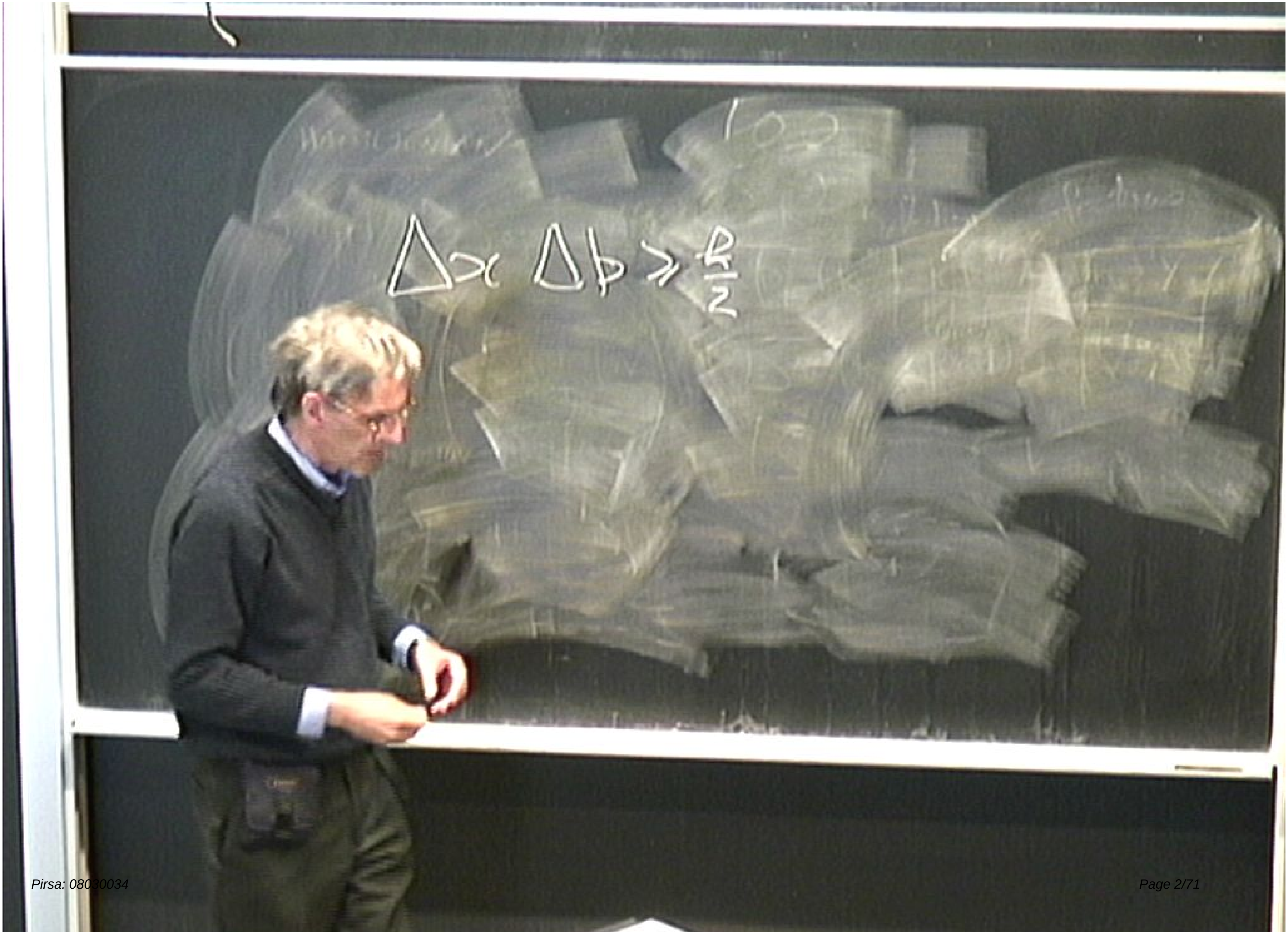
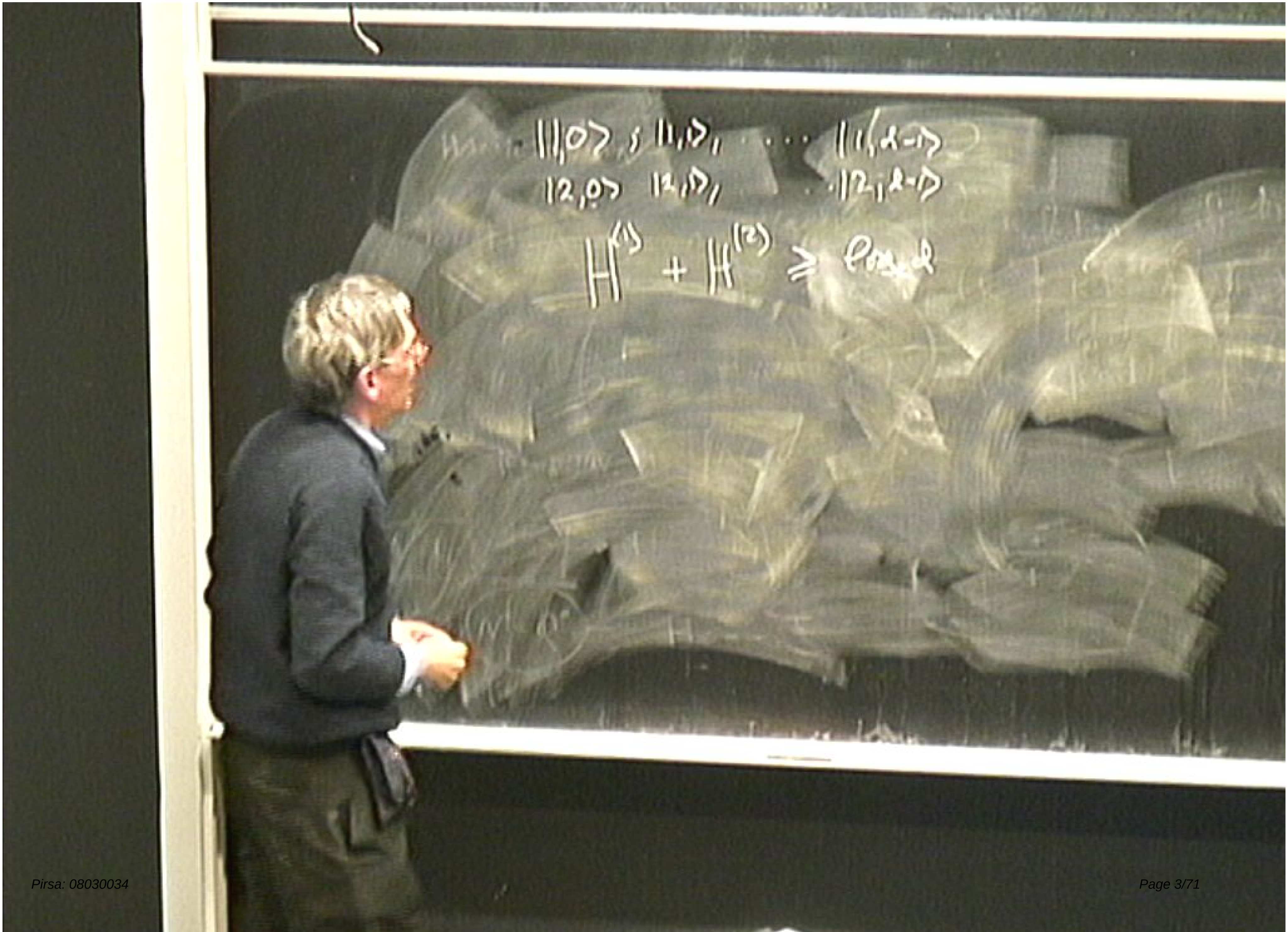
Title: Minimum Uncertainty States, the Clifford Group and Galois Extension Fields

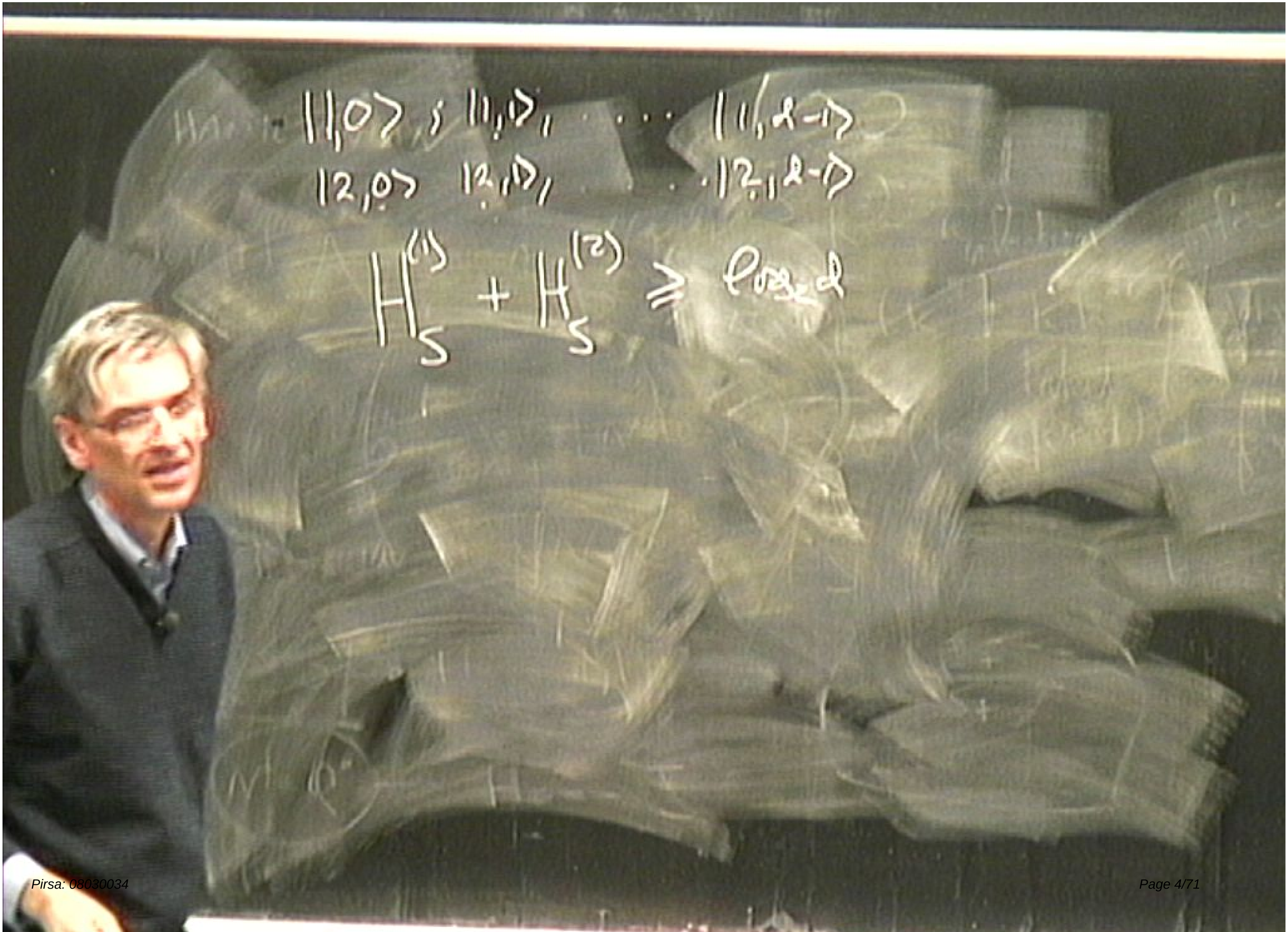
Date: Mar 26, 2008 04:00 PM

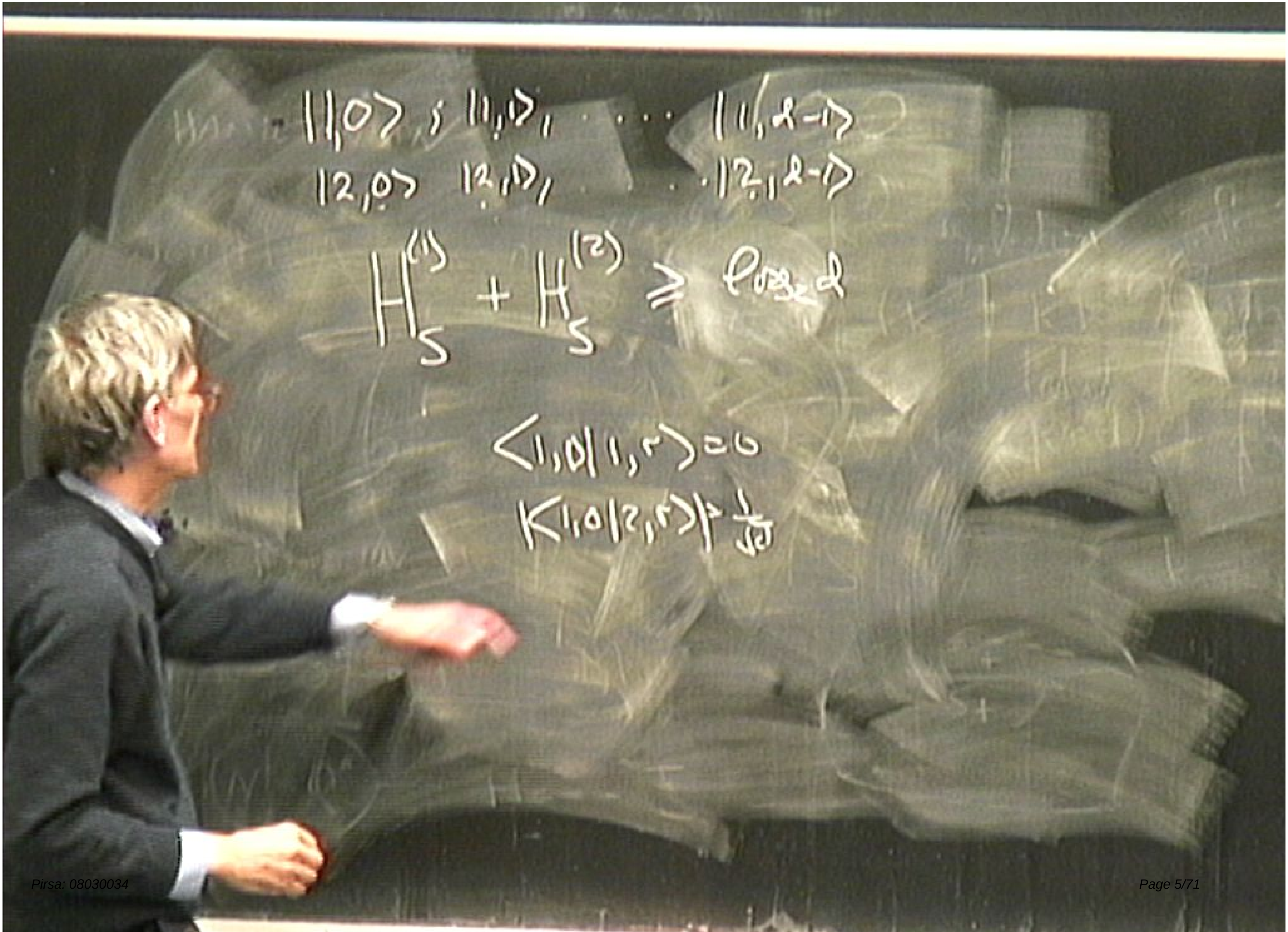
URL: http://pirsa.org/08030034

Abstract: The talk concerns a generalization of the concept of a minimum uncertainty state to the finite dimensional case. Instead of considering the product of the variances of two complementary observables we consider an uncertainty relation involving the quadratic Renyi entropies summed over a full set of mutually unbiased bases (MUBs). States which achieve the lower bound set by this inequality were introduced by Wootters and Sussman, who proved existence for every prime power dimension, and by Appleby, Dang and Fuchs who showed that in prime dimension the fiducial vector for a for a symmetric informationally complete positive operator valued measure (SIC-POVM) covariant under the Weyl-Heisenberg group is a state of this kind. Subsequently Sussman proved existence for a class of odd prime power dimensions. The purpose of this talk is to complete the existence proof by showing that minimum uncertainty states exist in every prime power dimension, without exception. Along the way we establish a number of properties of the Clifford group, and Galois extension fields, which might be of some independent interest.


$\Delta x \, \Delta p \geq \frac{\hbar}{2}$


|1,0> , |1,1>, ... |1,d-1>
|2,0> |2,1> . . |2,d-1>
H^(1) + H^(2) ≥ log_2 d


$|1,0\rangle$, $|1,1\rangle$, . . . $|1,d-1\rangle$
$|2,0\rangle$ $|2,1\rangle$, . . . $|2,d-1\rangle$
$H_S^{(1)} + H_S^{(2)} \geq$

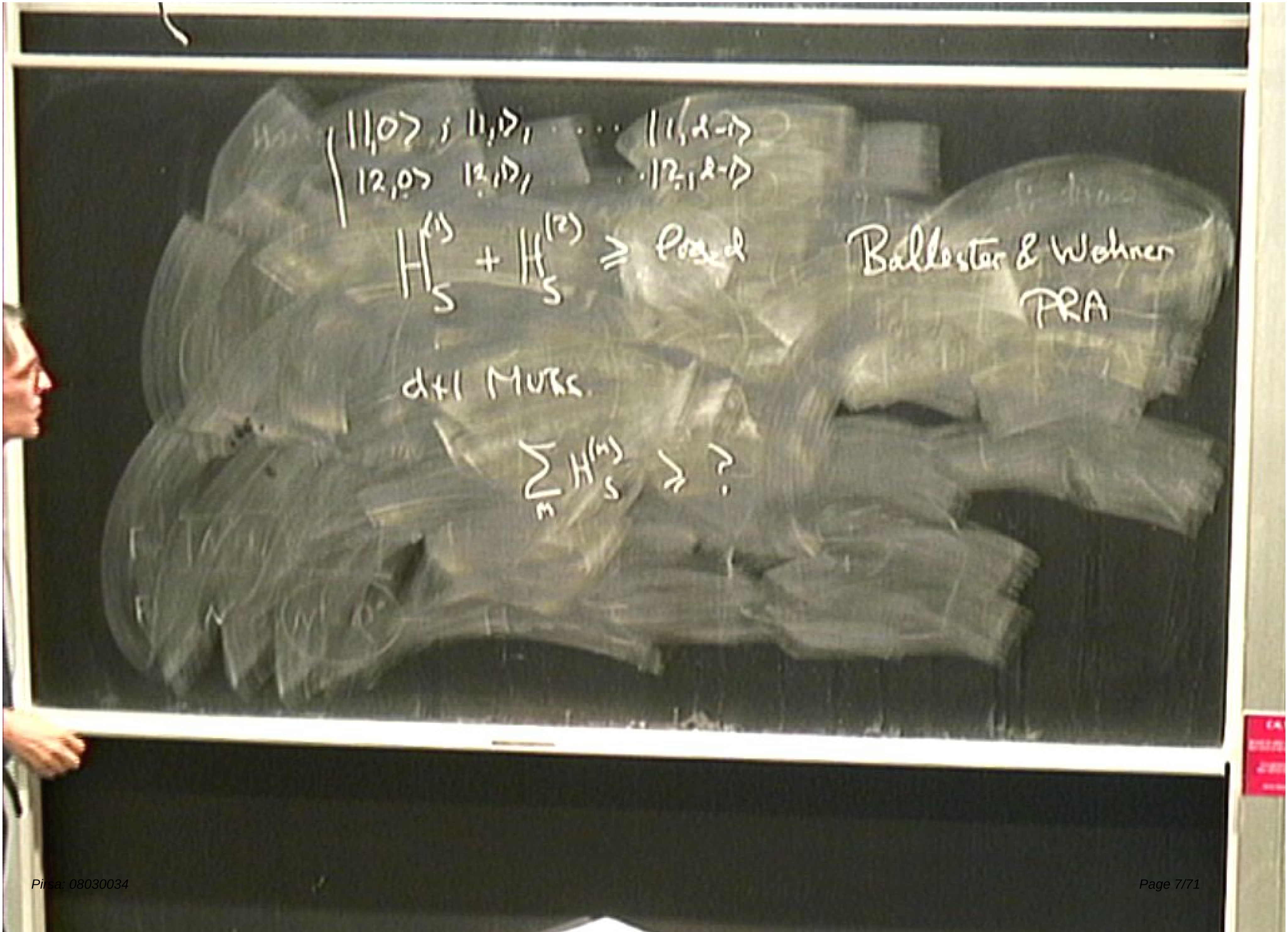

$|1,0\rangle$; $|1,1\rangle$, ... $|1,d-1\rangle$
$|2,0\rangle$ $|2,1\rangle$, ... $|2,d-1\rangle$
$H_S^{(1)} + H_S^{(2)} \geq \log_2 d$
$\langle 1,0|1,r\rangle = 0$
$|\langle 1,0|2,r\rangle| = \frac{1}{\sqrt{d}}$

$$|1,0\rangle \; ; \; |1,1\rangle, \; \cdots\cdots \; |1,d-1\rangle$$
$$|2,0\rangle \quad |2,1\rangle, \; \cdots\cdots \; |2,d-1\rangle$$

$$H_S^{(1)} + H_S^{(2)} \geq \log_2 d$$

$d+1$ MUBs.

$$\sum H_S^{(n)} \geq \, ?$$


$|1,0\rangle$; $|1,1\rangle$, ... $|1,d-1\rangle$
$|2,0\rangle$ $|2,1\rangle$, ... $|2,d-1\rangle$
$H_S^{(1)} + H_S^{(2)} \geq \log d$
Ballester & Wehner
PRA
d+1 MUBs
$\sum_m H_S^{(m)} \geq ?$

$|1,0\rangle, |1,1\rangle, \ldots |1,d-1\rangle$

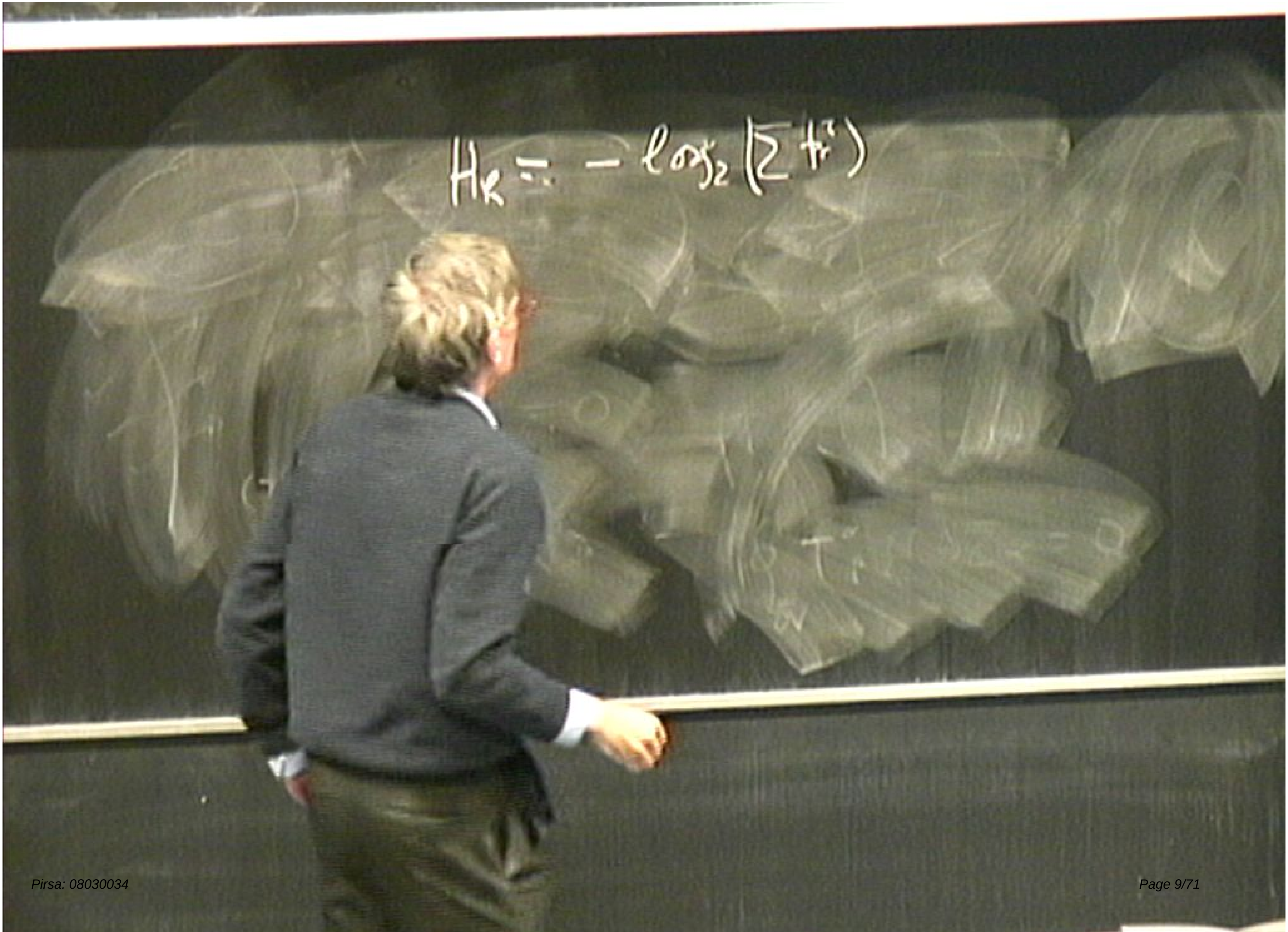
$|2,0\rangle \; |2,1\rangle \ldots |2,d-1\rangle$

$$H_S^{(1)} + H_S^{(2)} \geq \log_2 d$$

Ballester & Wehner PRA

$d+1$ MUBs

$$H_S^{(m_1)} + H_S^{(m_2)} \geq \log_2 d \qquad \sum_m H_S^{(m)} \geq \tfrac{1}{2}(d+1)\log_2 d$$


$H_R = -\log_2(\sum p_i^2)$

$$H_R = -\log_2\left(\sum p_i^2\right)$$

$$H_S \geq H_R.$$

$$H_R = -\log_2\left(\sum p_r^2\right)$$

$$H_S \geq H_R$$

$$\log_2\left(\sum_r p_r x_r\right) \geq \sum_r p_r \log_2 x_r$$

$$\sum |mr\rangle\langle mr|$$

$|1,0\rangle, |1,1\rangle, \ldots |1,d-1\rangle$
$|\phi,0\rangle \; |\phi,1\rangle \ldots |\phi,d-1\rangle$

$$H_S^{(1)} + H_S^{(2)} \geq \log_2 d$$

Ballester & Wehner PRA

d+1 MUBs

$$H_S^{(m_1)} + H_S^{(m_2)} \geq \log_2 d$$

$$\sum_m H_S^{(m)} \geq \frac{1}{2}(d+1)\log_2 d$$

$$H_R = -\log_2\left(\sum p_r^2\right)$$

$$\log_2\left(\sum_r p_r x_r\right) \geq \sum_r p_r \log_2 x_r$$

$$H_S \geq H_R.$$

$$\sum_{m,r} |mr\rangle\langle mr| \otimes |mr\rangle\langle mr| = 2\,\Pi_{sym}.$$

$$H_R = -\log_2\left(\sum p_r^2\right)$$

$$\log_2\left(\sum_r p_r x_r\right) \geq \sum_r p_r \log_2 x_r$$

$$H_S \geq H_R.$$

$$\sum_{m,r} |mr\rangle\langle mr| \otimes |mr\rangle\langle mr| = 2\,\Pi_{sym}.$$

$$\sum_{m,r} p_{mr}^2 = 1$$

$$\log \frac{2}{d+1} = \log\left(\frac{1}{d+1}\sum_m \left|\sum_r p_{mr}^2\right|\right) \geq \sum_m \frac{1}{d+1} \log\left(\sum_r p_{mr}^2\right)$$

$$\sum_m H_R^{(m)} \geq (d+1) \log_2 \frac{d+1}{2}$$

$$\log \frac{2}{d+1} = \log\left(\frac{1}{d+1}\sum_m \left|\sum_r p_{mr}^2\right|\right) \geq \sum_m \frac{1}{d+1}\log\left(\sum_r p_{mr}^2\right)$$

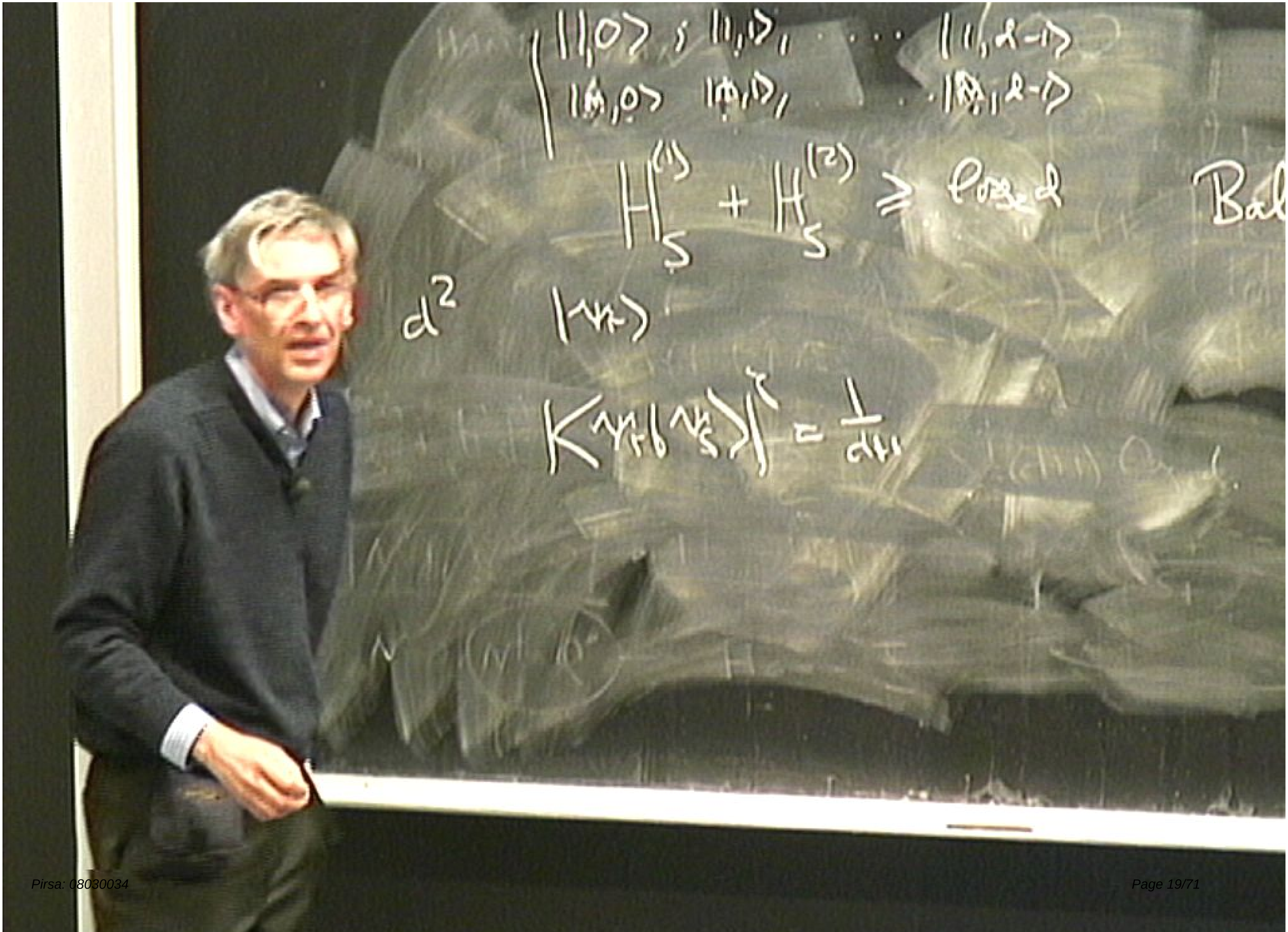
$$\sum_m H_S^{(m)} \geq \sum_m H_R^{(m)} \geq (d+1)\log_2 \frac{d+1}{2}$$

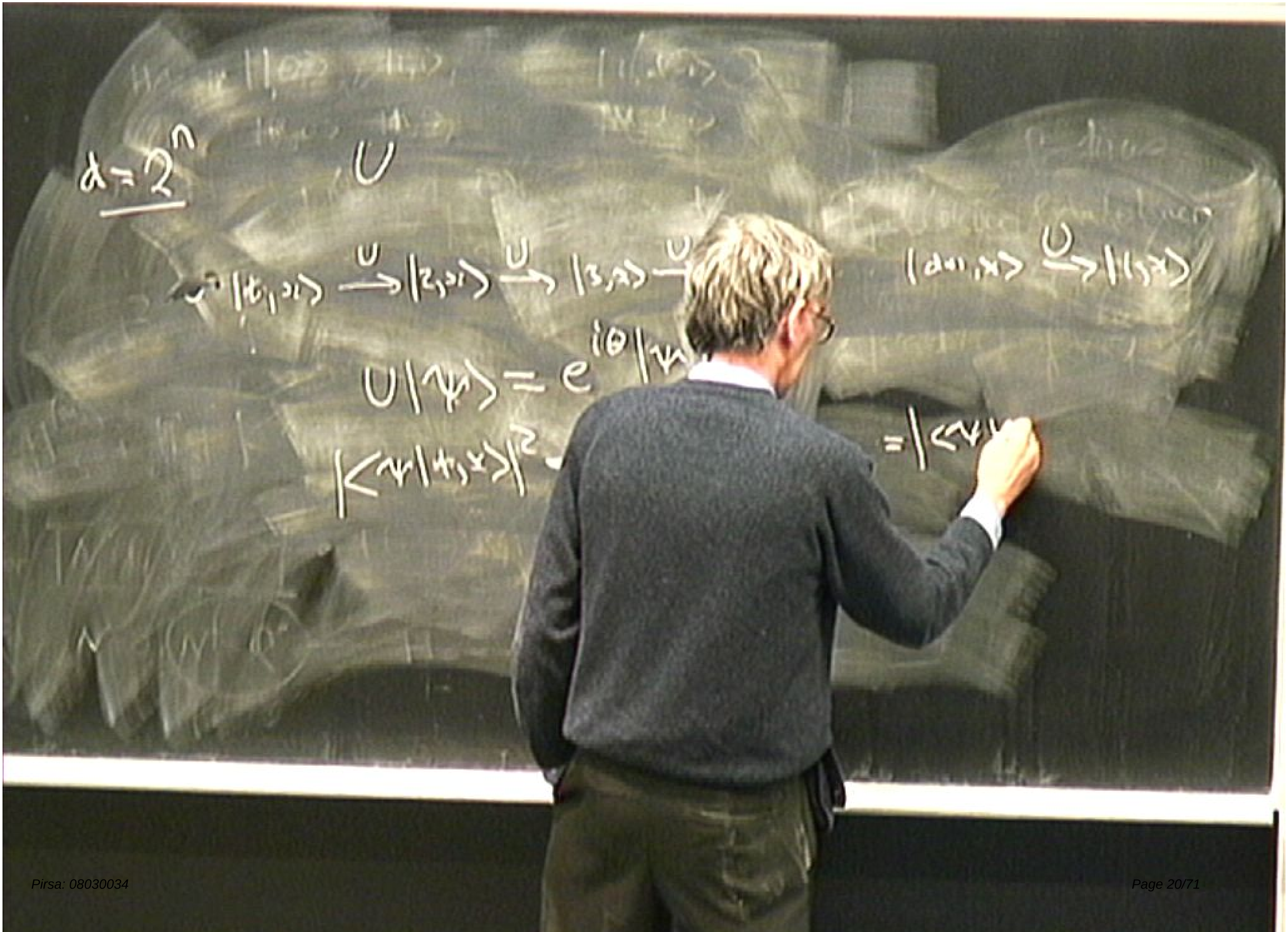
$$\log \frac{Z}{d+1} = \log\left(\frac{1}{d+1}\sum_m \left(\sum_r p_{mr}^2\right)\right) \geq \sum_m \frac{1}{d+1} \log\left(\sum_r p_{mr}^2\right)$$

$$\sum_m H_S^{(m)} \geq \sum_m H_R^{(m)} \geq (d+1)\log_2 \frac{d+1}{Z}$$

$$\log \frac{2}{d+1} = \log\left(\frac{1}{d+1} \sum_m \left(\sum_r p_{mr}^2\right)\right) \geq \sum_m \frac{1}{d+1} \log\left(\sum_r p_{mr}^2\right)$$

$$\sum_m H_S^{(m)} \geq \sum_m H_R^{(m)} \geq (d+1) \log_2 \frac{d+1}{2}$$


|1,0⟩ ; |1,1⟩, ... |1, d-1⟩
|φ,0⟩ |φ,1⟩, . . . |φ, d-1⟩
H_S^(1) + H_S^(2) ≥ log d
d^2 |ψ_r⟩
|⟨ψ_r|ψ_s⟩|^2 = 1/(d+1)



d = 2^n
U
U|ψ⟩ = e^{iθ}|ψ⟩

$d = 2^n$

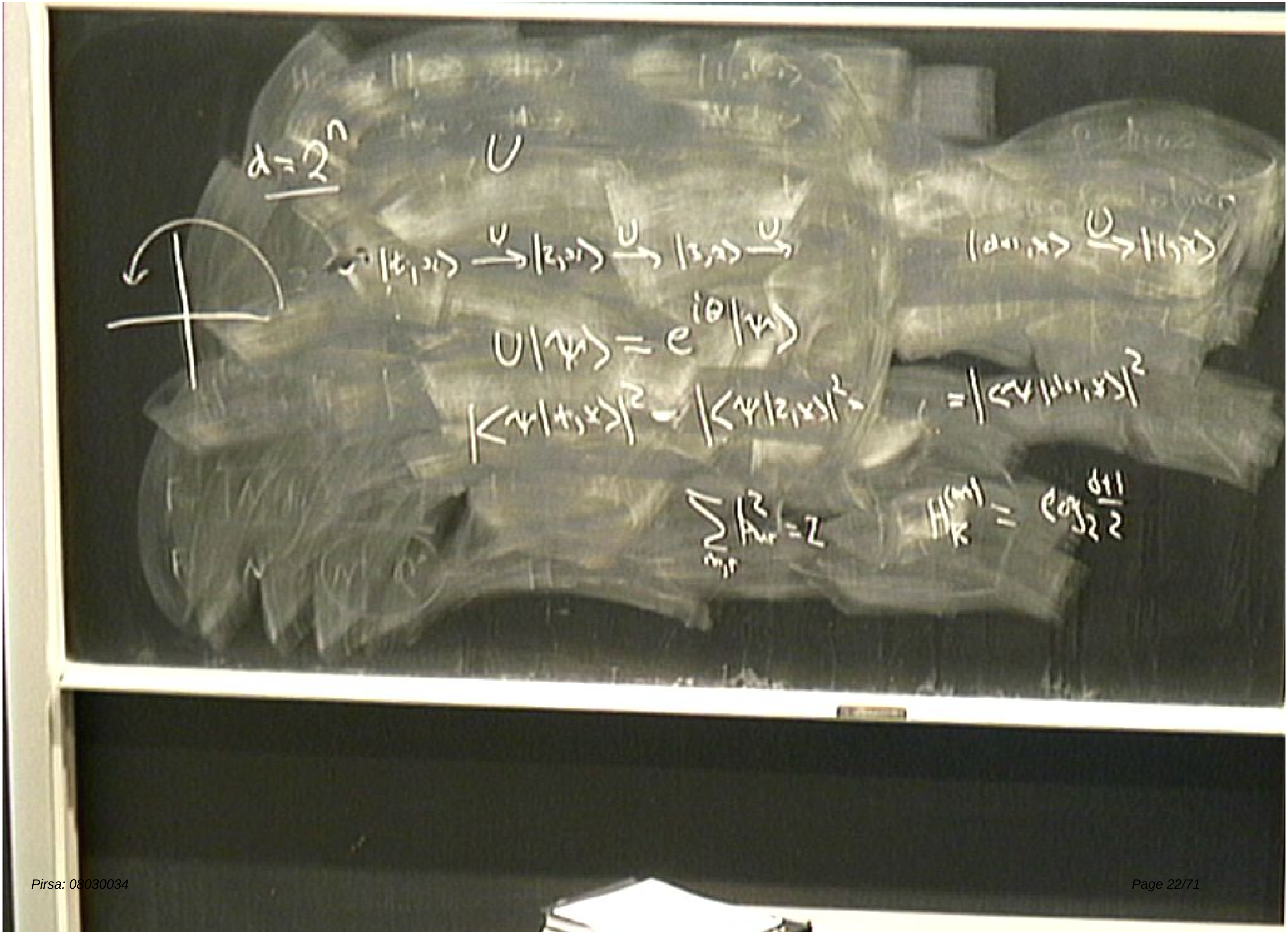
U

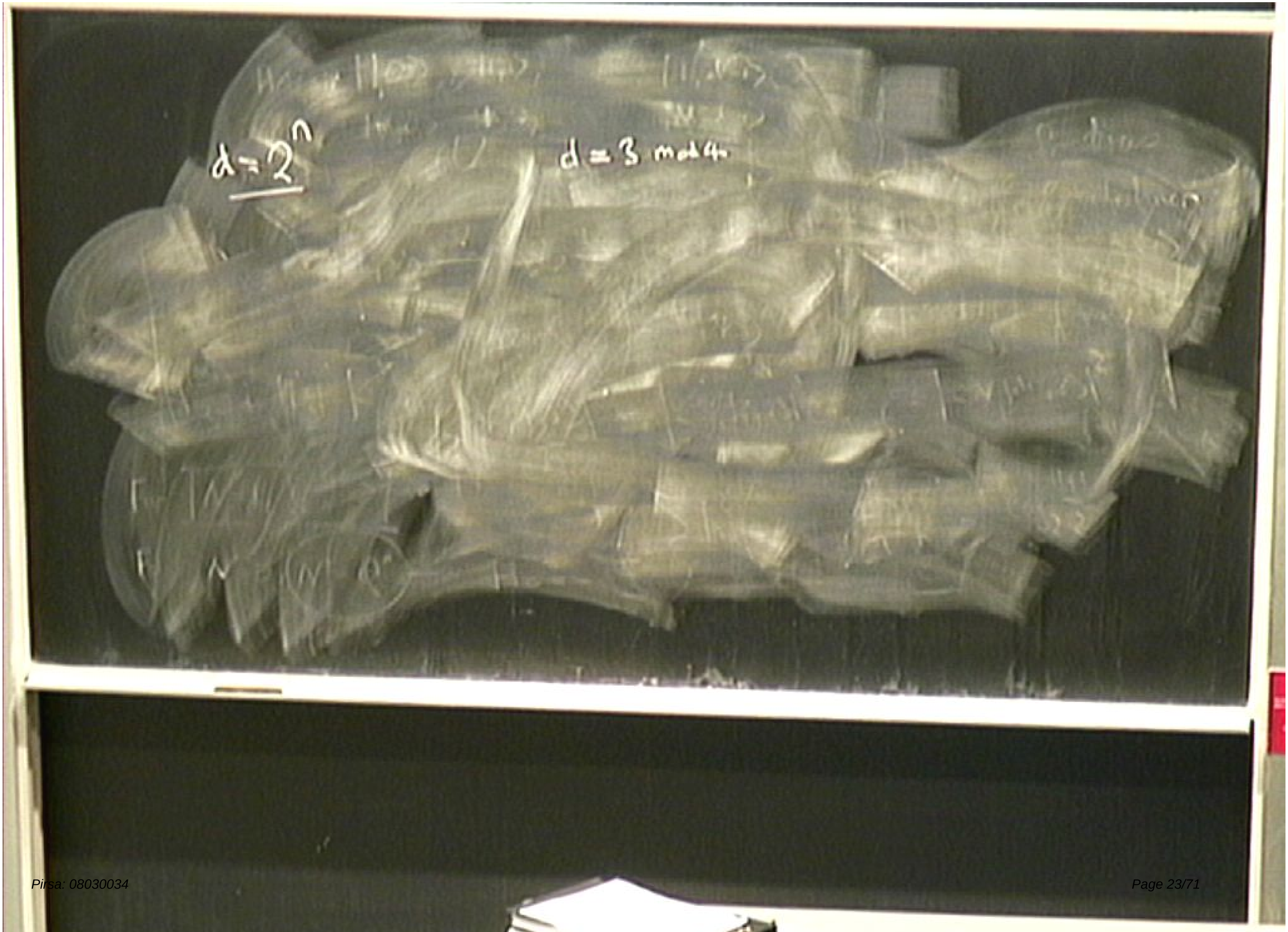
$|1,x\rangle \xrightarrow{U} |2,x\rangle \xrightarrow{U} |3,x\rangle \xrightarrow{U} \quad |d+1,x\rangle \xrightarrow{U} |1,x\rangle$

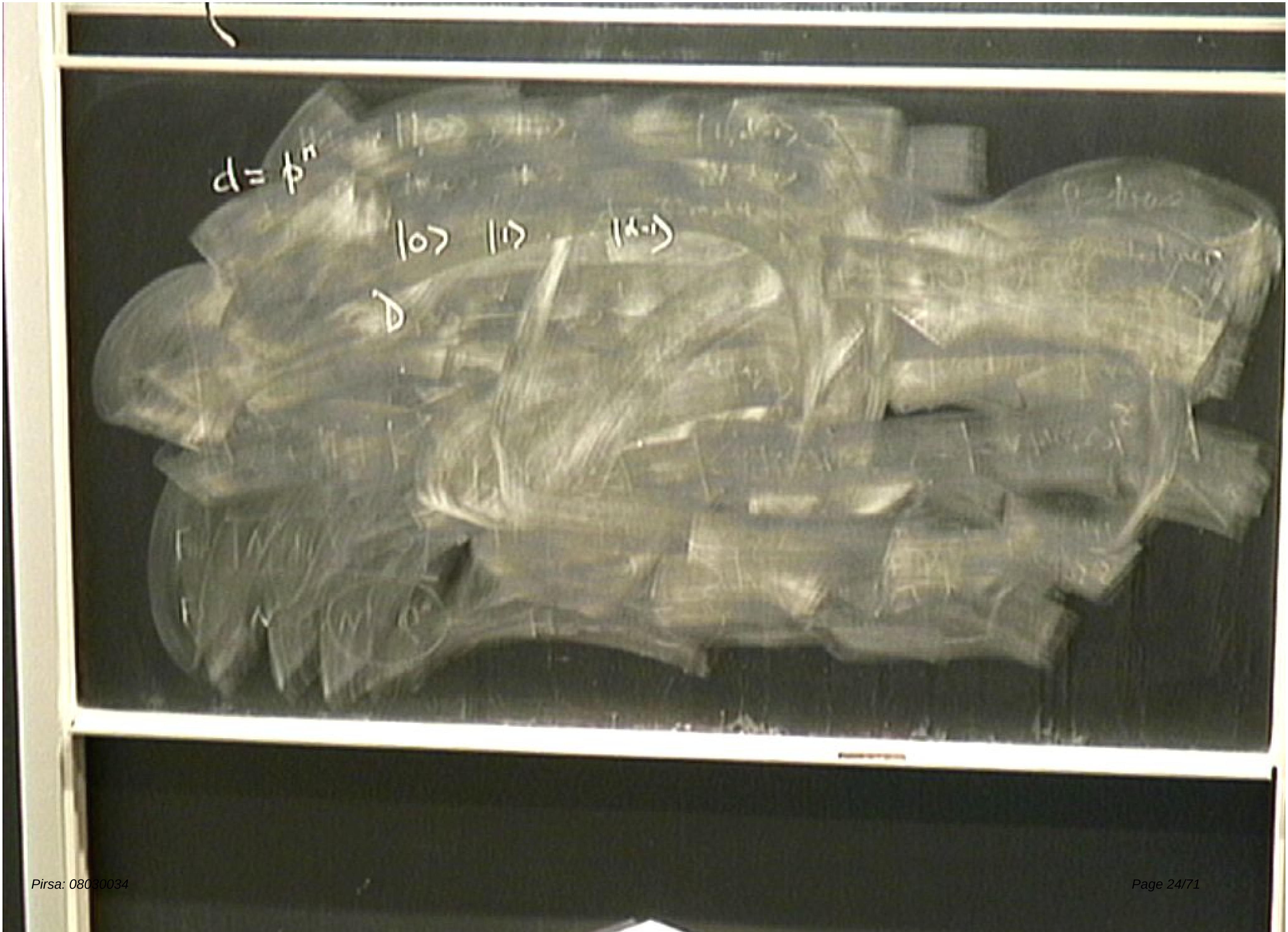
$$U|\psi\rangle = e^{i\theta}|\psi\rangle$$

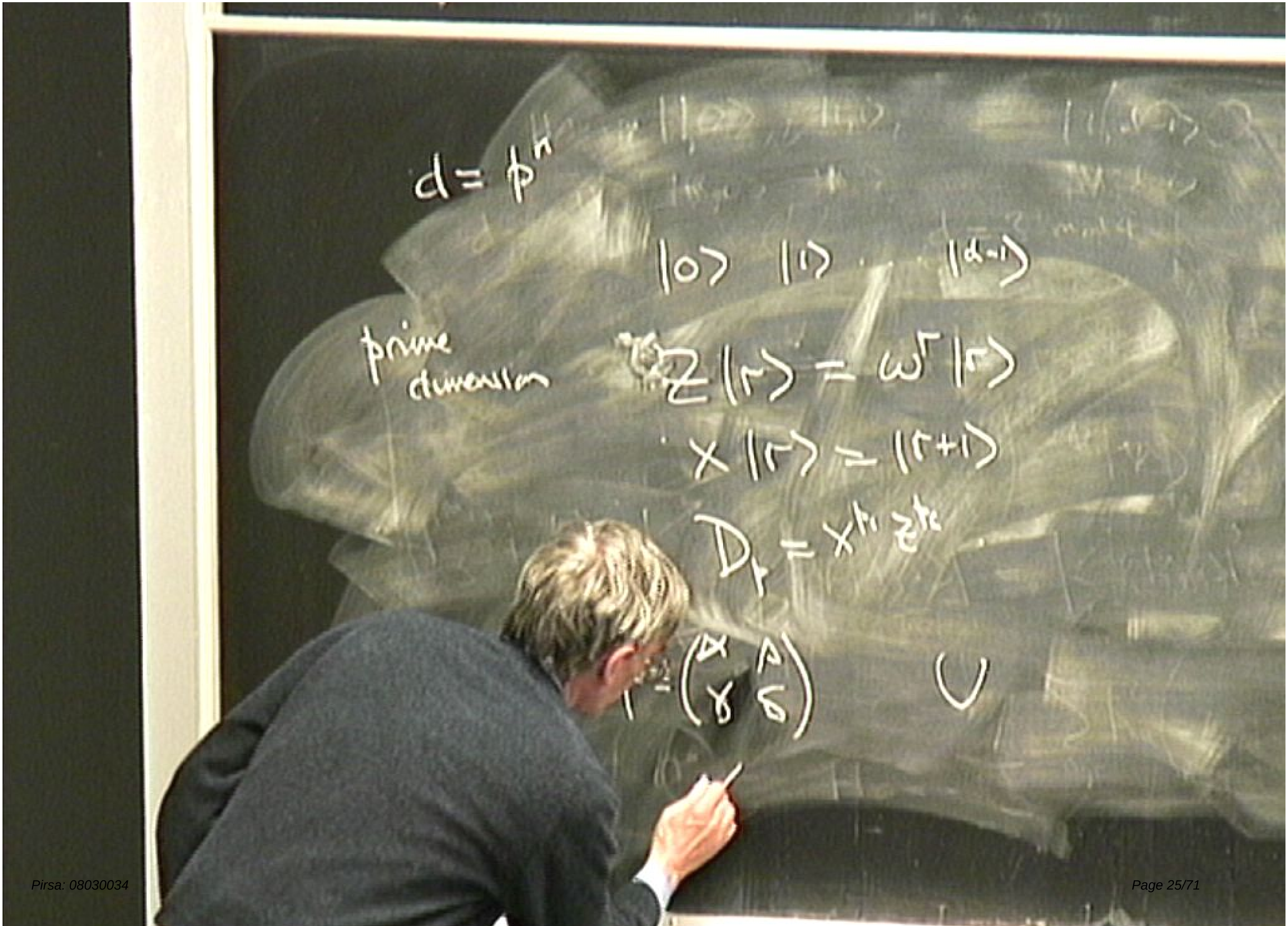
$$|\langle\psi|1,x\rangle|^2 = |\langle\psi|2,x\rangle|^2 = \quad = |\langle\psi|d+1,x\rangle|^2$$

$$\sum_{m,r} |h_{mr}|^2 = 1 \qquad H_k^{(m)} = \log_2 \frac{d+1}{2}$$


d = 2^n
U
|1,x⟩ →U |2,x⟩ →U |3,x⟩ →U
|d+1,x⟩ →U |1,x⟩
U|ψ⟩ = e^{iθ}|ψ⟩
|⟨ψ|1,x⟩|^2 = |⟨ψ|2,x⟩|^2 = … = |⟨ψ|d+1,x⟩|^2
∑_{m,r} |h_{mr}|^2 = 2
H_K^{(m)} = log_2 (d+1)/2


$d = 2^n$
$d = 3 \bmod 4$


d = p^n
|0> |1> |k-1>
D


d = p^n
|0⟩ |1⟩ ... |d-1⟩
prime dimension
Z|r⟩ = ω^r |r⟩
X|r⟩ = |r+1⟩
D_p = X^p1 Z^p2
U

$d = p^n$

$|0\rangle \quad |1\rangle \quad \ldots \quad |d-1\rangle$

prime dimension

$Z|r\rangle = \omega^r |r\rangle$

$X|r\rangle = |r+1\rangle$

$D_p = X^{p_1} Z^{p_2}$

$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad U_F D_p U_F^\dagger = D_{Fp}$

$\alpha\delta - \beta\gamma = \pm 1$

$d = p^n$

$|0\rangle \quad |1\rangle \quad |d-1\rangle$

prime dimension

$Z|r\rangle = \omega^r |r\rangle$

$X|r\rangle = |r+1\rangle$

$D_p = X^{p_1} Z^{p_2}$

$F \longrightarrow U_F$

$F_1 F_2 \longrightarrow U_{F_1} U_{F_2}$

$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad U_F D_p U_F^\dagger = D_{Fp}$

$\alpha\delta - \beta\gamma = \pm 1$

$d = p^n$

$|0\rangle \quad |1\rangle \quad |d-1\rangle$

prime dimension

$Z|r\rangle = \omega^r |r\rangle$

$X|r\rangle = |r+1\rangle$

$D_p = X^{p_1} Z^{p_2}$

$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad U_F D_p U_F^\dagger = D_{Fp}$

$\alpha\delta - \beta\gamma = \pm 1$

$Z_r |x\rangle = \omega^{Tr(rx)} |x\rangle$

$X_r |x\rangle = |x+r\rangle$

$F \longrightarrow U_F$

$F_1 F_2 \longrightarrow U_{F_1} U_{F_2}$

$d = p^n$

$|0\rangle \quad |1\rangle \quad |d-1\rangle$

prime dimension

$Z|r\rangle = \omega^r |r\rangle$

$X|r\rangle = |r+1\rangle$

$D_p = X^{p_1} Z^{p_2}$

$Z_r |x\rangle = \omega^{\mathrm{Tr}(rx)} |x\rangle$

$X_r |x\rangle = |x+r\rangle$

$F \longrightarrow U_F$

$F_1 F_2 \longrightarrow U_{F_1} U_{F_2}$

$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad U_F D_p U_F^\dagger = D_{Fp}$

$\alpha\delta - \beta\gamma = \pm 1$

$d = p^n$

prime dimension

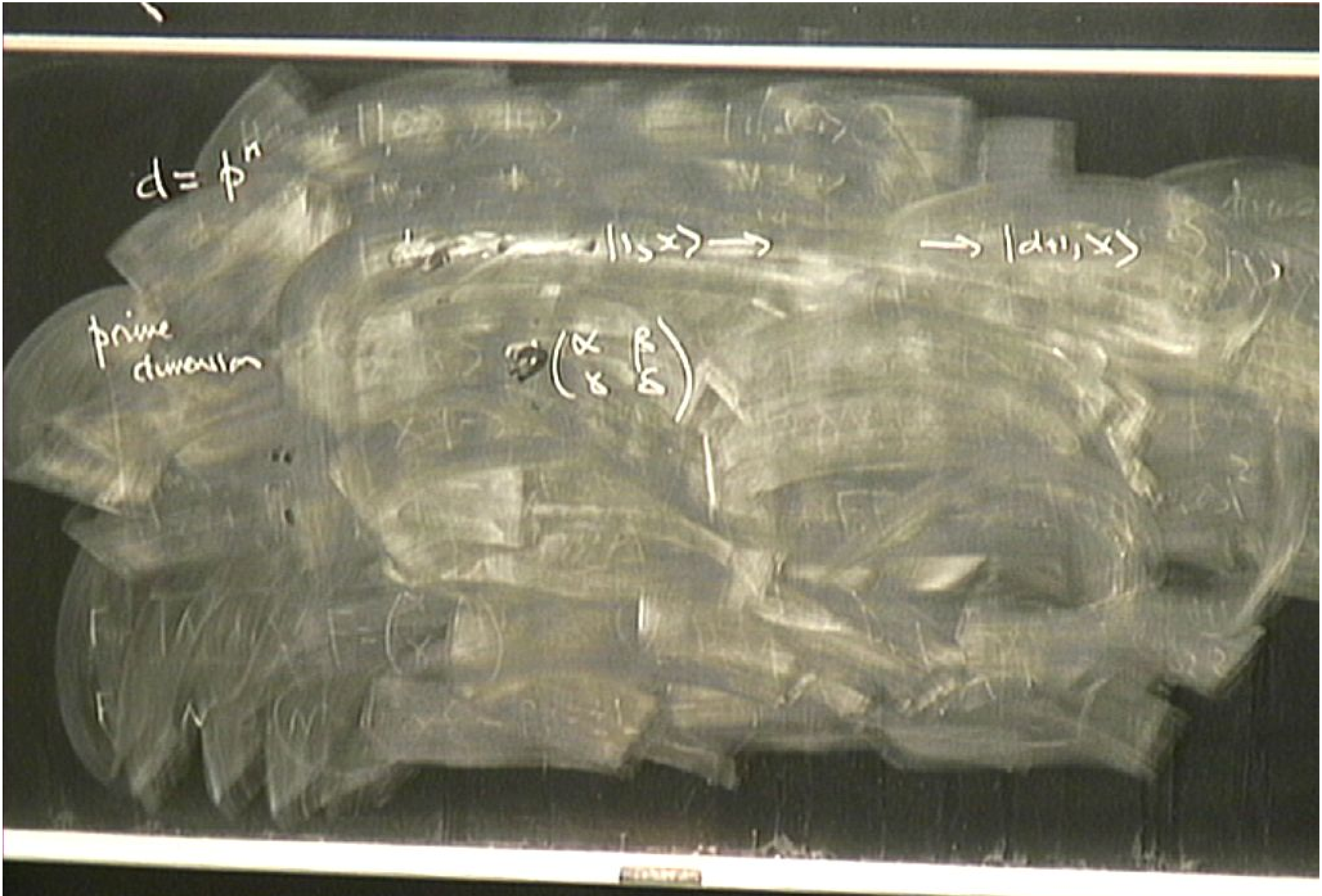
$|0,x\rangle \longrightarrow |1,x\rangle \longrightarrow \quad \longrightarrow |d-1,x\rangle$

$d = p^n$

prime dimension

$|0,x\rangle \longrightarrow |1,x\rangle \longrightarrow \quad \longrightarrow |d-1,x\rangle$

$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$


d = p^n
prime dimension
|1, x⟩ →
→ |d+1, x⟩
(α β / γ δ)

$d = p^n$

prime dimension

$|1, x\rangle \longrightarrow \qquad \longrightarrow |d+1, x\rangle$

$$\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix} = S\begin{pmatrix}\lambda_1 & 0 \\ 0 & \lambda_2\end{pmatrix}S^{-1}$$

$$\lambda_1^n = \lambda_2^n = 1$$

$d = p^n$

prime dimension

$|1, x\rangle \longrightarrow \quad \longrightarrow |d-1, x\rangle$

$$\Phi\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = S \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} S^{-1}$$

$\mathbb{Z}_d$

$$\lambda_1^n = \lambda_2^n = 1$$

$d = p^n$

prime dimension

$\mathbb{Z}_d$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\det \begin{pmatrix} \lambda & 1 \\ -1 & \lambda \end{pmatrix} = 0$$

$$\lambda^2 + 1 = 0$$

$$\lambda = \pm i$$

$d = p^n$

$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

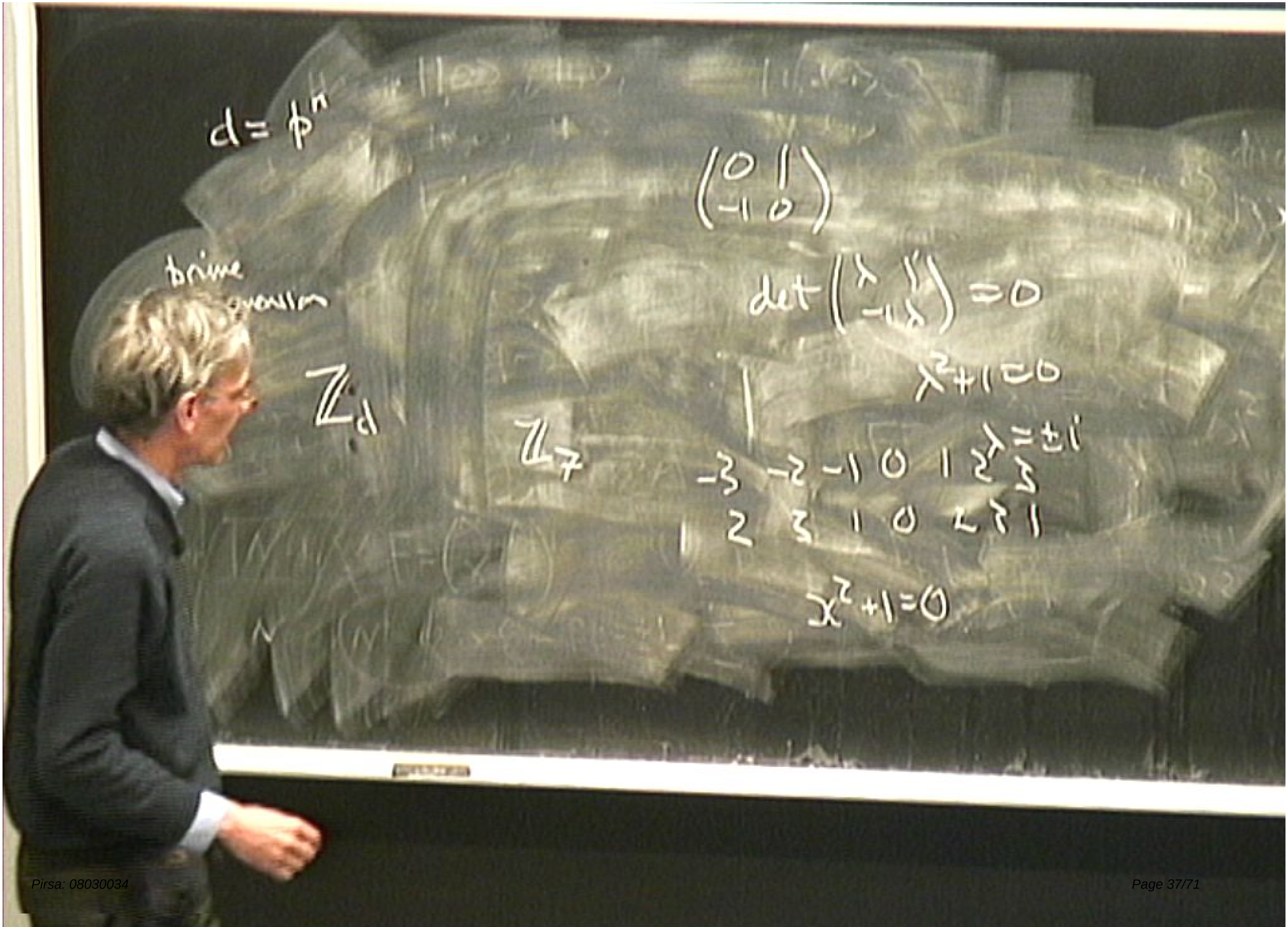
prime dimension

$\det\begin{pmatrix} \lambda & 1 \\ -1 & \lambda \end{pmatrix} = 0$

$\mathbb{Z}_d$

$\lambda^2 + 1 = 0$

$\lambda = \pm i$



d = p^n
prime
Z_d
Z_7
det = 0
λ^2+1=0
λ=±i
-3 -2 -1 0 1 2 3
x^2+1=0

$d = p^n$

prime dimension

$\mathbb{Z}_d$

$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$\det\begin{pmatrix} \lambda & 1 \\ -1 & \lambda \end{pmatrix} = 0$

$\lambda^2 + 1 = 0$

$\lambda = \pm i$

$\mathbb{Z}_7$

-3	-2	-1	0	1	2	3
2	3	1	0	2	3	1

$x^2 + 1 = 0$

$x + iy$

$i^2 = -1 \pmod 7$

$d = p^n$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

prime dimension

$$\det \begin{pmatrix} \lambda & 1 \\ -1 & \lambda \end{pmatrix} = 0$$

$\mathbb{Z}_d$

$$\lambda^2 + 1 = 0$$

$\mathbb{Z}_7$

$$\lambda = \pm i$$

$$\begin{array}{ccccccc} -3 & -2 & -1 & 0 & 1 & 2 & 3 \\ 2 & 3 & 1 & 0 & 2 & 2 & 1 \end{array}$$

$$x^2 + 1 = 0$$

$x + iy$ $\qquad$ $i^2 = -1 \mod 7$

$d = p^n$

prime dimension

$\mathbb{Z}_d$

$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$\det\begin{pmatrix} \lambda & 1 \\ -1 & \lambda \end{pmatrix} = 0$

$\mathbb{F}_{7^2}$

$\lambda^2 + 1 = 0$

$\lambda = \pm i$

$\mathbb{Z}_7$

$-3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3$

$2 \quad 3 \quad 1 \quad 0 \quad 2 \quad 3 \quad 1$

$\mathbb{F}_{49}$

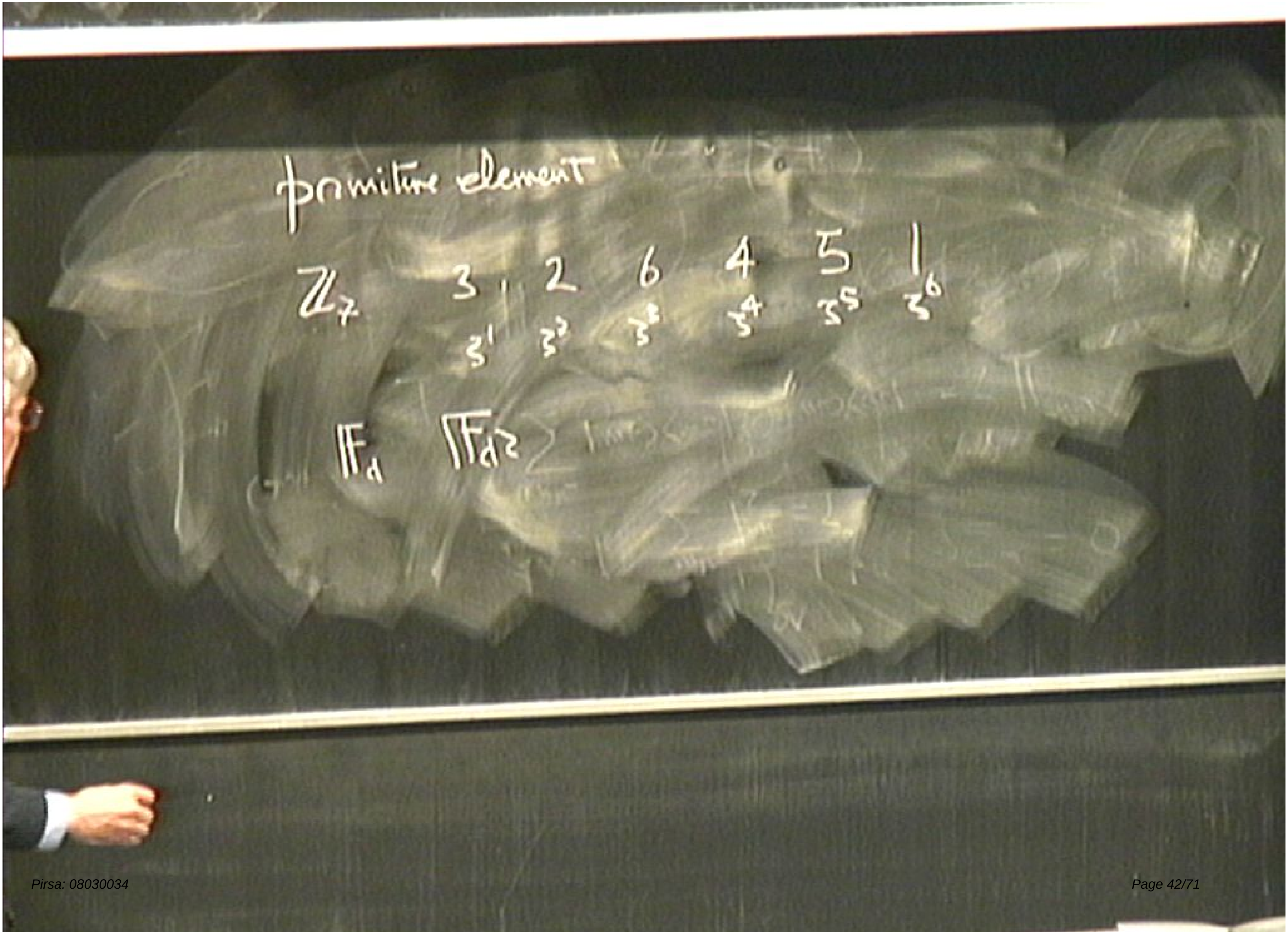
$x^2 + 1 = 0$

$x + iy$

$i^2 = -1 \pmod 7$

primitive element

$\mathbb{Z}_7$	3	2	6	4	5	1
	ζ^1	ζ^2	ζ^3	ζ^4	ζ^5	ζ^6


primitive element
$\mathbb{Z}_7$ 3 2 6 4 5 1
ζ^1 ζ^2 ζ^3 ζ^4 ζ^5 ζ^6
$\mathbb{F}_d$ $\mathbb{F}_{d^2}$

primitive element

$$\mathbb{Z}_7 \quad \begin{array}{cccccc} 3 & 2 & 6 & 4 & 5 & 1 \\ \zeta^1 & \zeta^2 & \zeta^3 & \zeta^4 & \zeta^5 & \zeta^6 \end{array}$$

$\mathbb{F}_d \quad \mathbb{F}_{d^2}$

Θ

primitive element

$$\mathbb{Z}_7 \quad \begin{array}{cccccc} 3, & 2 & 6 & 4 & 5 & 1 \\ \zeta^1 & \zeta^2 & \zeta^3 & \zeta^4 & \zeta^5 & \zeta^6 \end{array}$$

$\mathbb{F}_d \quad \mathbb{F}_{d^2}$

Θ primitive element of $\mathbb{F}_{d^2}$

$\xi = \Theta^{d+1}$ " " " $\mathbb{F}_d$

$x \in \mathbb{F}_{d^2}$ $\quad$ $x \in \mathbb{F}_d$ iff $x^d = x$

$x, y \in \mathbb{F}_{d^2}$ $\quad$ $(x+y)^d = x^d + y^d$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

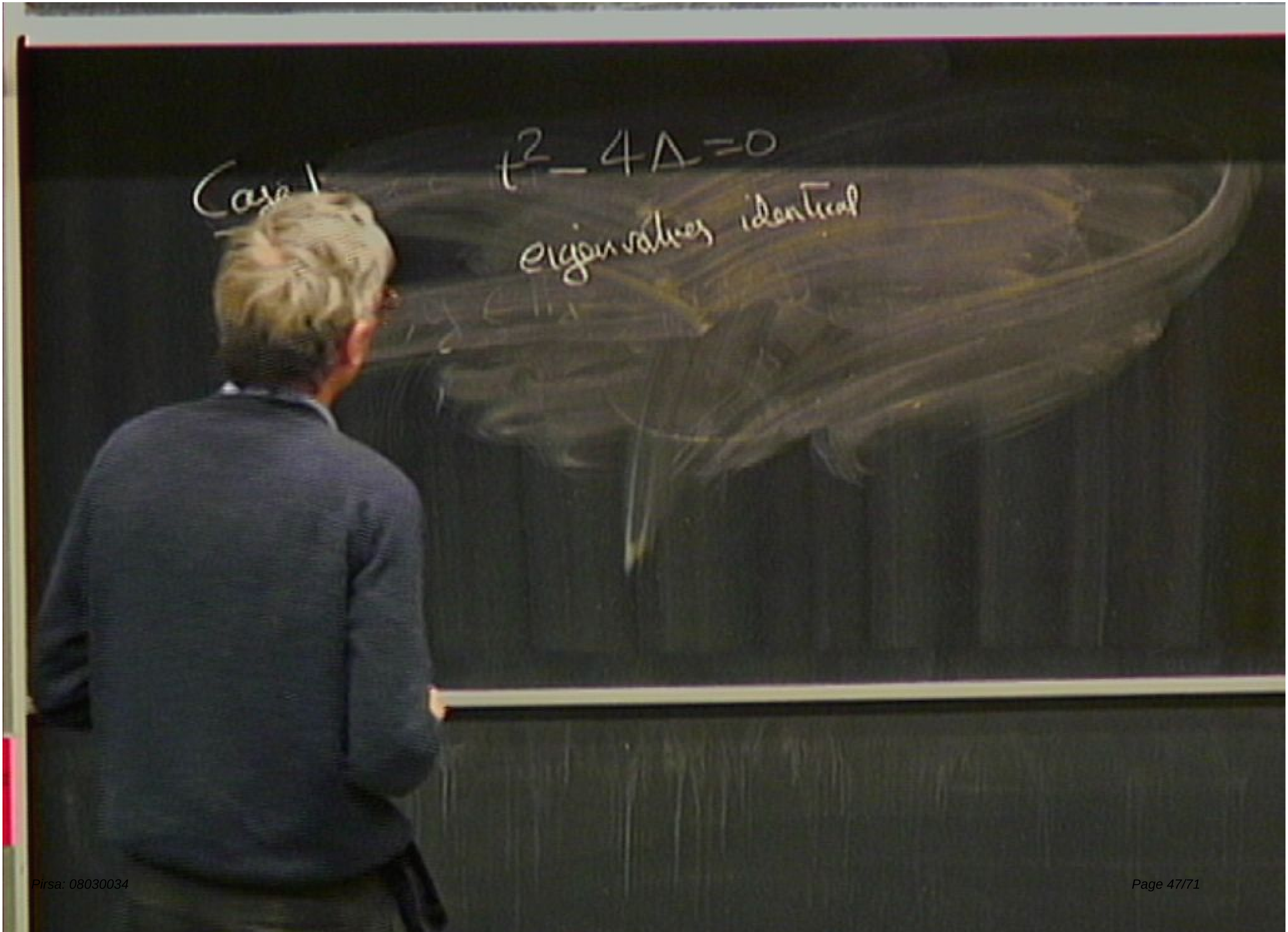
$$\det \begin{pmatrix} \alpha-\lambda & \beta \\ \gamma & \delta-\lambda \end{pmatrix} = 0$$

$$t = \mathrm{Tr} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

$$\lambda^2 - t\lambda + \Delta = 0$$

$$\Delta = \mathrm{Det} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

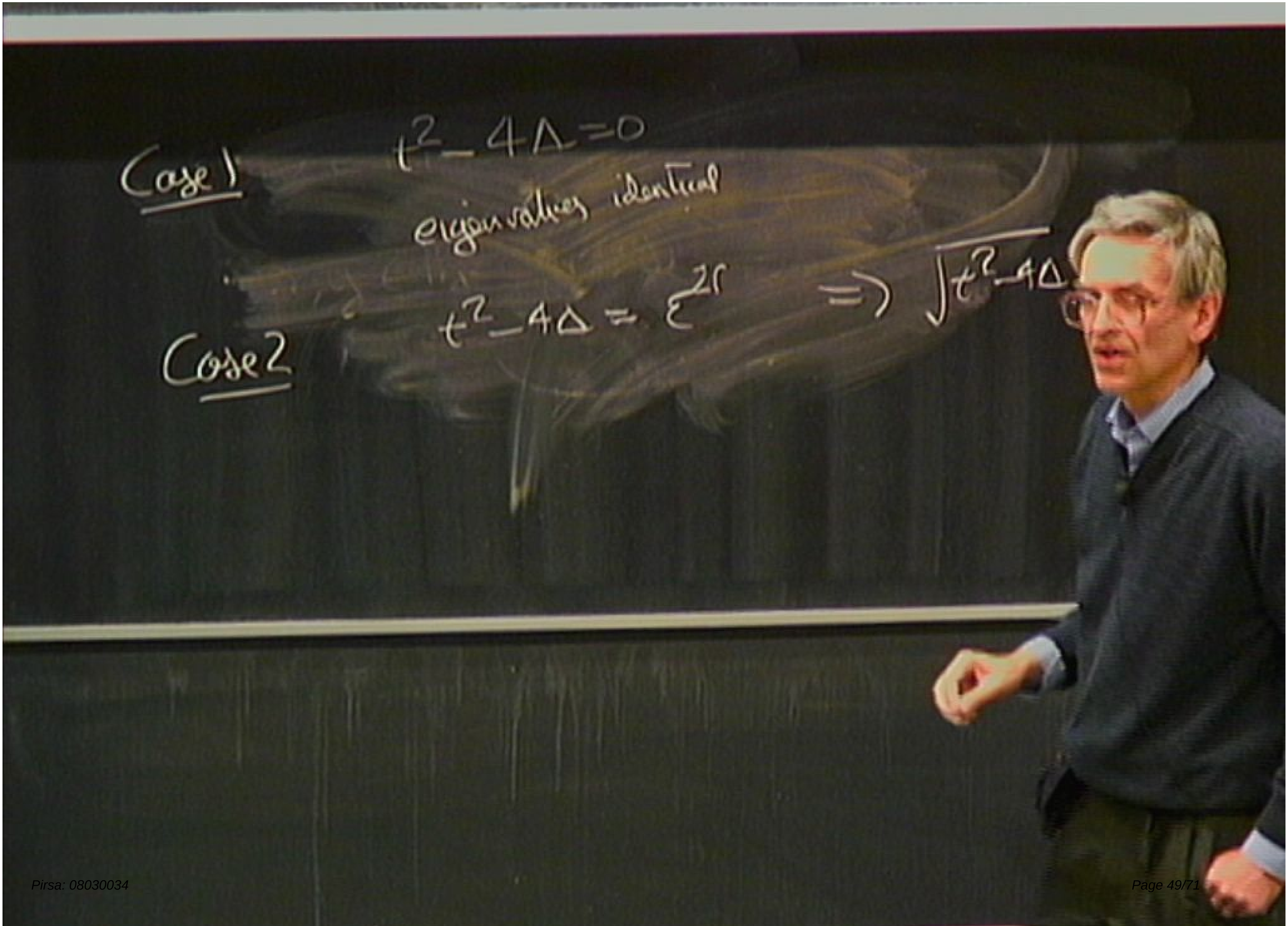
$$\lambda = \frac{t \pm \sqrt{t^2 - 4\Delta}}{2}$$


Case 1
$t^2 - 4\Delta = 0$
eigenvalues identical

Case 1

$t^2 - 4\Delta = 0$

eigenvalues identical


Case 1
$t^2 - 4\Delta = 0$
eigenvalues identical
Case 2
$t^2 - 4\Delta = \varepsilon^{2r}$
$\Rightarrow \sqrt{t^2 - 4\Delta}$

Case 1 $\quad t^2 - 4\Delta = 0 \qquad \varepsilon^{d-1} = 1$

eigenvalues identical

Case 2 $\quad t^2 - 4\Delta = \varepsilon^{2r} \quad \Rightarrow \sqrt{t^2 - 4\Delta} = \pm\varepsilon^r$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = S \begin{pmatrix} \varepsilon^k & 0 \\ 0 & \Delta\varepsilon^{-k} \end{pmatrix} S^{-1}$$

order: factor of $d-1$.

Case 1 $t^2 - 4\Delta = 0$ $\qquad \varepsilon^{d-1} = 1$

eigenvalues identical

Case 2 $t^2 - 4\Delta = \varepsilon^{2r}$ $\Rightarrow \sqrt{t^2 - 4\Delta} = \pm\varepsilon^{r}$

$$\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix} = S\begin{pmatrix}\varepsilon^{k} & 0 \\ 0 & \Delta\varepsilon^{-k}\end{pmatrix}S^{-1}$$

order : factor of $d-1$.

Case 3 $t^2 - 4\Delta = \varepsilon^{2r+1}$

Case 1 $t^2 - 4\Delta = 0$ $\varepsilon^{d-1} = 1$

eigenvalues identical

$t^2 - 4\Delta = \varepsilon^{2r}$ $\Rightarrow$ $\sqrt{t^2 - 4\Delta} = \pm\varepsilon^r$

Case 2

$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = S \begin{pmatrix} \varepsilon^k & 0 \\ 0 & \Delta\varepsilon^{-k} \end{pmatrix} S^{-1}$

$t^2 - 4\Delta = \varepsilon^{2r+1}$

Case 3

order: factor of d-1.

$\lambda_+ = m^r$ $\quad m \approx \theta^{\frac{d-1}{2}}$

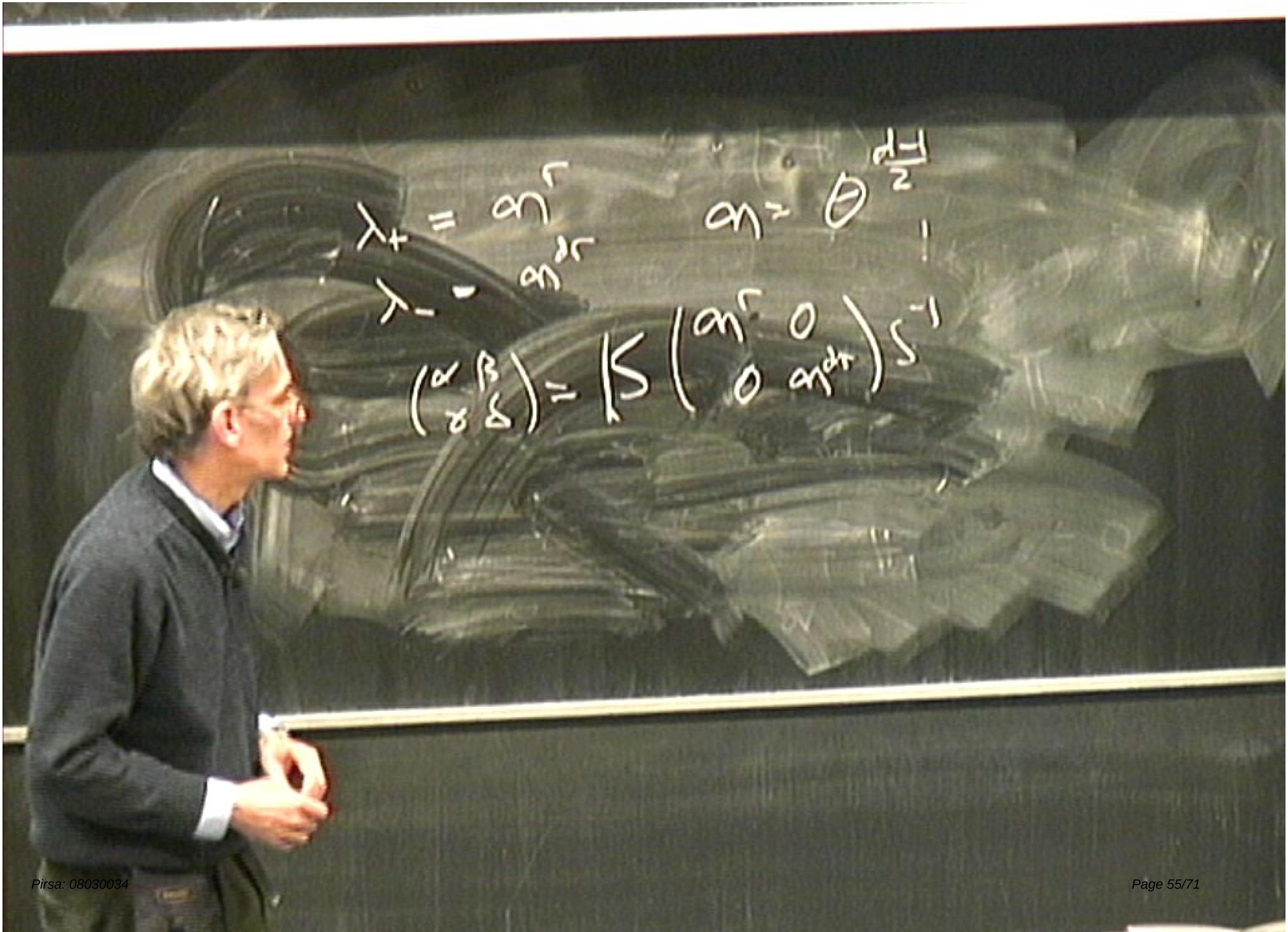
$\lambda_- = m^{dr}$

$(\alpha\ \beta$

$$\lambda_+ = m^r \qquad m = \theta^{\frac{d-1}{2}}$$

$$\lambda_- = m^{dr}$$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = S \begin{pmatrix} m^r & 0 \\ 0 & m^{dr} \end{pmatrix} S^{-1}$$


λ+ = m^r
m = θ^((d-1)/2)
λ- = m^(-r)
(α β / γ δ) = S (m^r 0 / 0 m^(-r)) S^(-1)

$$\lambda_+ = m^r \qquad m = \theta^{\frac{d-1}{2}}$$

$$\lambda_- = m^{dr}$$

$$m^r + m^{dr} \qquad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = S \begin{pmatrix} m^r & 0 \\ 0 & m^{dr} \end{pmatrix} S^{-1}$$

$$\begin{pmatrix} 0 & 1 \\ (-1)^r & m^r + m^{dr} \end{pmatrix}$$

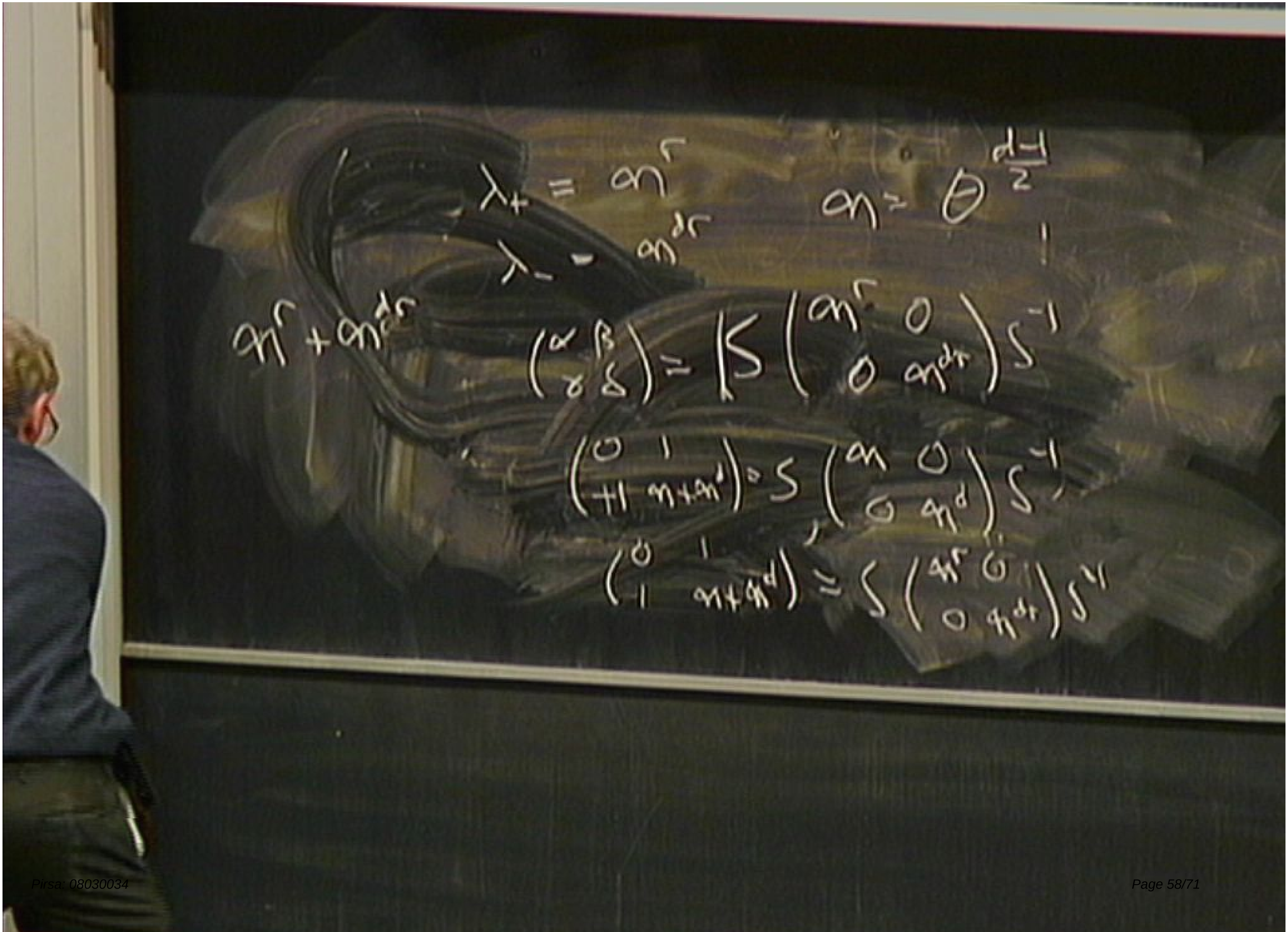
$$\lambda_+ = m^{r} \qquad m = \theta^{\frac{d-1}{2}}$$

$$\lambda_- = m^{dr}$$

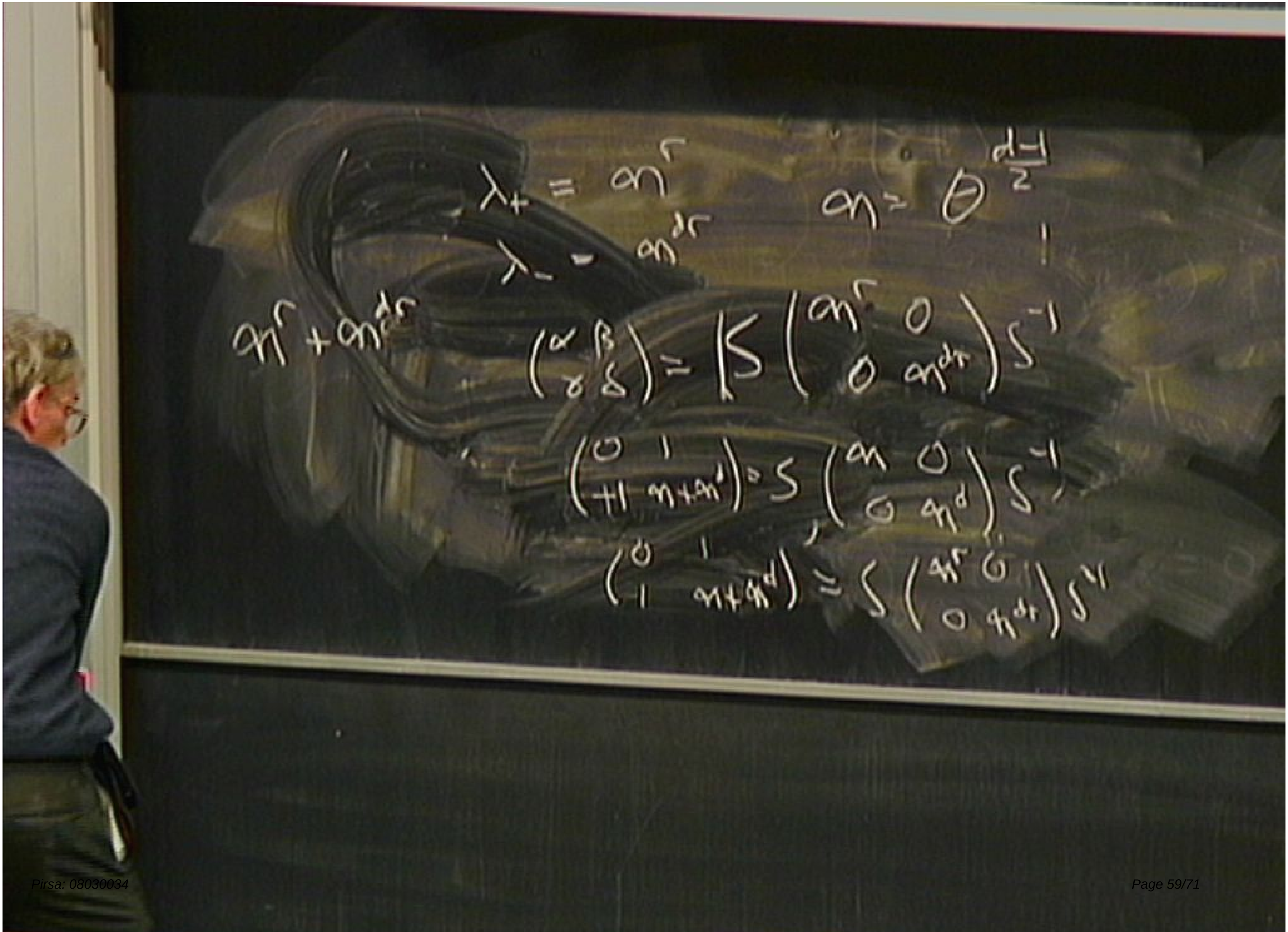
$$m^{r} + m^{dr}$$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = S \begin{pmatrix} m^{r} & 0 \\ 0 & m^{dr} \end{pmatrix} S^{-1}$$

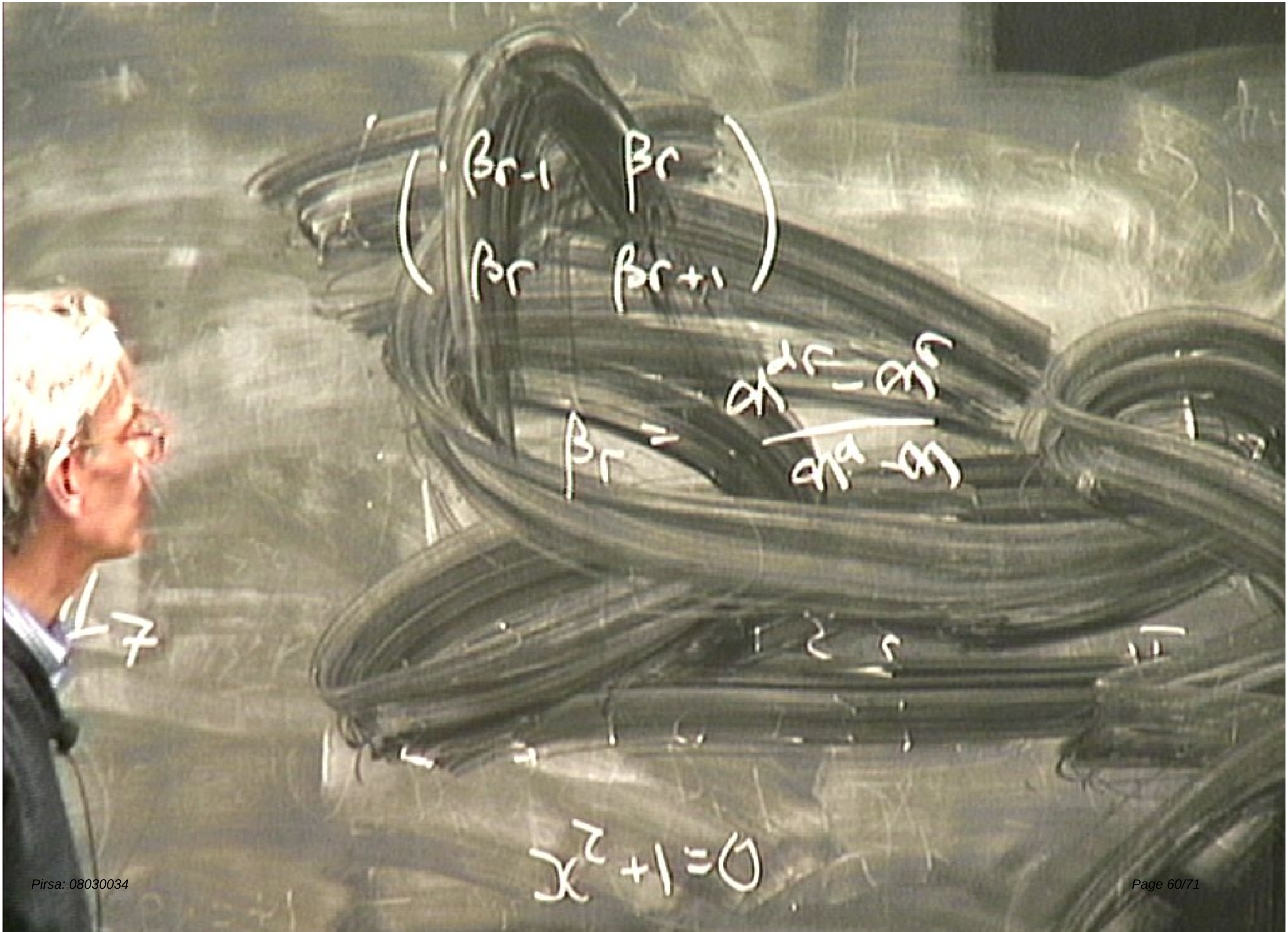
$$\begin{pmatrix} 0 & 1 \\ (-1)^{r} & m^{r} + m^{dr} \end{pmatrix}$$



$\lambda_+ = q^r$
$q = \theta^{\frac{d-1}{2}}$
$\lambda_- = q^{dr}$
$q^r + q^{dr}$
$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = S \begin{pmatrix} q^r & 0 \\ 0 & q^{dr} \end{pmatrix} S^{-1}$
$\begin{pmatrix} 0 & 1 \\ -1 & q+q^d \end{pmatrix} = S \begin{pmatrix} q & 0 \\ 0 & q^d \end{pmatrix} S^{-1}$
$\begin{pmatrix} 0 & 1 \\ 1 & q+q^d \end{pmatrix} = S \begin{pmatrix} q^r & 0 \\ 0 & q^{dr} \end{pmatrix} S^{-1}$



$\lambda_+ = \varphi^r$
$\varphi = \theta^{\frac{d-1}{2}}$
$\lambda_- = \varphi^{dr}$
$\varphi^r + \varphi^{dr}$
$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = S \begin{pmatrix} \varphi^r & 0 \\ 0 & \varphi^{dr} \end{pmatrix} S^{-1}$
$\begin{pmatrix} 0 & 1 \\ -1 & \varphi+\varphi^d \end{pmatrix} = S \begin{pmatrix} \varphi & 0 \\ 0 & \varphi^d \end{pmatrix} S^{-1}$
$\begin{pmatrix} 0 & 1 \\ 1 & \varphi+\varphi^d \end{pmatrix} = S \begin{pmatrix} \varphi^r & 0 \\ 0 & \varphi^{dr} \end{pmatrix} S^{-1}$


βr-1 βr
βr βr+1
x²+1=0

$\lambda_+ = \omega^r$ $\quad \omega = \Theta^{\frac{d+1}{2}}$ $\quad \Theta^{d^2-1} = 1$

$\lambda_- = \omega^{dr}$ $\quad \omega^n = 1$

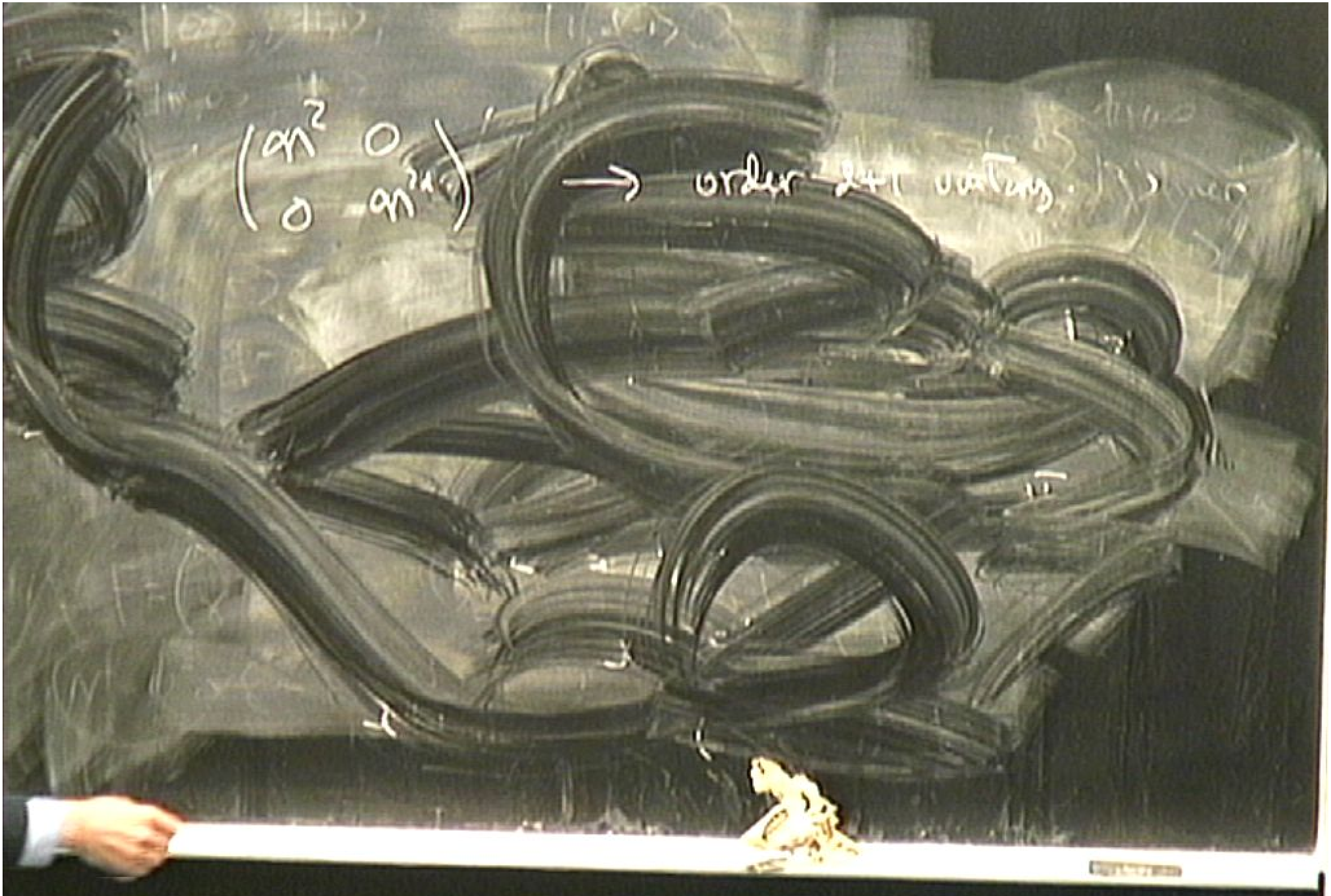
$\omega^r + \omega^{dr}$

$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = S \begin{pmatrix} \omega^r & 0 \\ 0 & \omega^{dr} \end{pmatrix} S^{-1}$

iff ω is a multiple of $2(\lambda+1)$

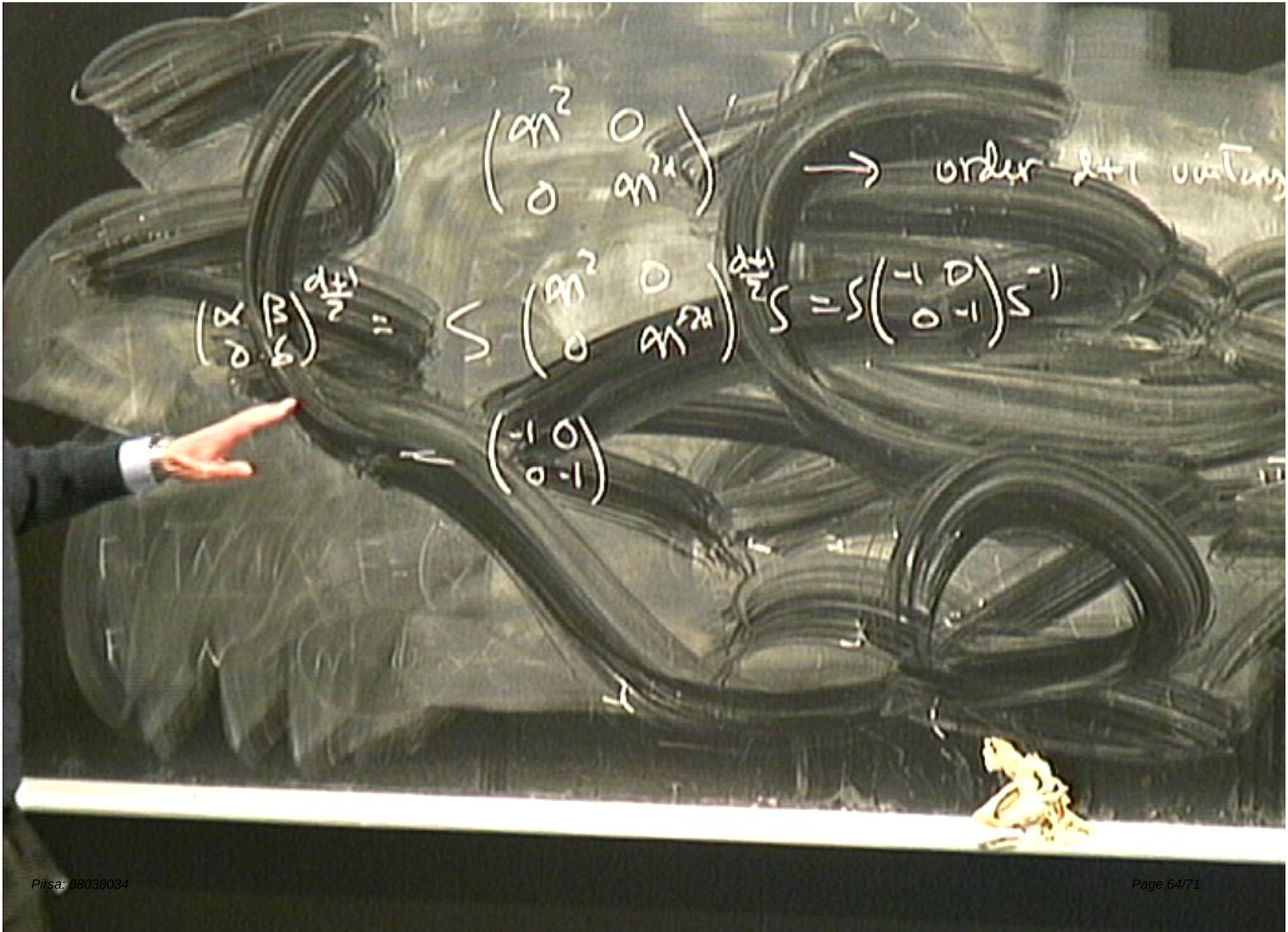
$\begin{pmatrix} 0 & 1 \\ +1 & \omega+\omega^d \end{pmatrix} = S \begin{pmatrix} \omega & 0 \\ 0 & \omega^d \end{pmatrix} S^{-1}$

$\begin{pmatrix} 0 & 1 \\ 1 & \omega+\omega^d \end{pmatrix}^r = S \begin{pmatrix} \omega^r & 0 \\ 0 & \omega^{dr} \end{pmatrix} S^{-1}$


order 2+1 vortex

$$\begin{pmatrix} \omega^2 & 0 \\ 0 & \omega^{2n} \end{pmatrix} \longrightarrow \text{order } 2n+1 \text{ unitary.}$$

$$S \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega^{2n} \end{pmatrix}^{\frac{2n+1}{2}} S = S \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} S^{-1}$$


$\begin{pmatrix} qn^2 & 0 \\ 0 & qn^{2l} \end{pmatrix} \longrightarrow$ order $l+1$
$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{\frac{d+1}{2}} = S \begin{pmatrix} qn^2 & 0 \\ 0 & qn^{2l} \end{pmatrix}^{\frac{d+1}{2}} S = S \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} S^{-1}$
$= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

$$\begin{pmatrix} \eta^2 & 0 \\ 0 & \eta^{2d} \end{pmatrix} \longrightarrow \text{order } d+1 \text{ unitary.}$$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{\frac{d+1}{2}} = S \begin{pmatrix} \eta^2 & 0 \\ 0 & \eta^{2d} \end{pmatrix}^{\frac{d+1}{2}} S = S \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} S^{-1}$$

$$\leftarrow \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\begin{pmatrix} q^n & 0 \\ 0 & q^{nd} \end{pmatrix} \longrightarrow \text{anti unitary } U^{-1}$$

$$\theta^{\frac{d-1}{2}}$$

$$U \; |1, x\rangle =$$

$$\begin{pmatrix} 1 & 0 \\ 0 & q^{d} \end{pmatrix} S^{-1}$$

$$\begin{pmatrix} 1 & q^n + q^{nd} \end{pmatrix} = S \begin{pmatrix} q^{r} & 0 \\ 0 & q^{dr} \end{pmatrix} S$$

$\begin{pmatrix} a^n & 0 \\ 0 & a^{n+1} \end{pmatrix} \longrightarrow$ anti unitary U

$\theta^{\frac{d-1}{2}}$ θ

$|1,x\rangle \xrightarrow{U} |2,x\rangle \xrightarrow{U} \cdots \xrightarrow{U} |d+1,x\rangle$ a^n

$\begin{pmatrix} \omega & 0 \\ 0 & \omega^d \end{pmatrix} \longrightarrow$ anti unitary U

$\Theta^{\frac{d-1}{2}}$

$\Theta^{d^2-1} = 1$

$\omega^n = 1$

iff ω is a multiple of $2(n+1)$

$|1,x\rangle \xrightarrow{U} |2,x\rangle \xrightarrow{U} \xrightarrow{U} |d+1,x\rangle$

$U|\psi\rangle = e^{i\theta}|\psi\rangle$

$U^2|\psi\rangle = U e^{i\theta}|\psi\rangle = e^{-i\theta}U|\psi\rangle$

$= e^{-i\theta}e^{i\theta}|\psi\rangle$

$= |\psi\rangle$

$d = 3 \mod 4$

$d = 1 \mod 4$

$d = 3 \bmod 4$

$d = 1 \bmod 4$

$$U^4 \quad |1, x\rangle \to |3, x\rangle \to$$

$$|2, x\rangle \to |4, x\rangle \to$$

$d = 3 \bmod 4$

$d = 1 \bmod 4$

U^4

$|1, x\rangle \to |3, x\rangle \to$

$|2, x\rangle \to |4, x\rangle \to$

1   1 dimensional eigenspace

$\frac{d-1}{2}$ 2 dimensional