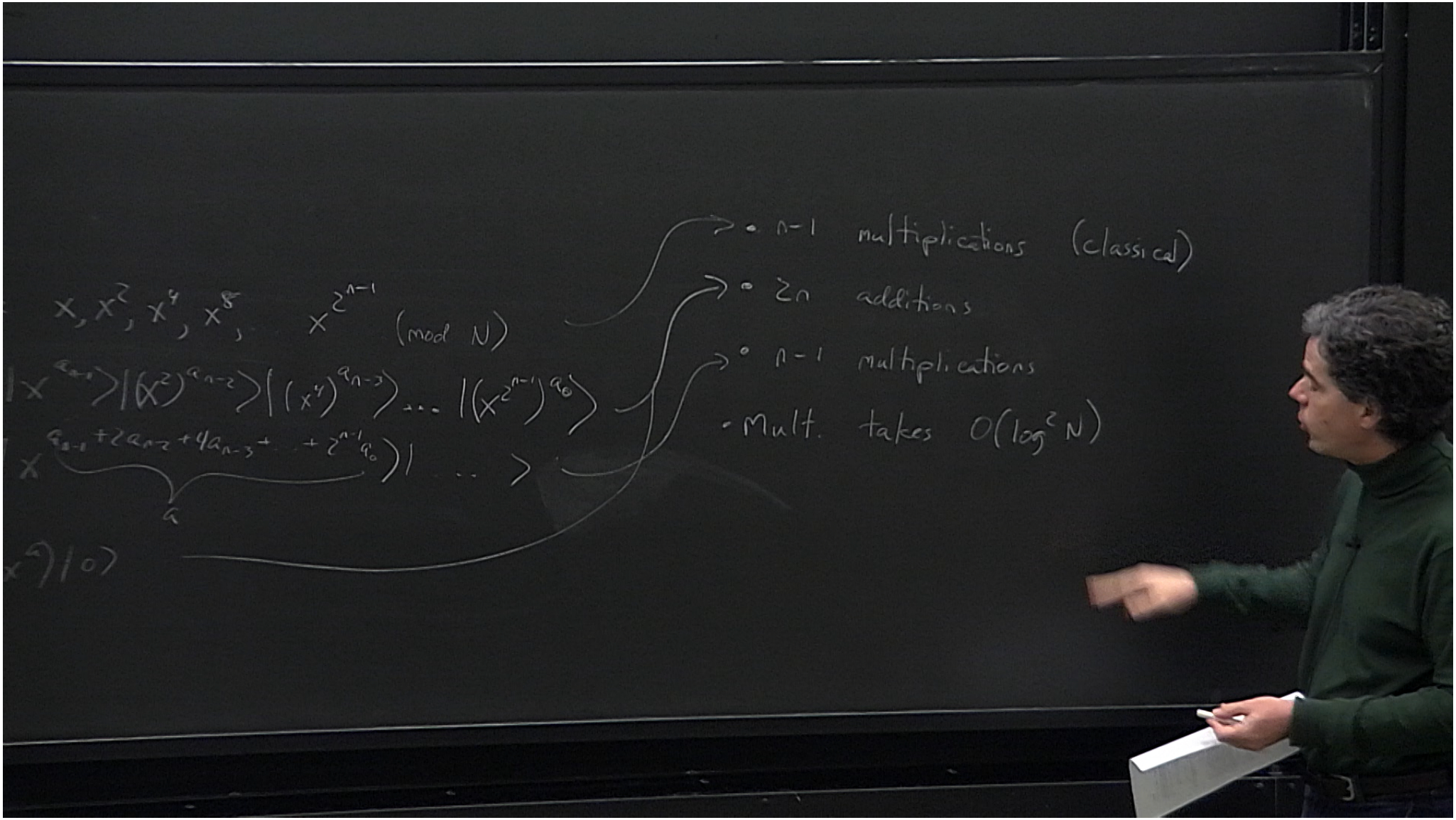
$$\longmapsto |a\rangle|x^{\overbrace{a_{n-1}+2a_{n-2}+4a_{n-3}+\cdots+2^{n-1}a_0}^{a}}\rangle|\ldots\rangle$$

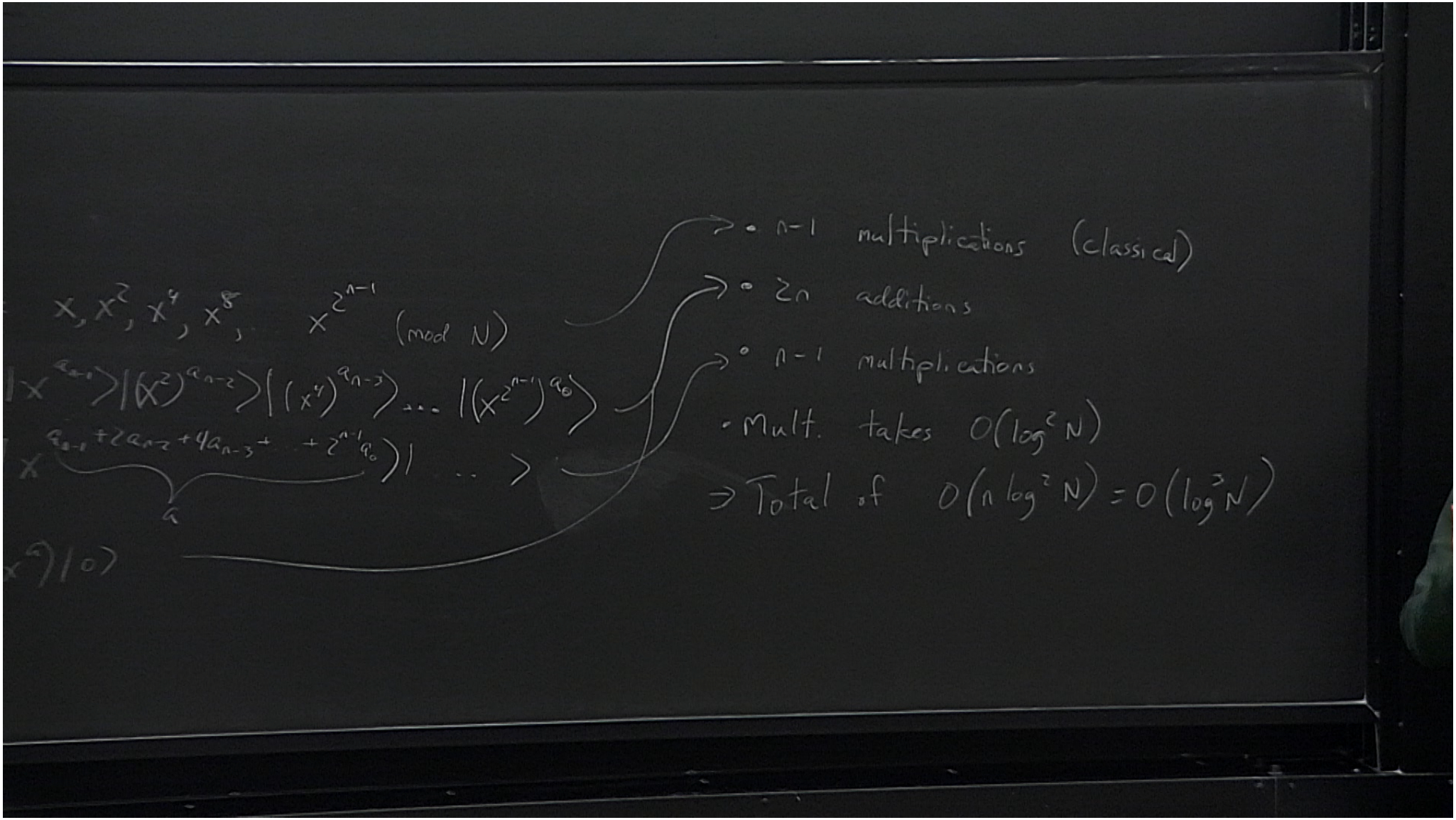
uncompute

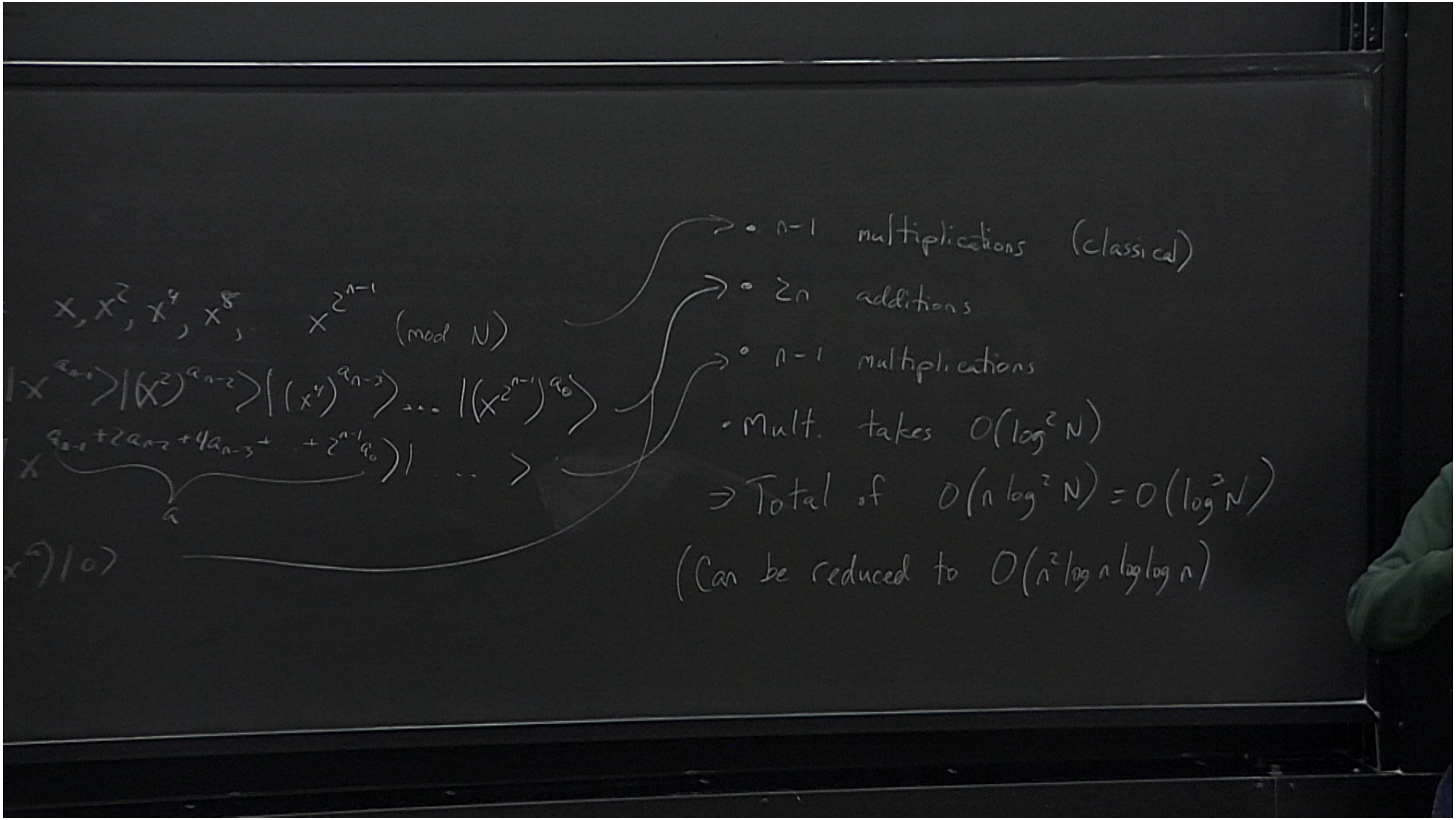
$$\longmapsto |a\rangle|x^a\rangle|0\rangle$$

scratch bits


Compute $x, x^2, x^4, x^8, \ldots x^{2^{n-1}} \pmod N$
a) $|x^{q_{n-1}}\rangle|(x^2)^{q_{n-2}}\rangle|(x^4)^{q_{n-3}}\rangle \ldots |(x^{2^{n-1}})^{q_0}\rangle$
a) $|x^{q_{n-1}+2q_{n-2}+4q_{n-3}+\ldots+2^{n-1}q_0}\rangle|\ldots\rangle$
a
b) $|x^q\rangle|0\rangle$
$n-1$ multiplications
$2n$ additions
$n-1$ multiplications


$x, x^2, x^4, x^8, \ldots x^{2^{n-1}} \pmod N$
$|x^{a_{n-1}}\rangle |(x^2)^{a_{n-2}}\rangle |(x^4)^{a_{n-3}}\rangle \ldots |(x^{2^{n-1}})^{a_0}\rangle$
$x^{a_{n-1}+2a_{n-2}+4a_{n-3}+\ldots+2^{n-1}a_0}$
$a$
$|q\rangle|0\rangle$
$n-1$ multiplications (classical)
$2n$ additions
$n-1$ multiplications
Mult. takes $O(\log^2 N)$


$x, x^2, x^4, x^8, \ldots x^{2^{n-1}} \pmod N$
$|x^{a_{n-1}}\rangle |(x^2)^{a_{n-2}}\rangle |(x^4)^{a_{n-3}}\rangle \ldots |(x^{2^{n-1}})^{a_0}\rangle$
$x^{a_{n-1}+2a_{n-2}+4a_{n-3}+\ldots+2^{n-1}a_0}$
$a$
$|a\rangle|0\rangle$
$\sim n-1$ multiplications (classical)
$\sim 2n$ additions
$\sim n-1$ multiplications
• Mult. takes $O(\log^2 N)$
$\Rightarrow$ Total of $O(n \log^2 N) = O(\log^3 N)$


$x, x^2, x^4, x^8, \ldots x^{2^{n-1}} \pmod N$
$|x^{a_{n-1}}\rangle |(x^2)^{a_{n-2}}\rangle |(x^4)^{a_{n-3}}\rangle \ldots |(x^{2^{n-1}})^{a_0}\rangle$
$x^{a_{n-1}+2a_{n-2}+4a_{n-3}+\ldots+2^{n-1}a_0}$
$a$
$\ldots\rangle$
$\ldots|0\rangle$
$n-1$ multiplications (classical)
$2n$ additions
$n-1$ multiplications
Mult. takes $O(\log^2 N)$
$\Rightarrow$ Total of $O(n\log^2 N) = O(\log^3 N)$
(Can be reduced to $O(n^2 \log n \log\log n)$

Fourier transform:

$$\mathcal{F}\,|a\rangle = \sum_b \omega^{ab}\,|b\rangle$$

$$a = a_0 z^{n-1} + a_1 z^{n-2} + a_2 z^{n-3} + \cdots + a_{n-1}$$

$$b = b_0 z^{n-1} + b_1 z^{n-2} + b_2 z^{n-3} + \cdots + b_{n-1}$$

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

$$ab = z^n(\ldots) + z^{n-1}(\ldots)$$

Fourier transform:

$$\mathcal{F}\,|a\rangle = \sum_b \omega^{ab}\,|b\rangle$$

$$a = a_0 z^{n-1} + a_1 z^{n-2} + a_2 z^{n-3} + \cdots + a_{n-1}$$

$$b = b_0 z^{n-1} + b_1 z^{n-2} + b_2 z^{n-3} + \cdots + b_{n-1}$$

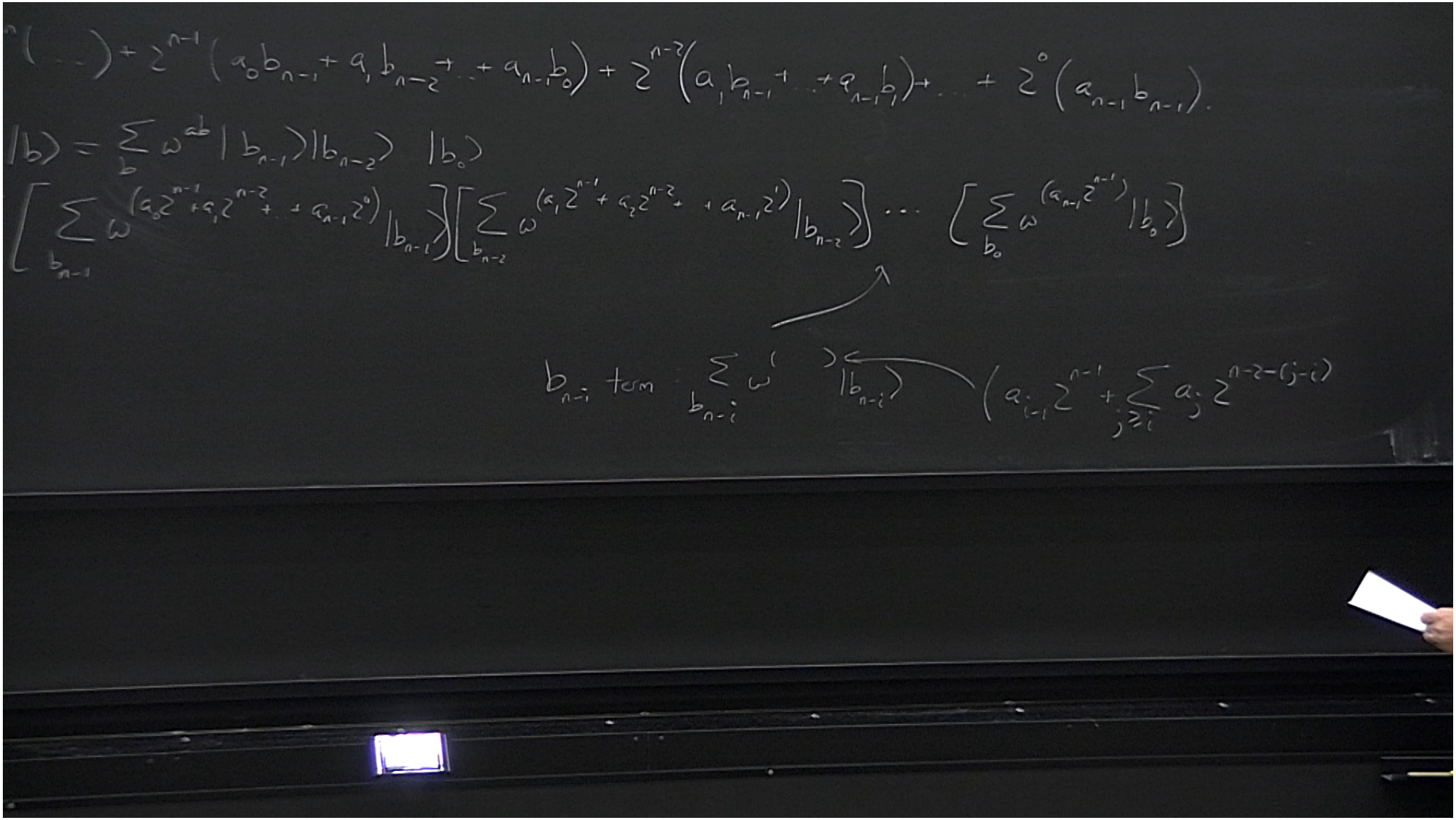
$$\omega = e^{2\pi i/z^n}$$

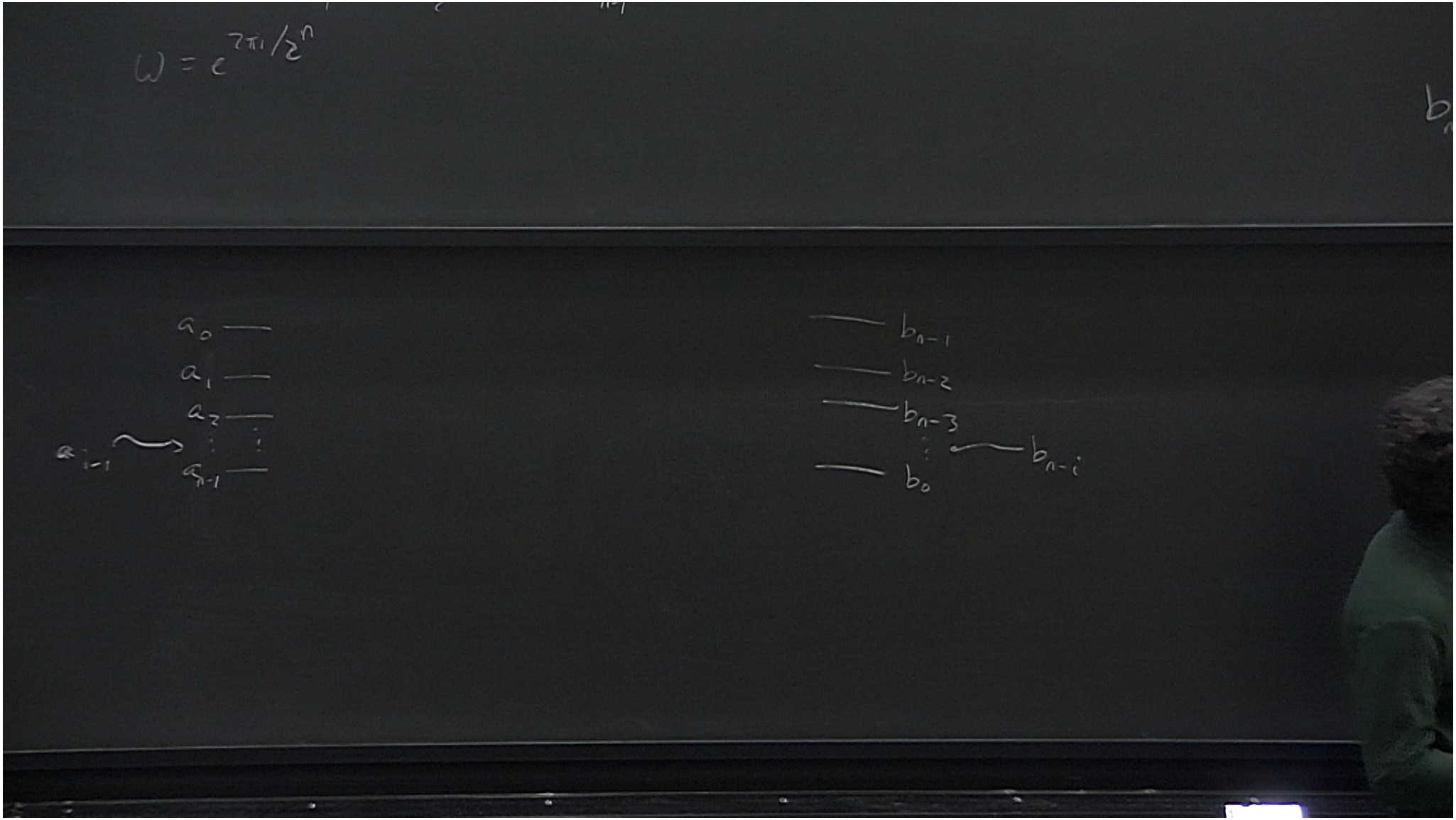
$$ab = z^n(\ldots) + z^{n-1}(\ldots)$$

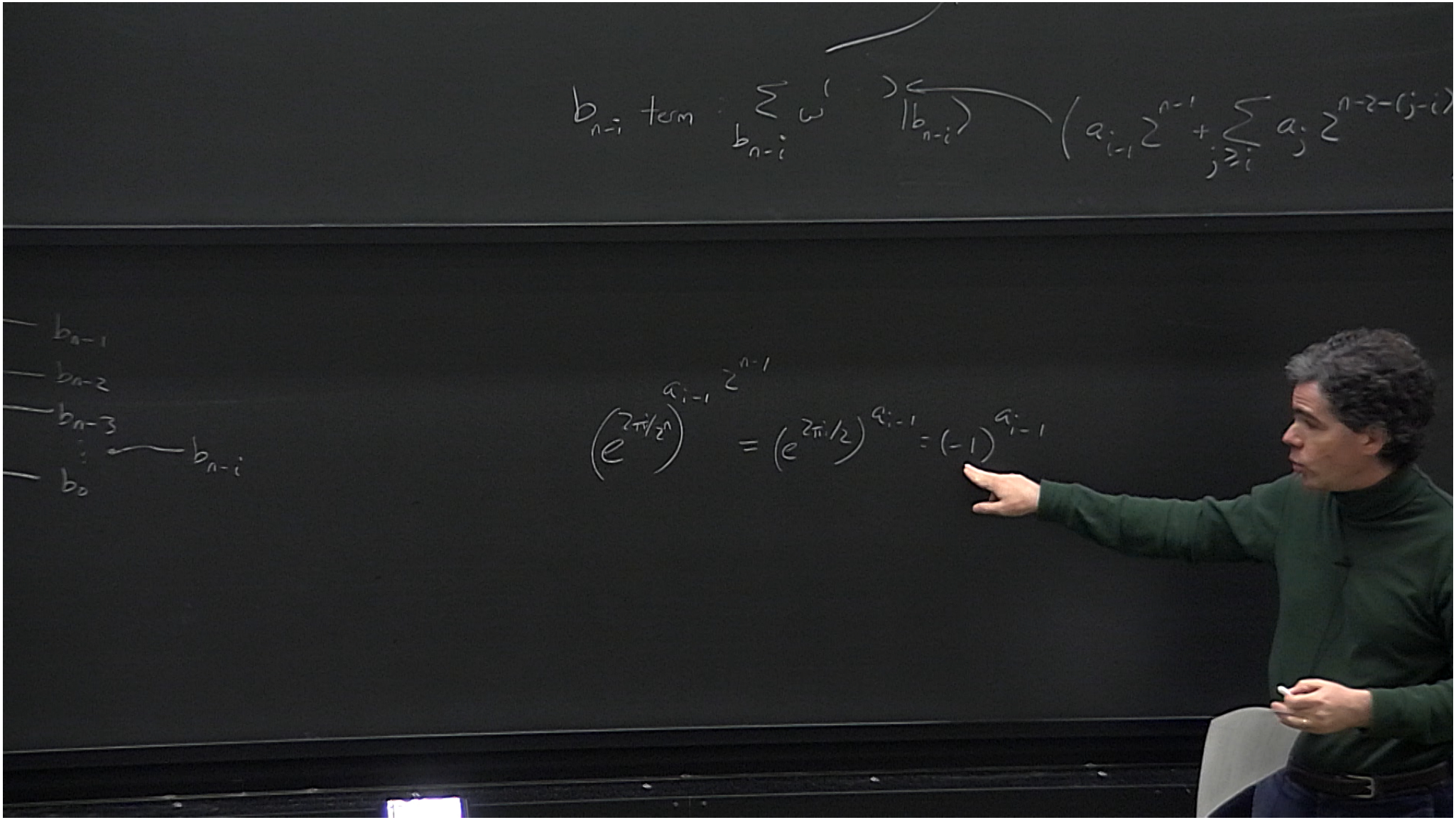
$$ab = z^n(\ldots) + z^{n-1}\left(a_0 b_{n-1} + a_1 b_{n-2} + \ldots + a_{n-1} b_0\right) + z^{n-2}\left(a_1 b_{n-1} + \ldots + a_{n-1} b_1\right) + \ldots + z^0\left(a_{n-1} b_{n-1}\right).$$

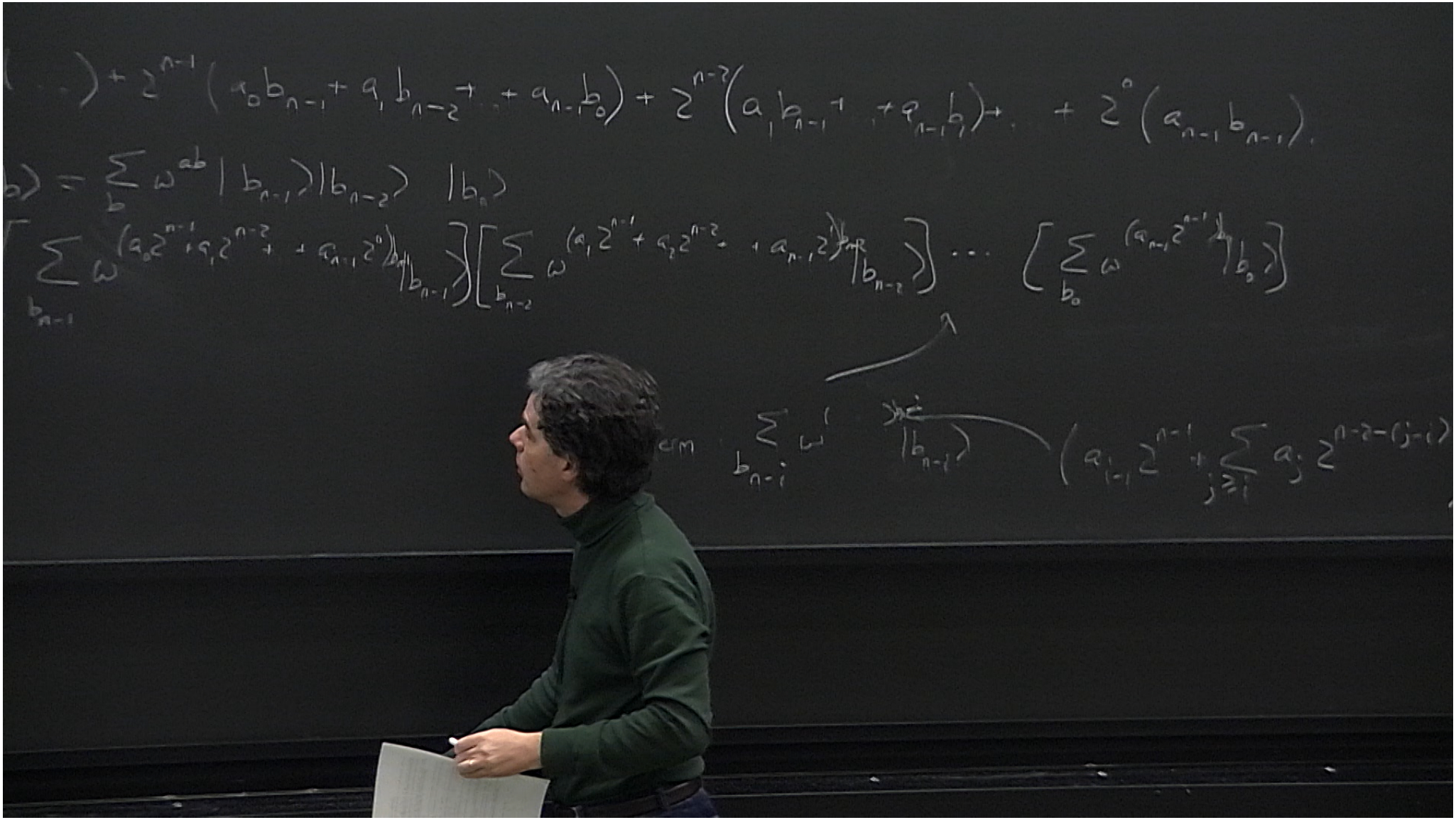
$$\sum_b \omega^{ab} |b\rangle = \sum_b \omega^{ab} |b_{n-1}\rangle |b_{n-2}\rangle \ldots |b_0\rangle$$

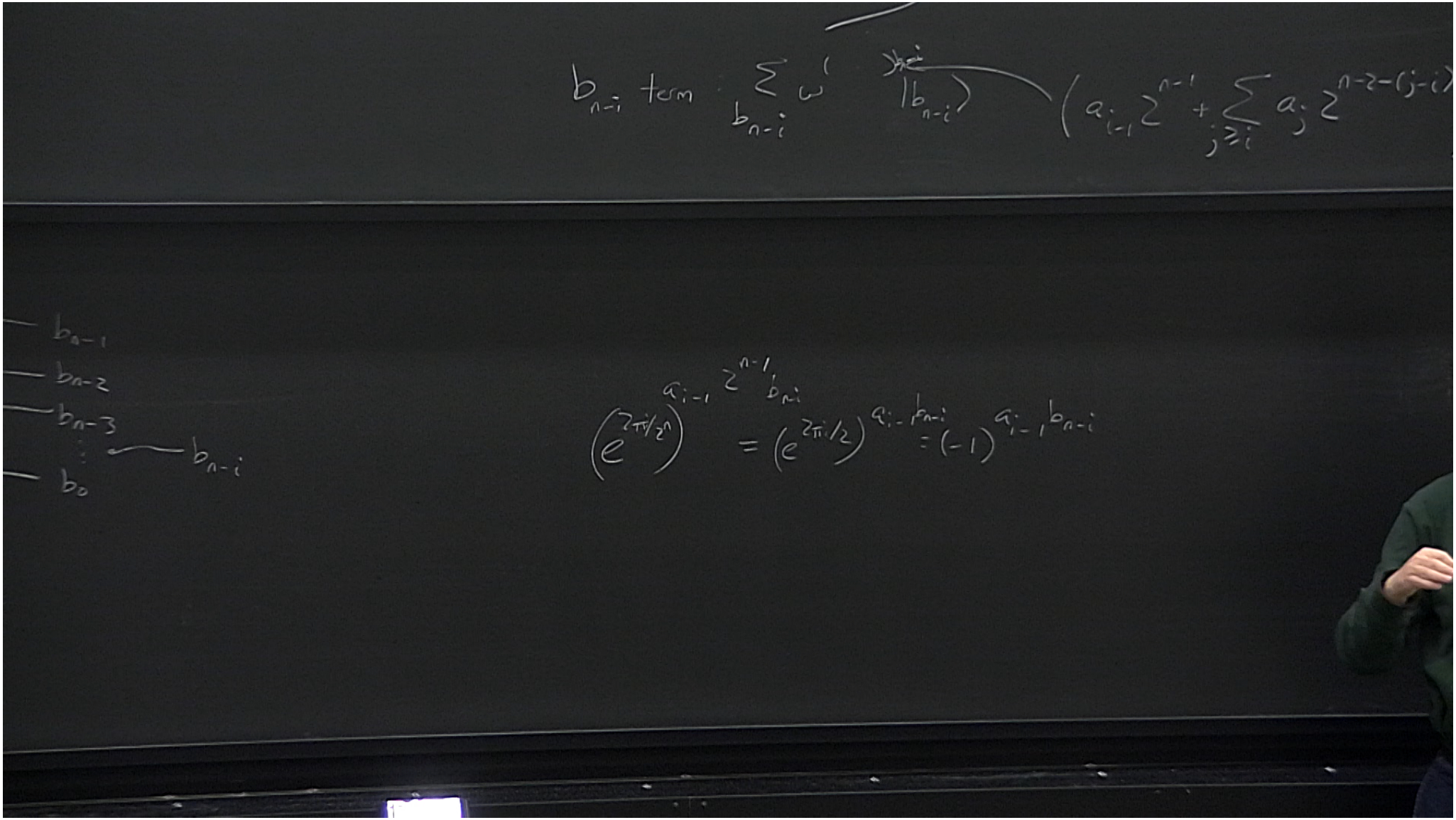
$$= \left[\sum_{b_{n-1}} \omega^{\left(a_0 z^{n-1} + a_1 z^{n-2} + \ldots + a_{n-1} z^0\right)} |b_{n-1}\rangle\right]\left[\sum_{b_{n-2}} \omega^{\left(a_1 z^{n-1} + a_2 z^{n-2} + \ldots + a_{n-1} z^1\right)} |b_{n-2}\rangle\right] \cdots \left[\sum_{b_0} \omega^{\left(a_{n-1} z^{n-1}\right)} |b_0\rangle\right]$$


$(\ldots) + z^{n-1}(a_0 b_{n-1} + a_1 b_{n-2} + \ldots + a_{n-1} b_0) + z^{n-2}(a_1 b_{n-1} + \ldots + a_{n-1} b_1) + \ldots + z^0 (a_{n-1} b_{n-1})$.
$|b\rangle = \sum_b \omega^{ab} |b_{n-1}\rangle |b_{n-2}\rangle \ldots |b_0\rangle$
$\left[\sum_{b_{n-1}} \omega^{(a_0 z^{n-1} + a_1 z^{n-2} + \ldots + a_{n-1} z^0)} |b_{n-1}\rangle\right]\left[\sum_{b_{n-2}} \omega^{(a_1 z^{n-1} + a_2 z^{n-2} + \ldots + a_{n-1} z^1)} |b_{n-2}\rangle\right] \cdots \left[\sum_{b_0} \omega^{(a_{n-1} z^{n-1})} |b_0\rangle\right]$
$b_{n-i}$ term $\sum_{b_{n-i}} \omega^{(\quad)} |b_{n-i}\rangle$ $\left(a_{i-1} z^{n-1} + \sum_{j \geq i} a_j z^{n-2-(j-i)}\right.$


$\omega = e^{2\pi i/2^n}$
$a_0$
$a_1$
$a_2$
$a_{i-1}$
$a_{n-1}$
$b_{n-1}$
$b_{n-2}$
$b_{n-3}$
$b_{n-i}$
$b_0$


$b_{n-i}$ term
$\sum_{b_{n-i}} \omega^{(\quad)} |b_{n-i}\rangle$
$(a_{i-1} z^{n-1} + \sum_{j>i} a_j z^{n-2-(j-i)}$
$b_{n-1}$
$b_{n-2}$
$b_{n-3}$
$b_{n-i}$
$b_0$
$\left(e^{2\pi i/2^n}\right)^{a_{i-1} z^{n-1}} = \left(e^{2\pi i/2}\right)^{a_{i-1}} = (-1)^{a_{i-1}}$



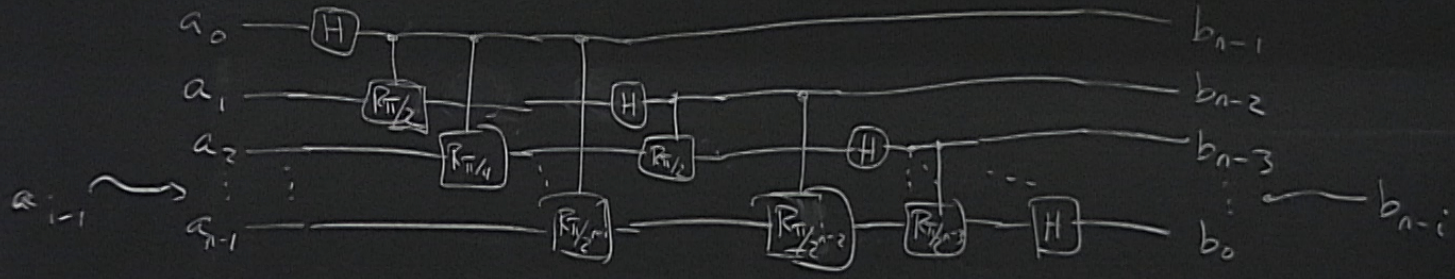

$b_{n-i}$ term
$\sum_{b_{n-i}} \omega^{(\quad)} |b_{n-i}\rangle$
$(a_{i-1} z^{n-1} + \sum_{j \geq i} a_j z^{n-2-(j-i)}$
$b_{n-1}$
$b_{n-2}$
$b_{n-3}$
$b_{n-i}$
$b_0$
$\left(e^{2\pi i/2^n}\right)^{a_{i-1} z^{n-1} b_{n-i}} = \left(e^{2\pi i/2}\right)^{a_{i-1} b_{n-i}} = (-1)^{a_{i-1} b_{n-i}}$

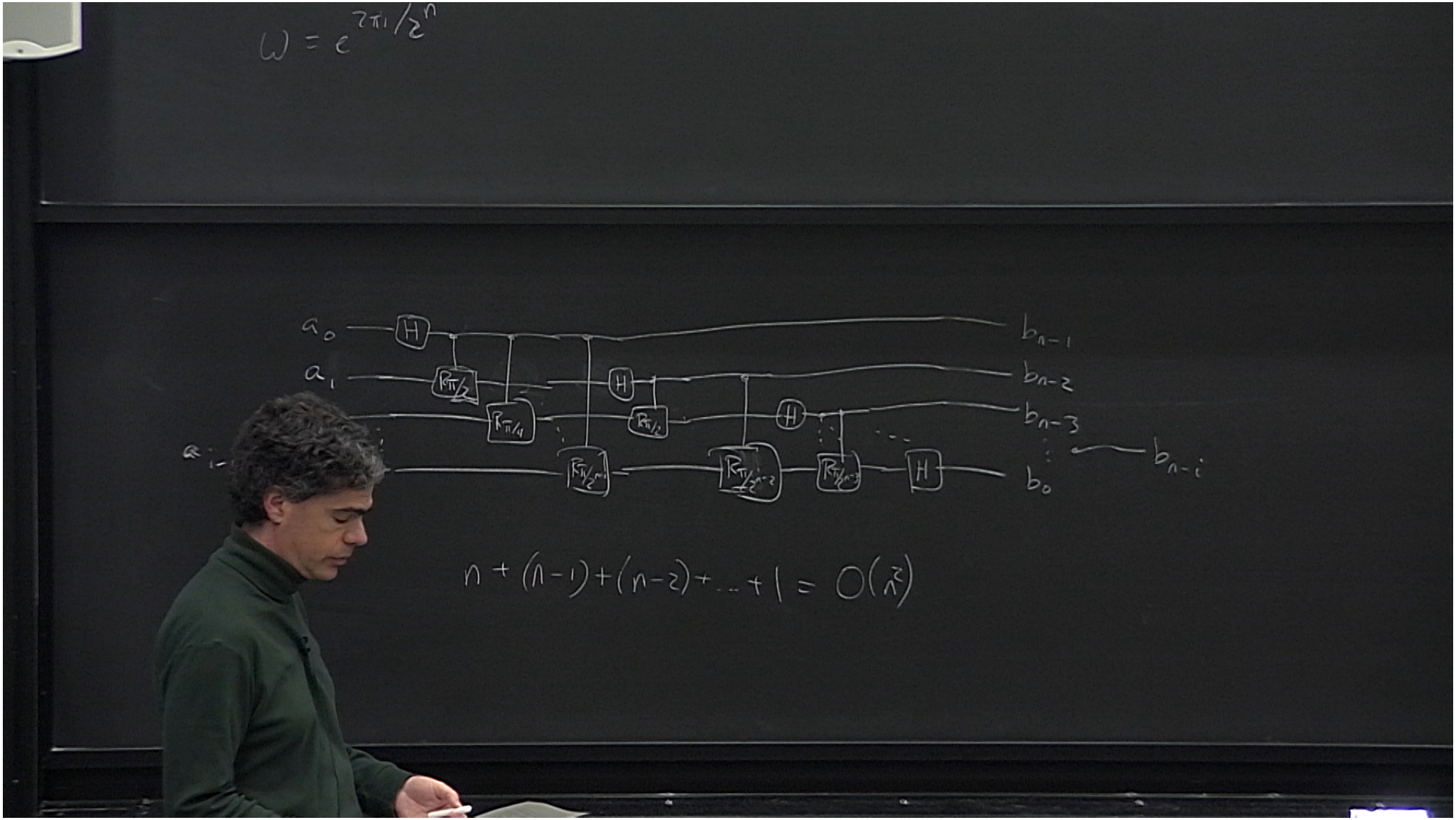
$b_{n-i}$ term $\sum_{b_{n-i}} \omega^{(\quad)} |b_{n-i}\rangle \left( a_{i-1} z^{n-1} + \sum_{j \geq i} a_j z^{n-2-(j-i)} \right)$

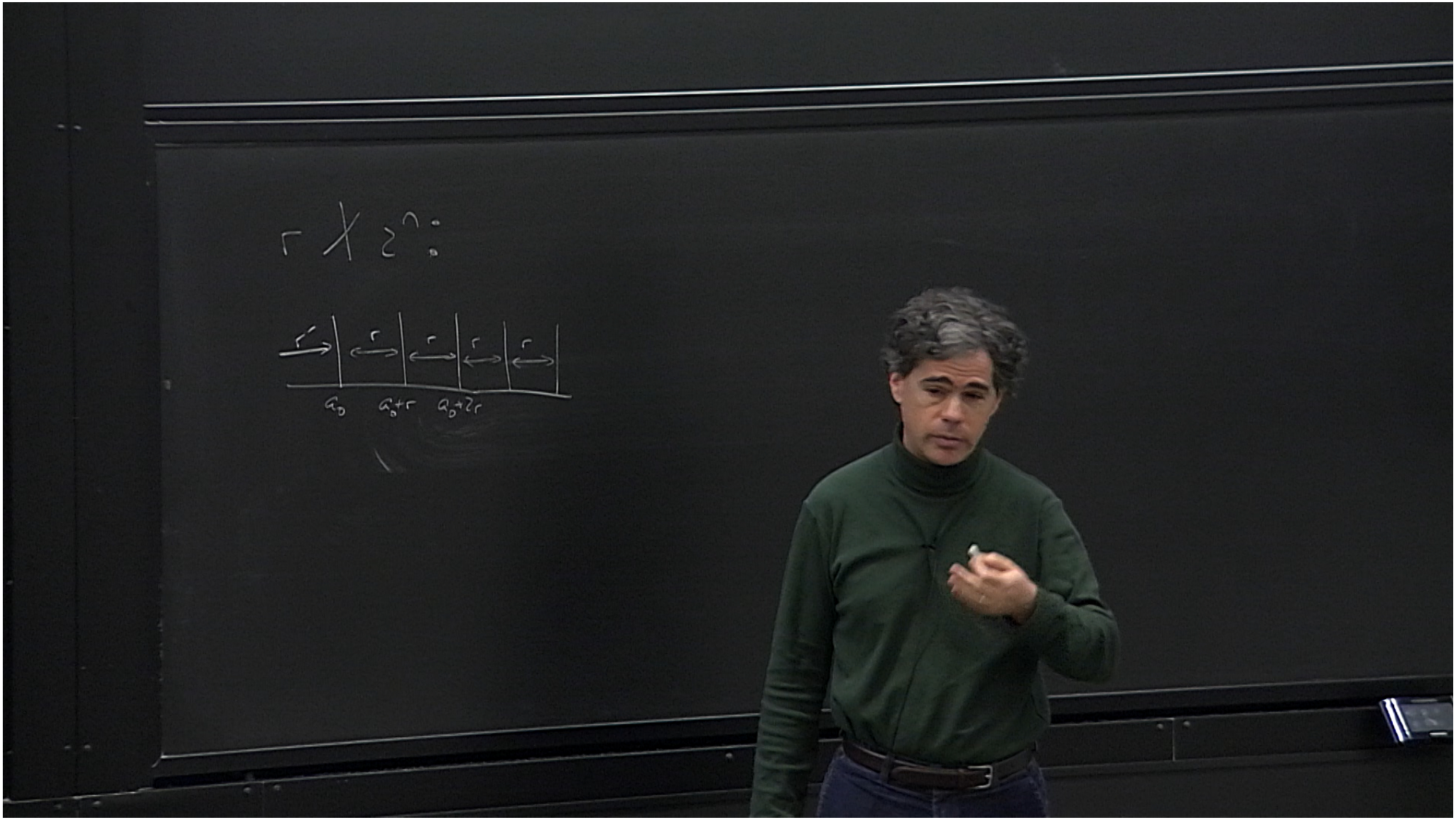
$\left(e^{2\pi i/2^n}\right)^{a_{i-1} z^{n-1} b_{n-i}} = \left(e^{2\pi i/2}\right)^{a_{i-1} b_{n-i}} = (-1)^{a_{i-1} b_{n-i}}$ → From Hadamard

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

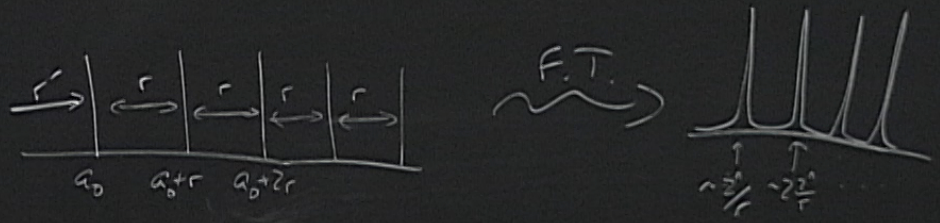
$\omega = e^{2\pi i / 2^n}$



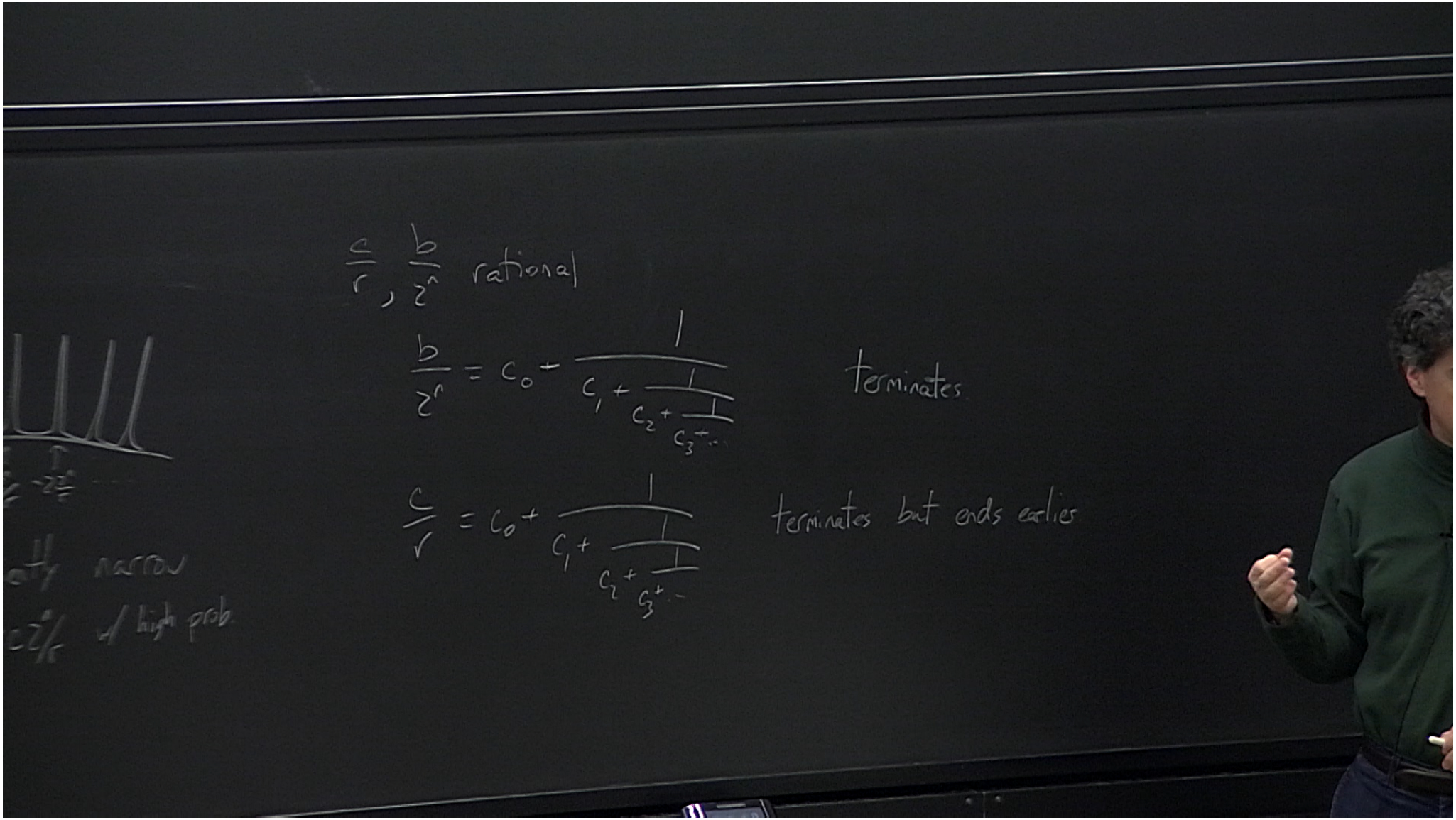

$\omega = e^{2\pi i/2^n}$
$a_0$
$a_1$
$a_{n-1}$
H
$R_{\pi/2}$
$R_{\pi/4}$
$R_{\pi/2^{n-1}}$
$R_{\pi/2^{n-2}}$
$R_{\pi/2^{n-3}}$
$b_{n-1}$
$b_{n-2}$
$b_{n-3}$
$b_{n-i}$
$b_0$
$n + (n-1) + (n-2) + \ldots + 1 = O(n^2)$


r
r
r
r
r
$a_0$
$a_0+r$
$a_0+2r$

$r \nmid \hat{z}$:




If $\hat{z} \approx N^2$, we get sufficiently narrow peaks so that the outcome $b \approx c\frac{\hat{z}}{r}$ w/ high prob


$\frac{c}{r}, \frac{b}{z^r}$ rational
$\frac{b}{z^r} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots}}}$
terminates
$\frac{c}{r} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cdots}}}$
terminates but ends earlier