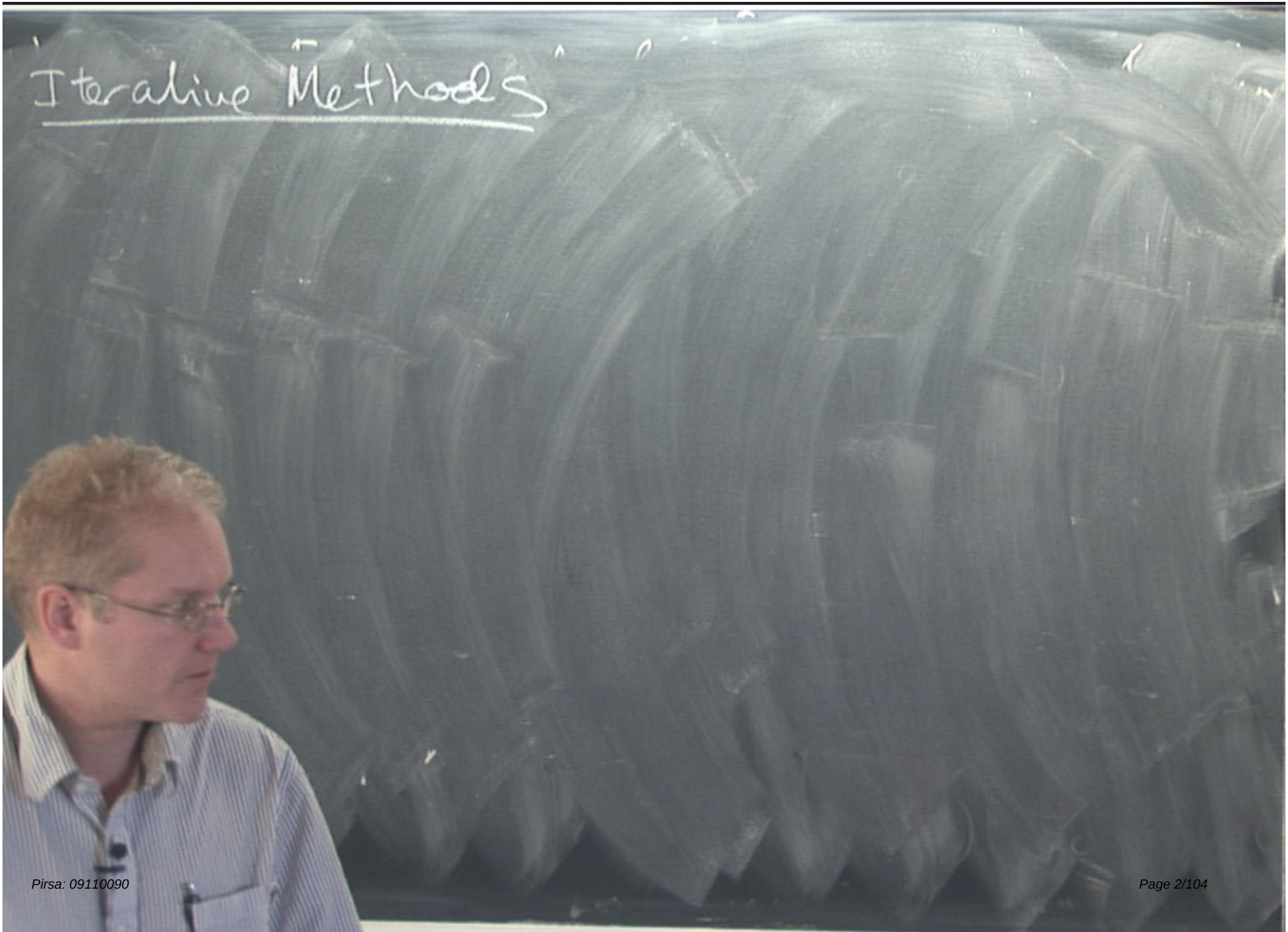
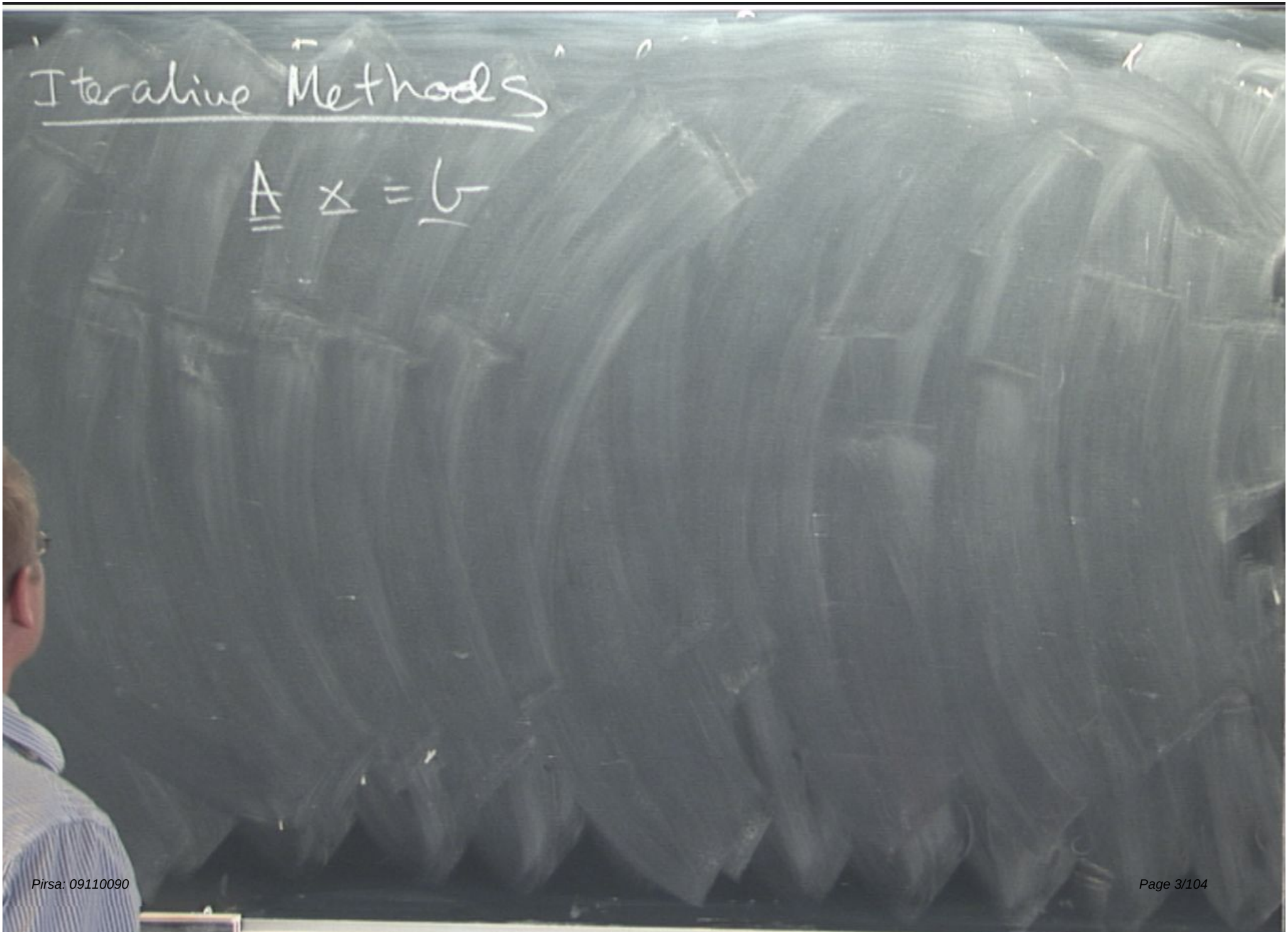
Title: Scientific Computation (PHYS 608) - Lecture 13

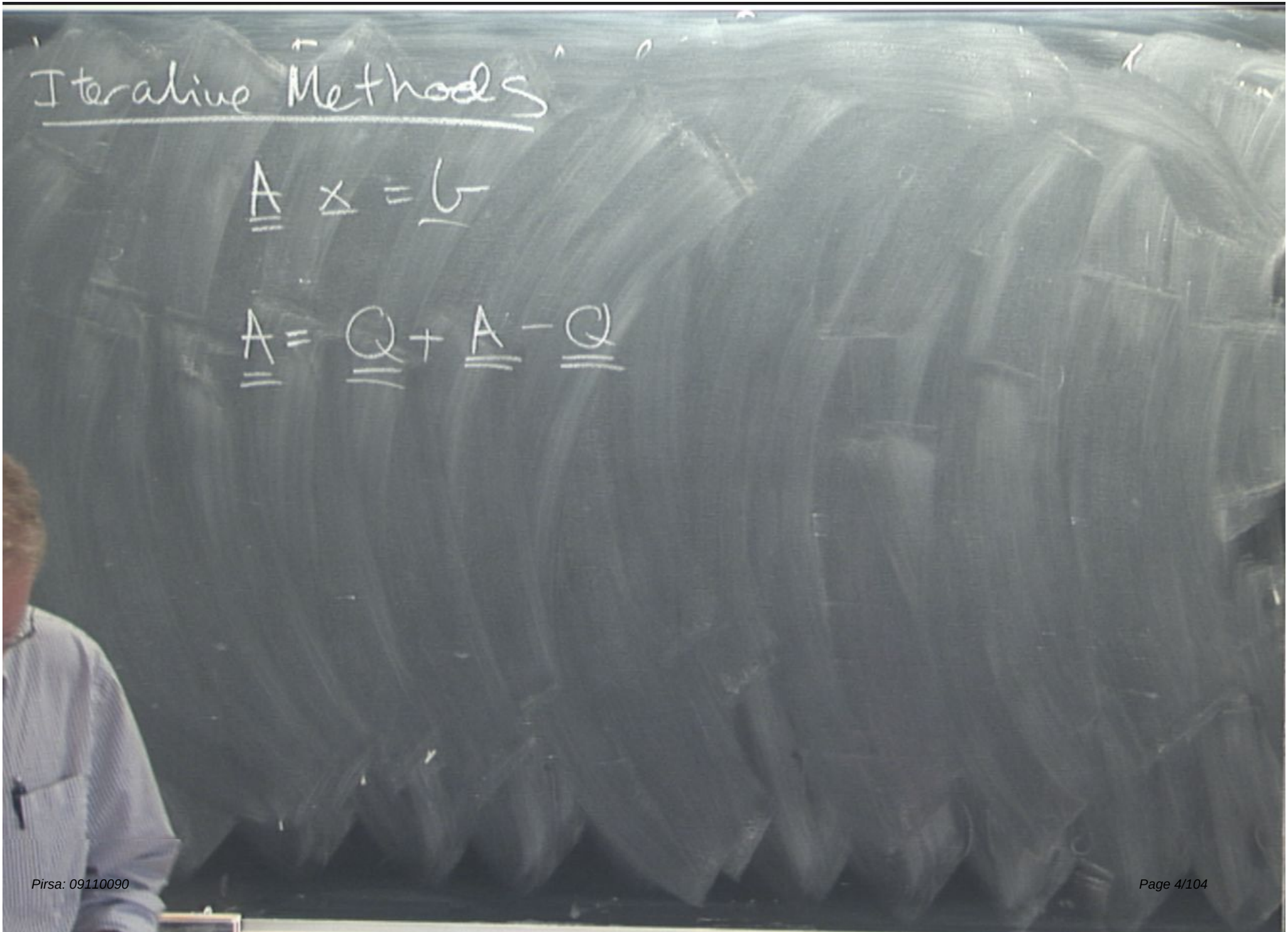
Date: Nov 11, 2009 10:30 AM

URL: http://pirsa.org/09110090

Abstract:


Iterative Methods


Iterative Methods
$\underline{\underline{A}}\,x = \underline{b}$


Iterative Methods
A x = b
A = Q + A - Q

Iterative Methods

(1) $\underline{\underline{A}}\, x = b$

$$\underline{\underline{A}} = \underline{\underline{Q}} + \underline{\underline{A}} - \underline{\underline{Q}}$$

Then (1)

$$Qx + (A - Q)x = b$$

or

$$Qx =$$

Iterative Methods

(1) $\underline{\underline{A}}\, x = b$

$$\underline{\underline{A}} = \underline{\underline{Q}} + \underline{\underline{A}} - \underline{\underline{Q}}$$

Then (1)

$$Qx + (A - Q)x = b$$

or

$$Qx = (Q - A)x + b$$

Iterative Methods

(1) $\underline{\underline{A}}\, x = b$

$$\underline{\underline{A}} = \underline{\underline{Q}} + \underline{\underline{A}} - \underline{\underline{Q}}$$

Then (1)

$$\underline{\underline{Q}}\, x + (\underline{\underline{A}} - \underline{\underline{Q}})\, x = b$$

or

$$\underline{\underline{Q}}\, x = (\underline{\underline{Q}} - \underline{\underline{A}})\, x + b$$

Iterative Methods

(1) $\underline{\underline{A}}\, x = b$

$$\underline{\underline{A}} = \underline{\underline{Q}} + \underline{\underline{A}} - \underline{\underline{Q}}$$

Then (1)

$$\underline{\underline{Q}} x + (\underline{\underline{A}} - \underline{\underline{Q}}) x = b$$

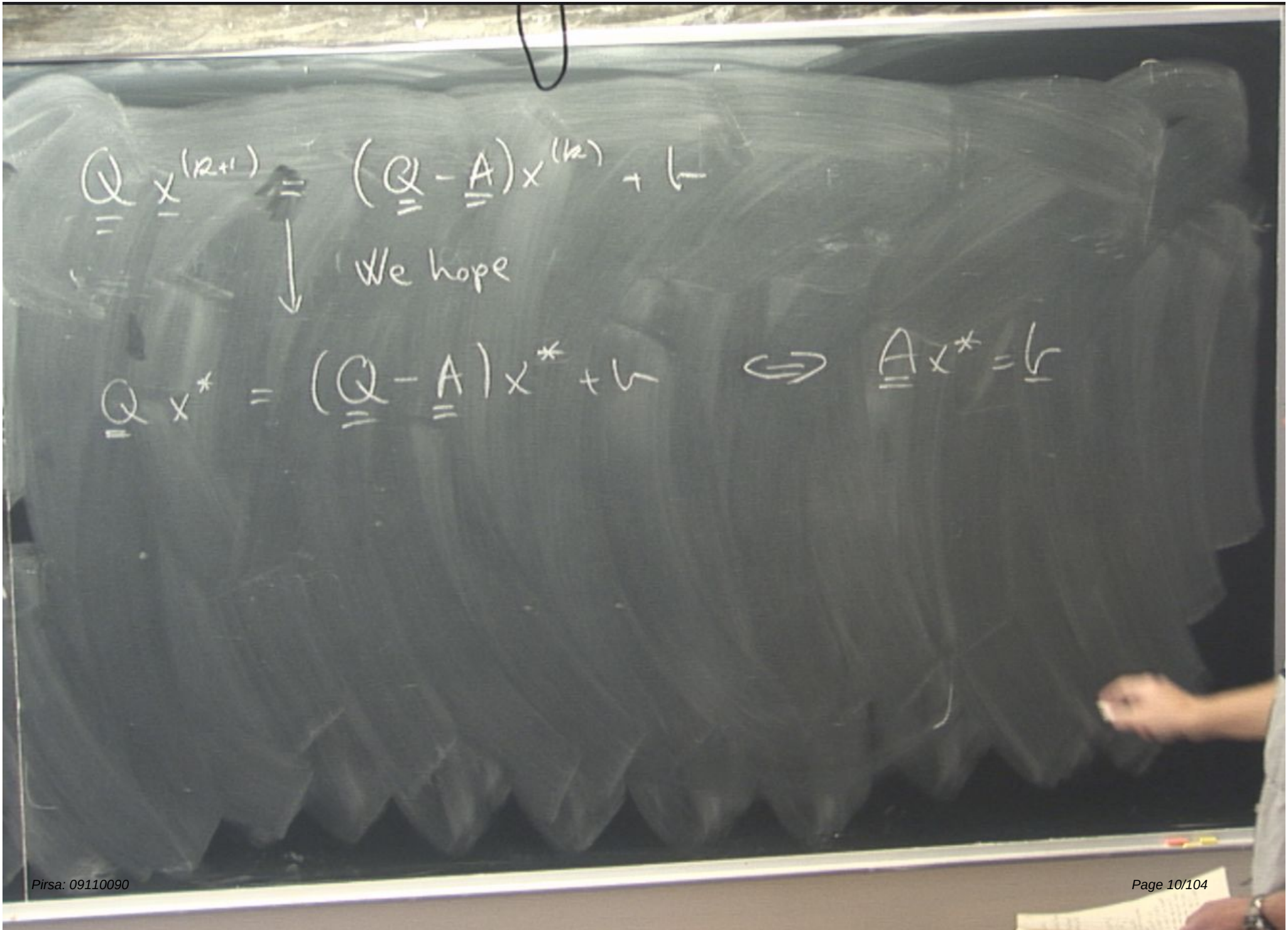
or

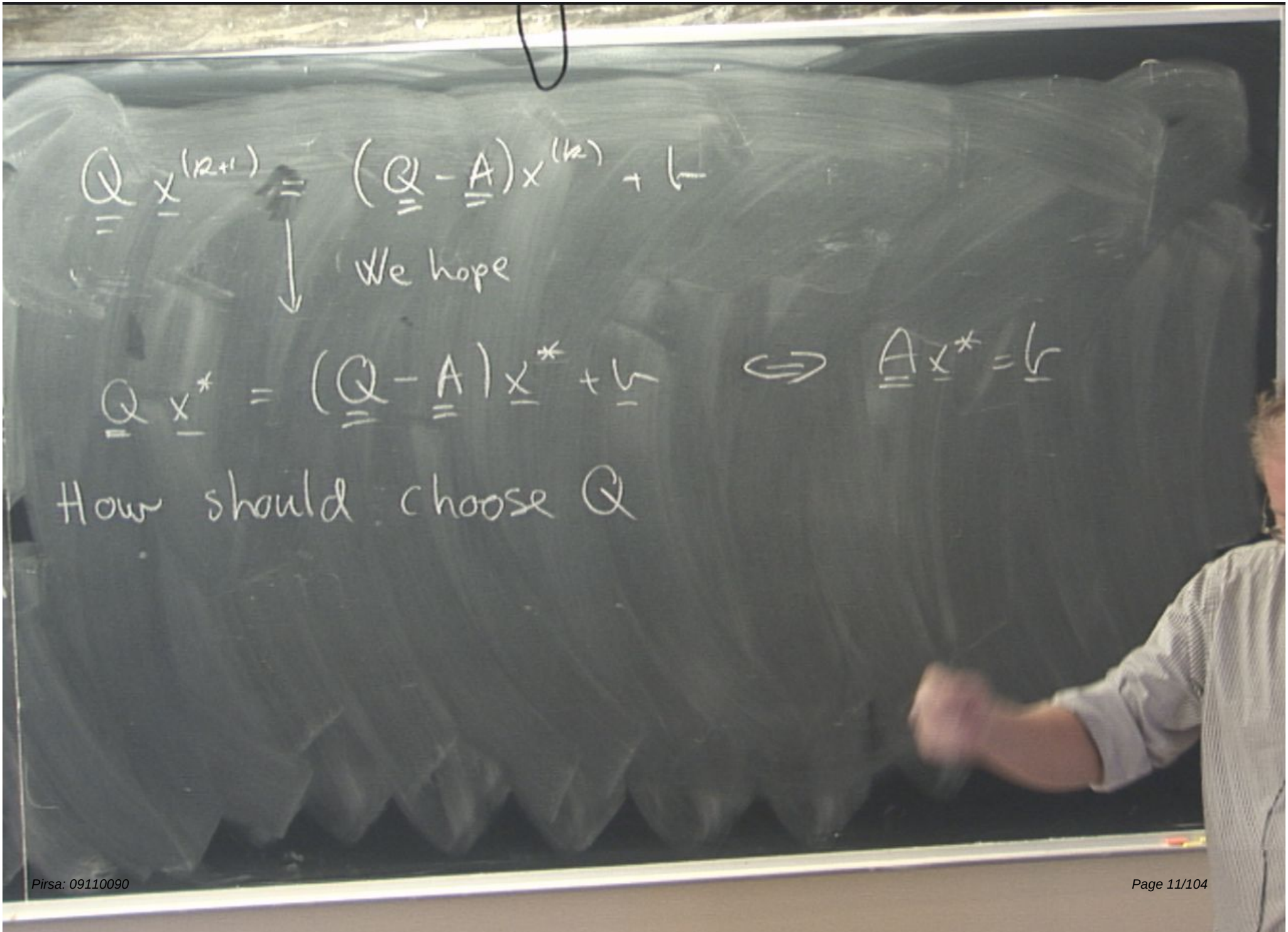
$$\underline{\underline{Q}} x = (\underline{\underline{Q}} - \underline{\underline{A}}) x + b \leftarrow \text{Iterating}$$

$$\underline{\underline{Q}}\,\underline{x}^{(k+1)} = (\underline{\underline{Q}} - \underline{\underline{A}})\,x^{(k)} + b$$

$\downarrow$ We hope

$$\underline{\underline{Q}}\,x^{*} = (\underline{\underline{Q}} - \underline{\underline{A}})\,x^{*} + b$$


$Q\,x^{(k+1)} = (Q - A)x^{(k)} + b$
We hope
$Q\,x^{*} = (Q - A)x^{*} + b \iff Ax^{*} = b$


$\underline{\underline{Q}}\,\underline{x}^{(k+1)} = (\underline{\underline{Q}} - \underline{\underline{A}})\,\underline{x}^{(k)} + \underline{b}$
We hope
$\underline{\underline{Q}}\,\underline{x}^{*} = (\underline{\underline{Q}} - \underline{\underline{A}})\,\underline{x}^{*} + \underline{b} \Leftrightarrow \underline{\underline{A}}\,\underline{x}^{*} = \underline{b}$
How should choose Q

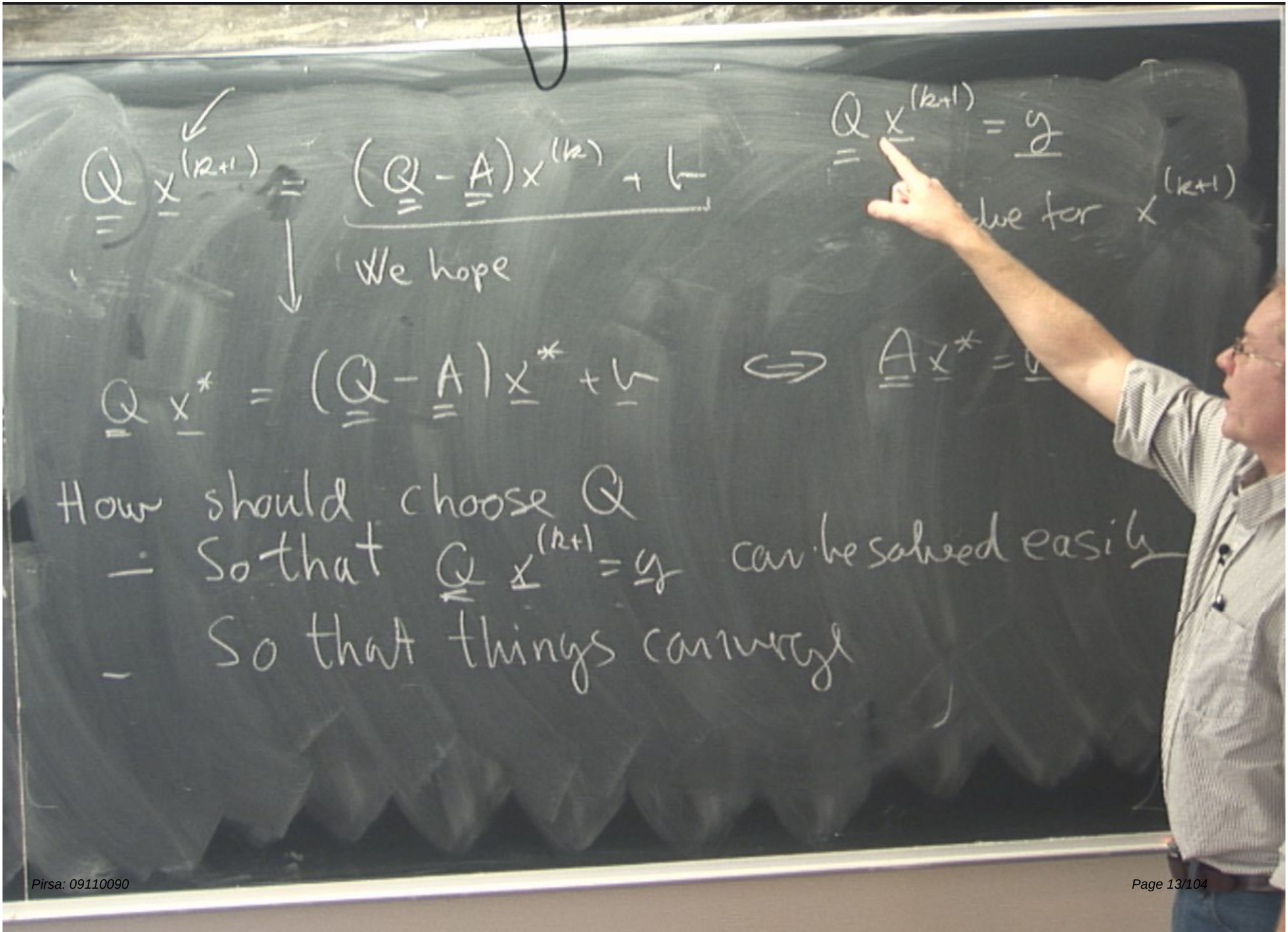
$$Q x^{(k+1)} = (Q - A)x^{(k)} + b$$

$$Q x^{(k+1)} = y$$

We hope

$$Q x^* = (Q - A)x^* + b \iff A x^* = b$$

How should choose Q


$Q\,x^{(k+1)} = (Q-A)x^{(k)} + b$
We hope
$Q\,x^{*} = (Q-A)x^{*} + b$
$Q\,x^{(k+1)} = y$
ve for $x^{(k+1)}$
$\Leftrightarrow$
$Ax^{*} = b$
How should choose Q
- So that $Q\,x^{(k+1)} = y$ can be solved easily
- So that things converge

$$\underline{\underline{Q}}\,\underline{x}^{(k+1)} = (\underline{\underline{Q}} - \underline{\underline{A}})\underline{x}^{(k)} + \underline{b}$$

We hope

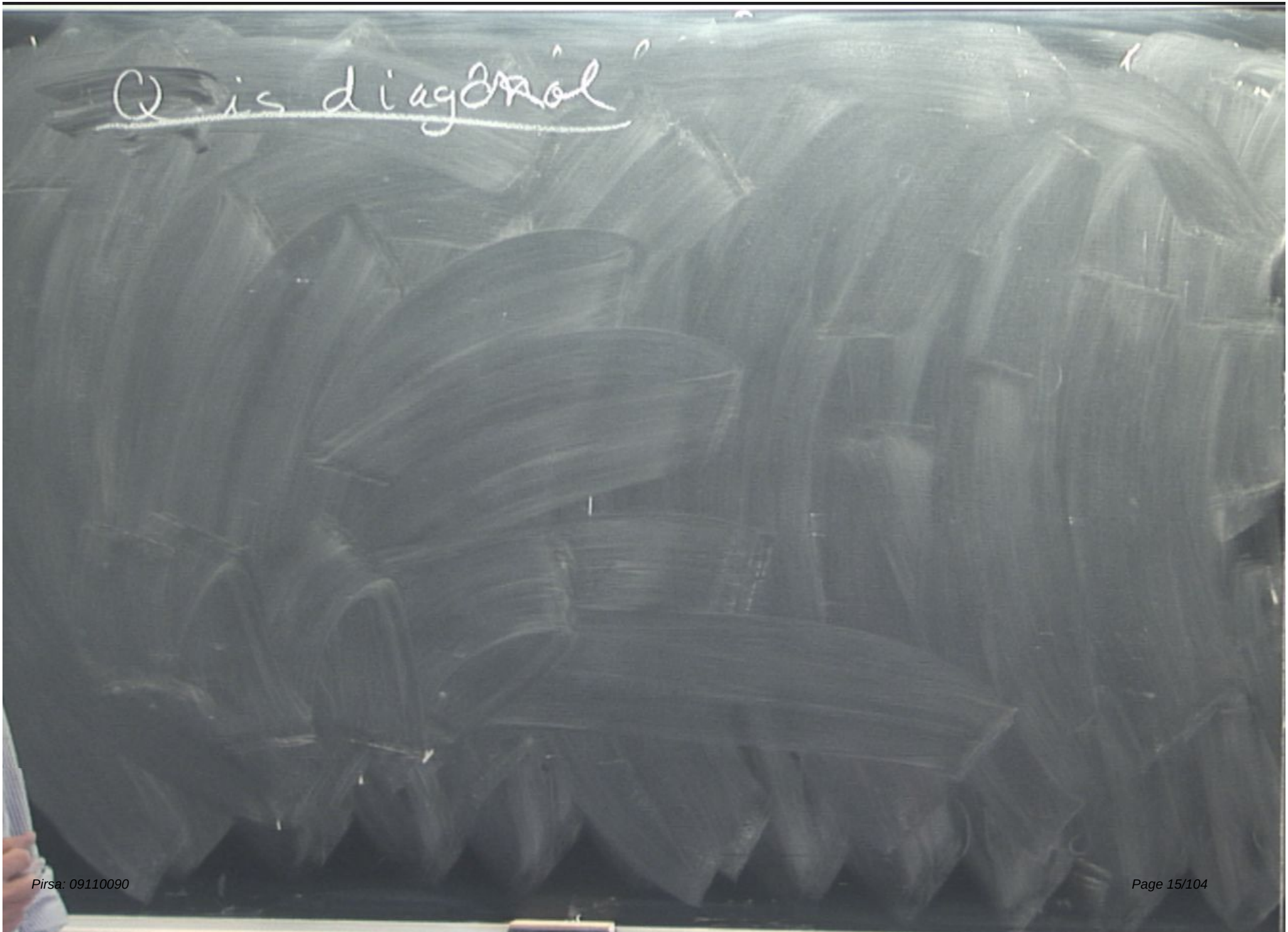
$$\underline{\underline{Q}}\,\underline{x}^{(k+1)} = \underline{y}$$

↑ Solve for $x^{(k+1)}$

$$\underline{\underline{Q}}\,\underline{x}^{*} = (\underline{\underline{Q}} - \underline{\underline{A}})\underline{x}^{*} + \underline{b} \iff \underline{\underline{A}}\,\underline{x}^{*} = \underline{b}$$

How should choose Q

- So that $\underline{\underline{Q}}\,\underline{x}^{(k+1)} = \underline{y}$ can be solved easily
- So that things converge


Q is diagonal

Q is diagonal

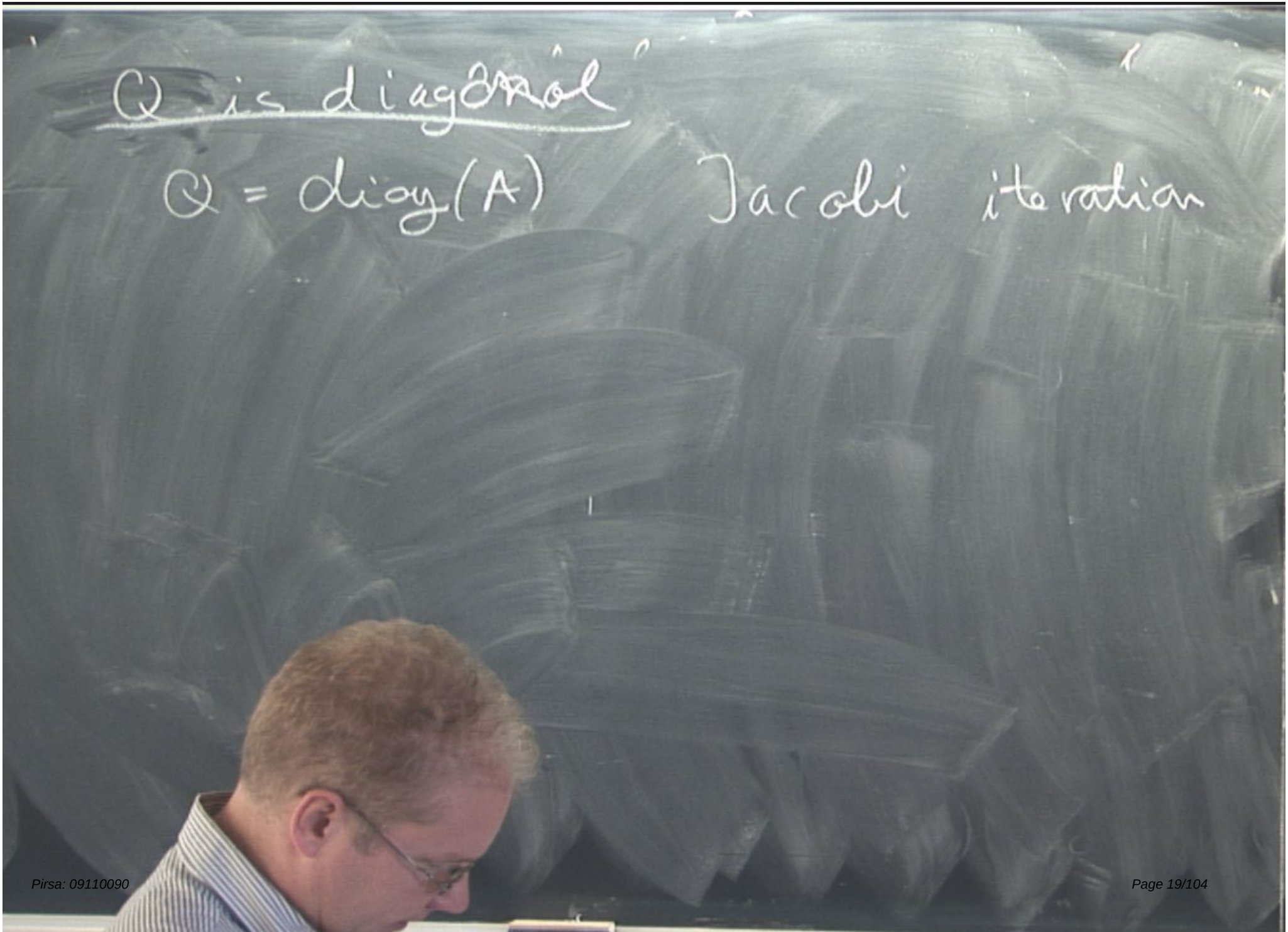
$Q = diag(A)$

Q is diagonal

Q = diag(A) Jacobi

Q is diagonal

$Q = diag(A)$ Jacobi


Q is diagonal
Q = diag(A)
Jacobi iteration

Q is diagonal

Q = diag(A) Jacobi iteration

Gauss-Seidel Iteration

Q is diagonal

$Q = diag(A)$ Jacobi iteration

Gauss-Seidel Iteration

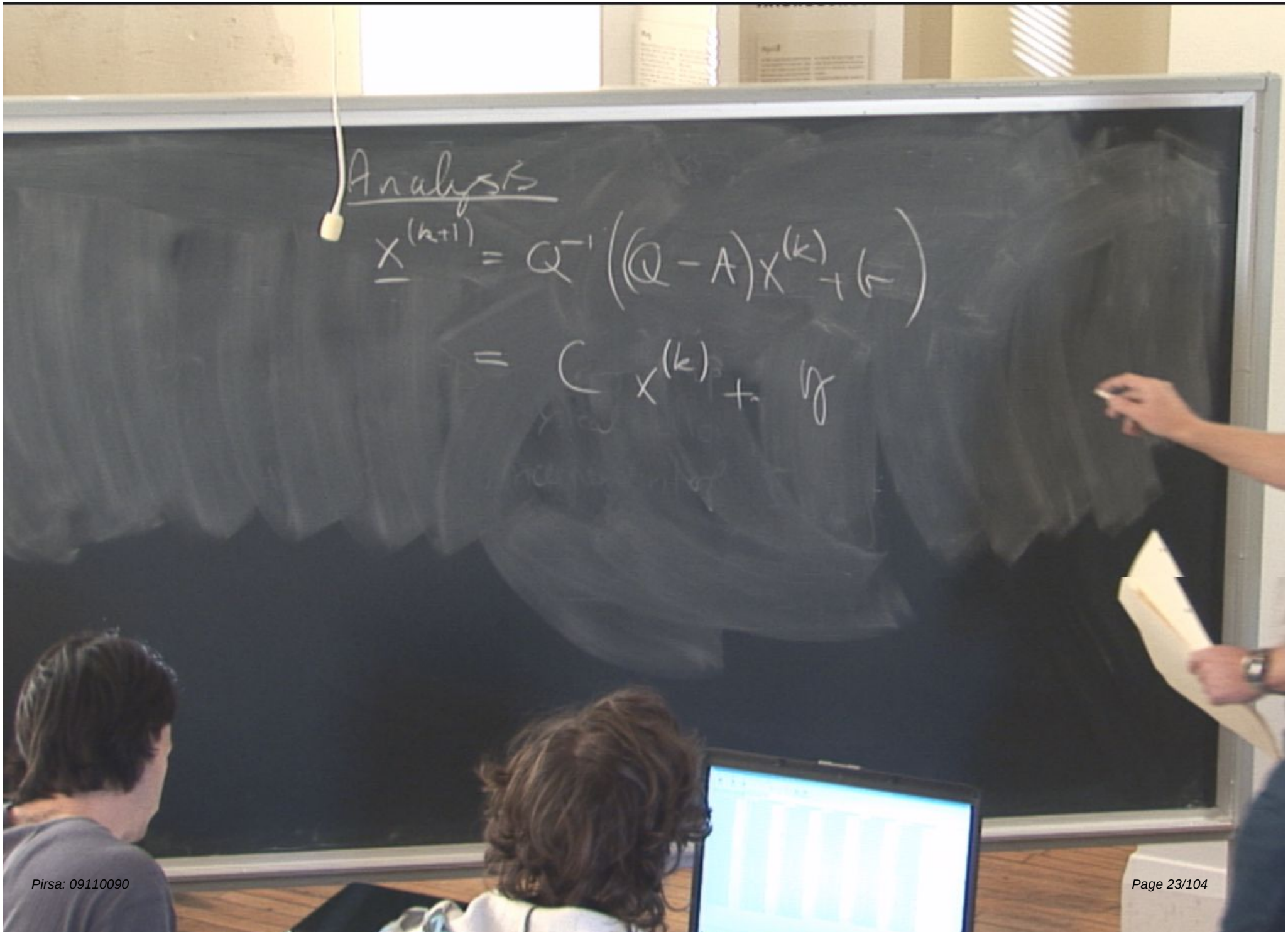
Q = lower/Upper triangular part of A

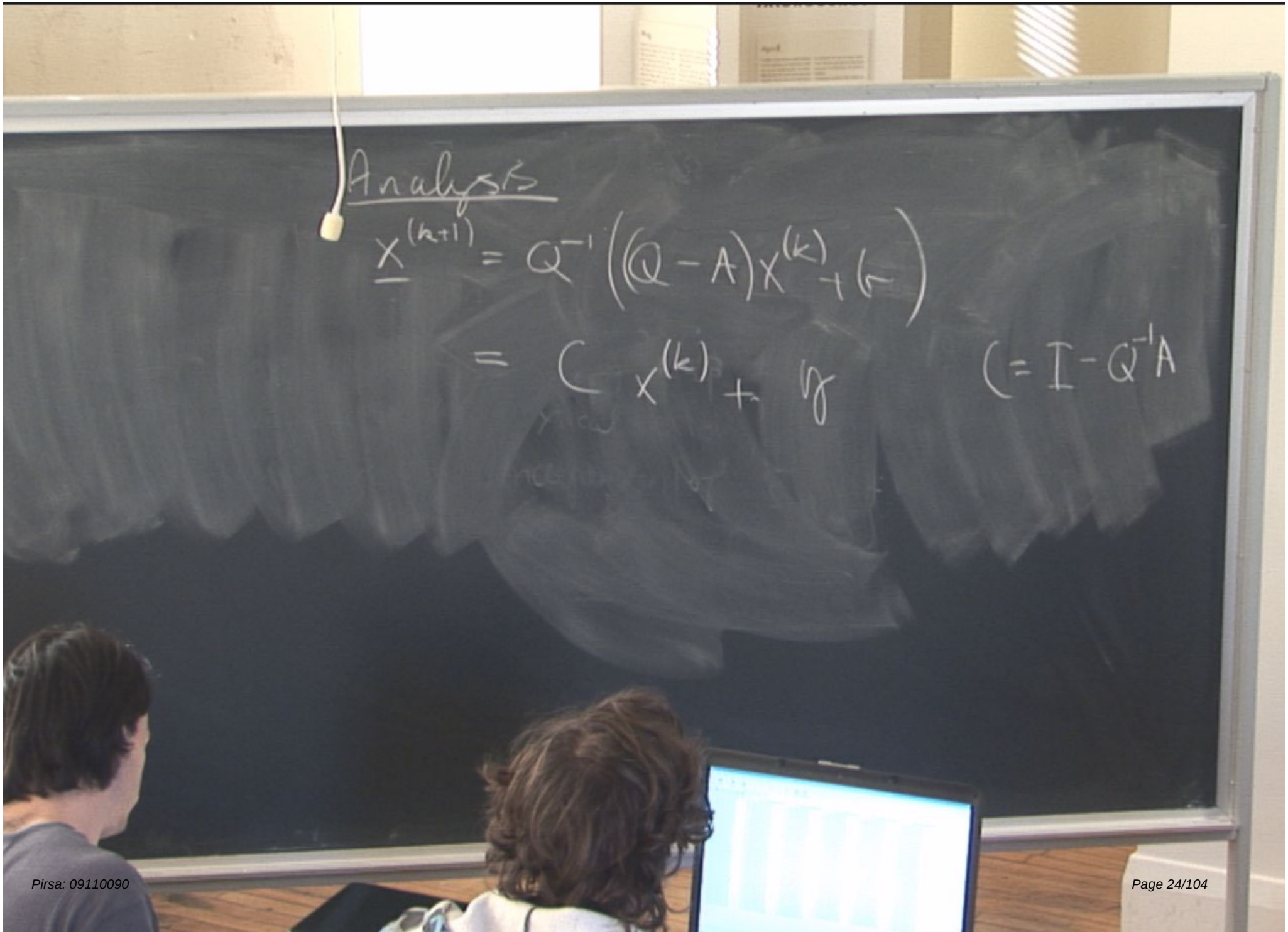
Q is diagonal

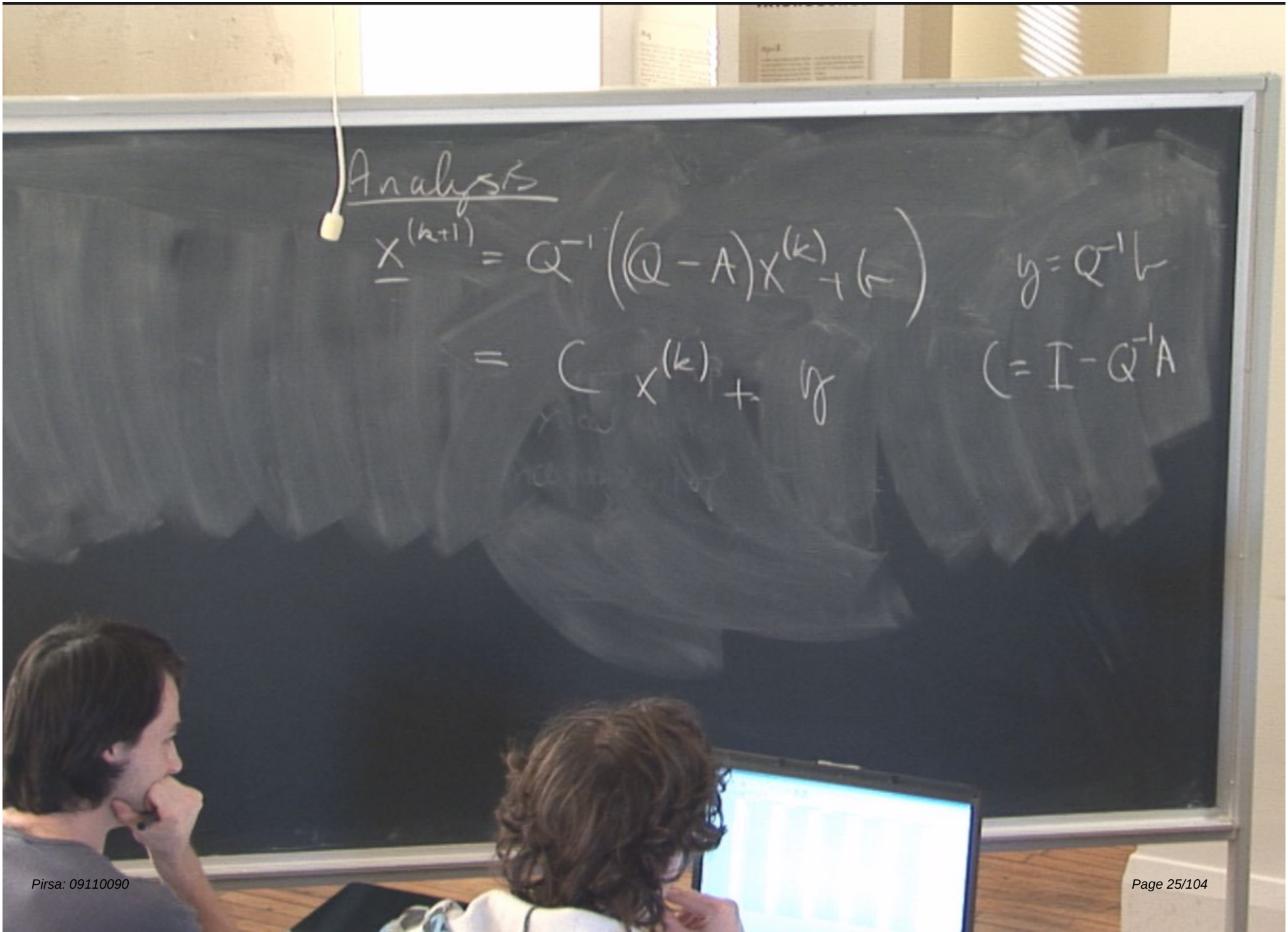
$Q = \mathrm{diag}(A)$ Jacobi iteration

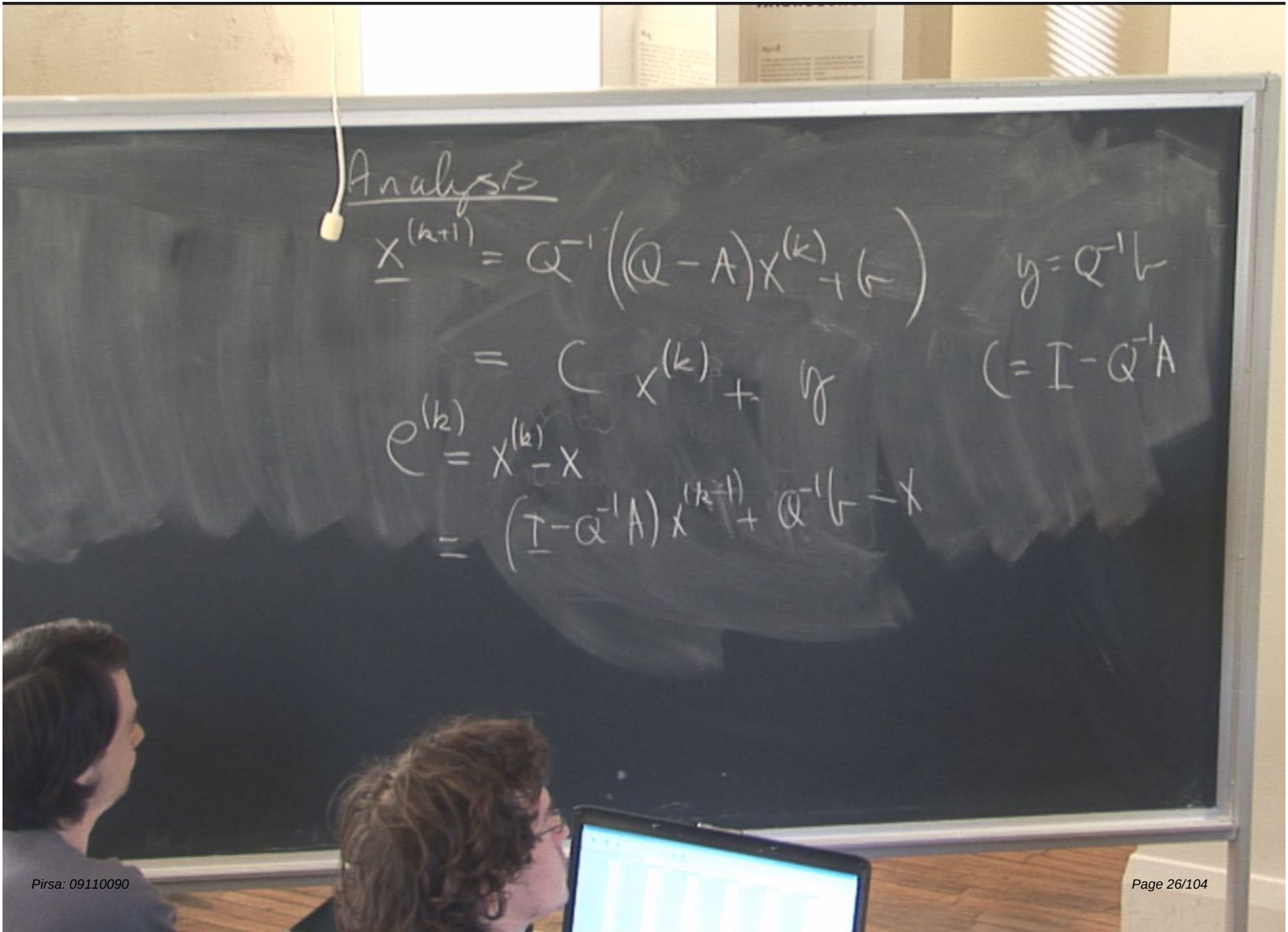
Gauss-Seidel Iteration

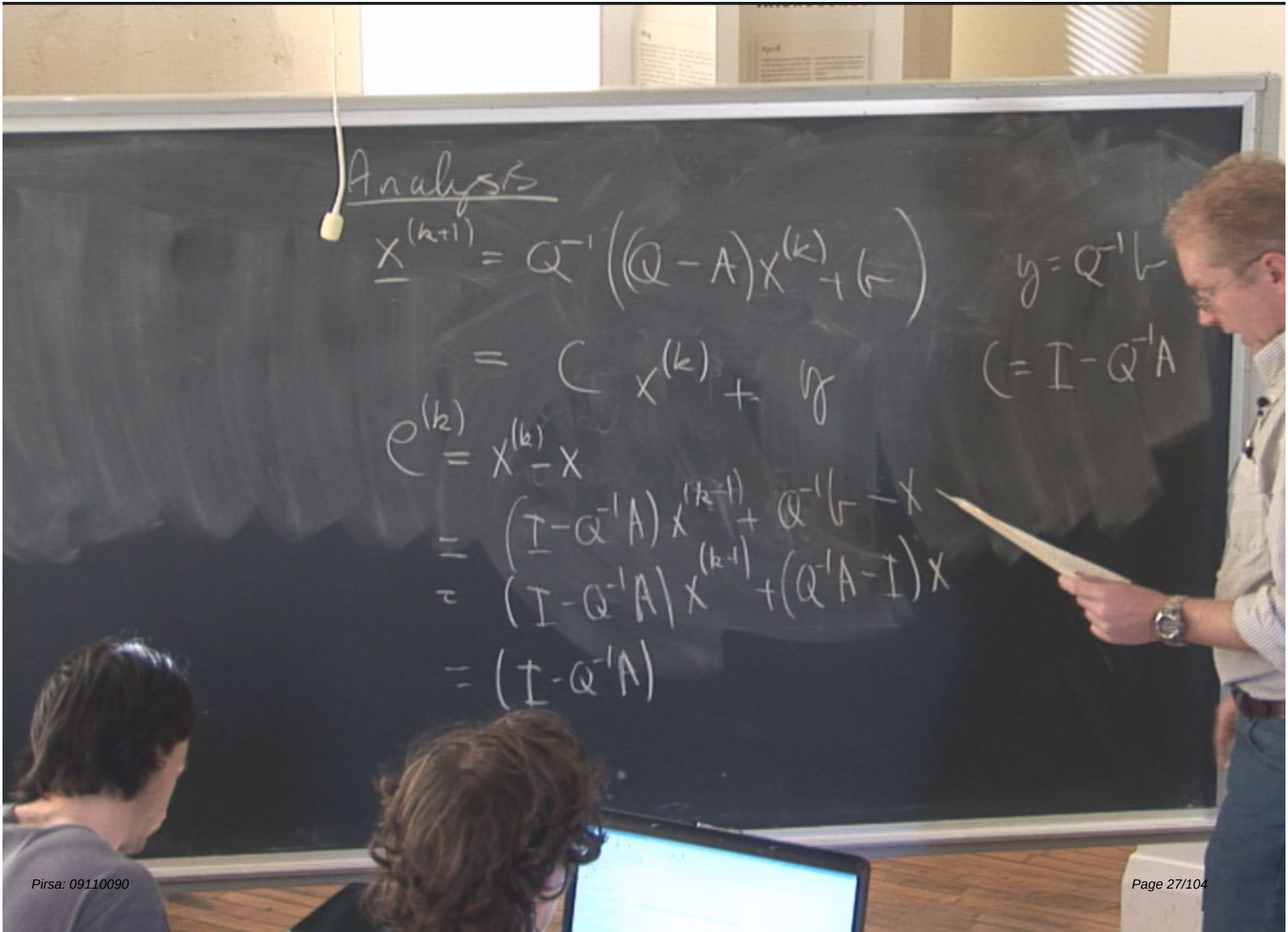
$Q =$ lower/Upper triangular part of A including the diagonal

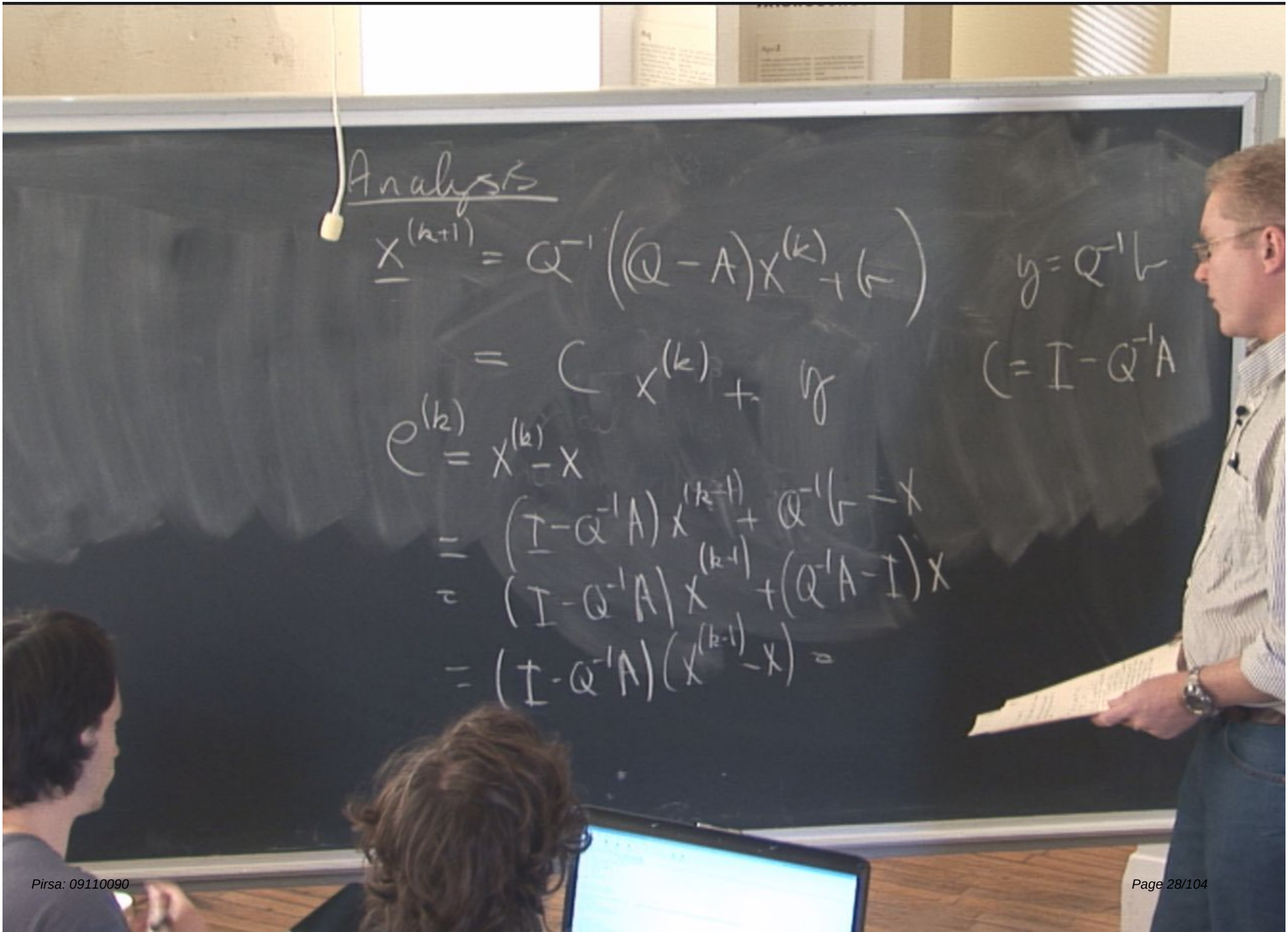

Analysis
$\underline{x}^{(k+1)} = Q^{-1}\left((Q-A)x^{(k)} + b\right)$
$= C x^{(k)} + g$

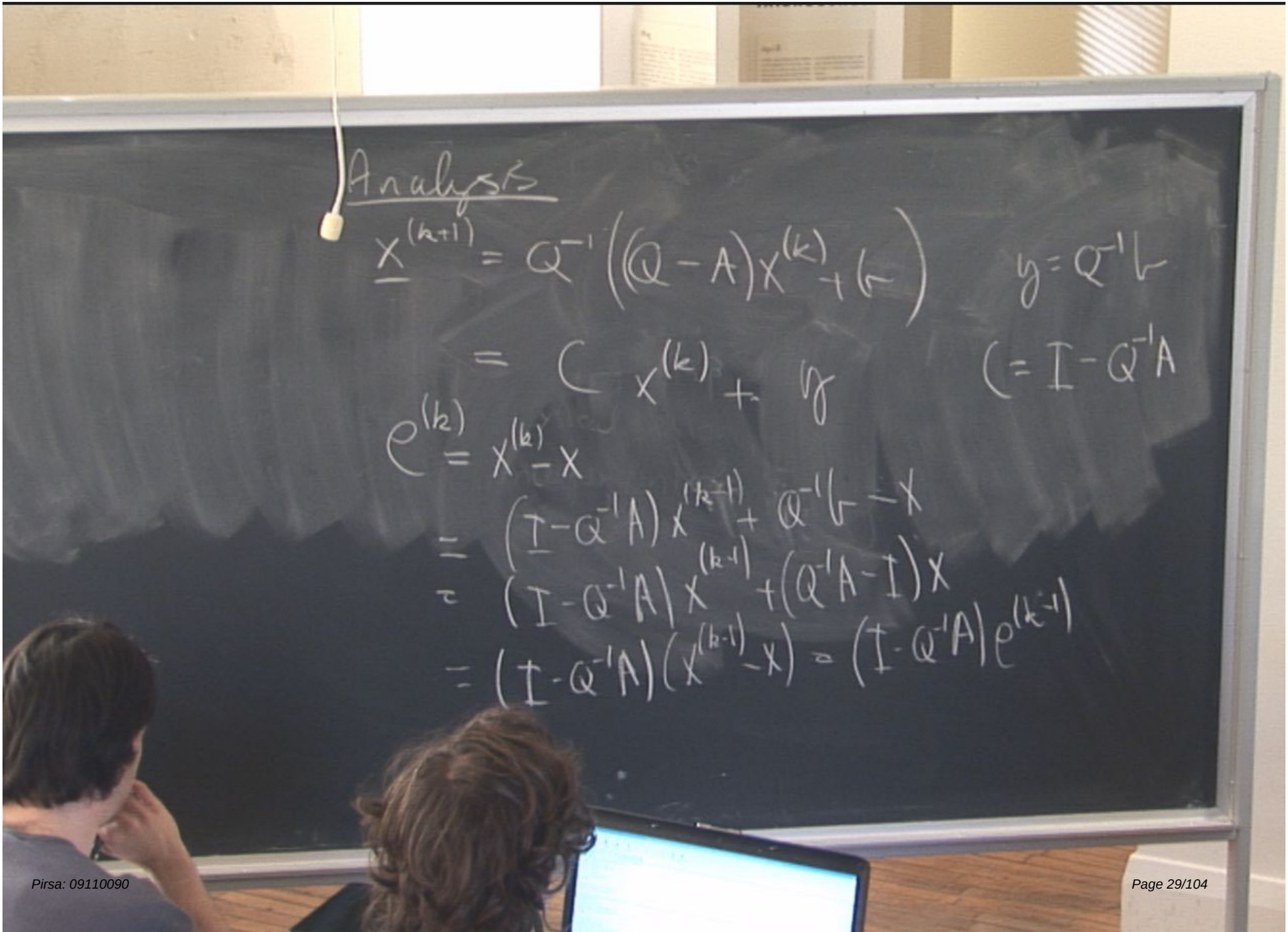

Analysis
$\underline{x}^{(k+1)} = Q^{-1}\left((Q-A)x^{(k)} + b\right)$
$= C x^{(k)} + g$
$(= I - Q^{-1}A$

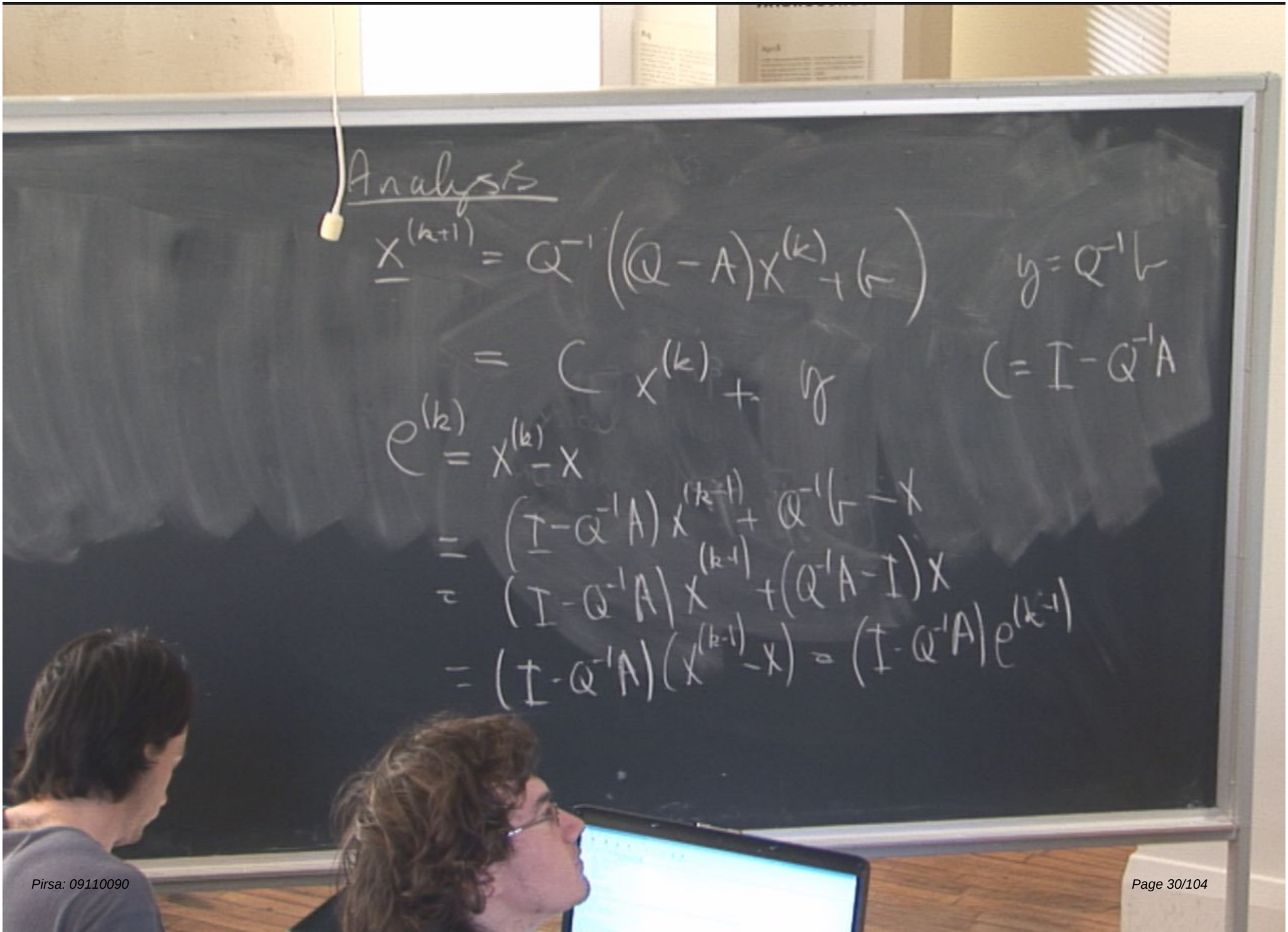

Analysis
$\underline{x}^{(k+1)} = Q^{-1}\left((Q-A)x^{(k)} + b\right)$
$= C x^{(k)} + g$
$y = Q^{-1}b$
$(= I - Q^{-1}A$


Analysis
$\underline{x}^{(k+1)} = Q^{-1}\left((Q-A)x^{(k)} + b\right)$
$y = Q^{-1}b$
$= C\,x^{(k)} + y$
$(= I - Q^{-1}A$
$e^{(k)} = x^{(k)} - x$
$= \left(I - Q^{-1}A\right)x^{(k-1)} + Q^{-1}b - x$


Analysis
$x^{(k+1)} = Q^{-1}\left((Q-A)x^{(k)} + b\right)$
$= C x^{(k)} + g$
$y = Q^{-1}b$
$C = I - Q^{-1}A$
$e^{(k)} = x^{(k)} - x$
$= \left(I - Q^{-1}A\right)x^{(k-1)} + Q^{-1}b - x$
$= \left(I - Q^{-1}A\right)x^{(k-1)} + \left(Q^{-1}A - I\right)x$
$= \left(I - Q^{-1}A\right)$


Analysis
$x^{(k+1)} = Q^{-1}\left((Q-A)x^{(k)} + b\right)$
$y = Q^{-1}b$
$= C\,x^{(k)} + y$
$C = I - Q^{-1}A$
$e^{(k)} = x^{(k)} - x$
$= \left(I - Q^{-1}A\right)x^{(k-1)} + Q^{-1}b - x$
$= \left(I - Q^{-1}A\right)x^{(k-1)} + \left(Q^{-1}A - I\right)x$
$= \left(I - Q^{-1}A\right)\left(x^{(k-1)} - x\right) =$


Analysis
$\underline{x}^{(k+1)} = Q^{-1}\left((Q-A)x^{(k)} + b\right)$
$y = Q^{-1}b$
$= C\,x^{(k)} + y$
$(= I - Q^{-1}A$
$e^{(k)} = x^{(k)} - x$
$= \left(I - Q^{-1}A\right)x^{(k-1)} + Q^{-1}b - x$
$= \left(I - Q^{-1}A\right)x^{(k-1)} + \left(Q^{-1}A - I\right)x$
$= \left(I - Q^{-1}A\right)\left(x^{(k-1)} - x\right) = \left(I - Q^{-1}A\right)e^{(k-1)}$


Analysis
$\underline{x}^{(k+1)} = Q^{-1}\left((Q-A)x^{(k)} + b\right)$
$y = Q^{-1}b$
$= C\,x^{(k)} + y$
$(= I - Q^{-1}A$
$e^{(k)} = x^{(k)} - x$
$= \left(I - Q^{-1}A\right)x^{(k-1)} + Q^{-1}b - x$
$= \left(I - Q^{-1}A\right)x^{(k-1)} + \left(Q^{-1}A - I\right)x$
$= \left(I - Q^{-1}A\right)\left(x^{(k-1)} - x\right) = \left(I - Q^{-1}A\right)e^{(k-1)}$

$$\underline{\underline{Q}}\,\underline{x}^{(k+1)} = (\underline{\underline{Q}} - \underline{\underline{A}})\underline{x}^{(k)} + \underline{b}$$

We hope

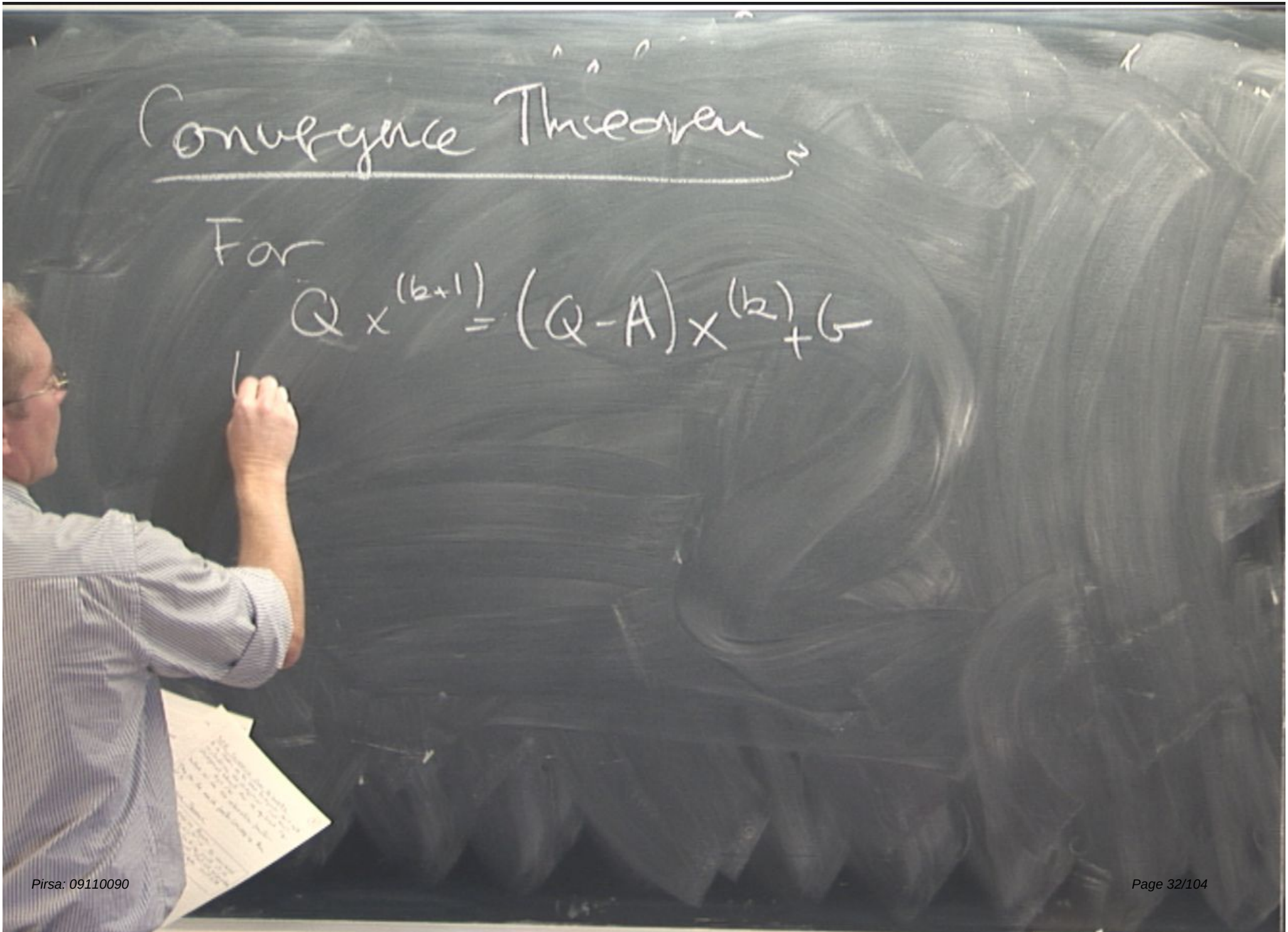
$$\underline{\underline{Q}}\,\underline{x}^{(k+1)} = \underline{y}$$

↑ Solve for $x^{(k+1)}$

$$\underline{\underline{Q}}\,\underline{x}^{*} = (\underline{\underline{Q}} - \underline{\underline{A}})\underline{x}^{*} + \underline{b} \iff \underline{\underline{A}}\,\underline{x}^{*} = \underline{b}$$

How should choose Q

- So that $\underline{\underline{Q}}\,\underline{x}^{(k+1)} = \underline{y}$ can be solved easily
- So that things converge ($Q^{-1}A$ should be "close" to I)


Convergence Theorem
For
$Q x^{(k+1)} = (Q - A) x^{(k)} + b$

Convergence Theorem:

For

$$Q x^{(k+1)} = (Q - A) x^{(k)} + b$$

to independent of $x^{(0)}$

Convergence Theorem

For

$$Q x^{(k+1)} = (Q - A) x^{(k)} + b$$

to independent of $x^{(0)}$

it is a necessary and sufficient

condition that all eigenvalues

of $I - Q^{-1} A$

Convergence Theorem

For

$$Q x^{(k+1)} = (Q - A) x^{(k)} + b$$

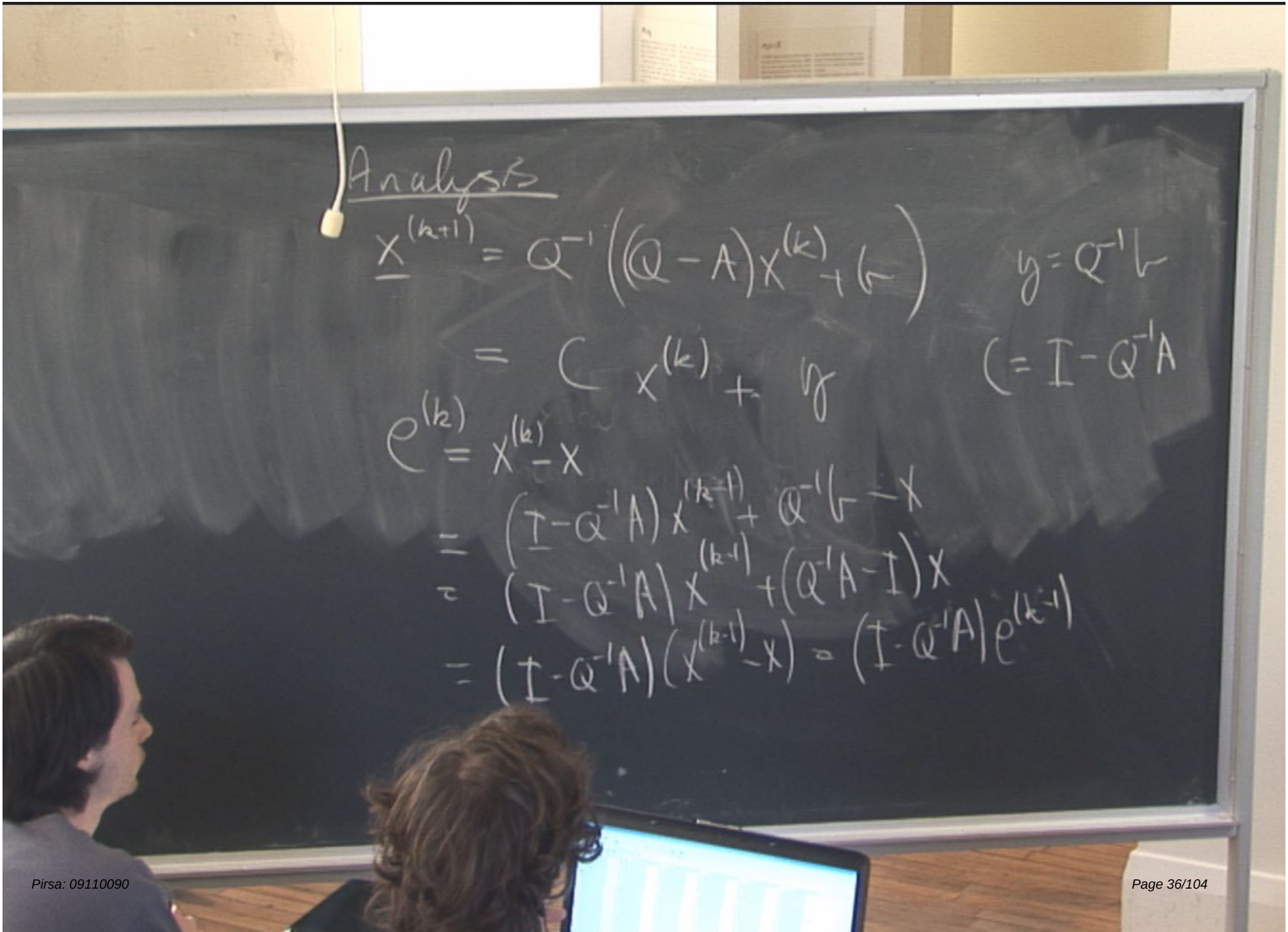
to independent of $x^{(0)}$

it is a necessary and sufficient

condition that all eigenvalues

of $I - Q^{-1}A$ lie in the open

unit circle $\rho(I - Q^{-1}A) < 1$


Analysis
$x^{(k+1)} = Q^{-1}\left((Q-A)x^{(k)} + b\right)$
$y = Q^{-1}b$
$= C x^{(k)} + y$
$(= I - Q^{-1}A$
$e^{(k)} = x^{(k)} - x$
$= \left(I - Q^{-1}A\right)x^{(k-1)} + Q^{-1}b - x$
$= \left(I - Q^{-1}A\right)x^{(k-1)} + \left(Q^{-1}A - I\right)x$
$= \left(I - Q^{-1}A\right)\left(x^{(k-1)} - x\right) = \left(I - Q^{-1}A\right)e^{(k-1)}$

Convergence Theorem

Spectral radius theorem

For

$$Q x^{(k+1)} = (Q - A) x^{(k)} + b$$

to independent of $x^{(0)}$

it is a necessary and sufficient condition that all eigenvalues of $I - Q^{-1}A$ lie in the open unit circle

$$\rho(I - Q^{-1}A) < 1$$

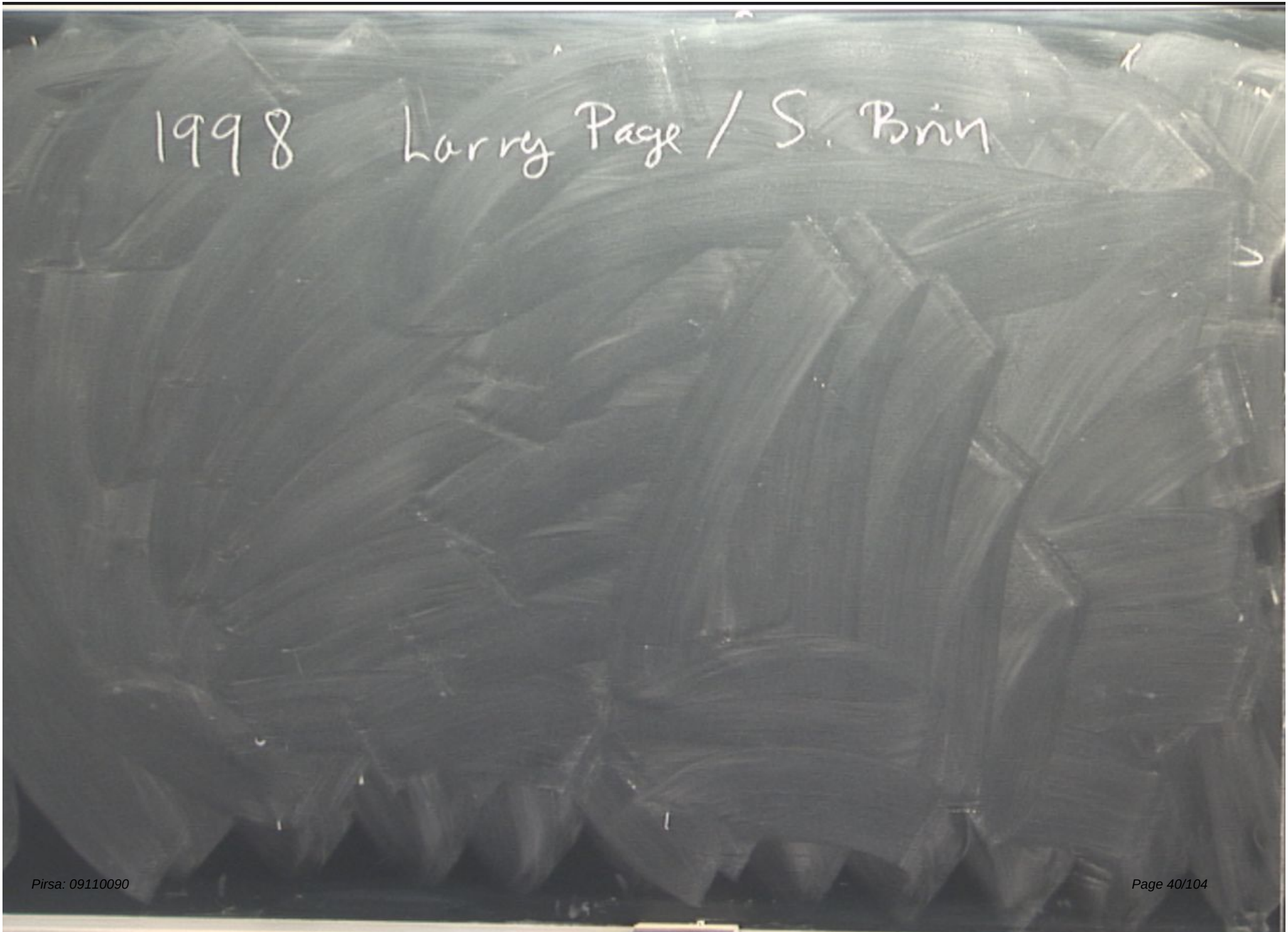
Diagonally dominance

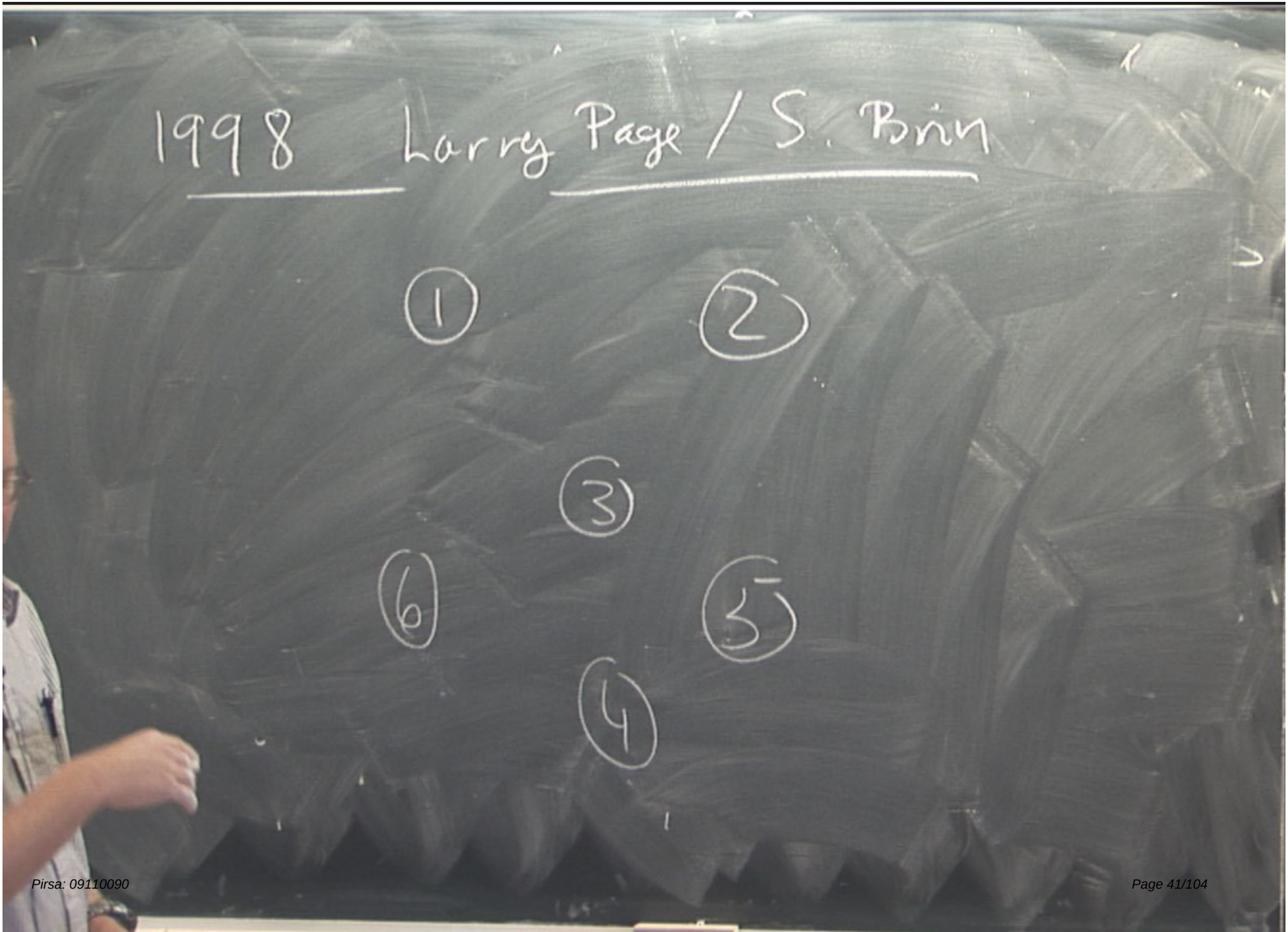
$$|a_{ii}| > \sum_{\substack{j=1 \\ j \neq i}} |a_{ij}|$$

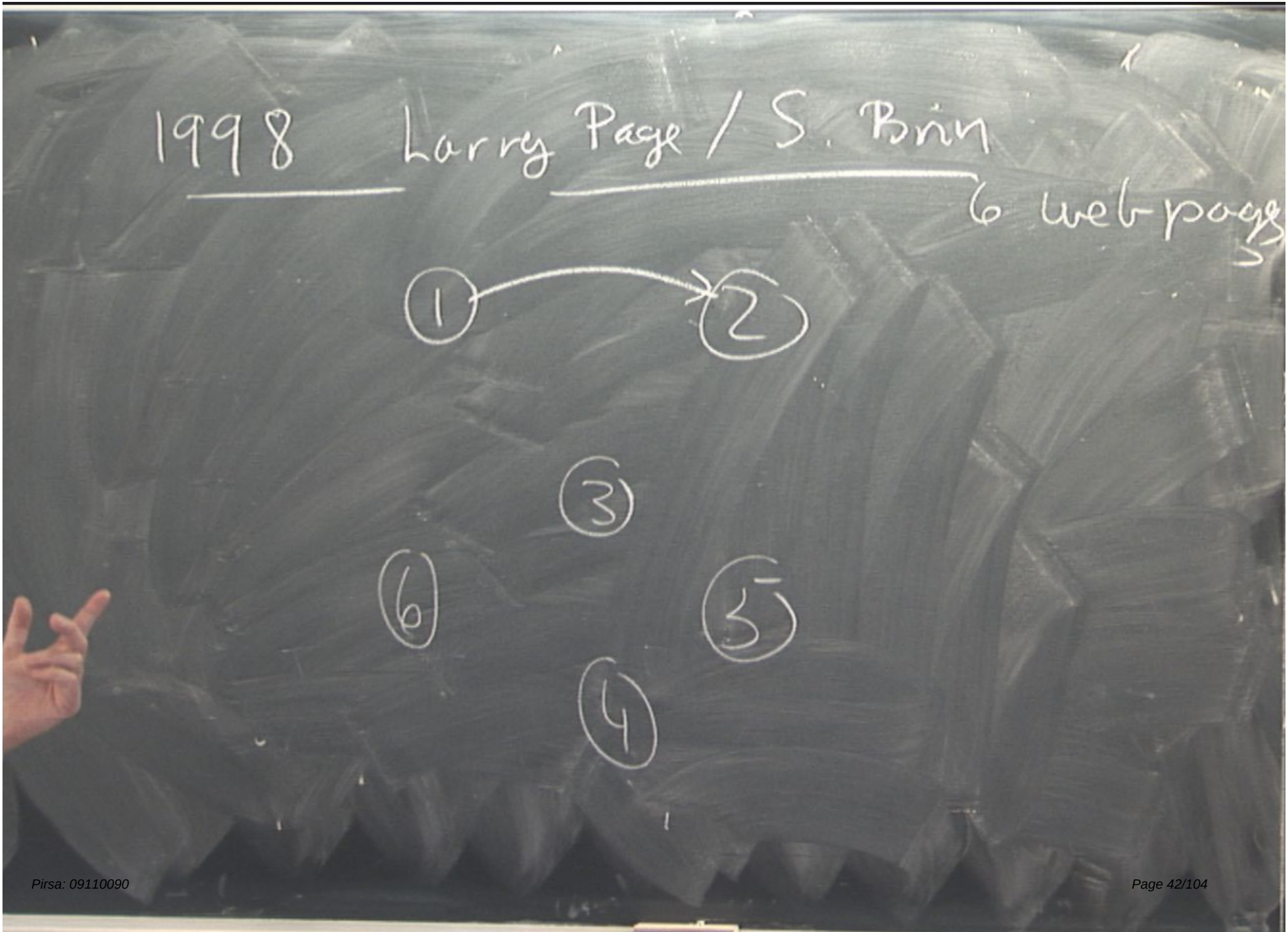
Diagonally dominance

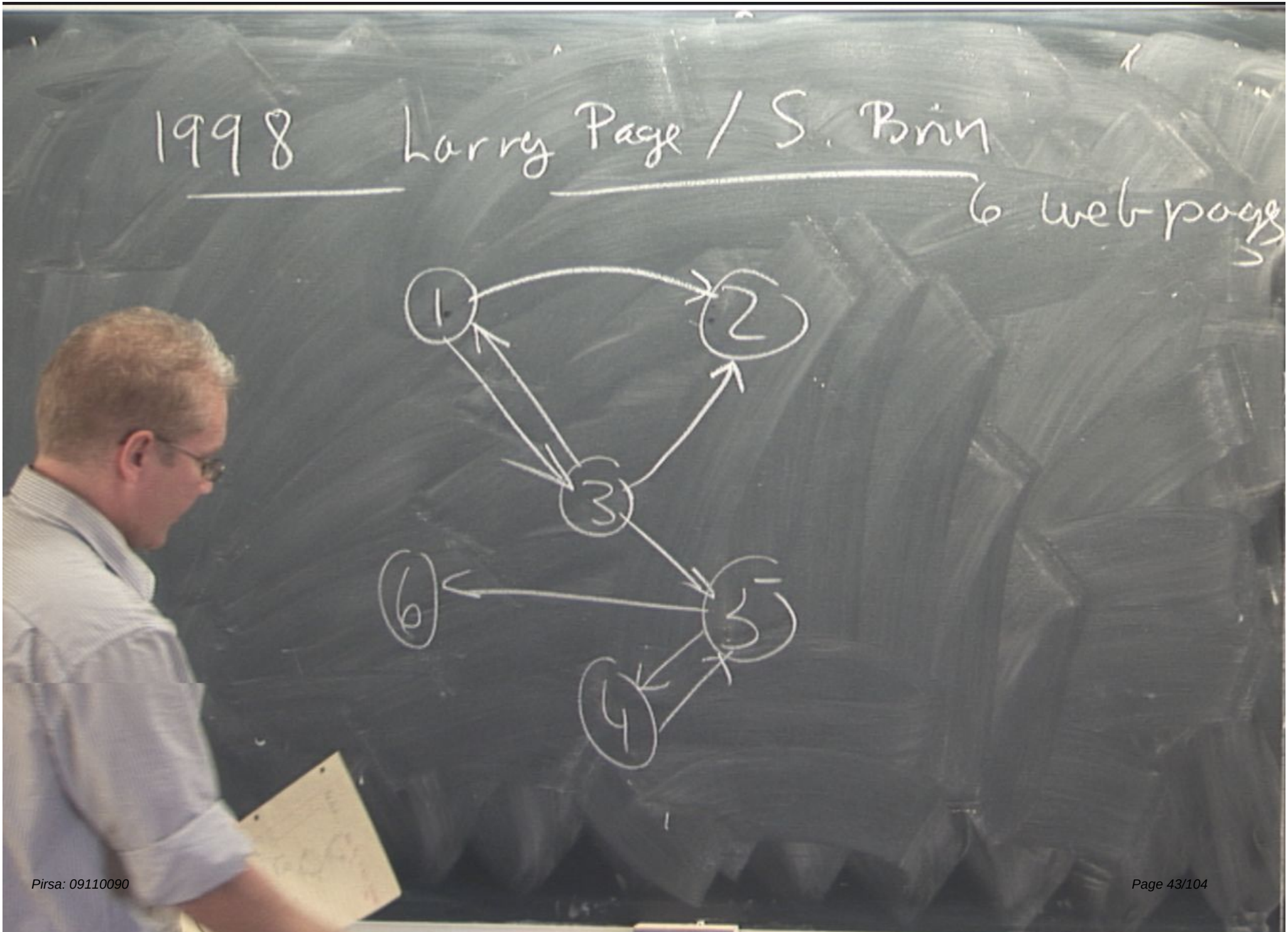
$$|a_{ii}| > \sum_{\substack{j=1 \\ j \neq i}} |a_{ij}|$$

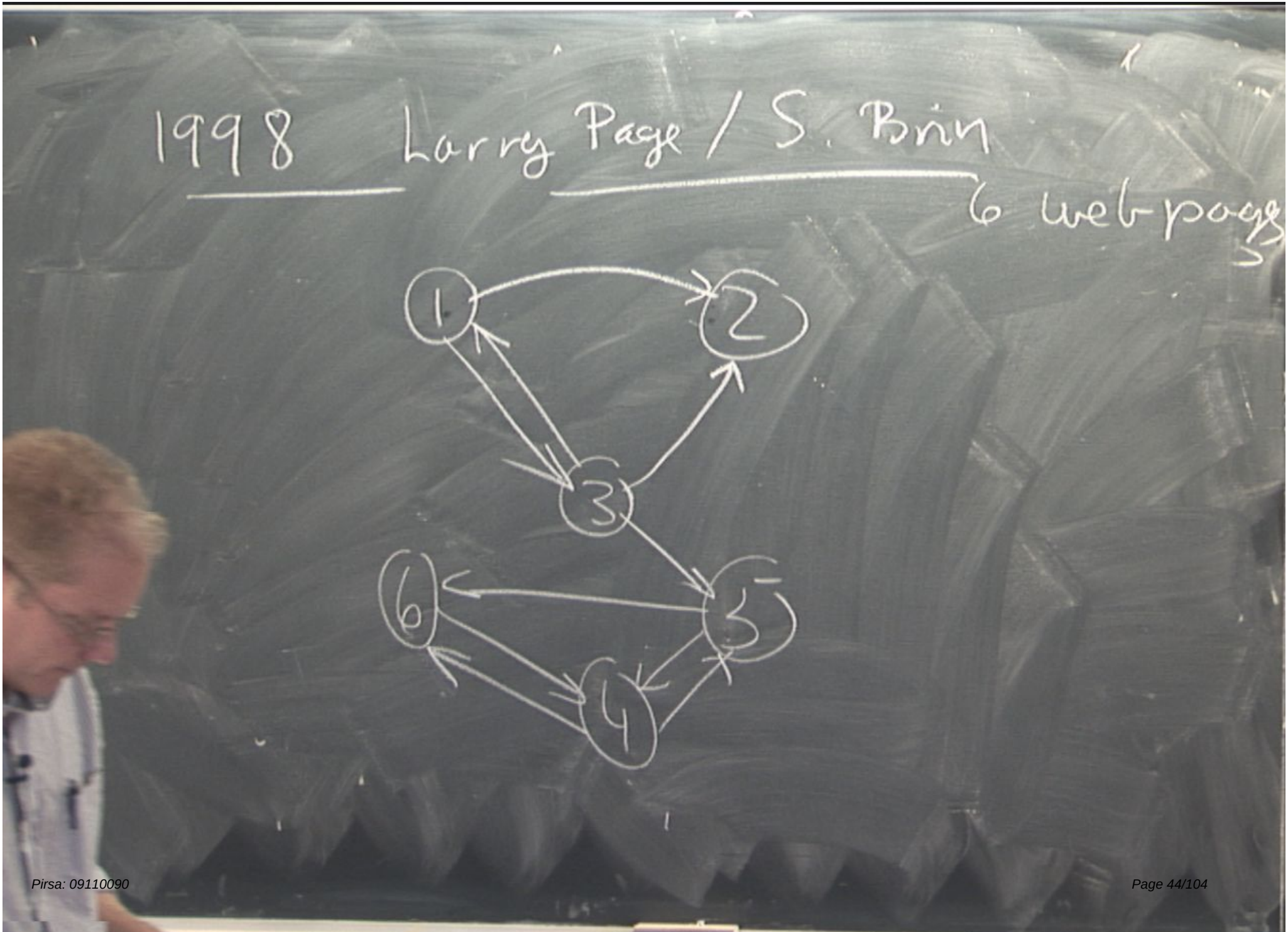
If A is diagonally dominant then Jacobi and G-S converge for any $x^{(0)}$

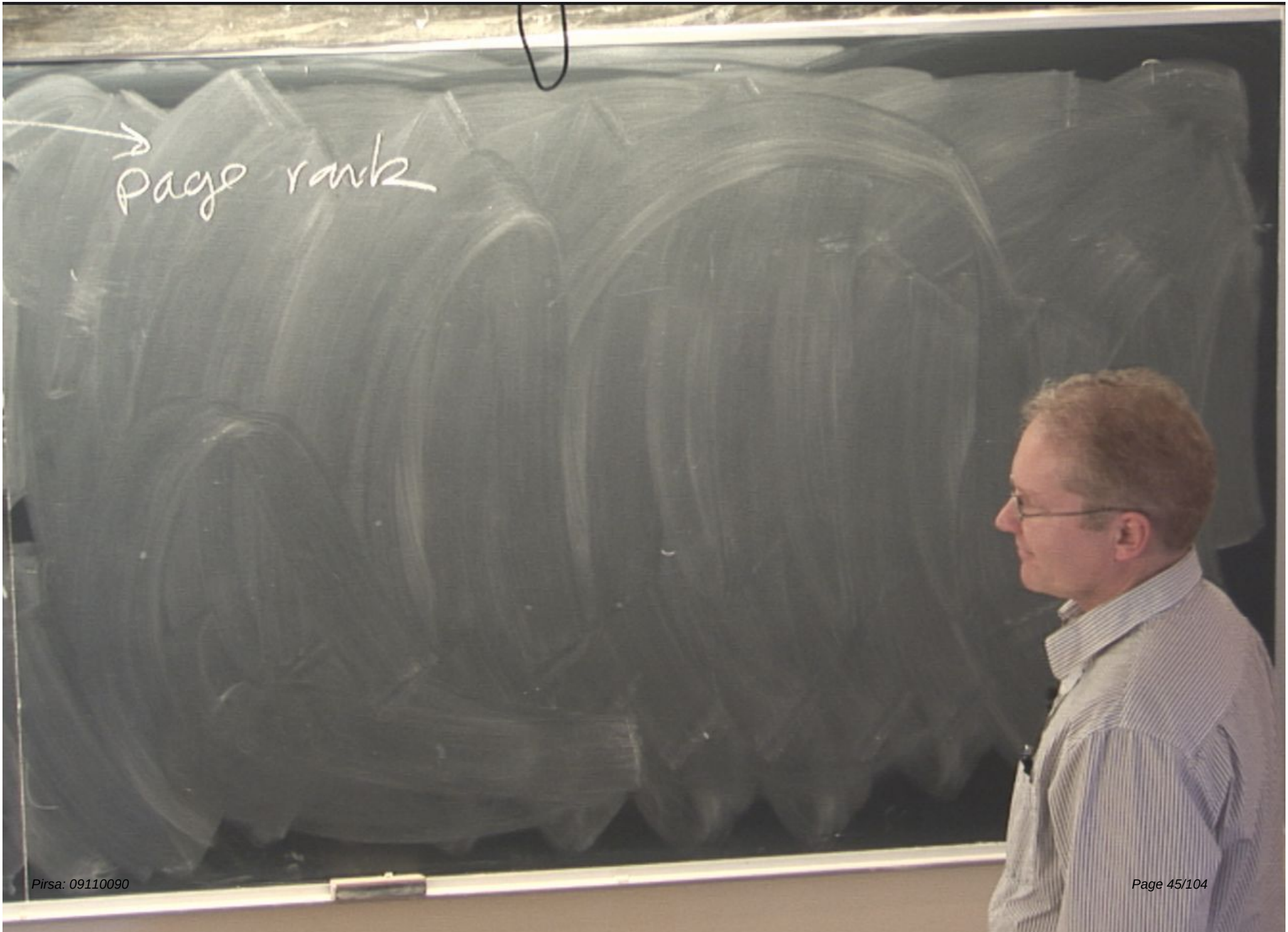

1998 Larry Page / S. Brin

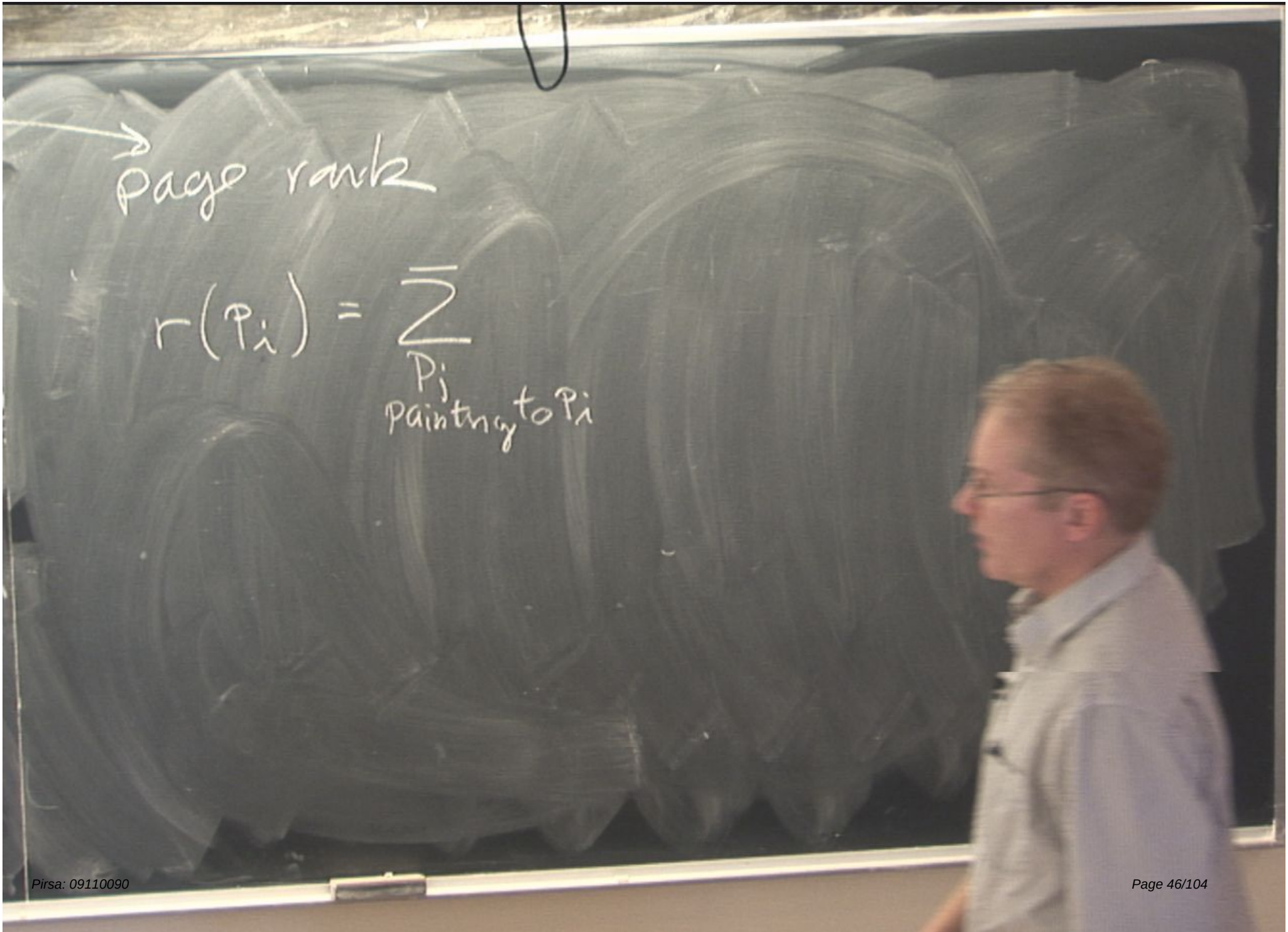

1998 Larry Page / S. Brin
1
2
3
6
5
4

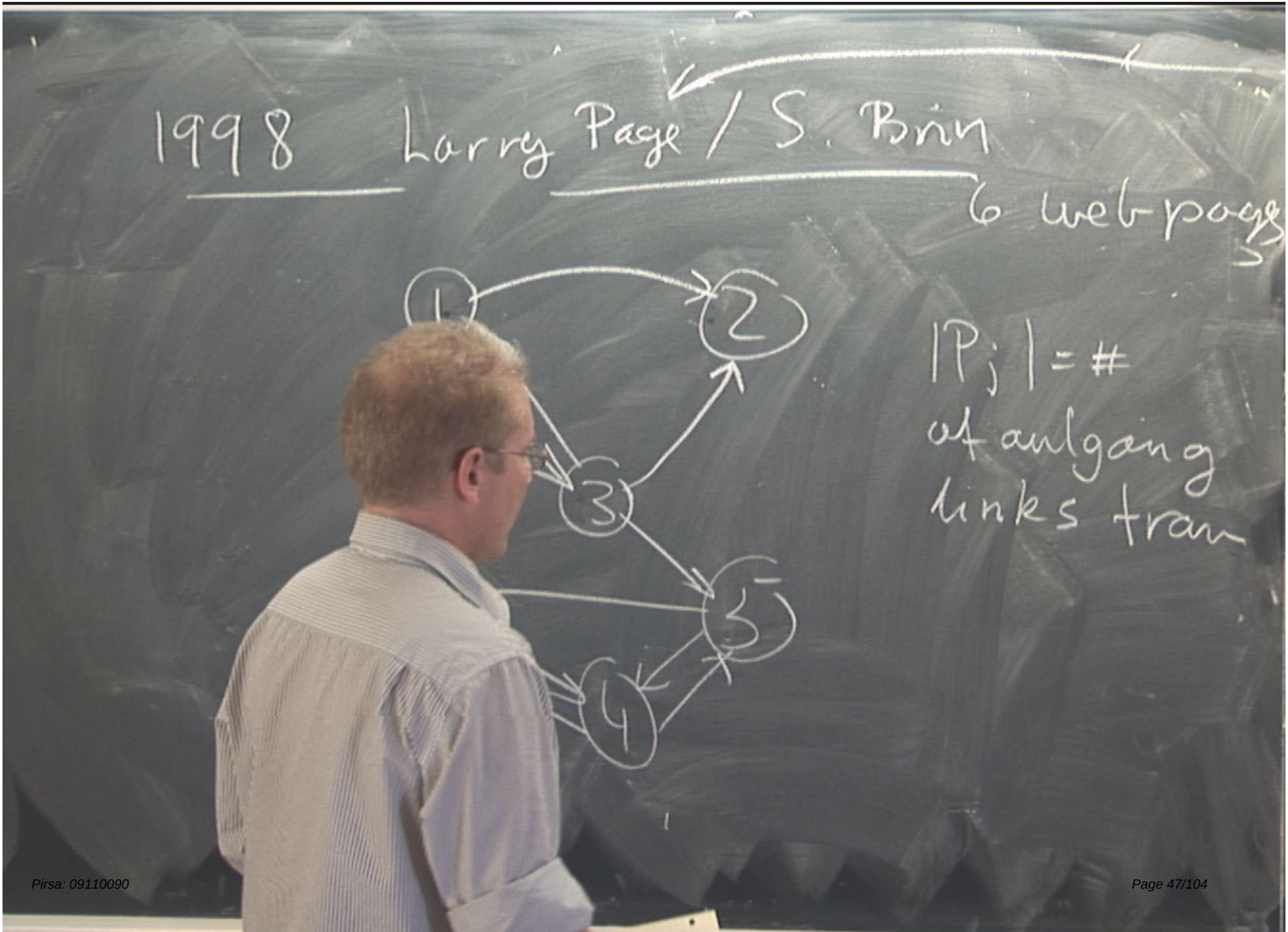

1998 Larry Page / S. Brin
6 web-pages
1
2
3
6
5
4

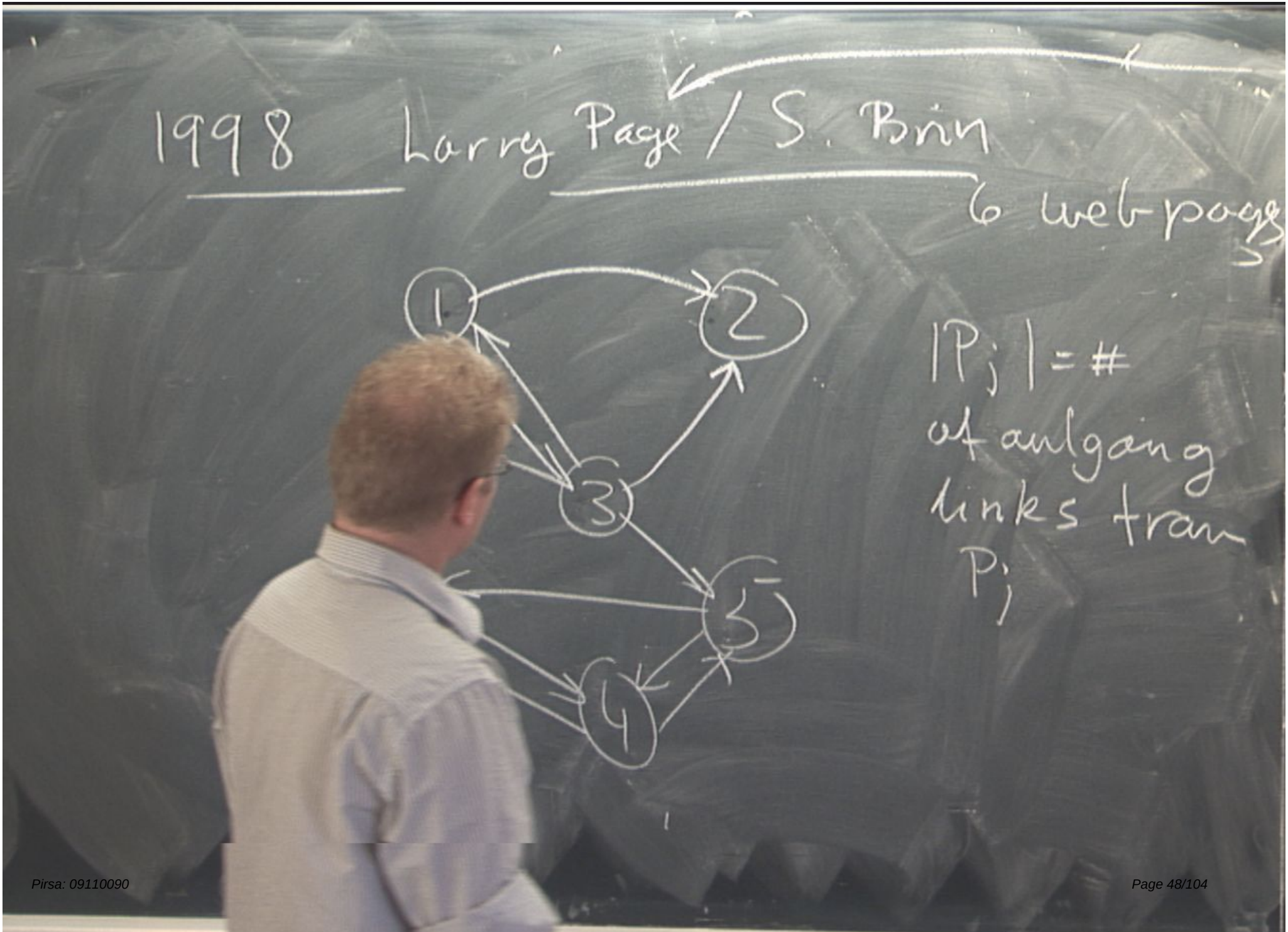

1998 Larry Page / S. Brin
6 web-pages
1
2
3
6
5
4


1998 Larry Page / S. Brin
6 web-pages
1
2
3
6
5
4


Page rank

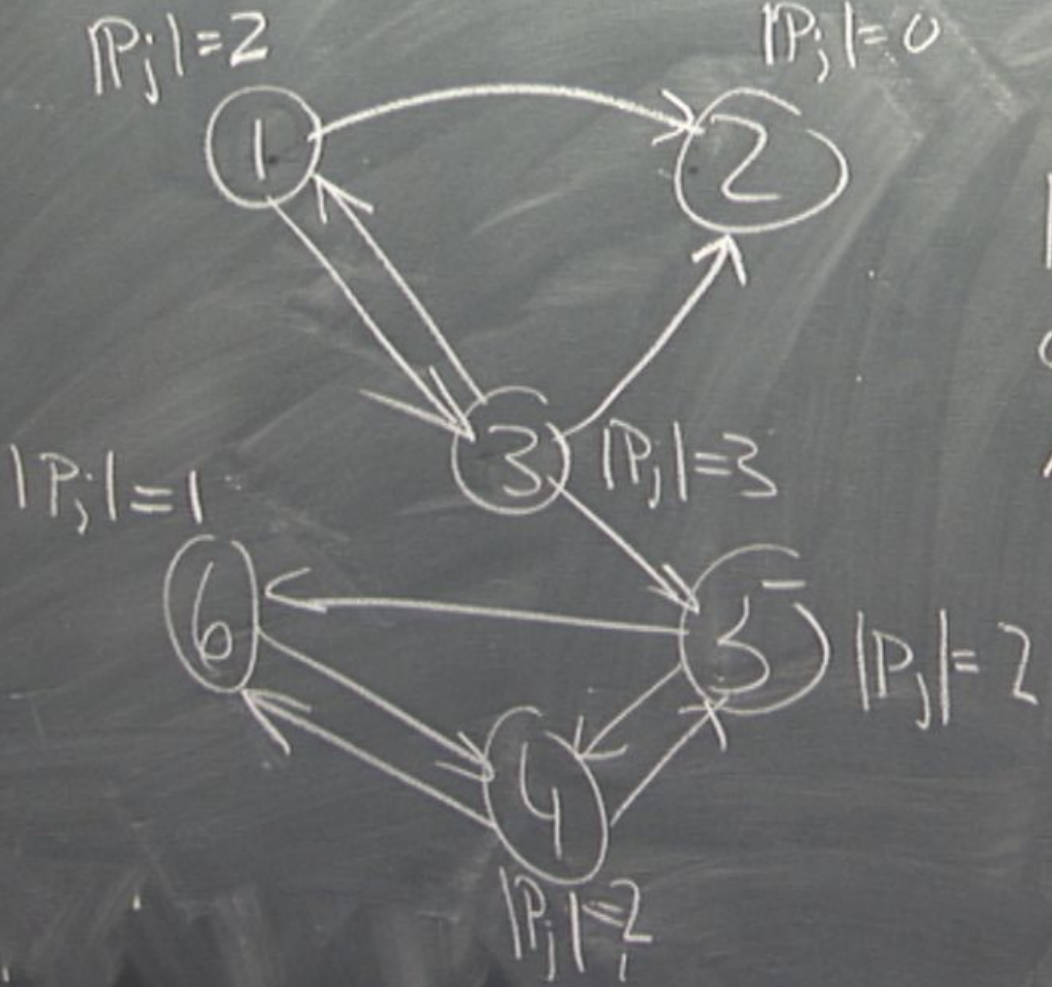

page rank
$r(p_i) = \sum_{p_j \text{ pointing to } p_i}$


1998 Larry Page / S. Brin
6 web-pages
1
2
3
5
4
|Pj| = #
of outgoing
links from

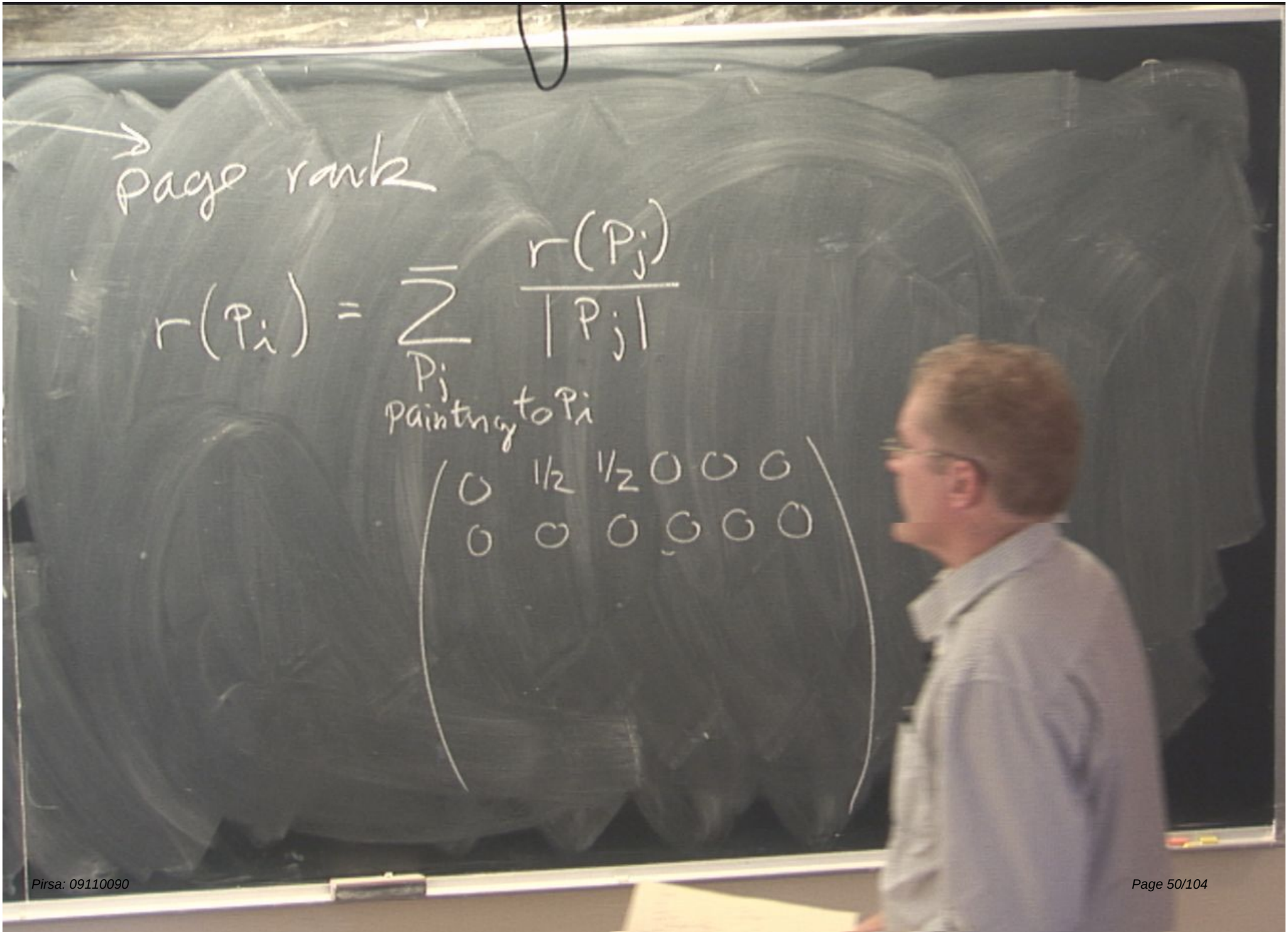

1998 Larry Page / S. Brin
6 web-pages
1
2
3
5
4
|Pj| = # of outgoing links from Pj

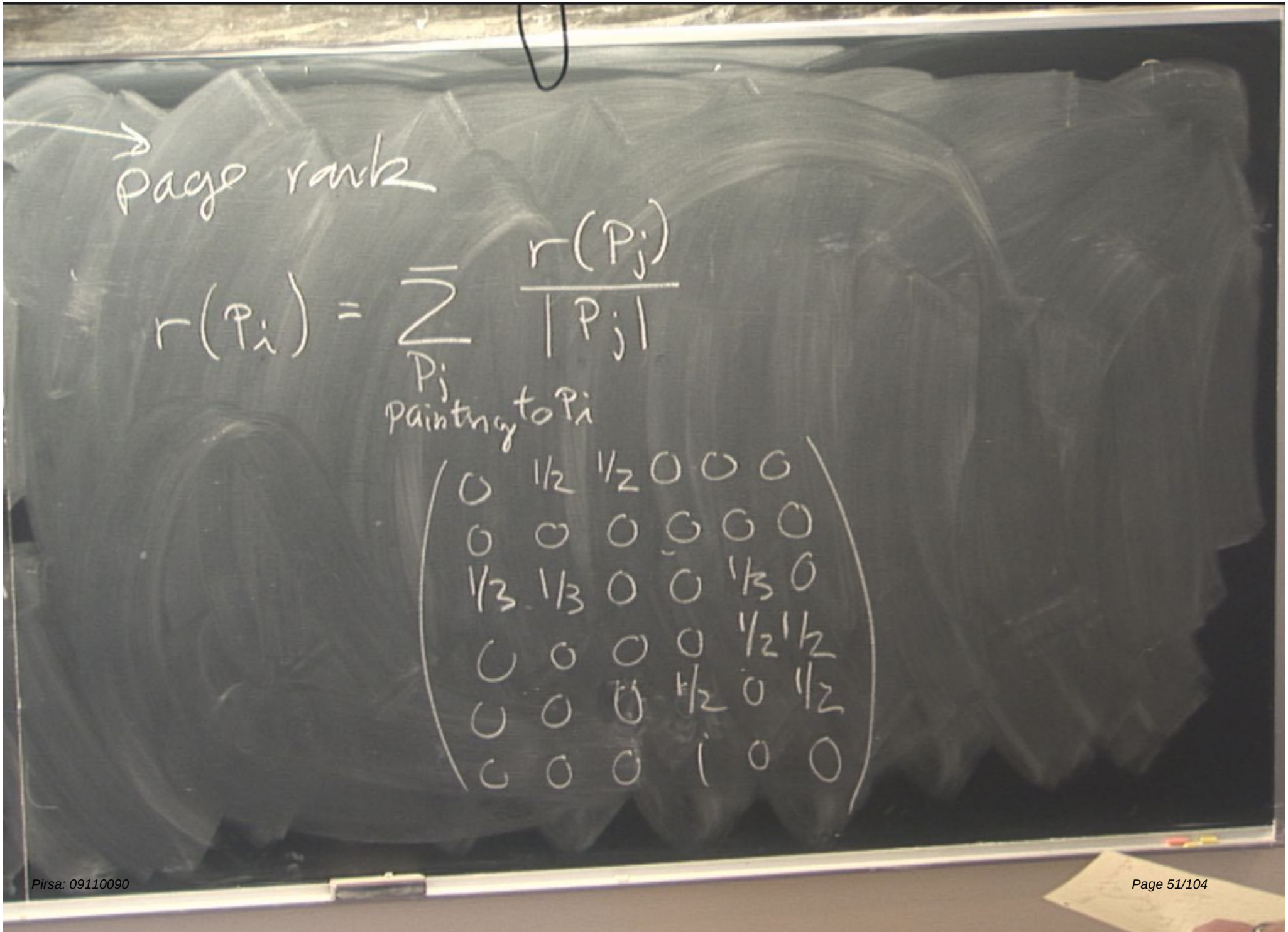
1998 Larry Page / S. Brin

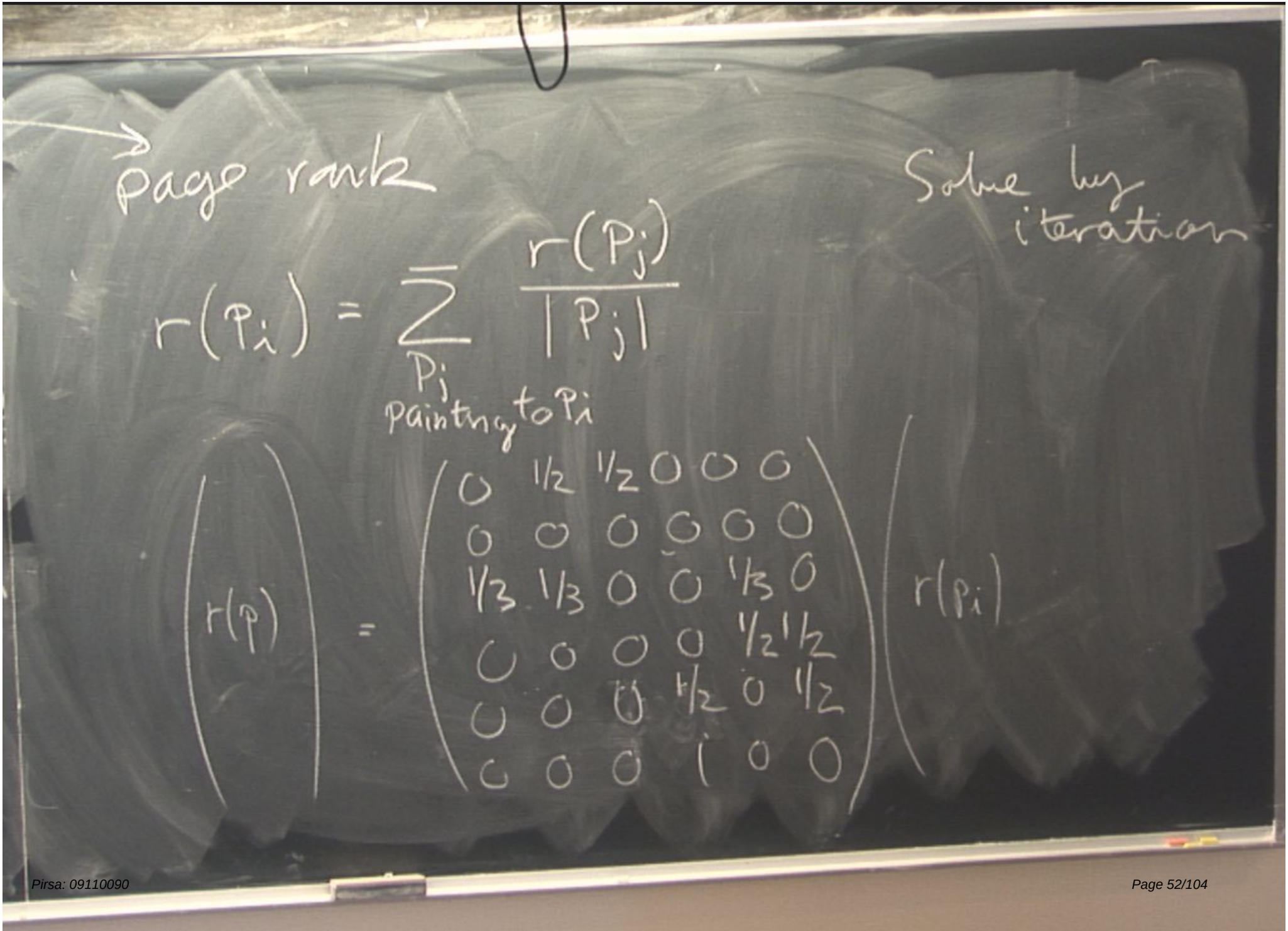
6 web-pages

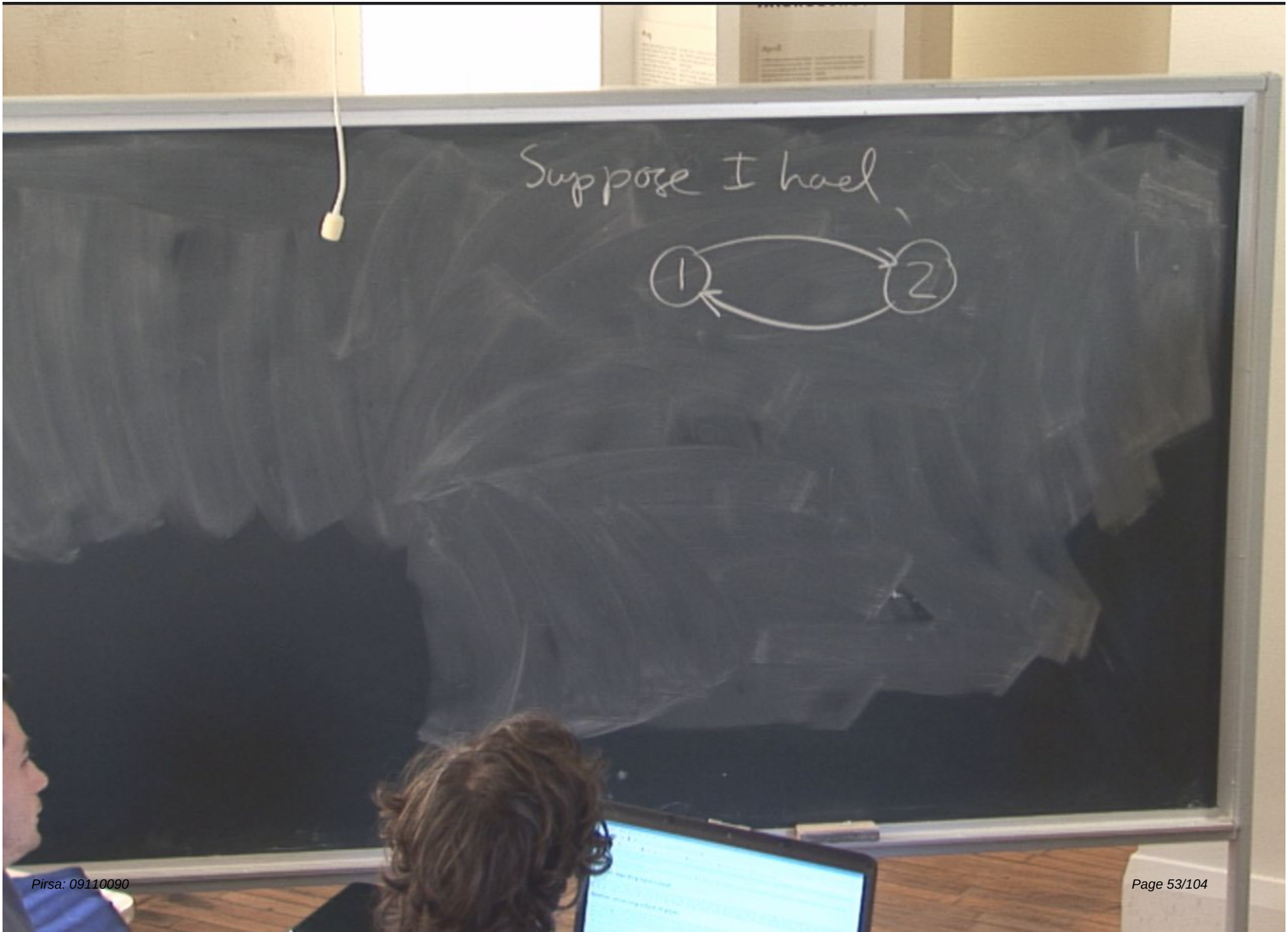


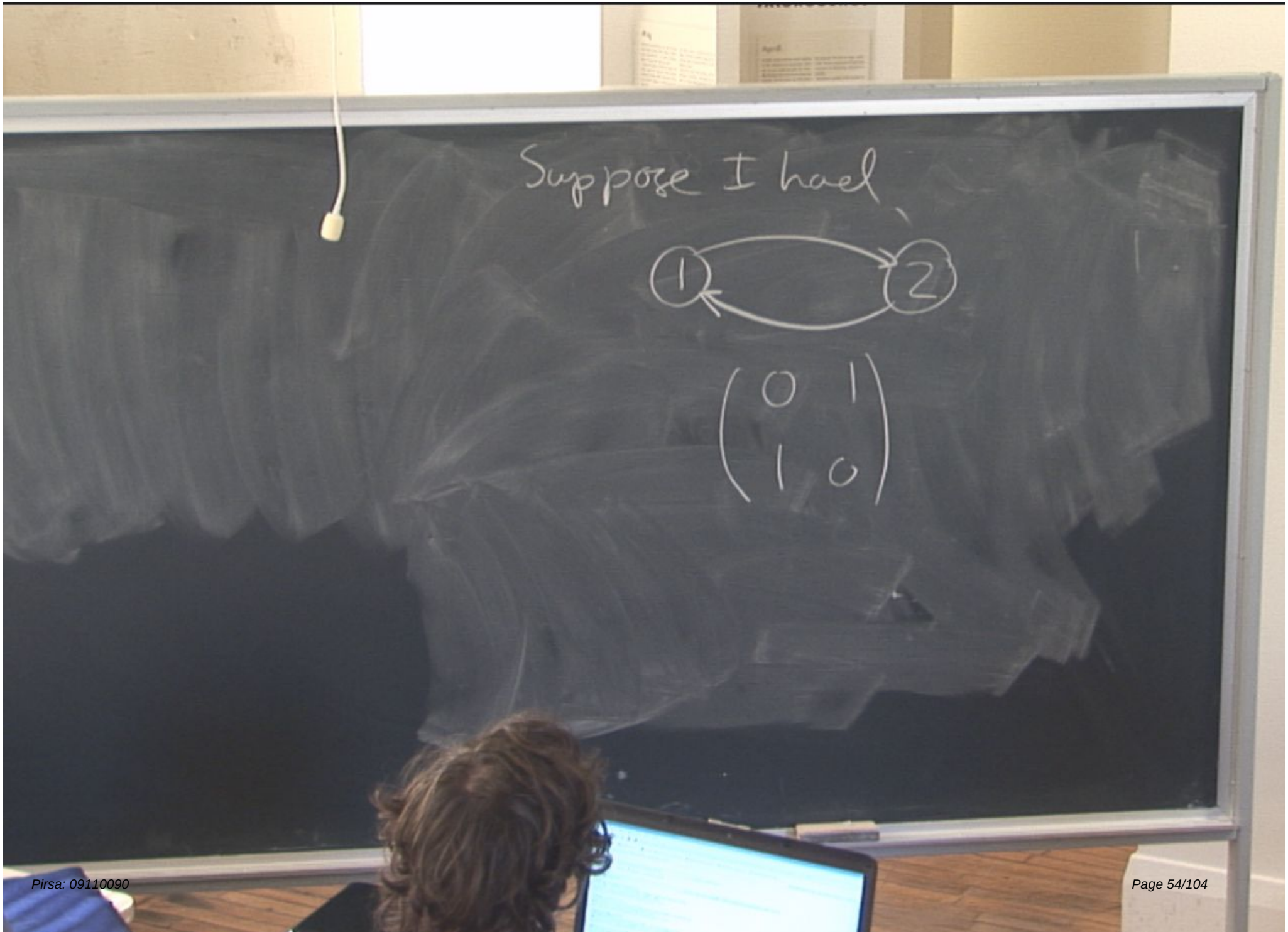
$|P_j|$ = # of outgoing links from P_j

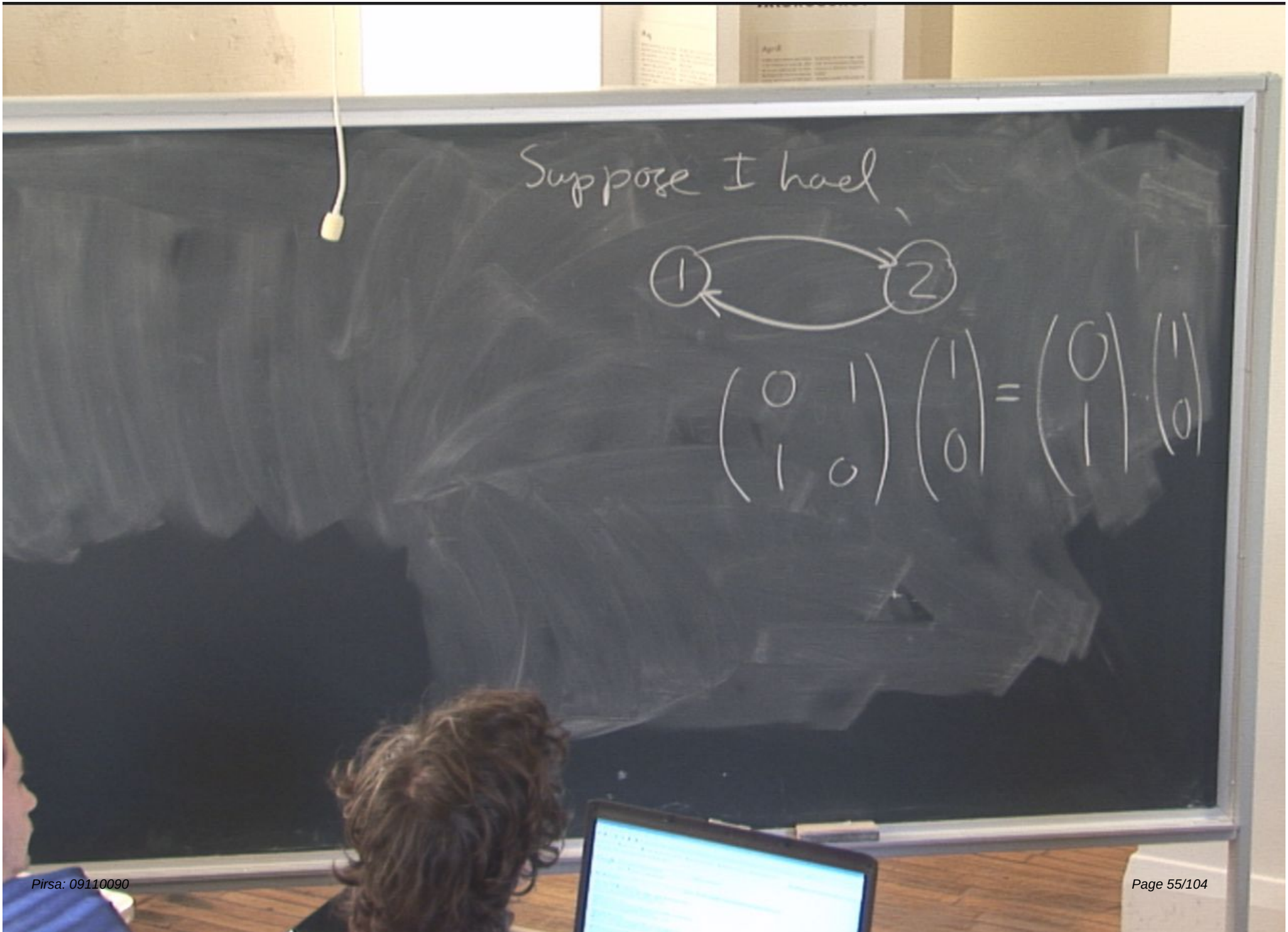

page rank
$r(P_i) = \sum_{P_j \text{ pointing to } P_i} \frac{r(P_j)}{|P_j|}$
$\begin{pmatrix} 0 & 1/2 & 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$

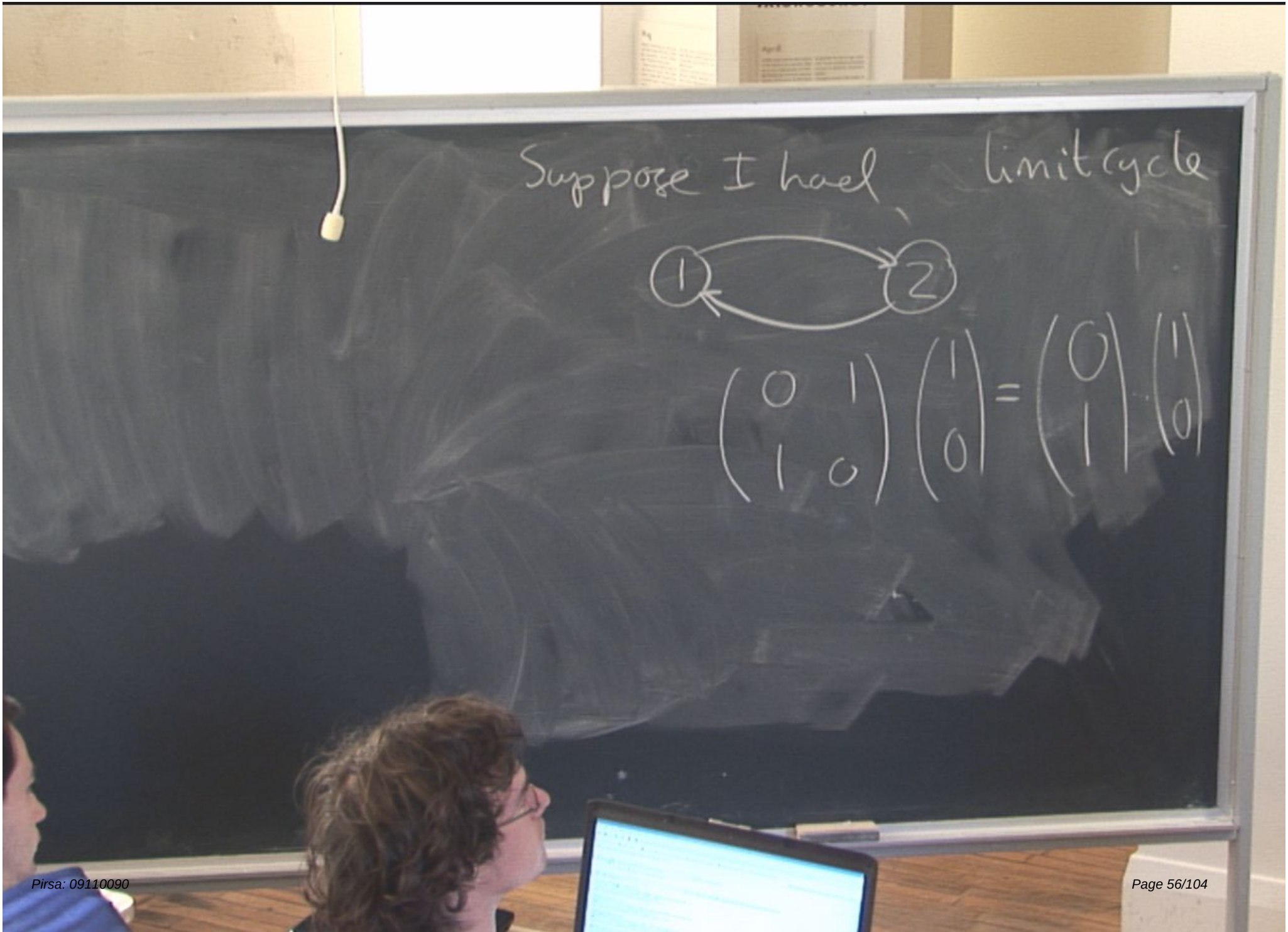

Page rank
$r(P_i) = \sum_{P_j \text{ pointing to } P_i} \frac{r(P_j)}{|P_j|}$
$\begin{pmatrix} 0 & 1/2 & 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1/3 & 1/3 & 0 & 0 & 1/3 & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 0 & 1/2 & 0 & 1/2 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$

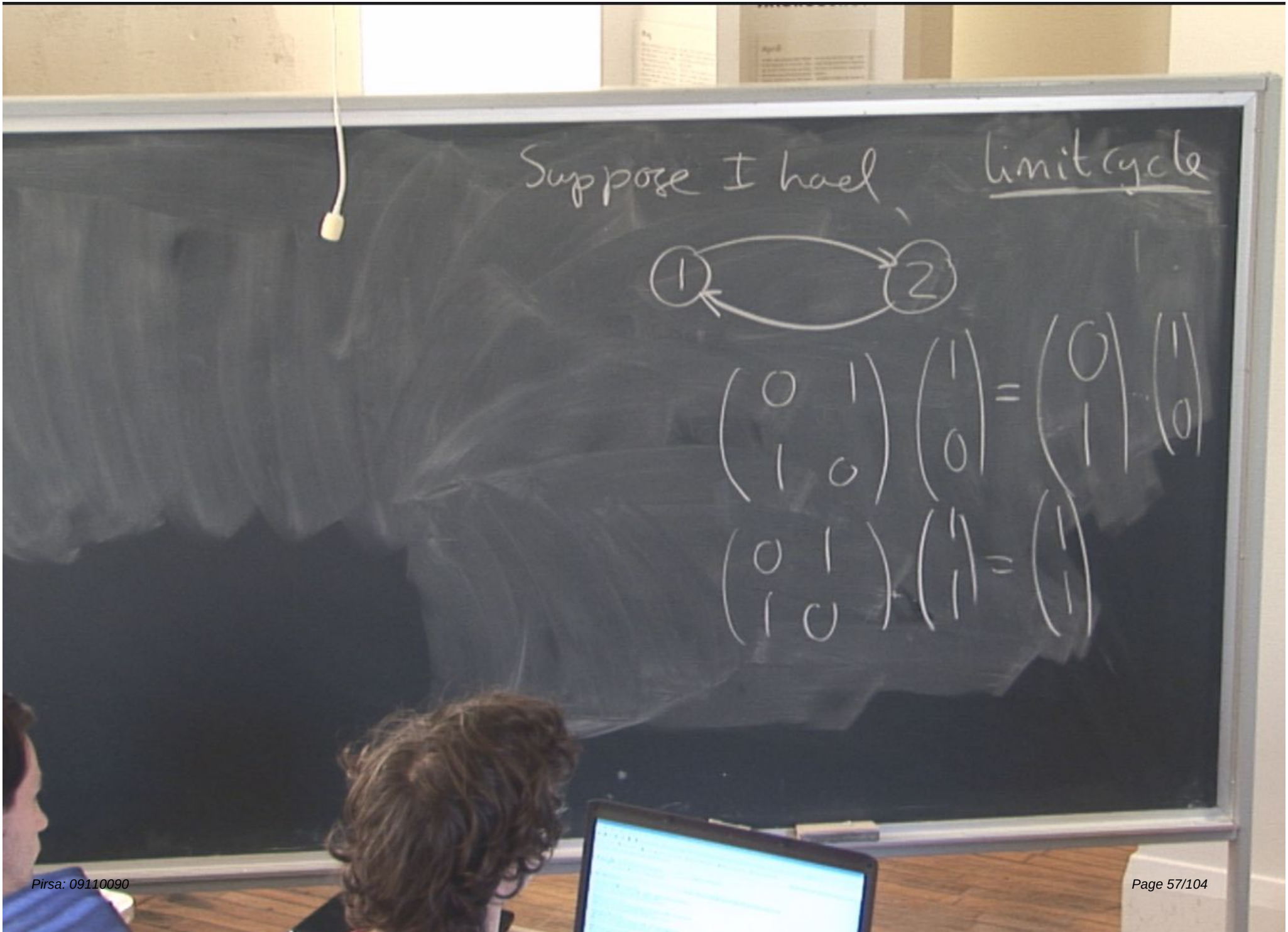

Page rank
Solve by iteration
$r(P_i) = \sum_{P_j \text{ pointing to } P_i} \frac{r(P_j)}{|P_j|}$
$r(P) = \begin{pmatrix} 0 & 1/2 & 1/2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1/3 & 1/3 & 0 & 0 & 1/3 & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 0 & 1/2 & 0 & 1/2 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} r(P_i)$

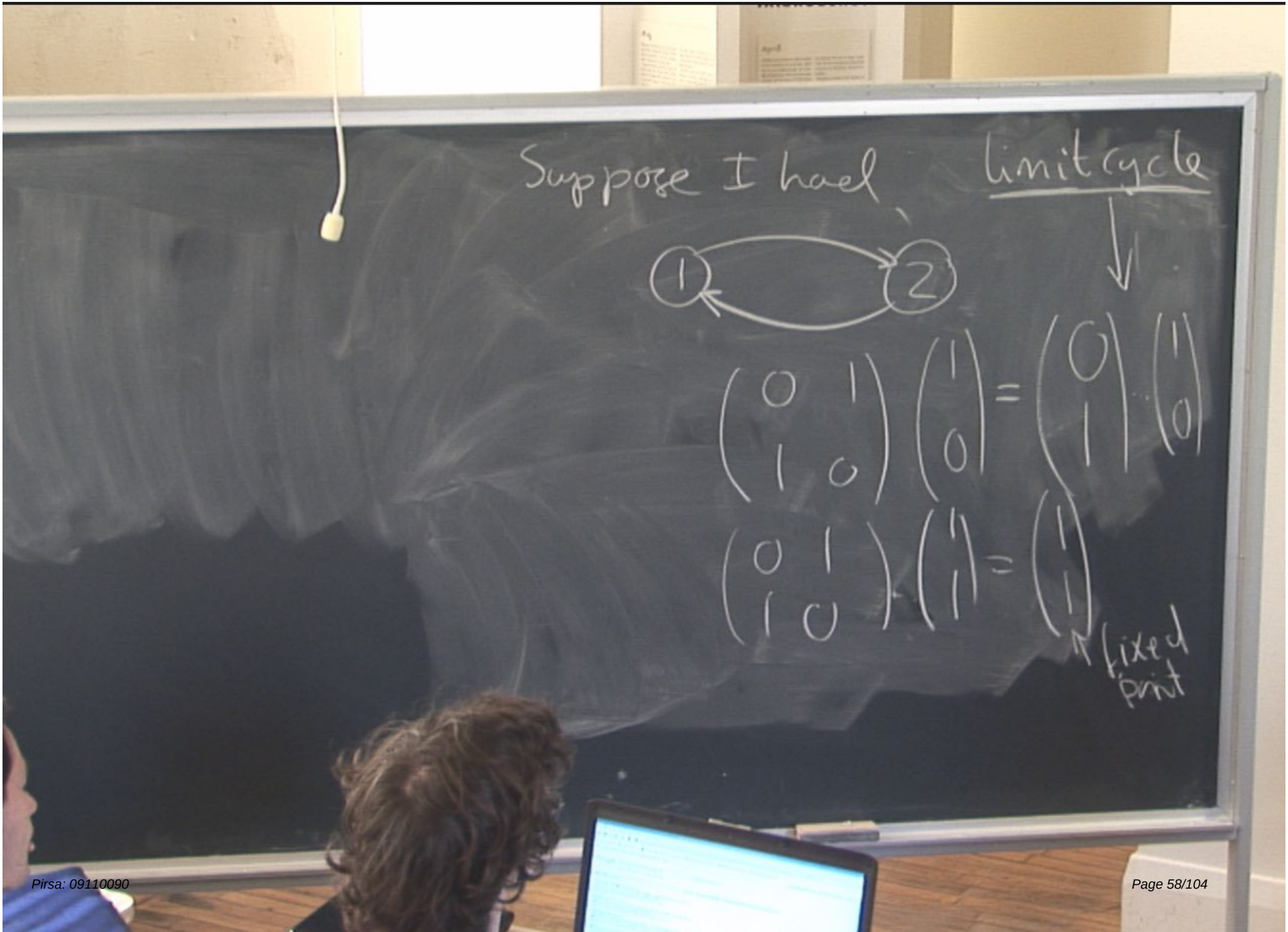

Suppose I had
1
2

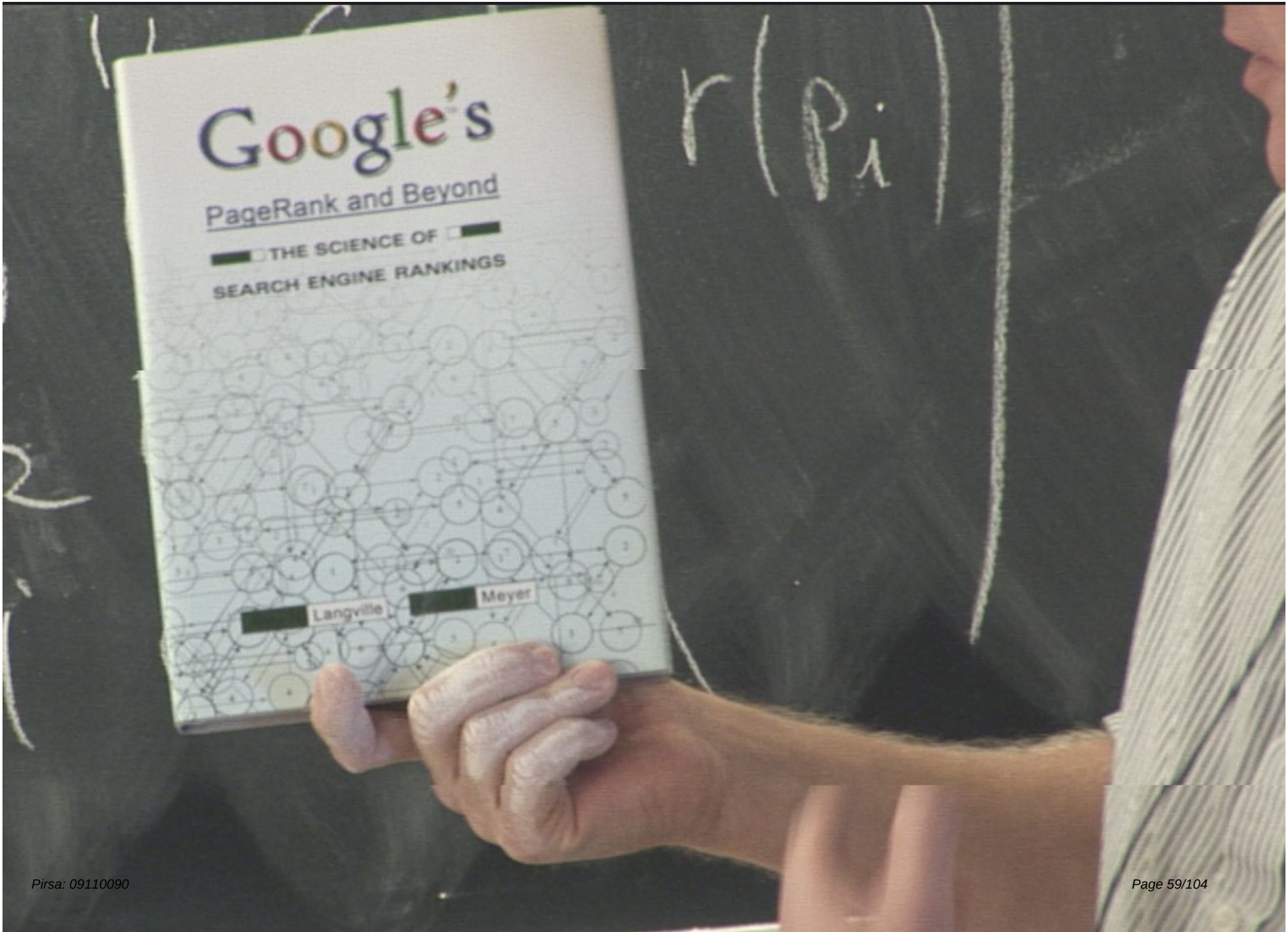

Suppose I had
1
2
0 1
1 0

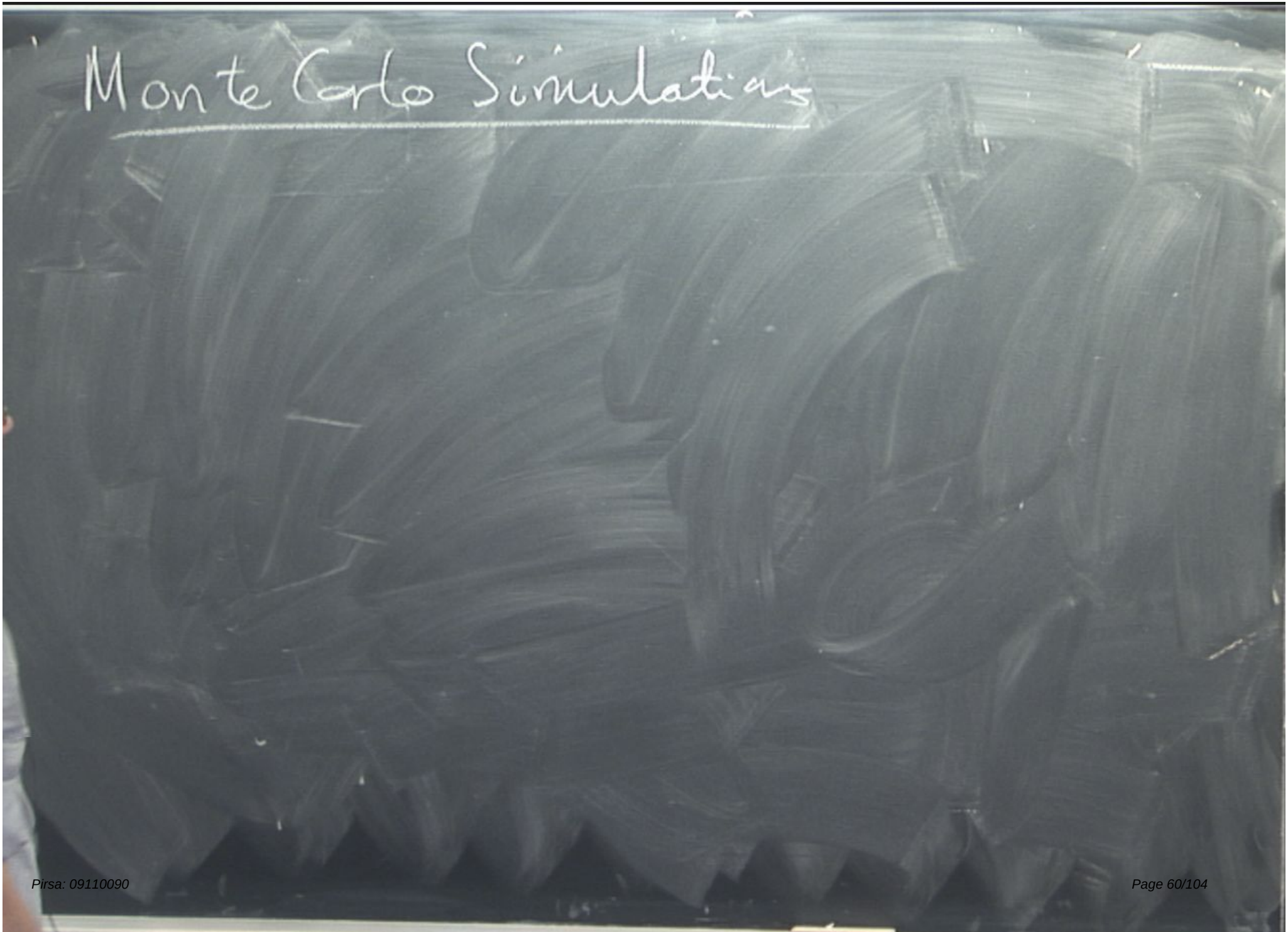

Suppose I had,
1
2
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$


Suppose I had a limit cycle
1
2
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$


Suppose I had
limit cycle
1
2
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

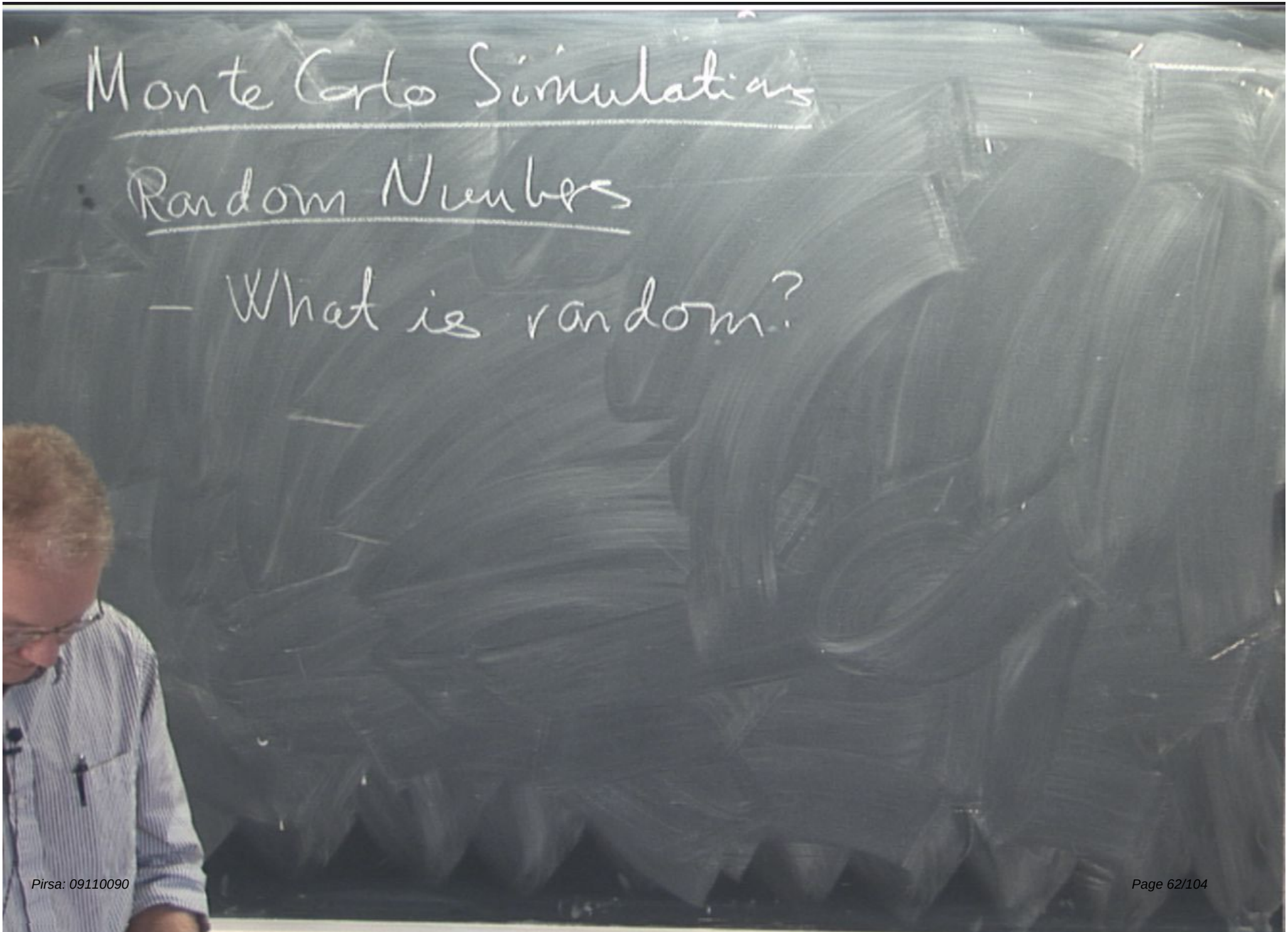

Suppose I had
limit cycle
1
2
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
fixed point


Google's
PageRank and Beyond
THE SCIENCE OF
SEARCH ENGINE RANKINGS
Langville
Meyer
r(Pi


Monte Carlo Simulations

Monte Carlo Simulations

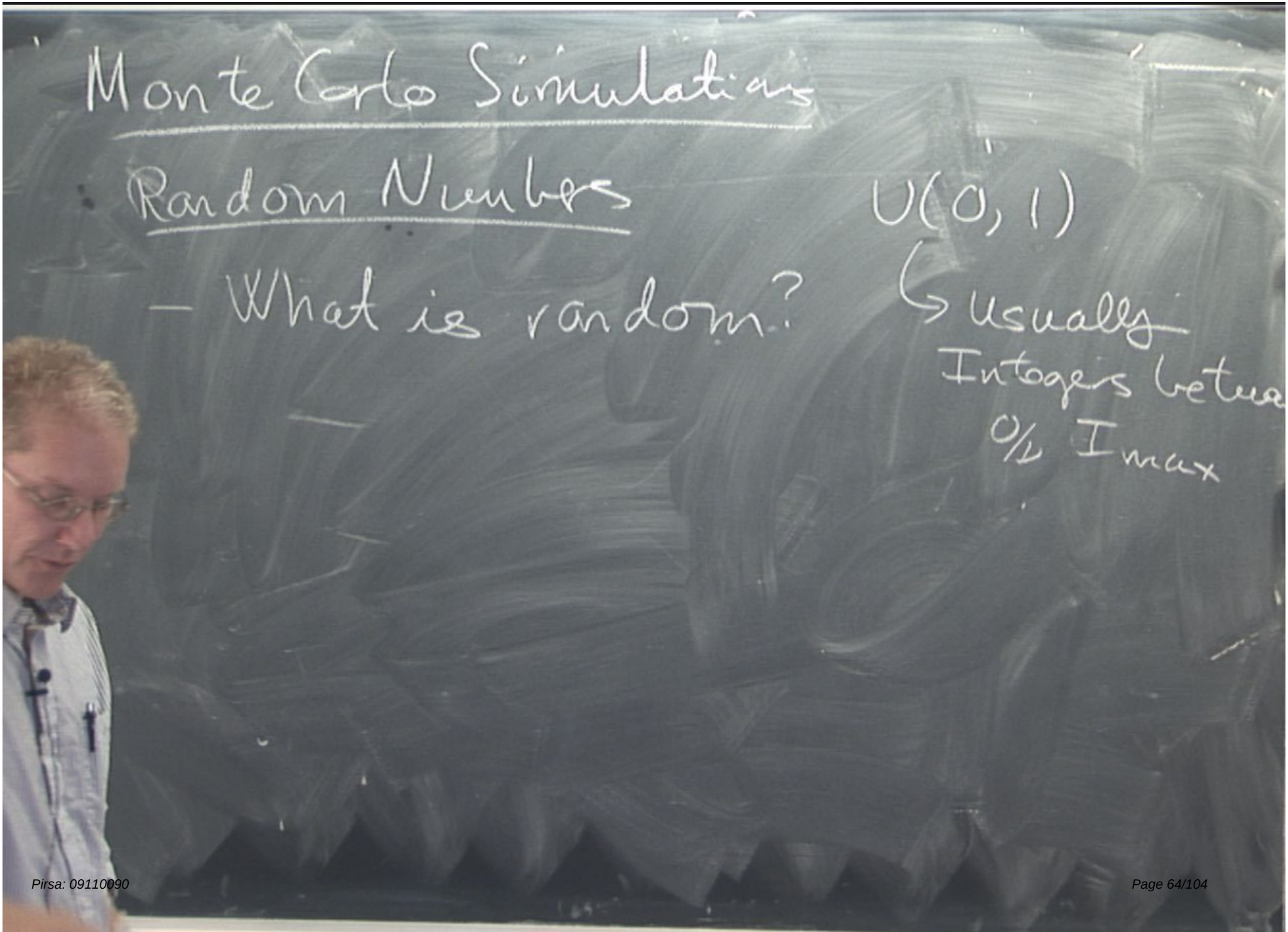
Random Numbers


Monte Carlo Simulations
Random Numbers
– What is random?

Monte Carlo Simulations

Random Numbers $U(0,1)$

– What is random?


Monte Carlo Simulations
Random Numbers
– What is random?
U(0, 1)
↳ Usually
Integers betwe
0/1 Imax

Monte Carlo Simulations

Random Numbers

- What is random?
- Pseudo-Random Numbers

$U(0,1)$

↳ Usually Integers between 0 & I_{max}

Monte Carlo Simulations

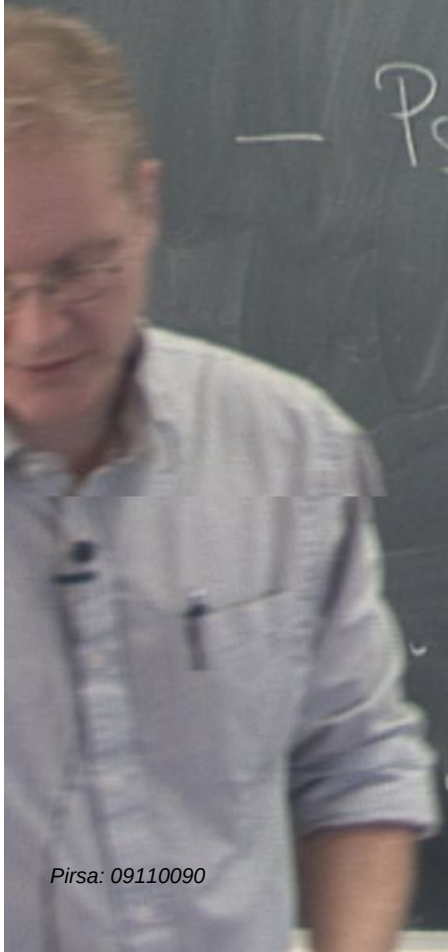
Random Numbers

- What is random?
- Pseudo-Random Numbers
  deterministic

$U(0,1)$

↳ usually Integers between 0 & I_{max}

$I^{(k+1)}$ from $I^{(k)}$

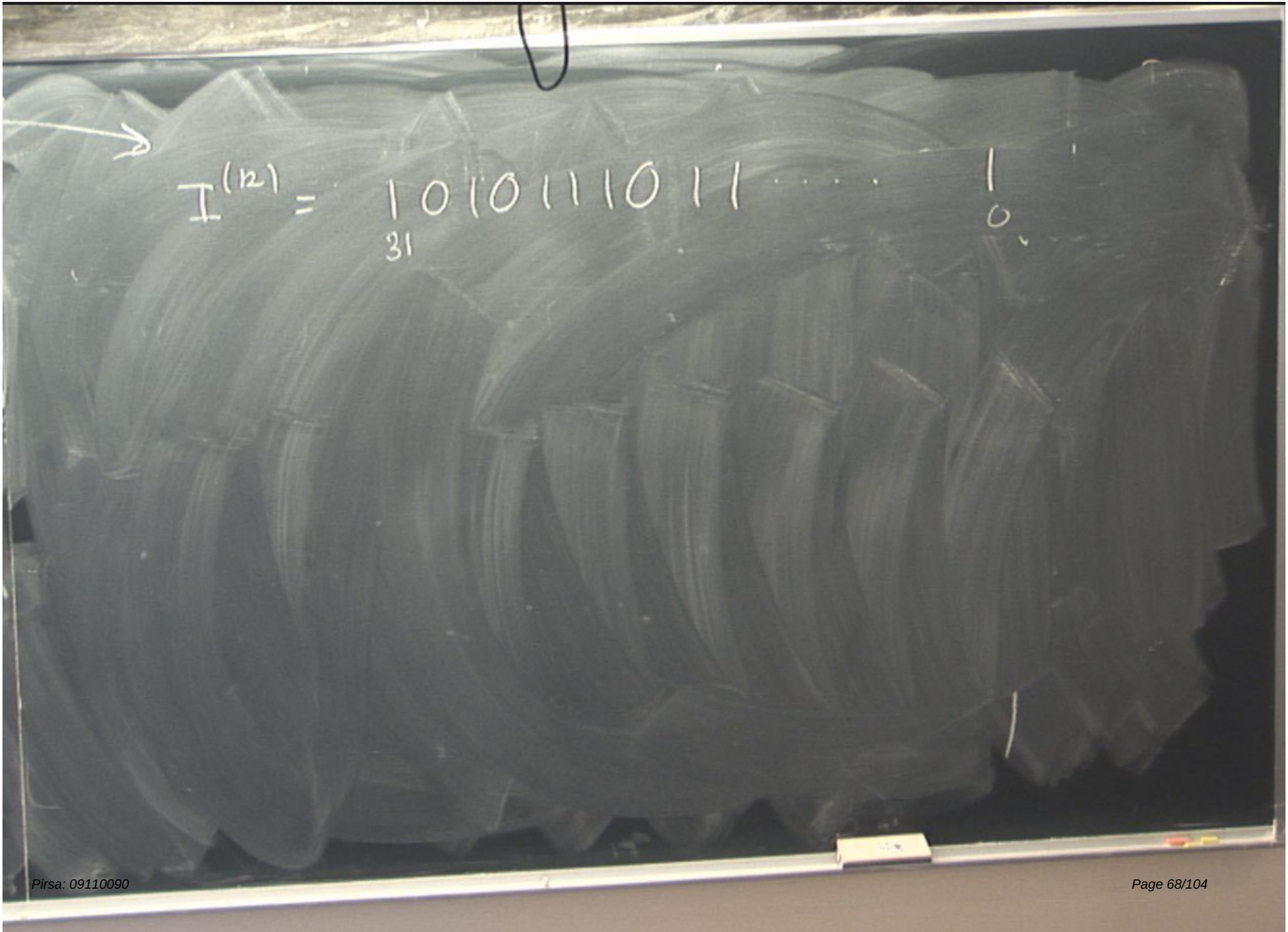


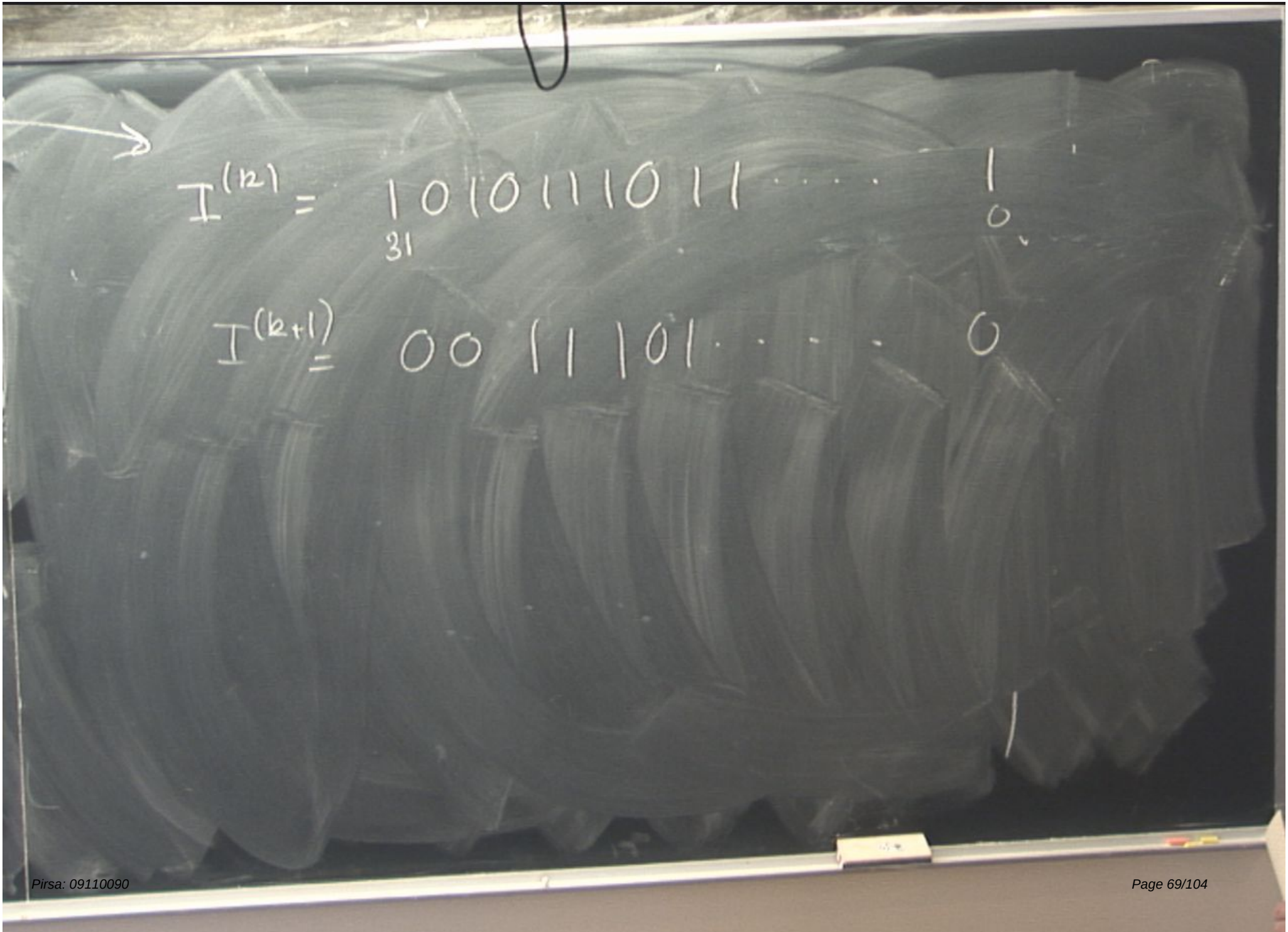
Monte Carlo Simulations

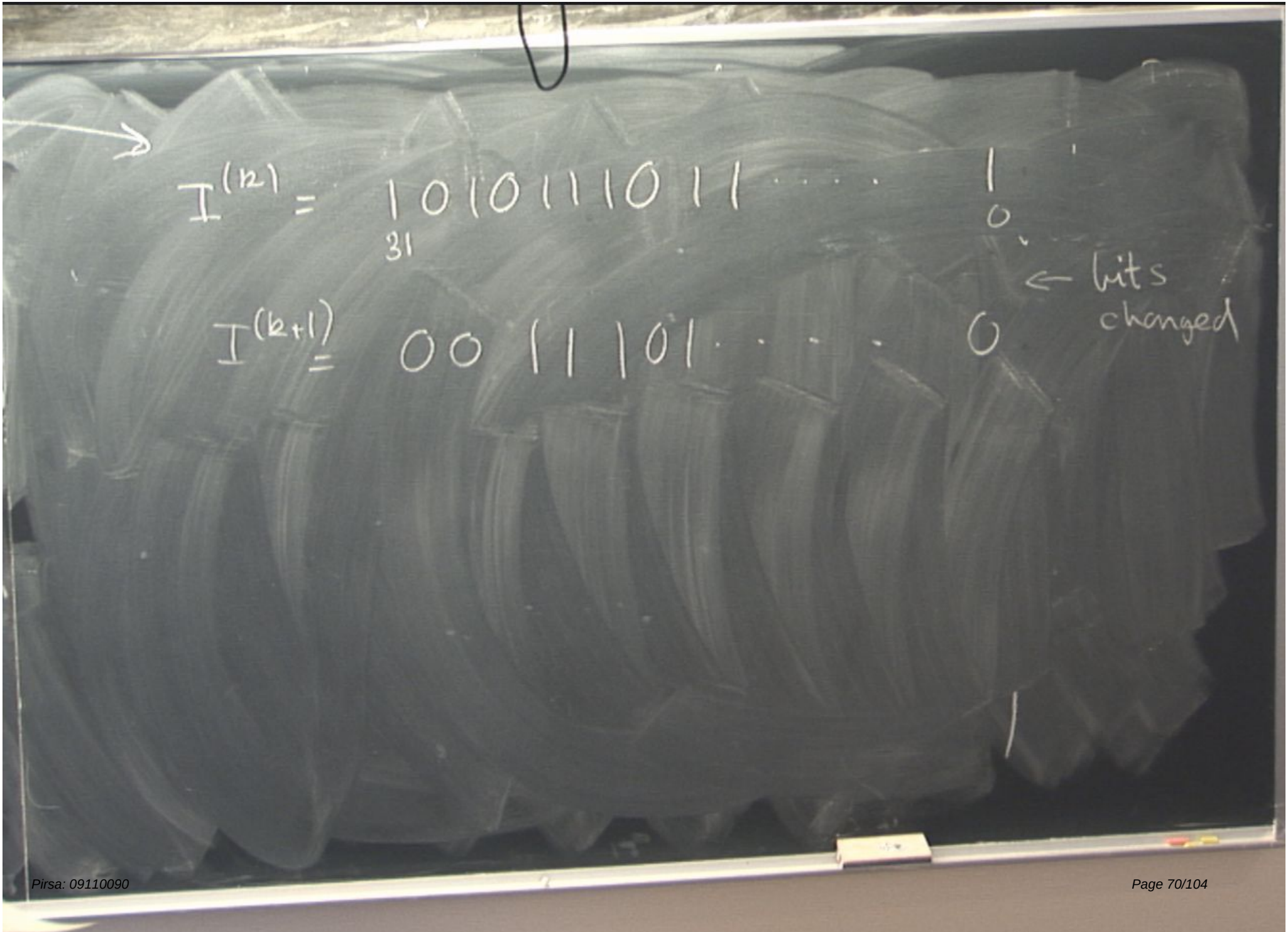
Random Numbers

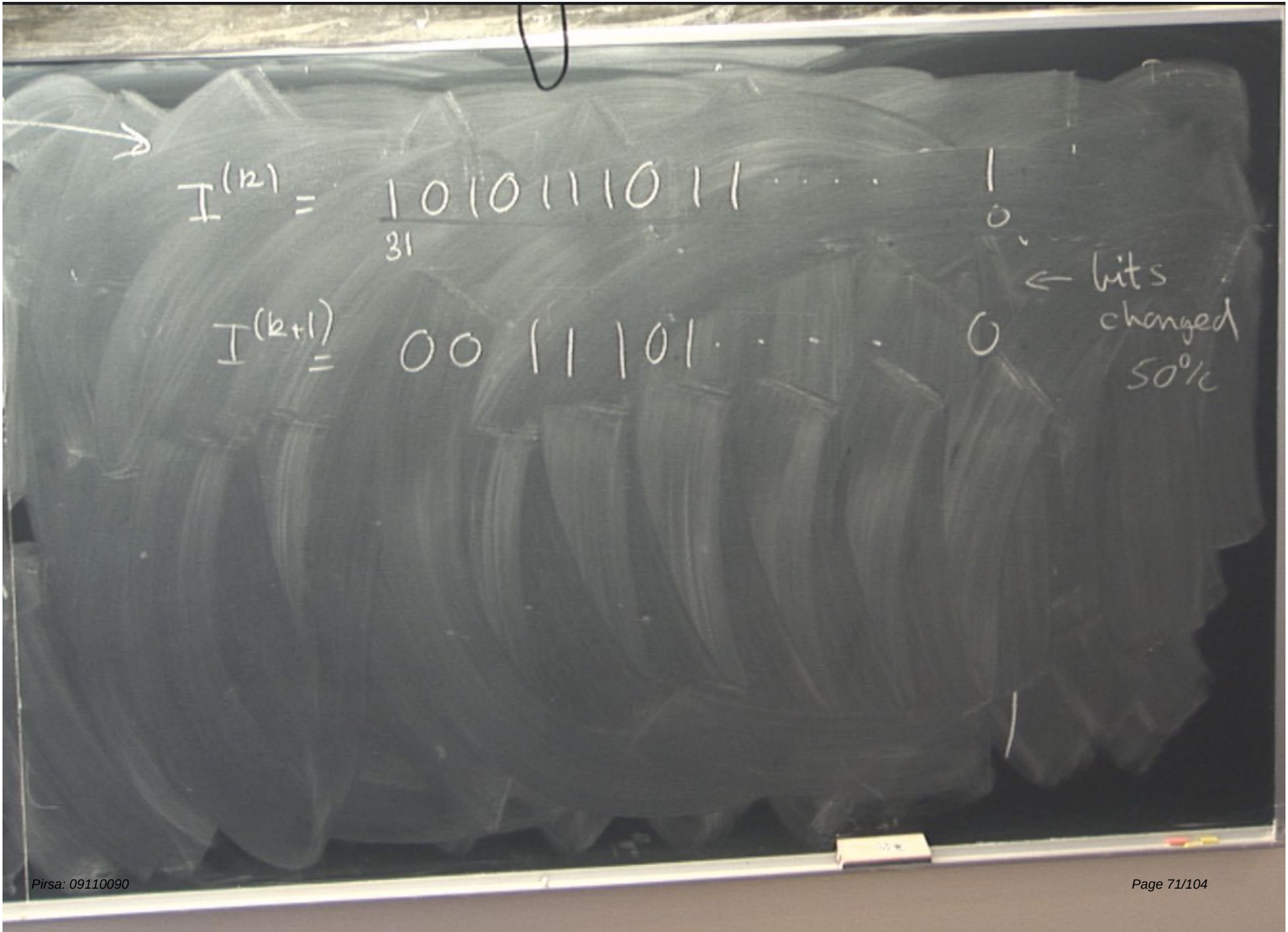
$U(0,1)$

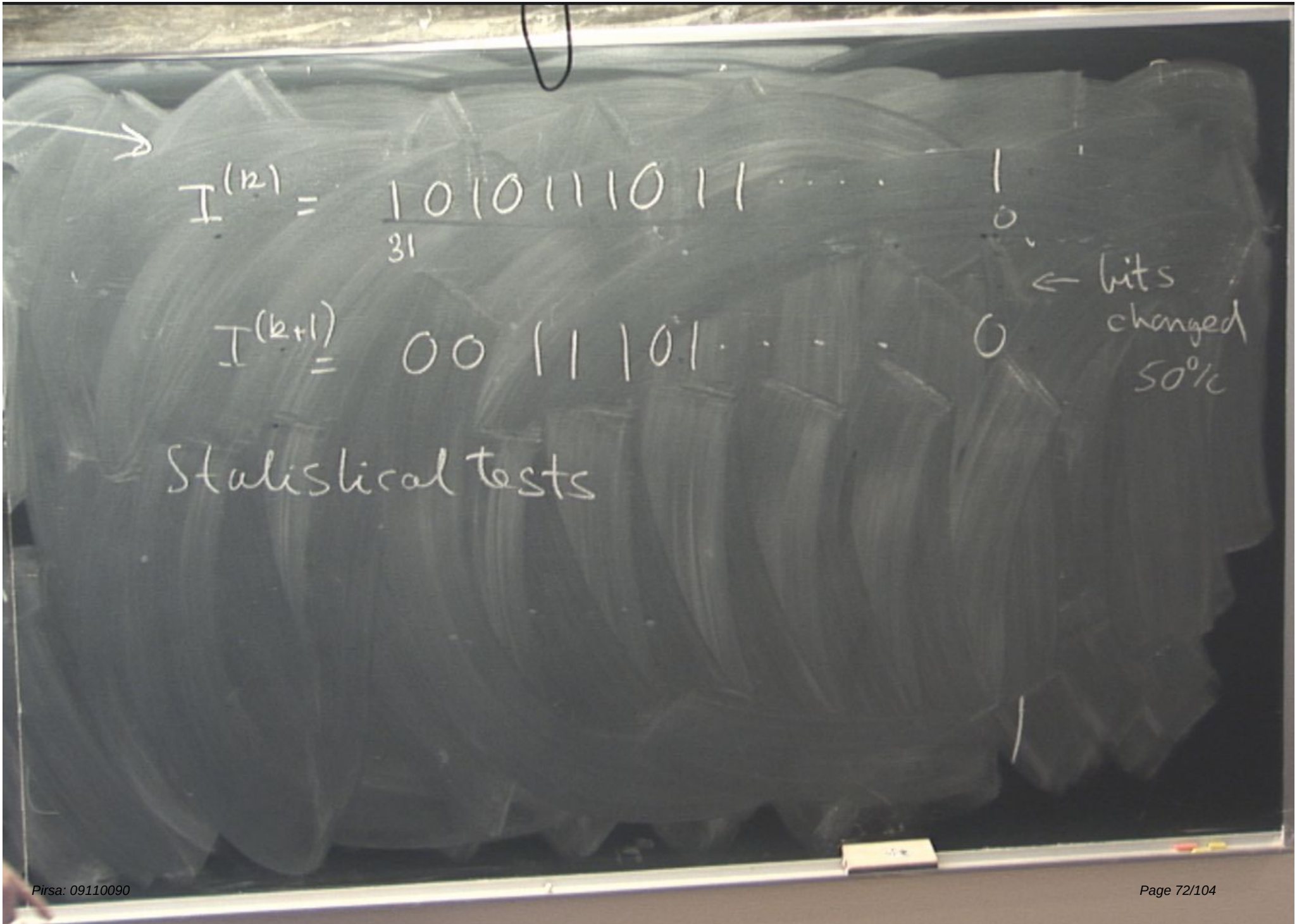
- What is random?
  - ↳ Usually Integers between 0 & I_{max}
- Pseudo-Random Numbers
  - deterministic $I^{(k+1)}$ from $I^{(k)}$
  - RNG must be avoided in correlation

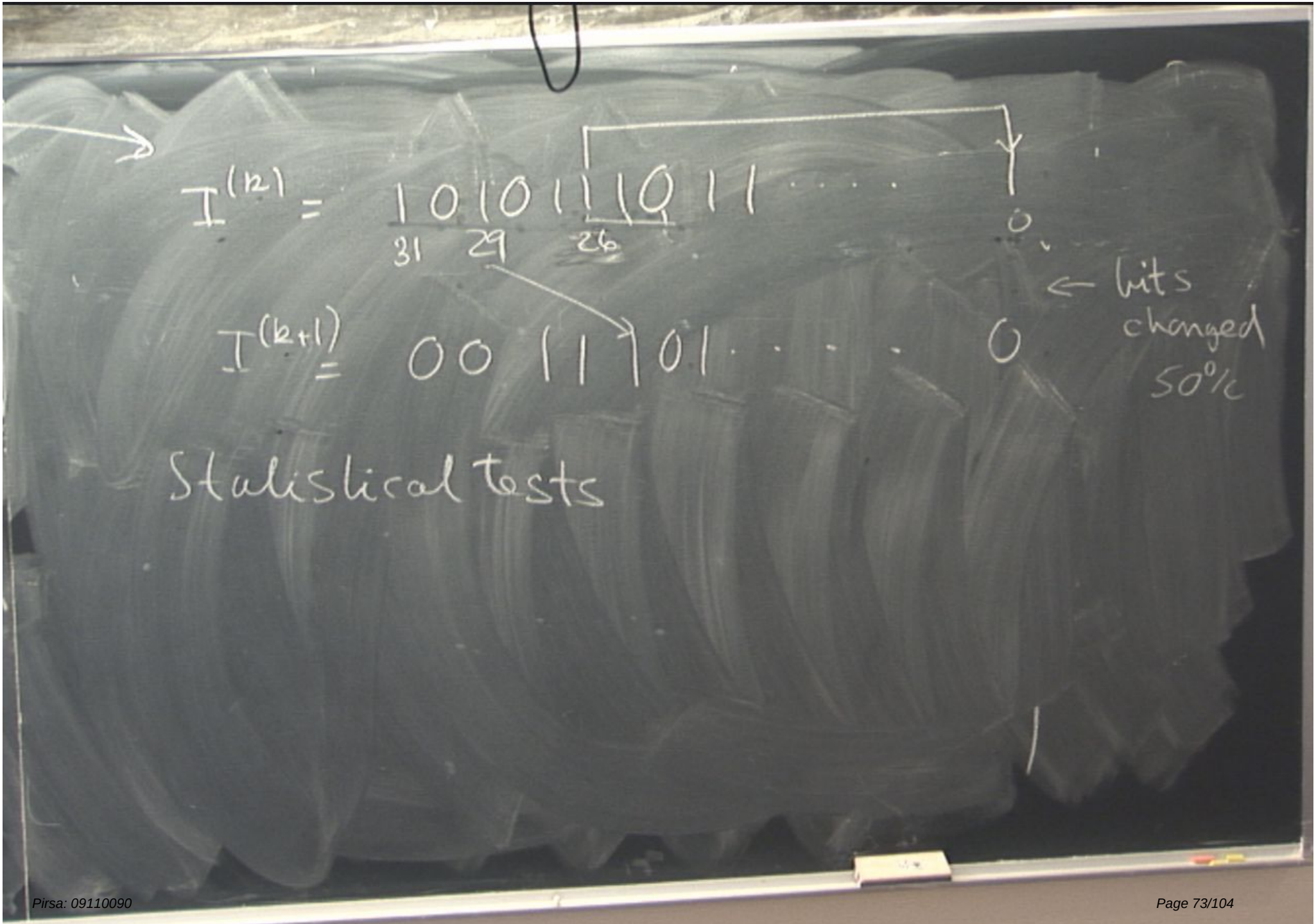

$I^{(h)} = 1\,0\,1\,0\,1\,1\,1\,0\,1\,1 \cdots 1$
31
0

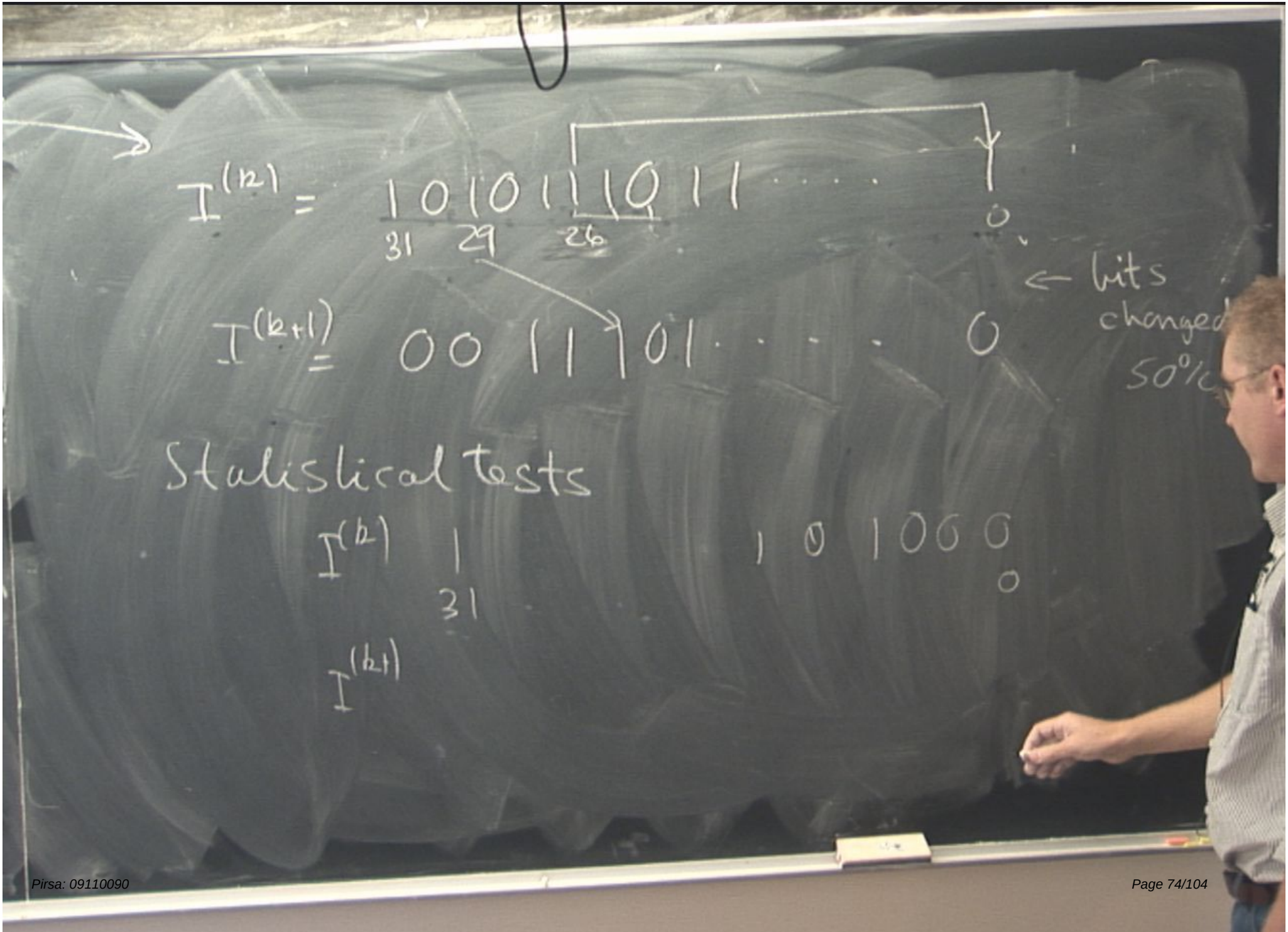

$I^{(k)} = 1\,0\,1\,0\,1\,1\,1\,0\,1\,1 \cdots 1\,0$
31
$I^{(k+1)} = 0\,0\,1\,1\,1\,1\,0\,1 \cdots 0$

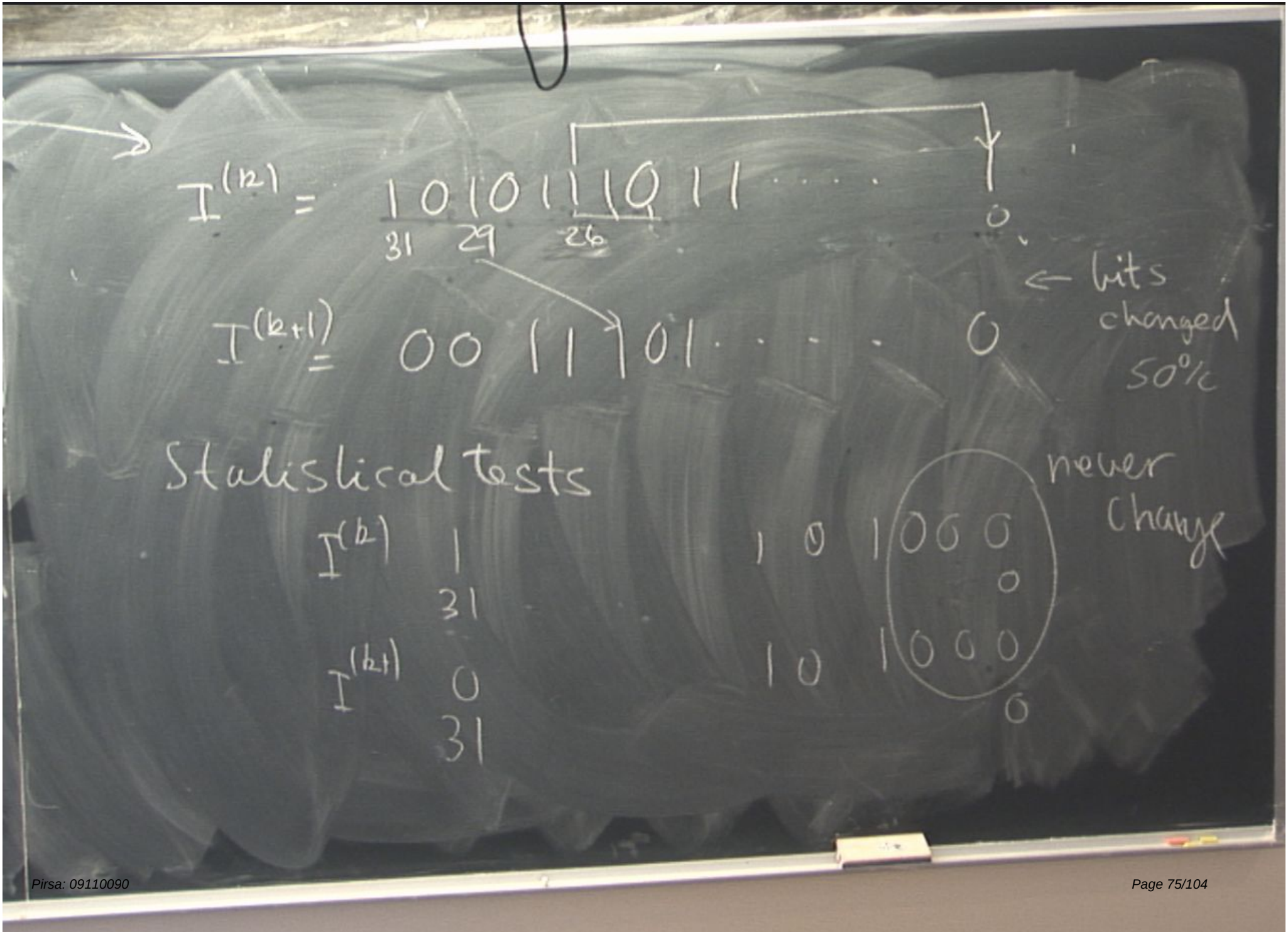

$I^{(k)} = 1\,0\,1\,0\,1\,1\,1\,0\,1\,1 \cdots 1\,0$
31
← bits changed
$I^{(k+1)} = 0\,0\,1\,1\,1\,1\,0\,1 \cdots 0$


$I^{(k)} = \underset{31}{1}\,0\,1\,0\,1\,1\,1\,0\,1\,1\,\cdots\,!$
$I^{(k+1)} = 0\,0\,1\,1\,1\,1\,0\,1\,\cdots\,0$
← bits changed 50%


$I^{(k)} = \underset{31}{1}\,0\,1\,0\,1\,1\,1\,0\,1\,1 \cdots 1\,0$
$I^{(k+1)} = 0\,0\,1\,1\,1\,1\,0\,1 \cdots 0$
← bits changed 50%
Statistical tests

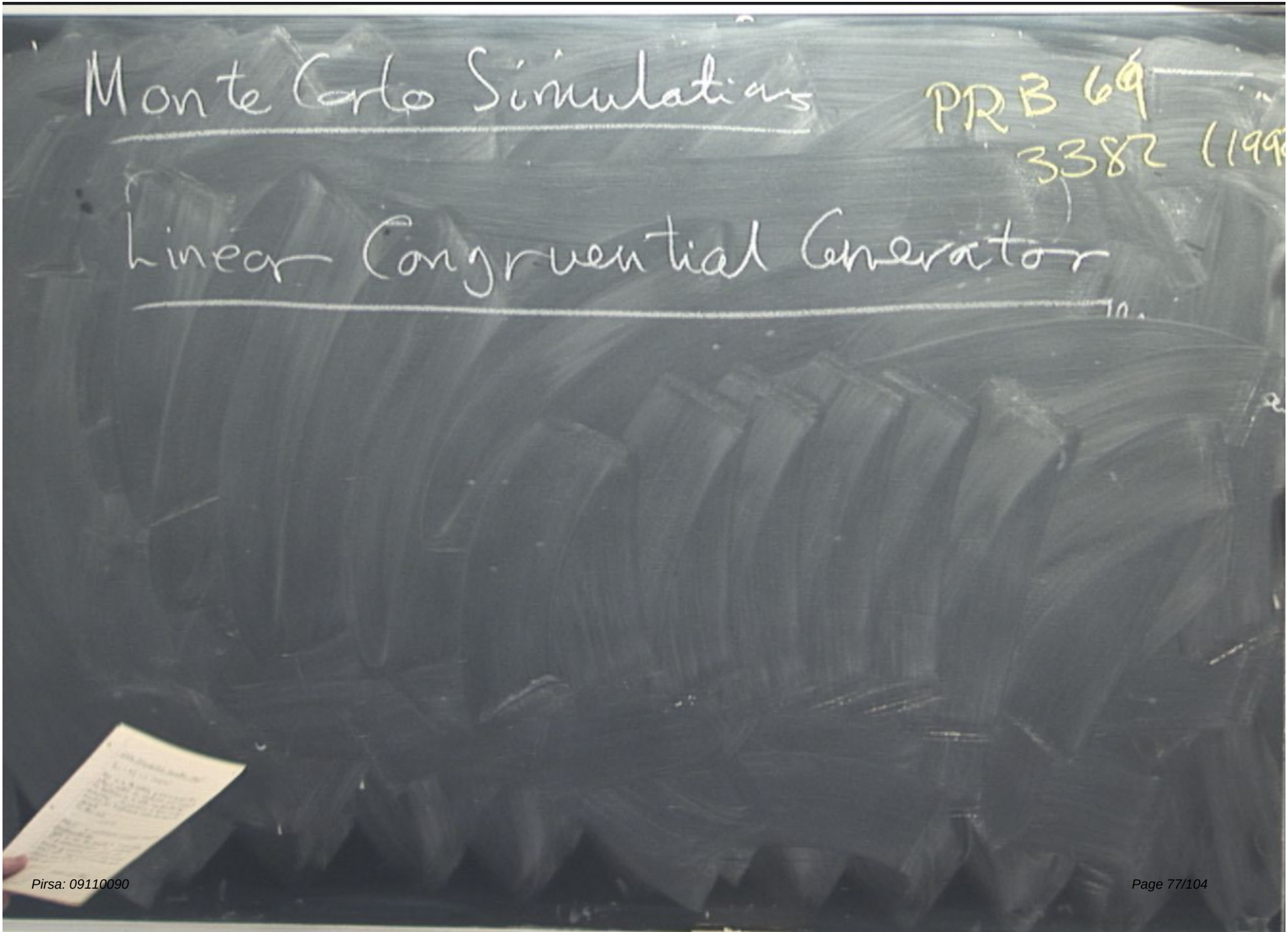

$I^{(k)}$ = 1 0 1 0 1 1 1 0 1 1 0
31 29 26
$I^{(k+1)}$ = 0 0 1 1 1 0 1 0
← bits changed 50%
Statistical tests

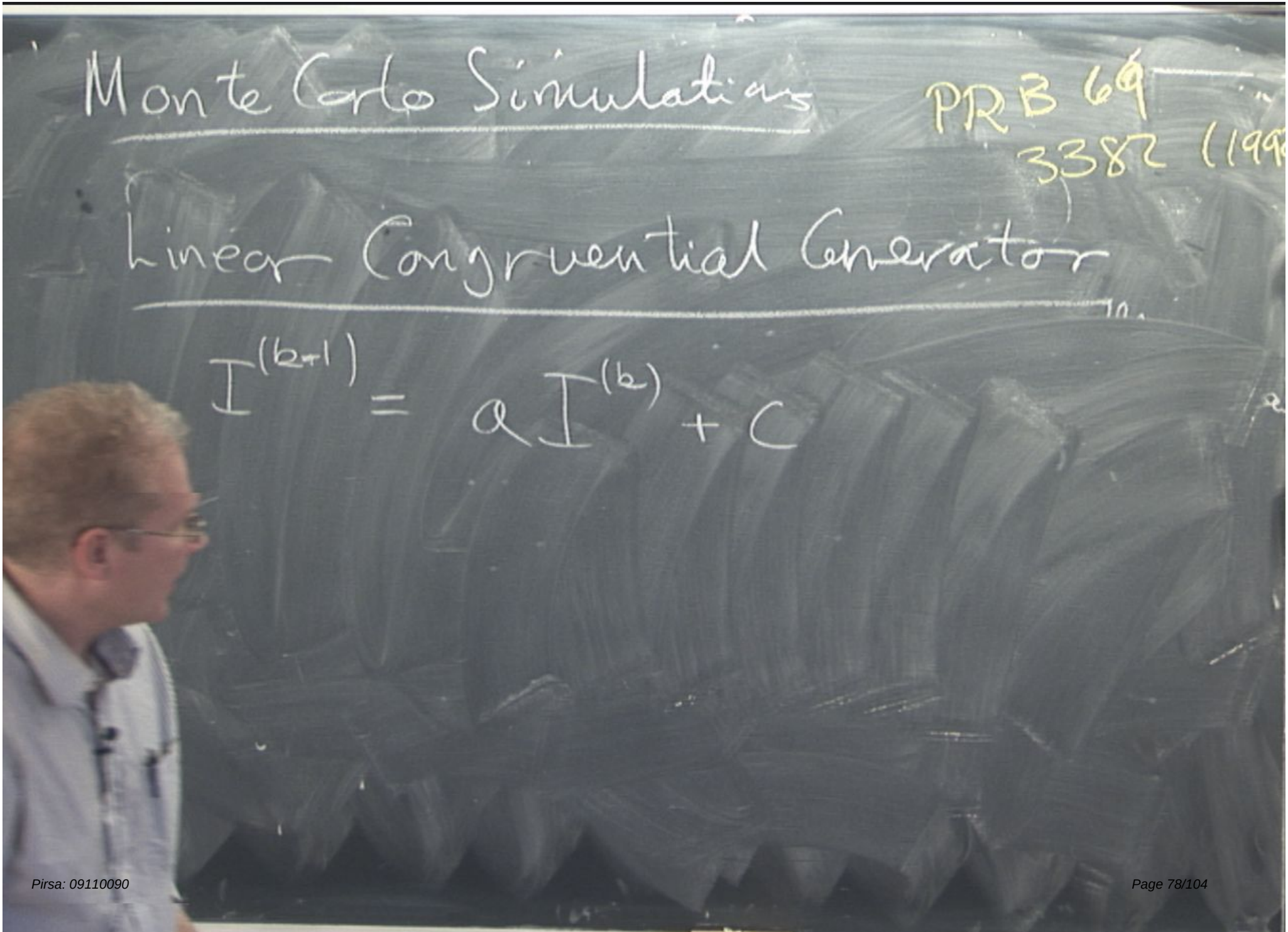

$I^{(k)} = 1\,0\,1\,0\,1\,1\,0\,1\,1 \ldots 0$
31 29 26
$I^{(k+1)} = 0\,0\,1\,1\,1\,0\,1 \ldots 0$
← bits changed
50%
Statistical tests
$I^{(k)}$ 1 1 0 1 0 0 0
31 0
$I^{(k+1)}$


$I^{(k)} = 1\,0\,1\,0\,1\,1\,1\,0\,1\,1 \ldots 0$
31 29 26
bits changed 50%
$I^{(k+1)} = 0\,0\,1\,1\,1\,0\,1 \ldots 0$
Statistical tests
$I^{(k)}$ 1 ... 31
$I^{(k+1)}$ 0 ... 31
1 0 1 0 0 0 ... 0
1 0 1 0 0 0 ... 0
never Change

Monte Carlo Simulations

PRB 69
3382 (1992)


Monte Carlo Simulations
PRB 69
3382 (199
Linear Congruential Generator


Monte Carlo Simulations
PRB 69
3382 (199
Linear Congruential Generator
$I^{(k+1)} = a I^{(k)} + C$

Monte Carlo Simulations

PRB 69 3382 (199

Linear Congruential Generator

$$I^{(k+1)} = a I^{(k)} + c \pmod{m}$$

Monte Carlo Simulations

PRB 69 3382 (199

Linear Congruential Generator

$$I^{(k+1)} = a I^{(k)} + c \pmod{m}$$

ANSI C standard

Monte Carlo Simulations

PRB 69 3382 (199

Linear Congruential Generator

$$I^{(k+1)} = a I^{(k)} + c \pmod{m}$$

ANSI C standard

$a = 1103515245$ $c =$

Monte Carlo Simulations

PRB 69 3382 (199

Linear Congruential Generator

$$I^{(k+1)} = a I^{(k)} + c \pmod{m}$$

ANSI C standard

$a = 1103515245$ $c = 12345$

$m = 2^{32}$

Monte Carlo Simulations

PRB 69 3382 (199

Linear Congruential Generator

$$I^{(b+1)} = a I^{(b)} + c \pmod{m}$$

ANSI C standard

$a = 1103515245$ $c = 12345$

$m = 2^{32}$


Erb's RNG
a=3
C=2
m=32

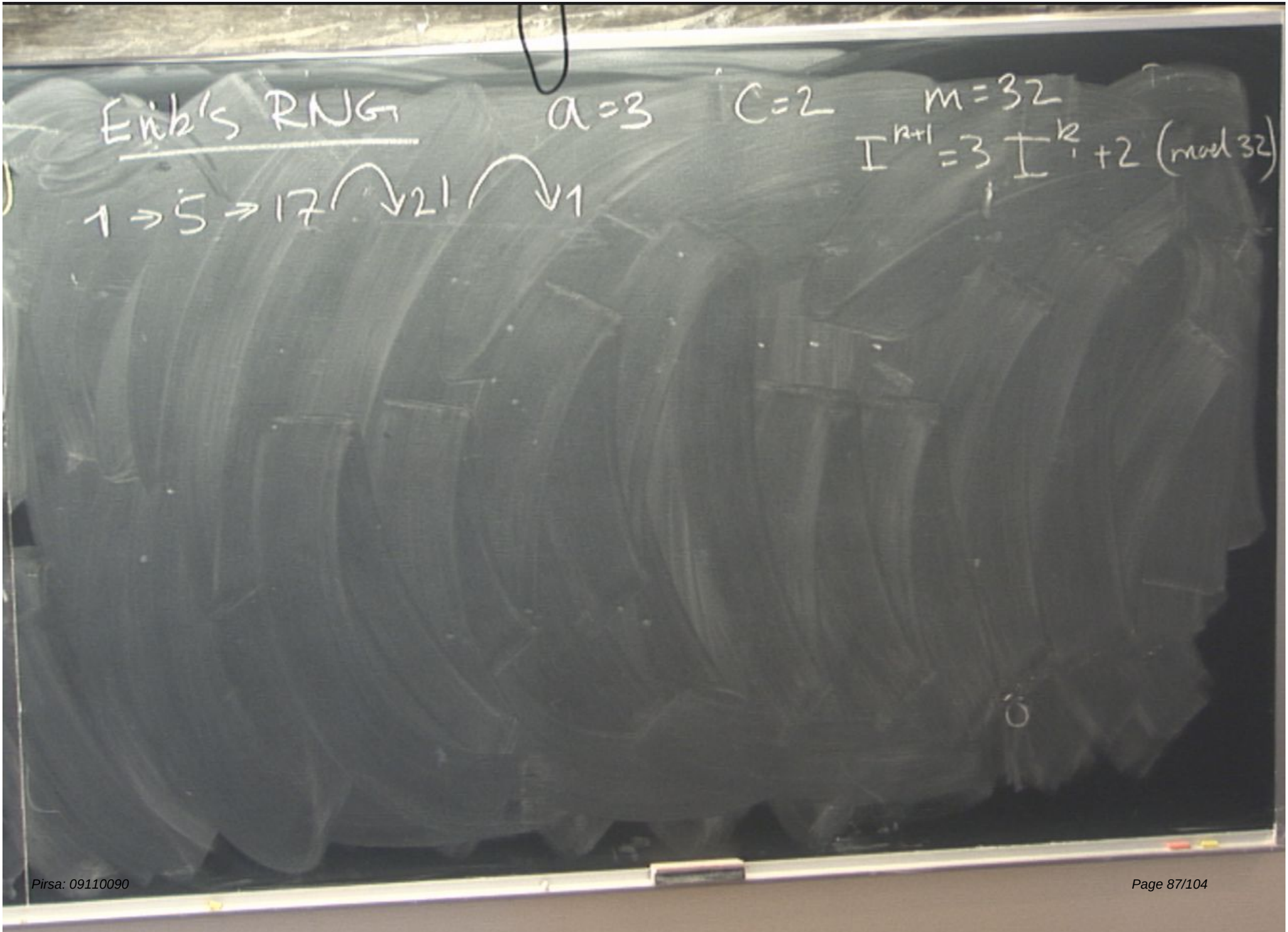
Enb's RNG $a=3$ $C=2$ $m=32$

$$I^{k+1} = 3 I^k + 2 \pmod{32}$$

Enb's RNG $a=3$ $C=2$ $m=32$

$I^{k+1} = 3 I^k + 2 \pmod{32}$

1 → 5 →


Eñb's RNG
a=3
C=2
m=32
$I^{k+1} = 3 I^k + 2 \pmod{32}$
1 → 5 → 17 → 21 → 1

Eñb's RNG $a=3$ $C=2$ $m=32$

$I^{k+1} = 3 I^k + 2 \pmod{32}$

$1 \to 5 \to 17 \to 21 \to 1$ cycle small !

Enb's RNG $a=3$ $C=2$ $m=32$

$I^{k+1} = 3 I^k + 2 \pmod{32}$

$1 \to 5 \to 17 \to 21 \to 1$ cycle small cycle length 4

Enb's RNG $a=3$ $C=2$ $m=32$

$I^{k+1} = 3 I^k + 2 \pmod{32}$

$1 \to 5 \to 17 \to 21 \to 1$ cycle small cycle length 4

$P \leq m$

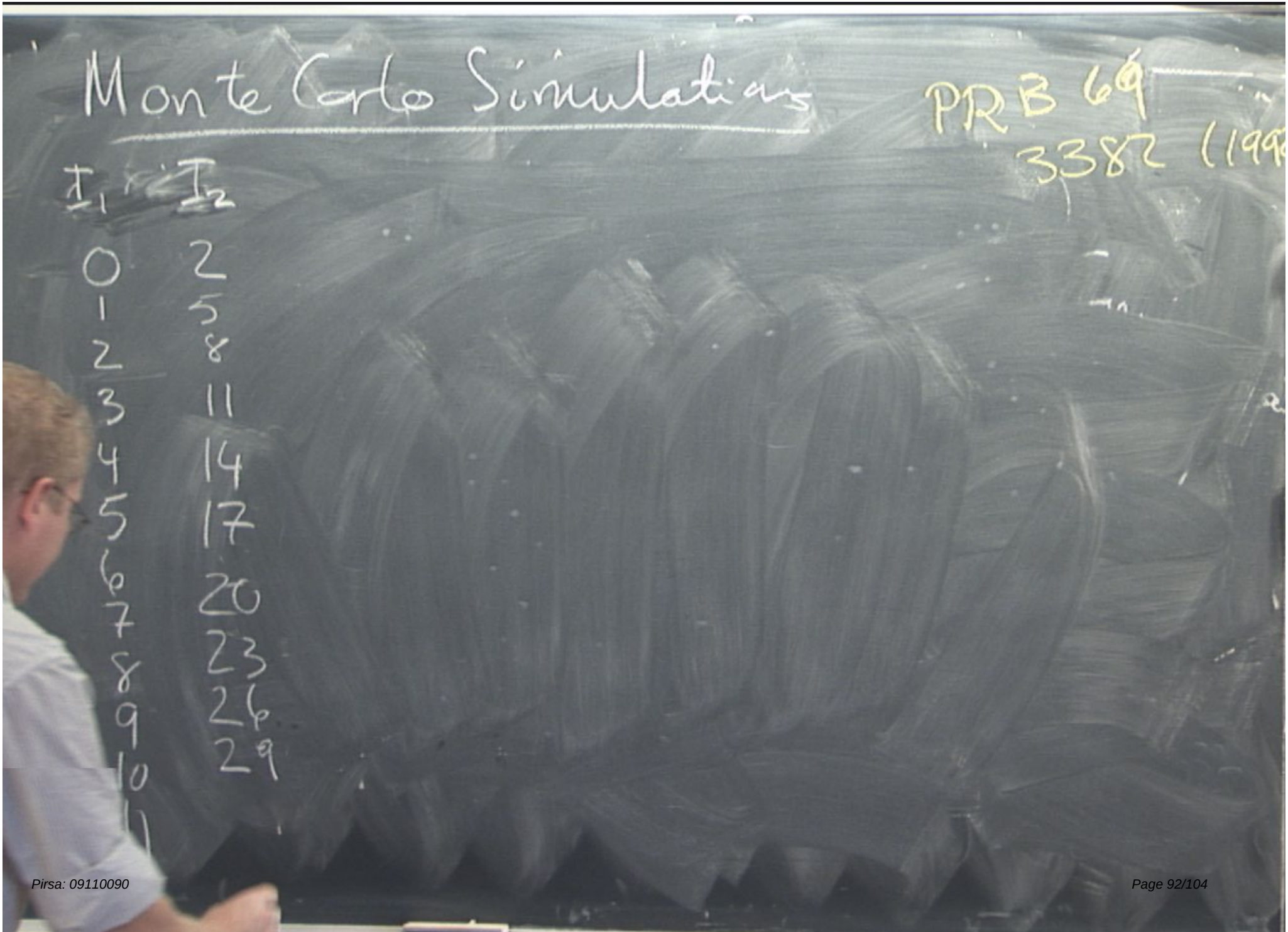
Enb's RNG $a=3$ $C=2$ $m=32$

$I^{k+1} = 3 I^k + 2 \pmod{32}$

$1 \to 5 \to 17 \to 21 \to 1$ cycle small

$2 \to 8 \to 26 \to 16 \to 18 \to 24 \to 10 \to 0 \to 2$ cycle length 4

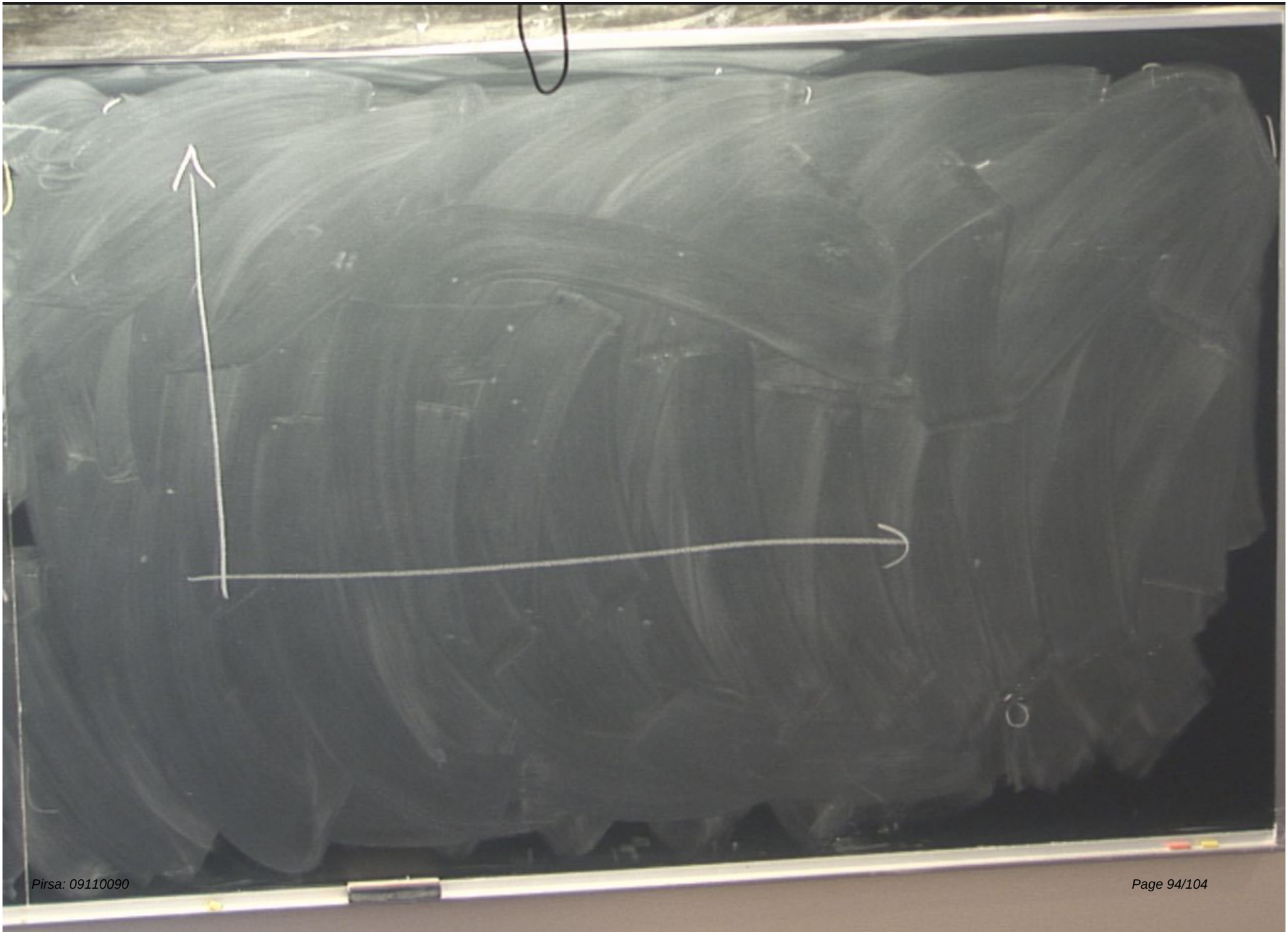
$P \leq m$

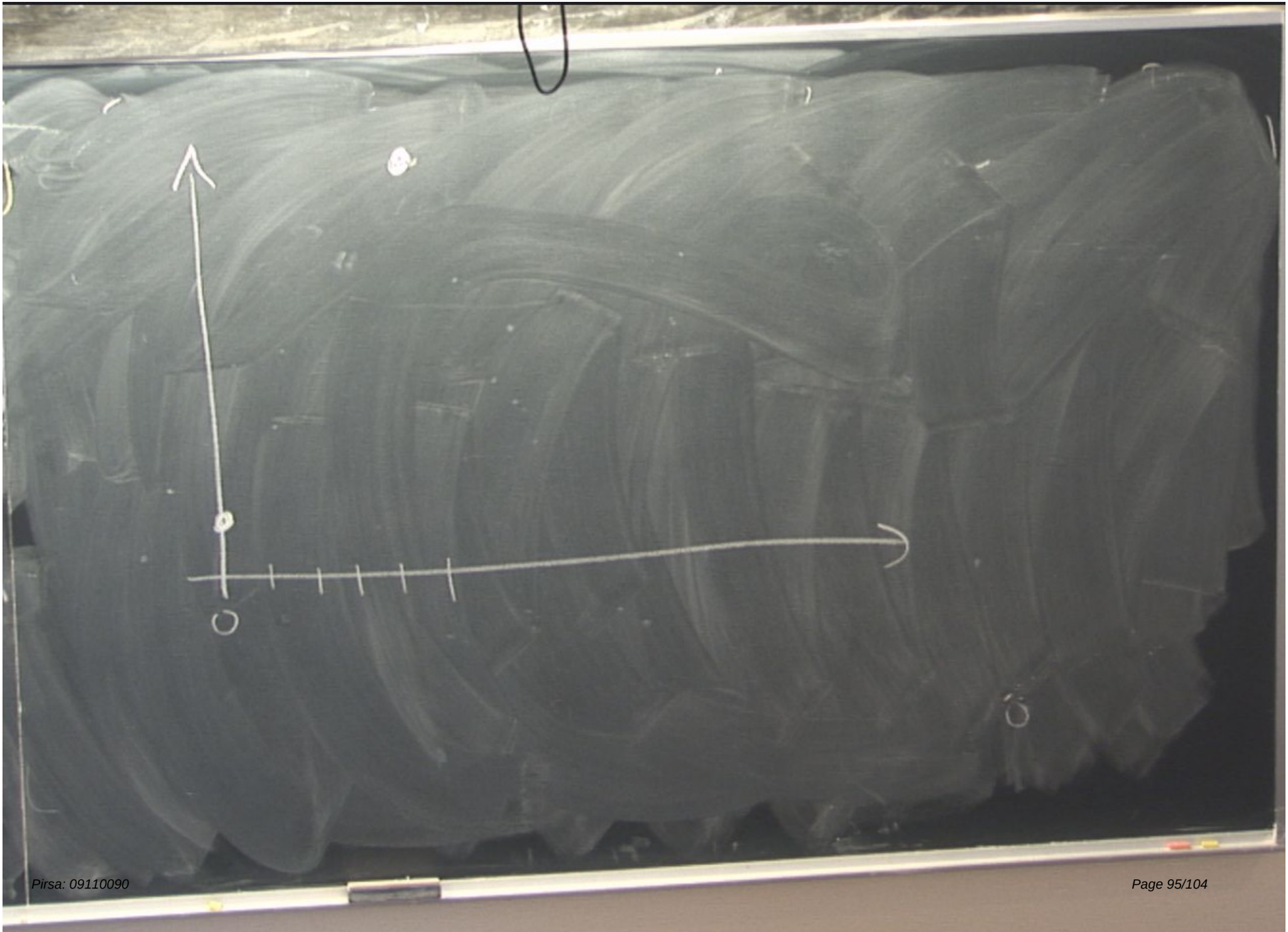

Monte Carlo Simulations
PRB 69
3382 (199
I1 I2
0 2
1 5
2 8
3 11
4 14
5 17
6 20
7 23
8 26
9 29

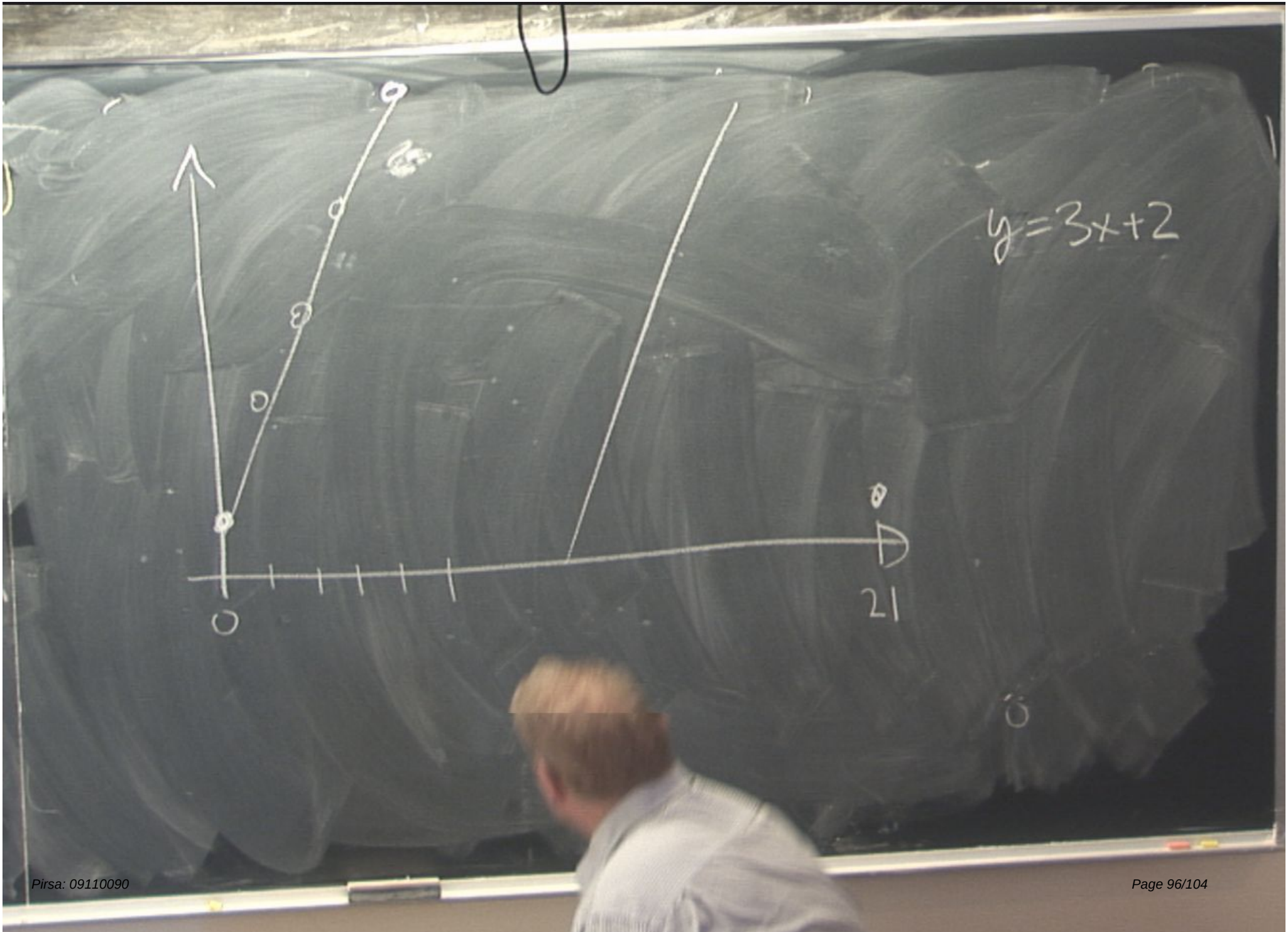
Monte Carlo Simulations

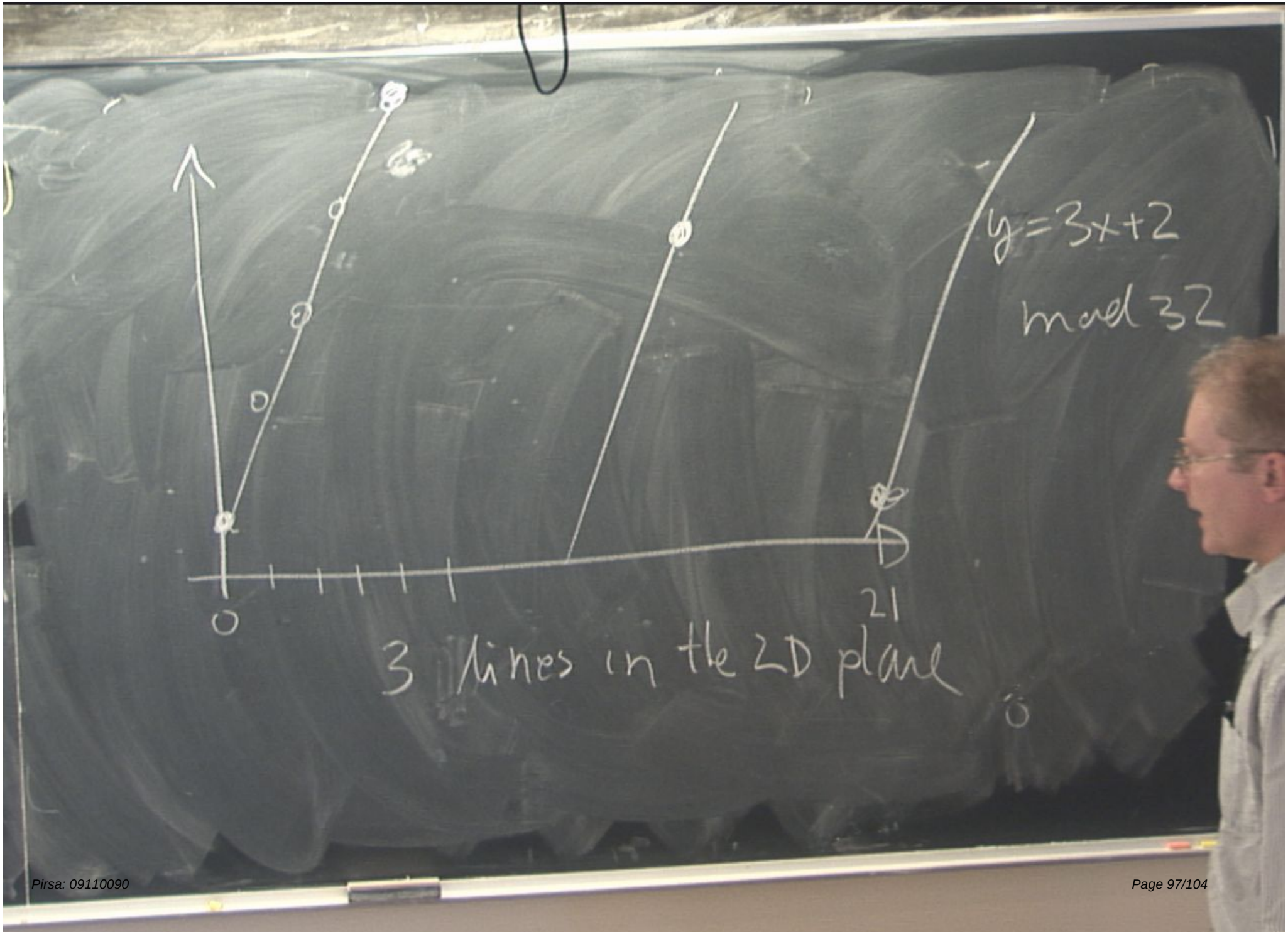
PRB 69
3382 (199

I_1	I_2
0	2
1	5
2	8
3	11
4	14
5	17
6	20
7	23
8	26
9	29
10	0
11	




O


y=3x+2
0
21


y=3x+2
mod 32
0
21
3 lines in the 2D plane

ANSI C $m = 2^{36}$

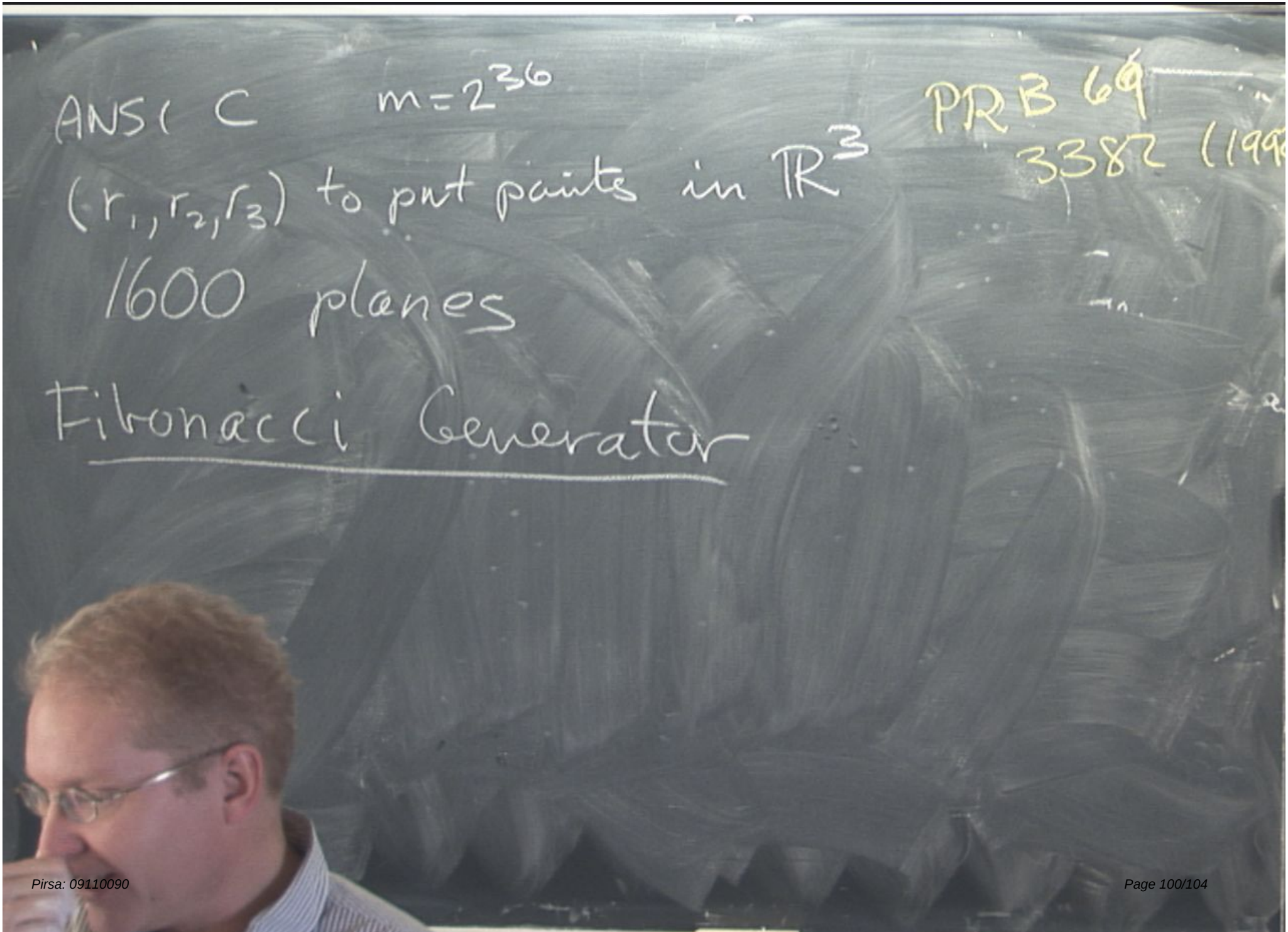
(r_1, r_2, r_3) to put points in $\mathbb{R}^3$ PRB 69 3382 (199

ANSI C $m = 2^{36}$

(r_1, r_2, r_3) to put points in $\mathbb{R}^3$

1600 planes

PRB 69 3382 (199


ANSI C
$m = 2^{36}$
PRB 69
3382 (199
(r_1, r_2, r_3) to put points in $\mathbb{R}^3$
1600 planes
Fibonacci Generator

ANSI C $m = 2^{36}$

(r_1, r_2, r_3) to put points in $\mathbb{R}^3$ PRB 69 3382 (199

1600 planes

Fibonacci Generator

$$I^{(k)} = I^{k-1} + I^{k-2} \quad \text{mod } c$$

ANSI C $m = 2^{36}$

(r_1, r_2, r_3) to put points in $\mathbb{R}^3$

1600 planes

PRB 69 3382 (199

Fibonacci Generator

$$I^{(k)} = I^{k-1} + I^{k-2} \quad \text{mod } c$$

Lagged Fibannacci

$$I^{(k)} = I^{(k-r)} \; I^{(k-s)}$$

ANSI C $m = 2^{36}$

(r_1, r_2, r_3) to put points in $\mathbb{R}^3$

PRB 69 3382 (199

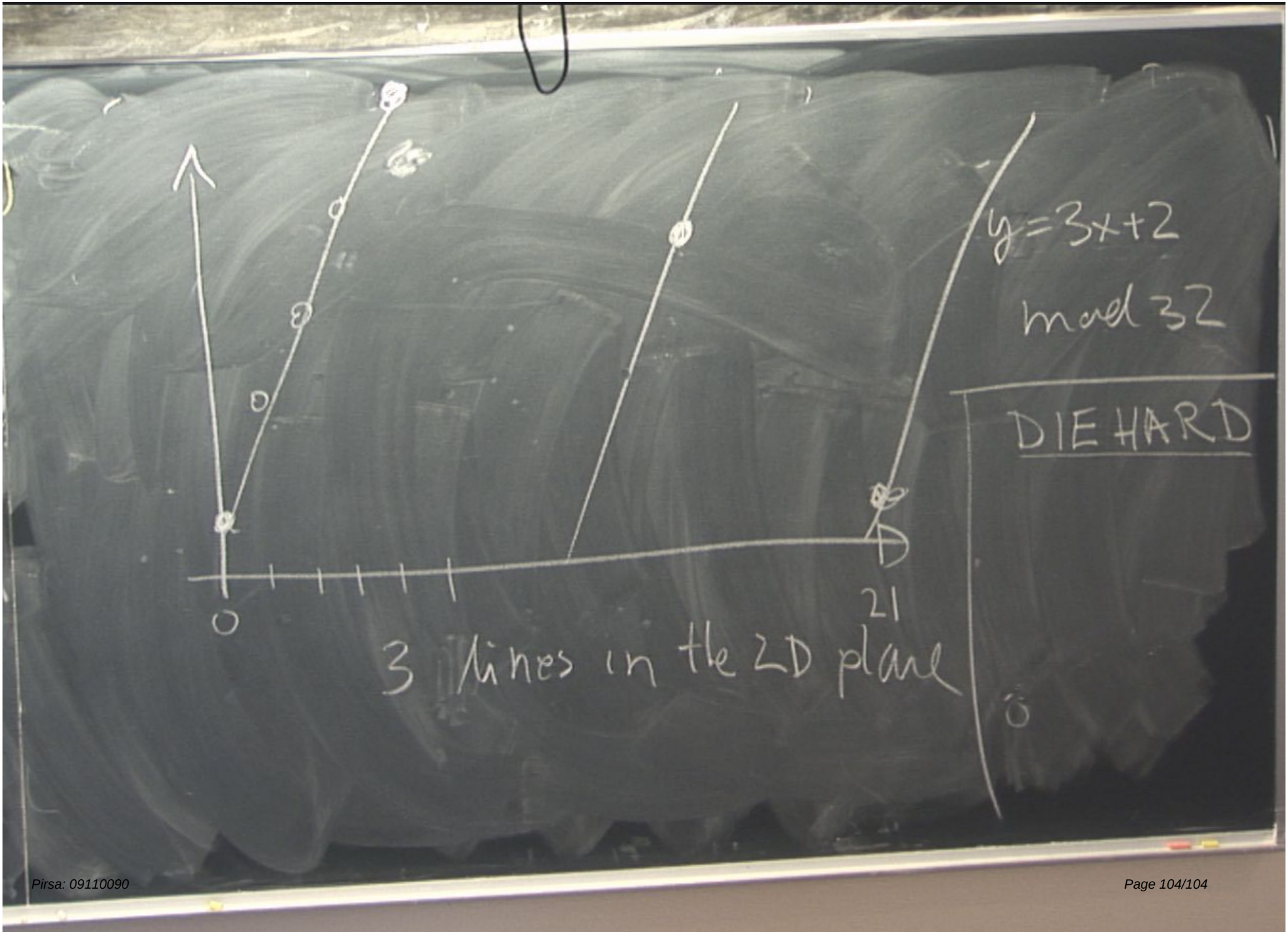
1600 planes

Fibonacci Generator

$$I^{(k)} = I^{k-1} + I^{k-2} \quad \text{mod } c$$

Lagged Fibannacci

$$I^{(k)} = I^{(k-r)} \pm I^{(k-s)} \quad \text{mod } c$$


y=3x+2
mod 32
DIE HARD
0
21
3 lines in the 2D plane