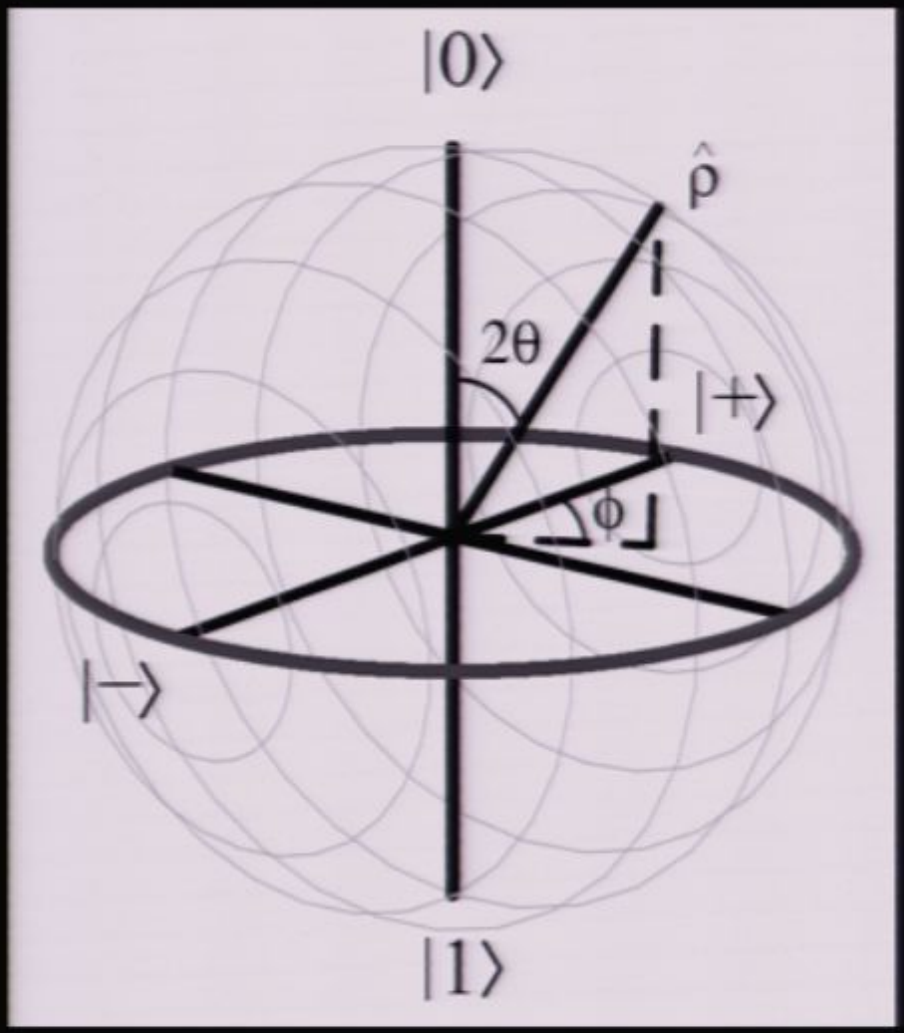
Title: Quantum Information Theory #2

Date: Mar 13, 2008 06:30 PM

URL: http://pirsa.org/08030008

Abstract: Teleportation, quantum key distribution, and quantum algorithms.

Density operators and the Bloch sphere representation of states.




$|\psi_i\rangle \to p_i$
$|j\rangle$

$|\psi_i\rangle \rightarrow p_i$

$|j\rangle$

$$P(j) = \sum_i p_i |\langle \psi_i | j \rangle|^2$$

$|\psi_i\rangle \to p_i$

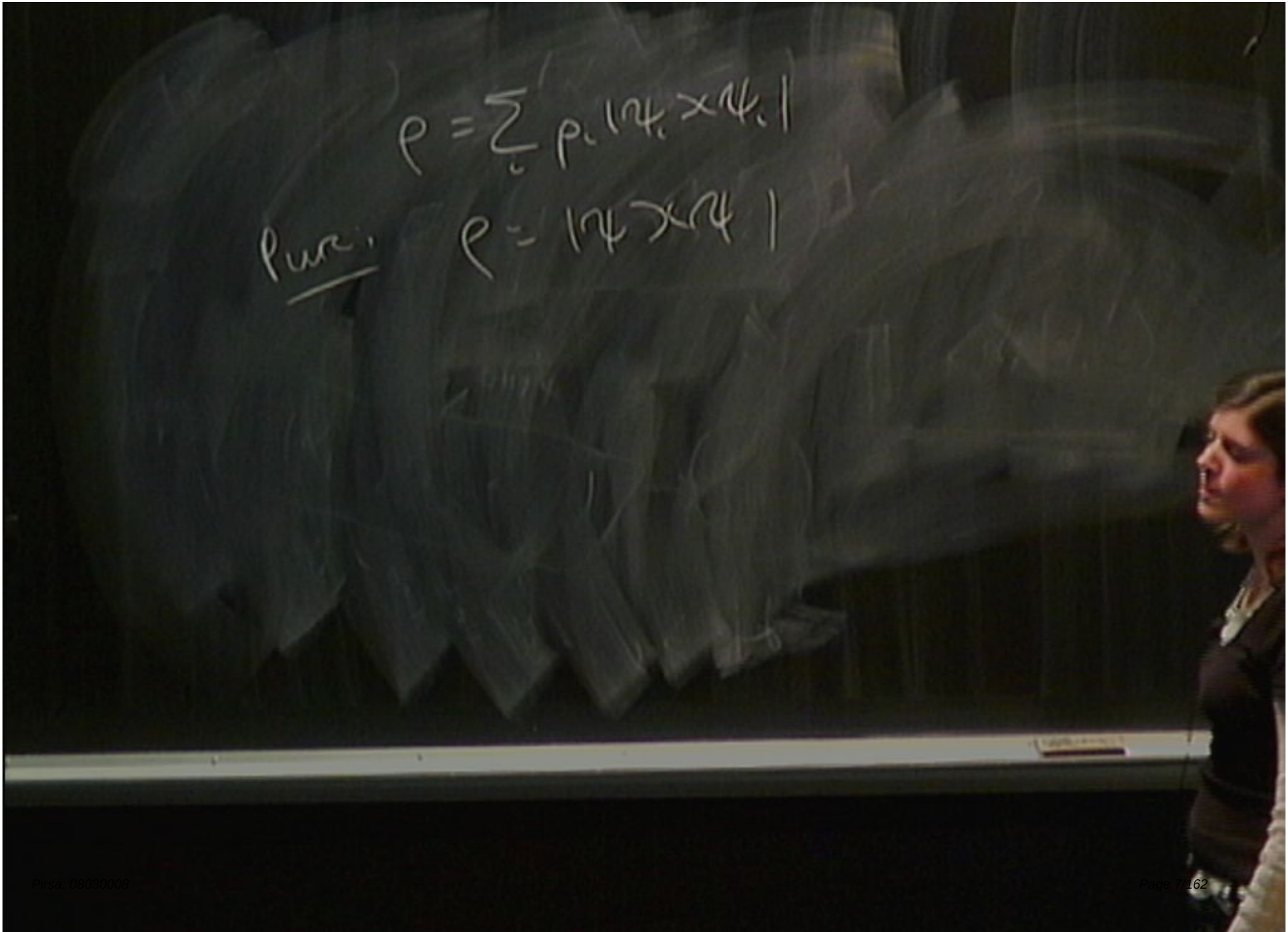
$|j\rangle$

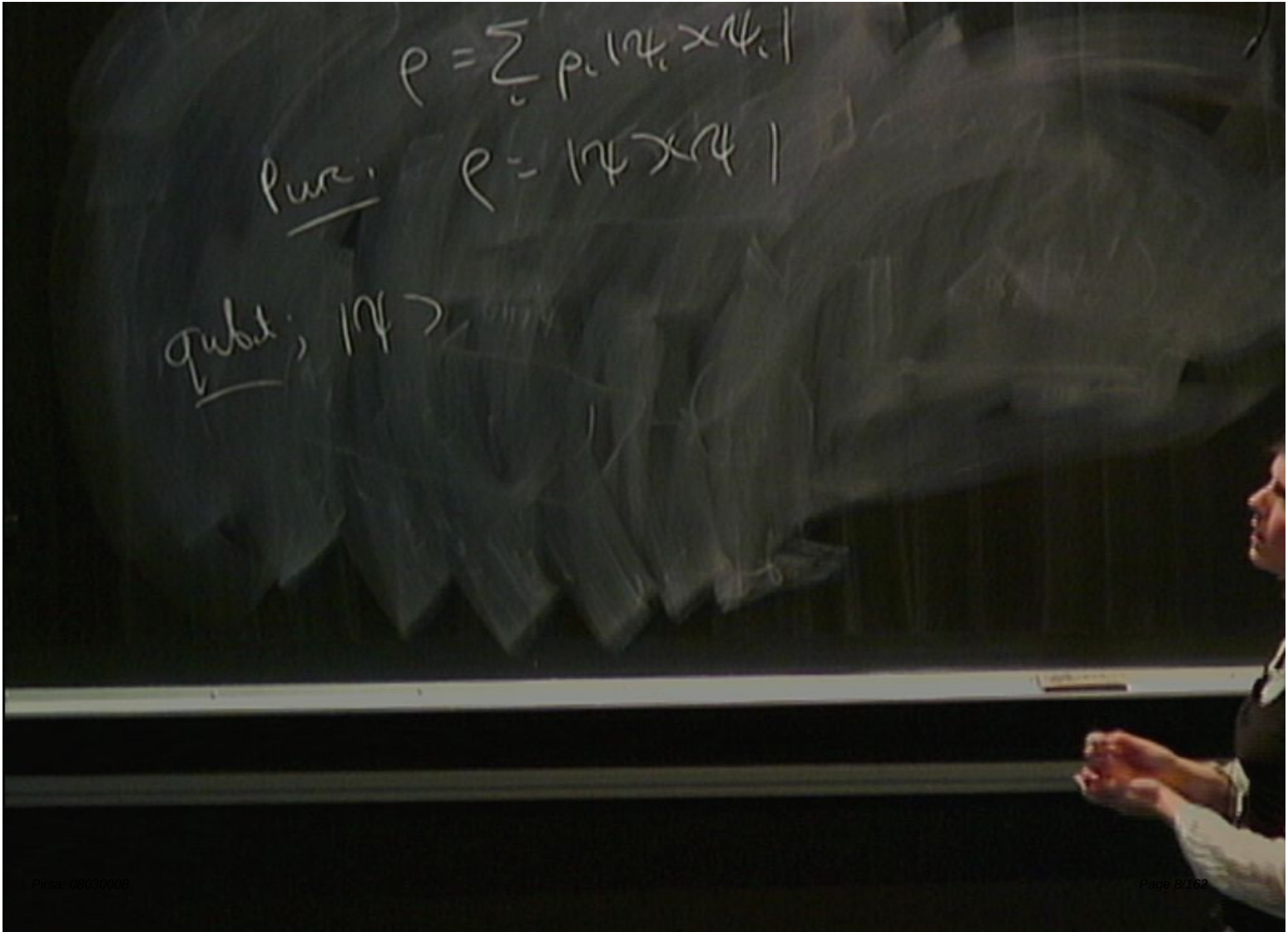
$$P(j) = \sum_i p_i |\langle \psi_i | j \rangle|^2$$

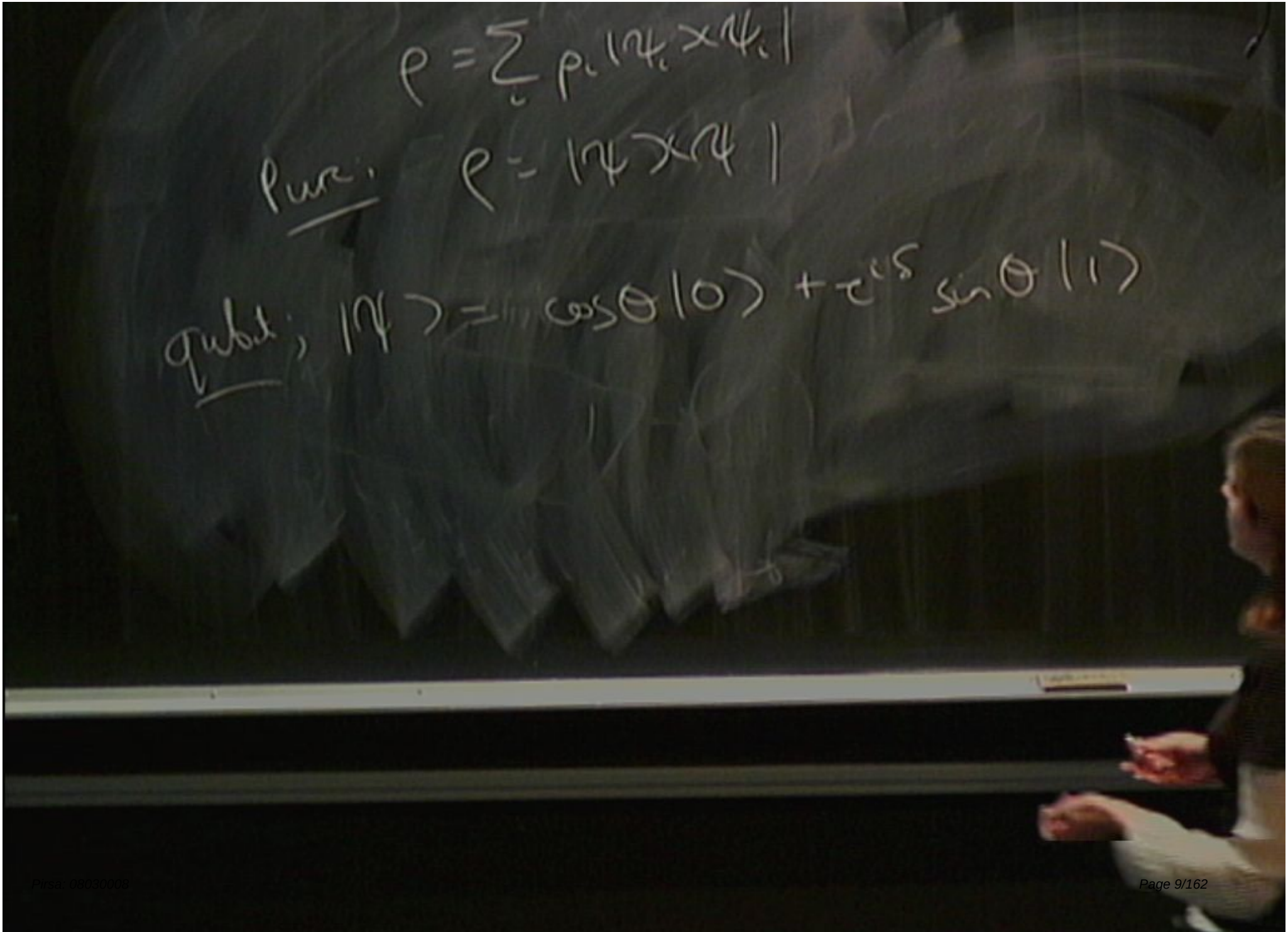
$$= \langle j | \left(\sum_i p_i |\psi_i\rangle\langle\psi_i| \right) |j\rangle$$

$$= \mathrm{Tr}(\rho\, |j\rangle\langle j|)$$

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$


$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$
Pure: $\rho = |\psi\rangle\langle\psi|$

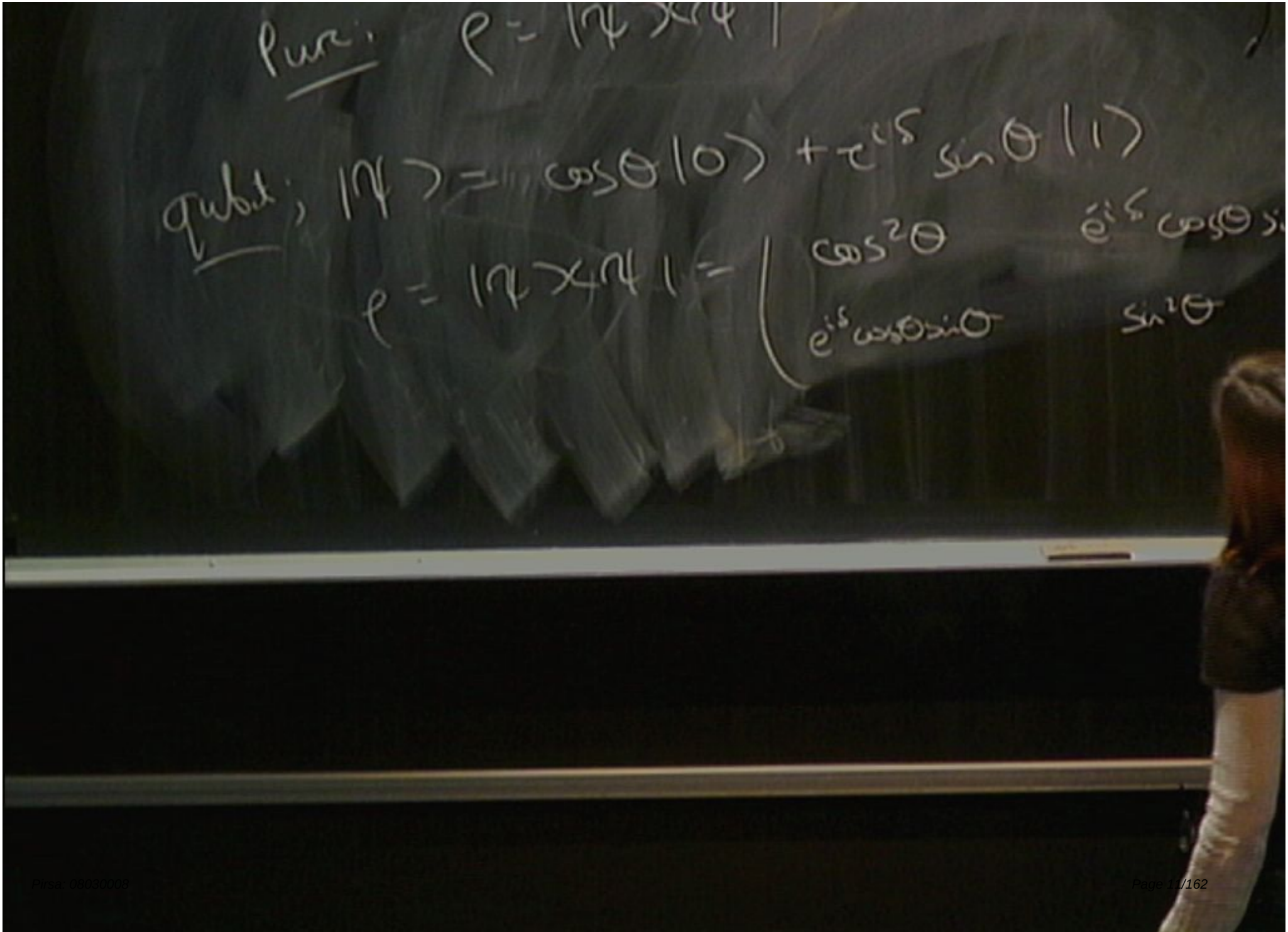

$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$
Pure: $\rho = |\psi\rangle\langle\psi|$
qubit; $|\psi\rangle$


$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$
Pure: $\rho = |\psi\rangle\langle\psi|$
Qubit; $|\psi\rangle = \cos\theta|0\rangle + e^{i\delta}\sin\theta|1\rangle$

Pure: $\rho = |\psi\rangle\langle\psi|$

qubit: $|\psi\rangle = \cos\theta|0\rangle + e^{i\delta}\sin\theta|1\rangle$

$\rho = |\psi\rangle\langle\psi| =$

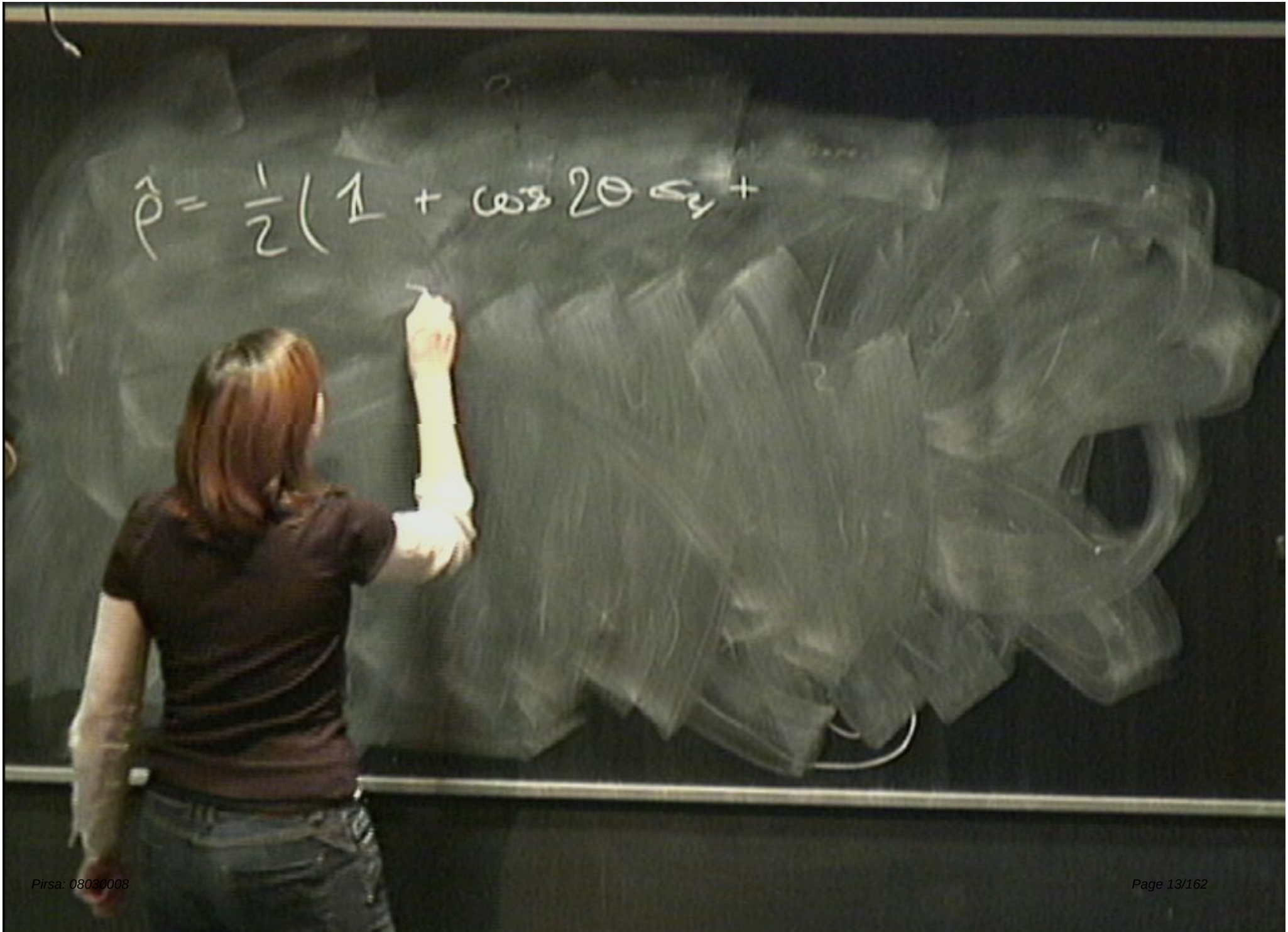

Pure: $\rho = |\psi\rangle\langle\psi|$
qubit; $|\psi\rangle = \cos\theta|0\rangle + e^{i\delta}\sin\theta|1\rangle$
$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \cos^2\theta & e^{i\delta}\cos\theta\sin \\ e^{i\delta}\cos\theta\sin\theta & \sin^2\theta \end{pmatrix}$

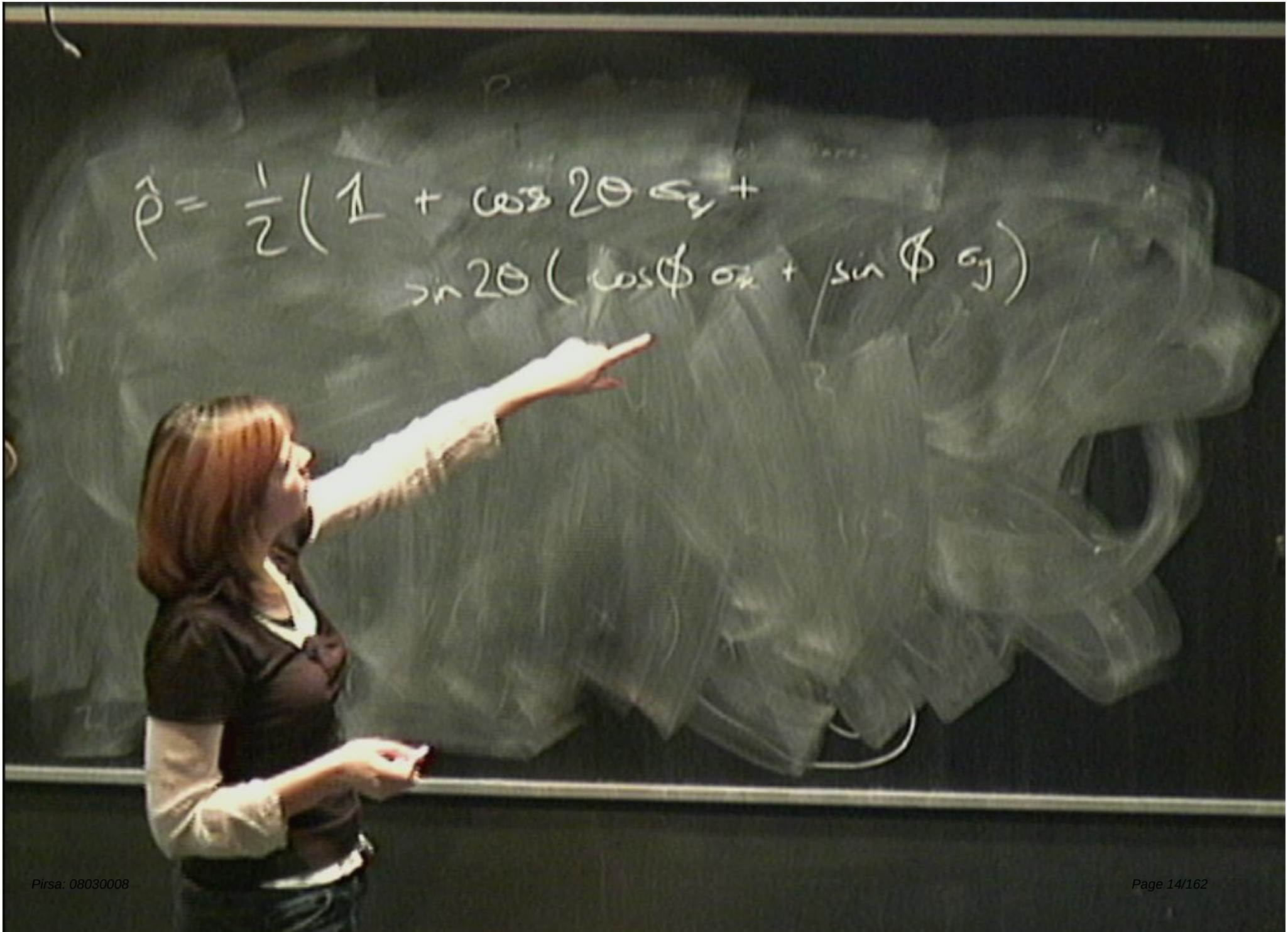
$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

Pure: $\rho = |\psi\rangle\langle\psi|$

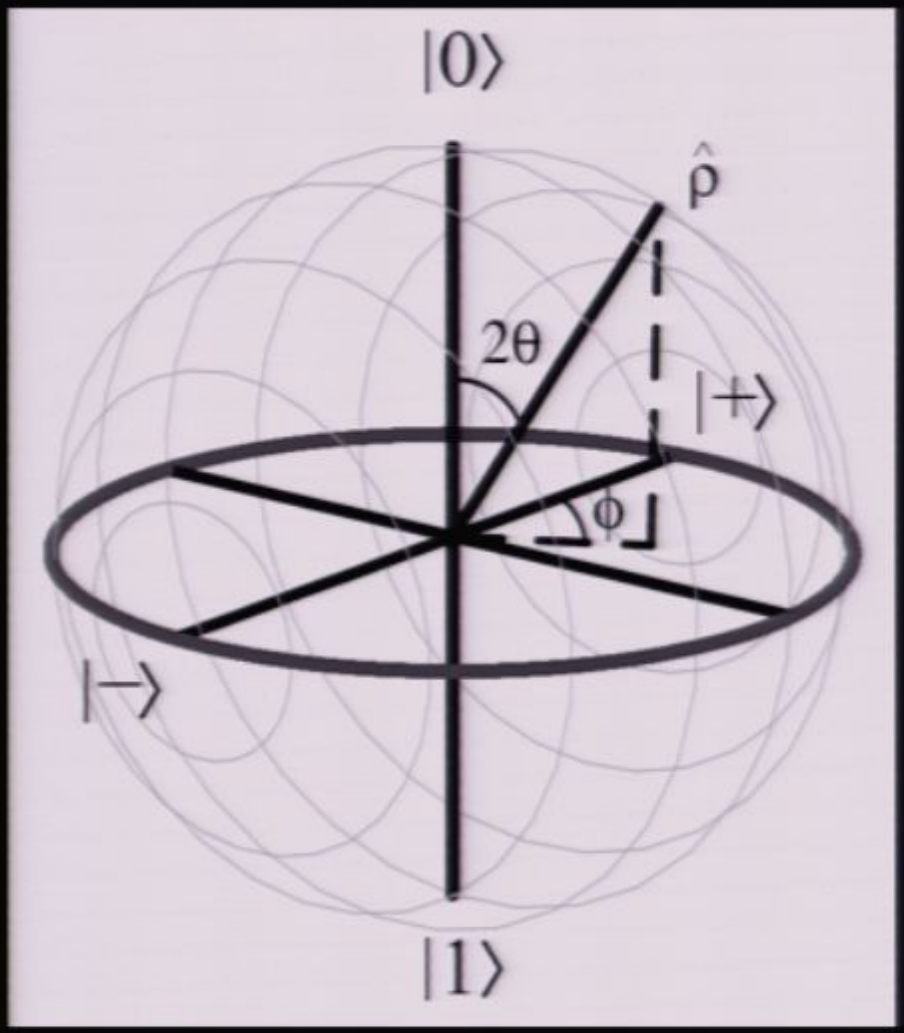
qubit; $|\psi\rangle = \cos\theta|0\rangle + e^{i\delta}\sin\theta|1\rangle$

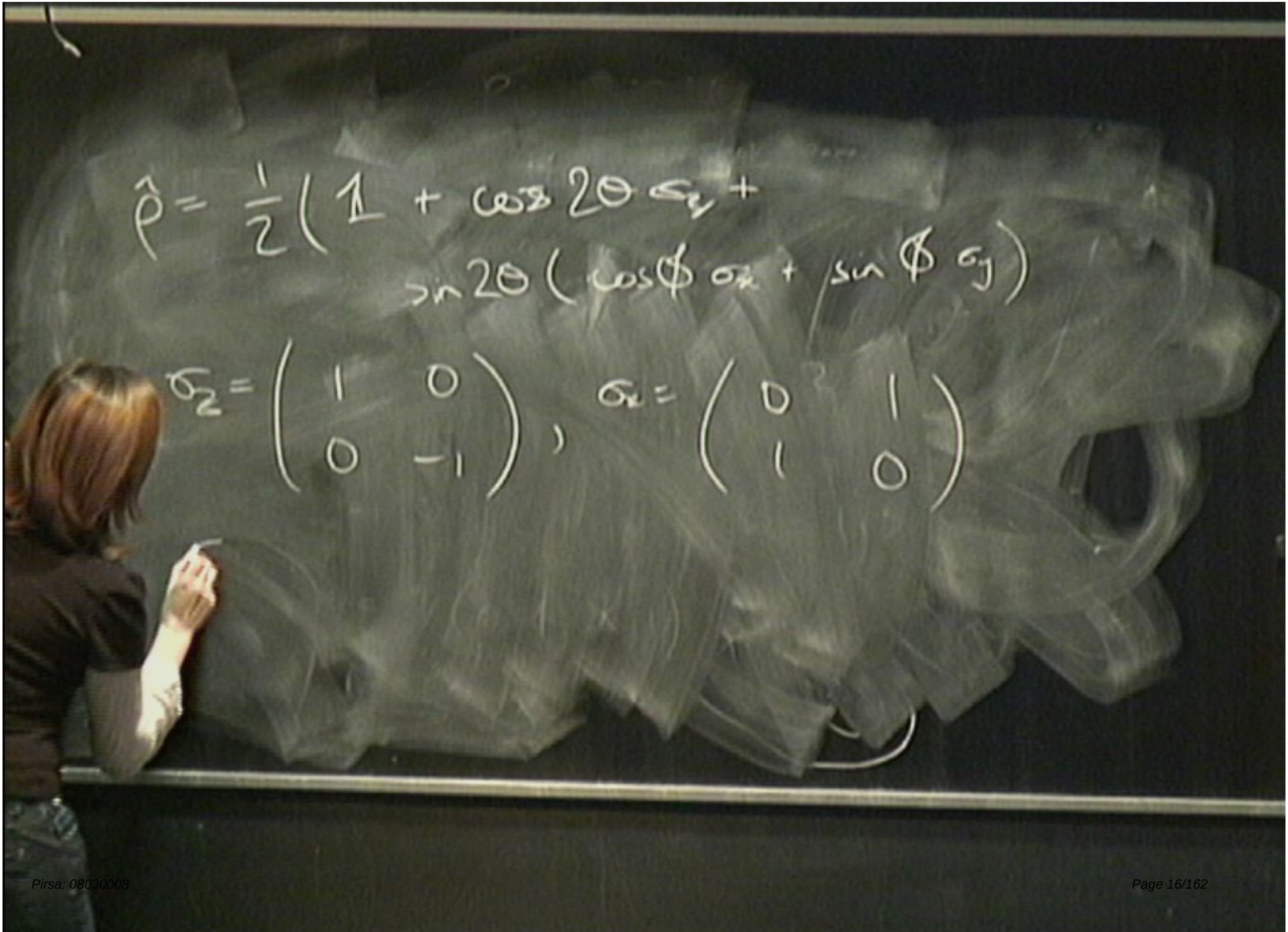
$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \cos^2\theta & e^{i\delta}\cos\theta\sin\theta \\ e^{i\delta}\cos\theta\sin\theta & \sin^2\theta \end{pmatrix}$$


$\hat{\rho} = \frac{1}{2}(1 + \cos 2\theta \sigma_z +$


$\hat{\rho} = \frac{1}{2}(1 + \cos 2\theta\, \sigma_z +$
$\sin 2\theta\,(\cos\phi\, \sigma_x + \sin\phi\, \sigma_y)$

Density operators and the Bloch sphere representation of states.




$\hat{\rho} = \frac{1}{2}(1 + \cos 2\theta\, \sigma_z +$
$\sin 2\theta\,(\cos\phi\, \sigma_x + \sin\phi\, \sigma_y)$
$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$$\hat{\rho} = \frac{1}{2}\left(1 + \cos 2\theta\, \sigma_z + \sin 2\theta\,(\cos\phi\, \sigma_x + \sin\phi\, \sigma_y)\right.$$

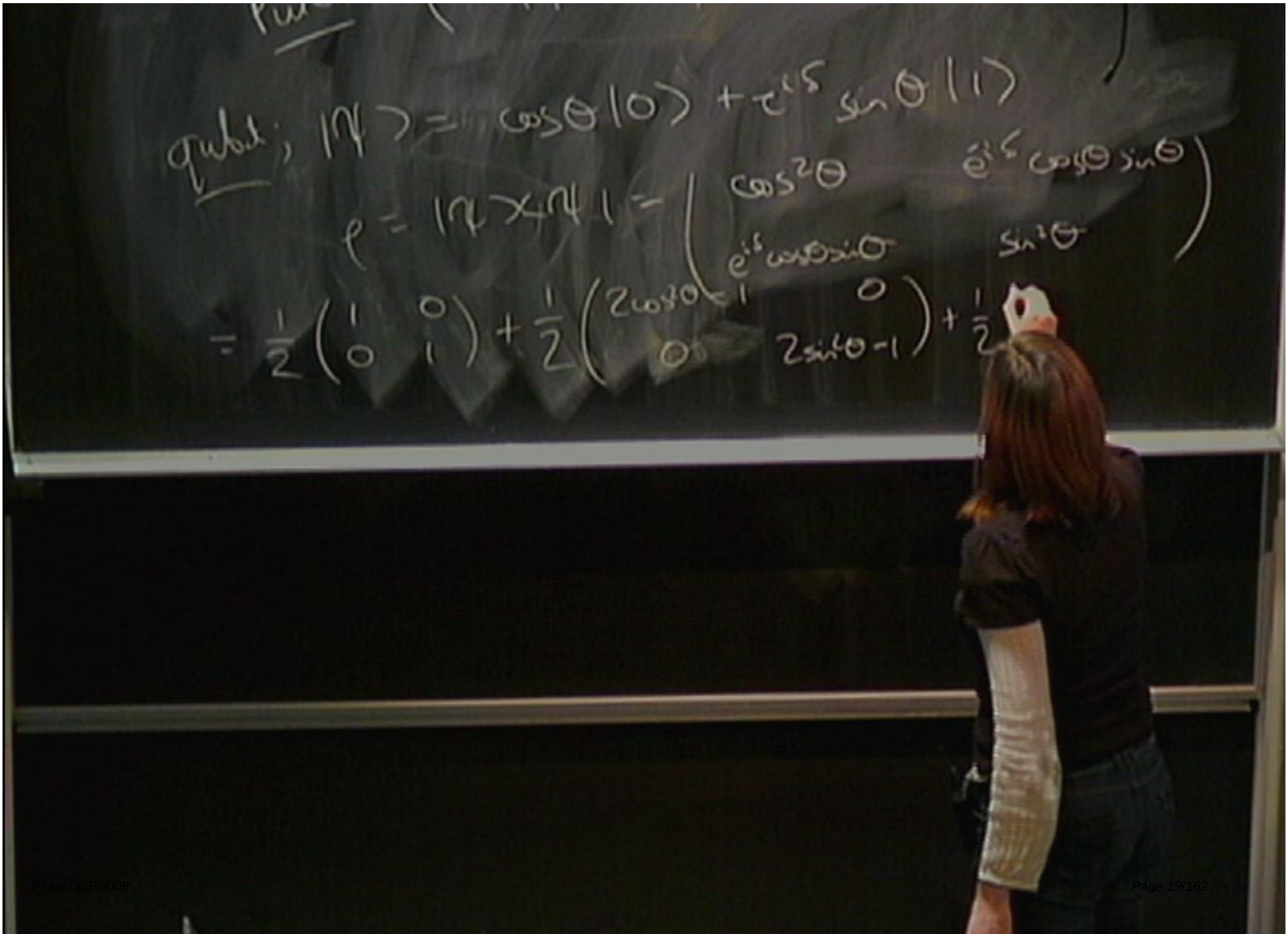
$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\hat{\rho} = \frac{1}{2}\left(1 + \cos 2\theta\, \sigma_z + \sin 2\theta\left(\cos\phi\, \sigma_x + \sin\phi\, \sigma_y\right)\right.$$

$$Z = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad X = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$


qubit; $|\psi\rangle = \cos\theta|0\rangle + e^{i\delta}\sin\theta|1\rangle$
$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \cos^2\theta & e^{i\delta}\cos\theta\sin\theta \\ e^{i\delta}\cos\theta\sin\theta & \sin^2\theta \end{pmatrix}$
$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 2\cos^2\theta - 1 & 0 \\ 0 & 2\sin^2\theta - 1 \end{pmatrix} + \frac{1}{2}$

Pure

qubit; $|\psi\rangle = \cos\theta|0\rangle + e^{i\delta}\sin\theta|1\rangle$

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \cos^2\theta & e^{i\delta}\cos\theta\sin\theta \\ e^{i\delta}\cos\theta\sin\theta & \sin^2\theta \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 2\cos^2\theta - 1 & 0 \\ 0 & 2\sin^2\theta - 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & e^{-i\delta}\sin 2\theta \\ e^{i\delta}\sin 2\theta & 0 \end{pmatrix}$$

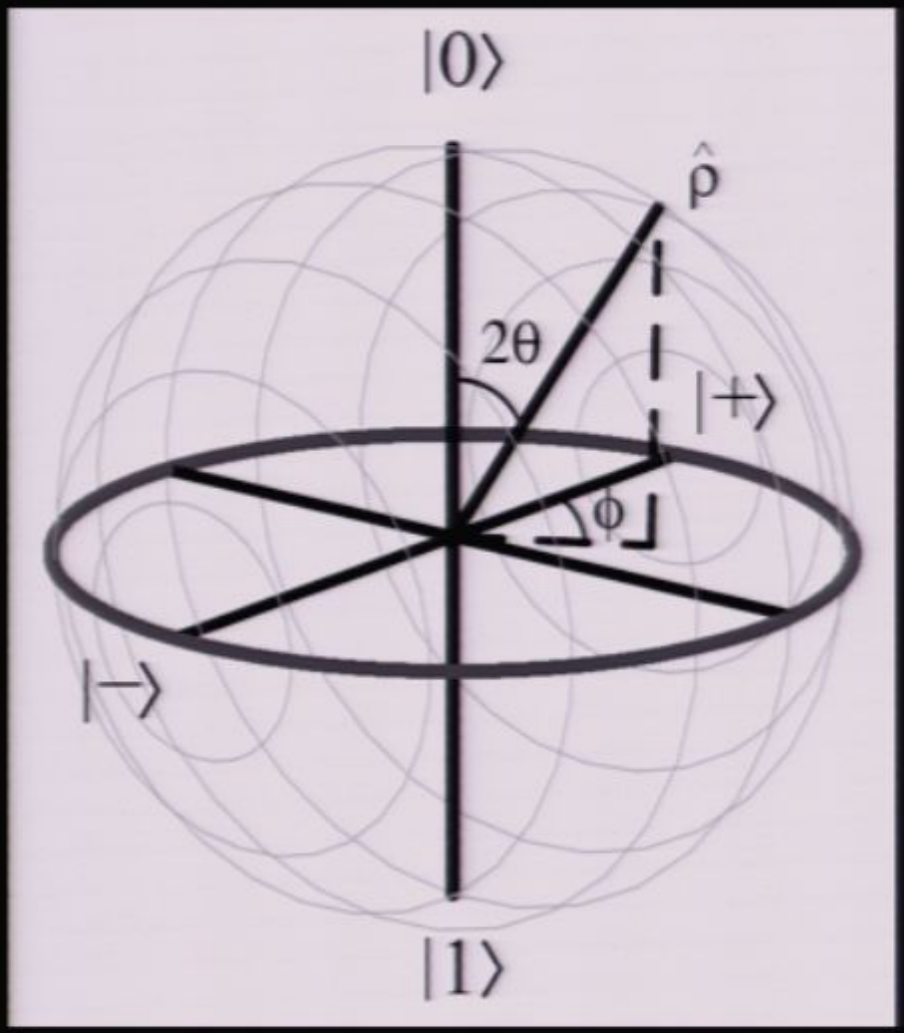
Pure

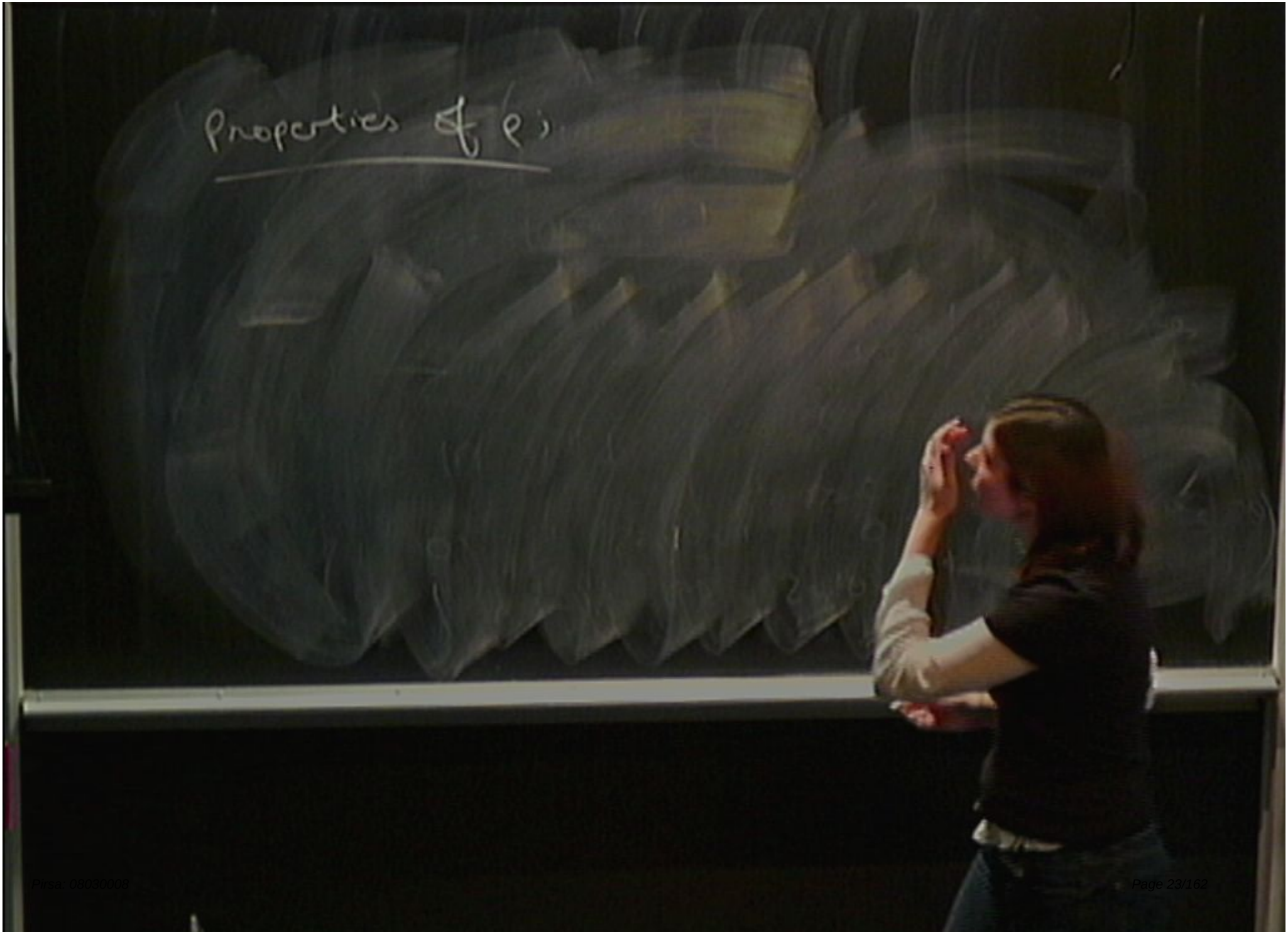
qubit; $|\eta\rangle = \cos\theta|0\rangle + e^{i\delta}\sin\theta|1\rangle$

$$\rho = |\eta\rangle\langle\eta| = \begin{pmatrix} \cos^2\theta & e^{i\delta}\cos\theta\sin\theta \\ e^{i\delta}\cos\theta\sin\theta & \sin^2\theta \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 2\cos^2\theta - 1 & 0 \\ 0 & 2\sin^2\theta - 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & e^{-i\delta}\sin 2\theta \\ e^{i\delta}\sin 2\theta & 0 \end{pmatrix}$$

Density operators and the Bloch sphere representation of states.

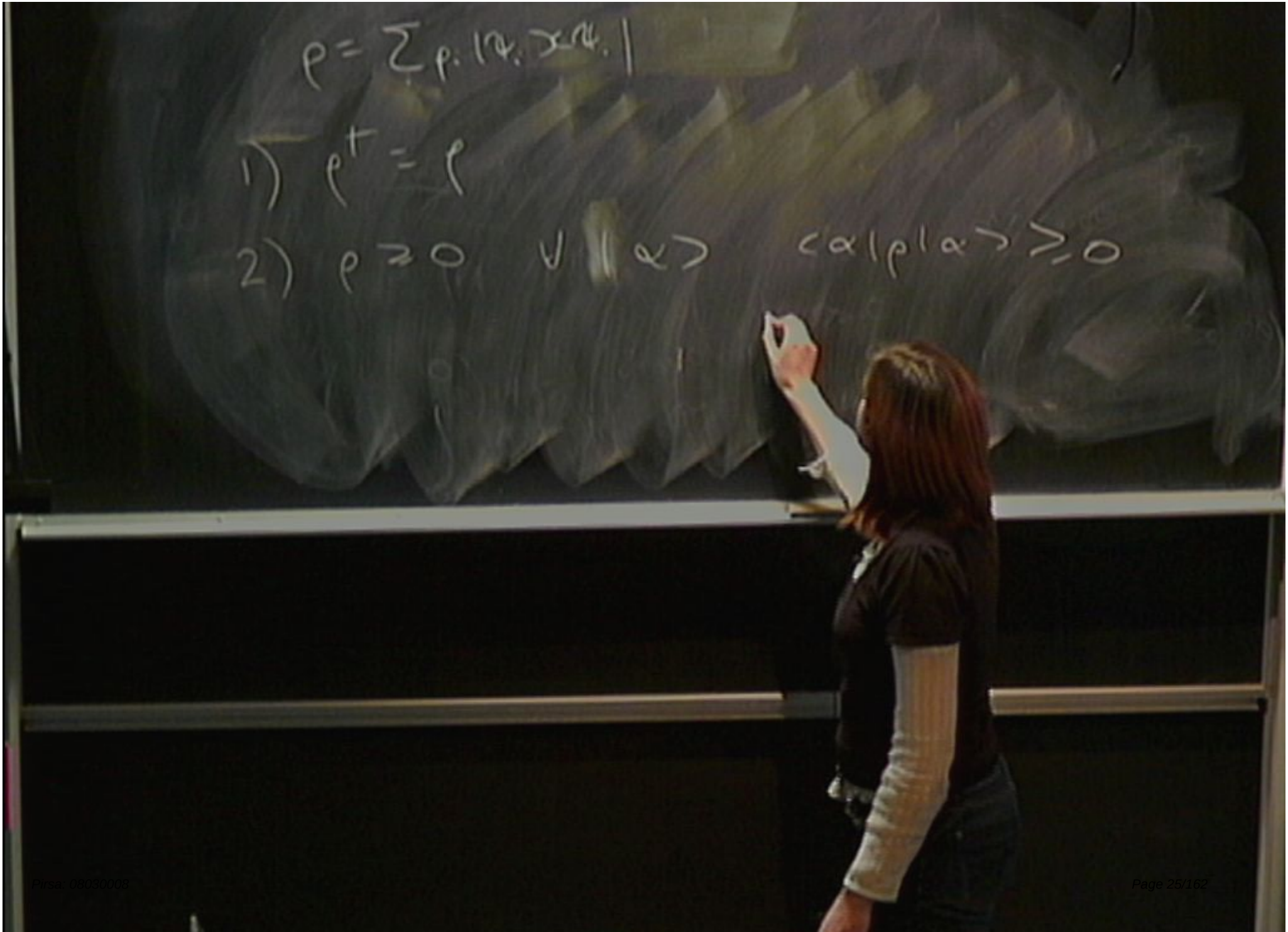


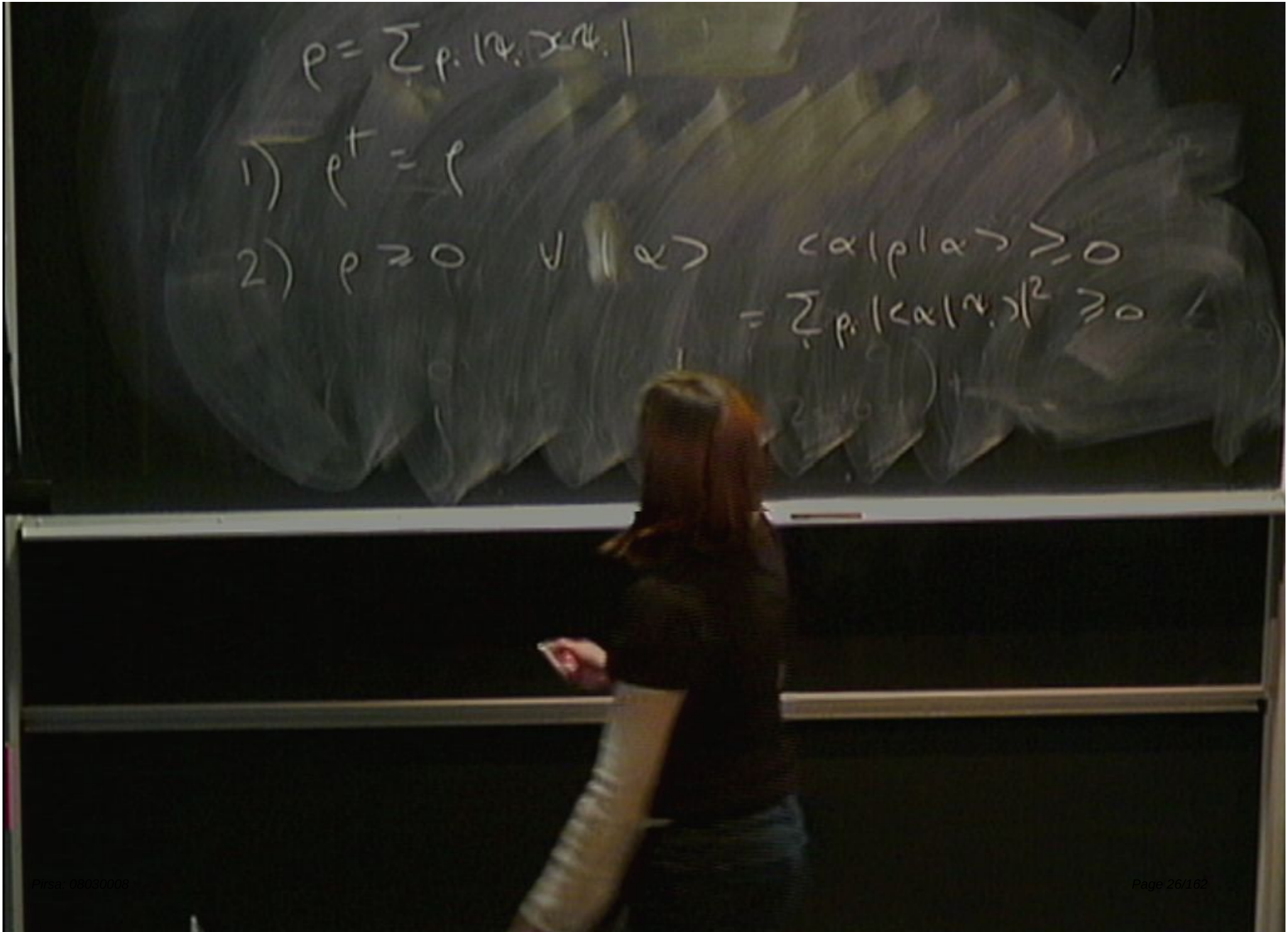

Properties of ρ

Properties of ρ:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

1) $\rho^\dagger = \rho$


$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$
1) $\rho^\dagger = \rho$
2) $\rho \geq 0 \quad \forall\, |\alpha\rangle \quad \langle\alpha|\rho|\alpha\rangle \geq 0$


$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$
1) $\rho^\dagger = \rho$
2) $\rho \geq 0$ $\forall\, |\alpha\rangle$ $\langle\alpha|\rho|\alpha\rangle \geq 0$
$= \sum_i p_i |\langle\alpha|\psi_i\rangle|^2 \geq 0$

1) $\rho^\dagger = \rho$

2) $\rho \geq 0 \quad \forall\, |\alpha\rangle \qquad \langle\alpha|\rho|\alpha\rangle \geq 0$

$= \sum_i p_i |\langle\alpha|\alpha_i\rangle|^2 \geq 0$

3) $\mathrm{Tr}(\rho) = 1 \qquad \mathrm{Tr}(\rho) = \sum_i p_i \langle\alpha_i|\alpha_i\rangle = \sum_i p_i = 1$

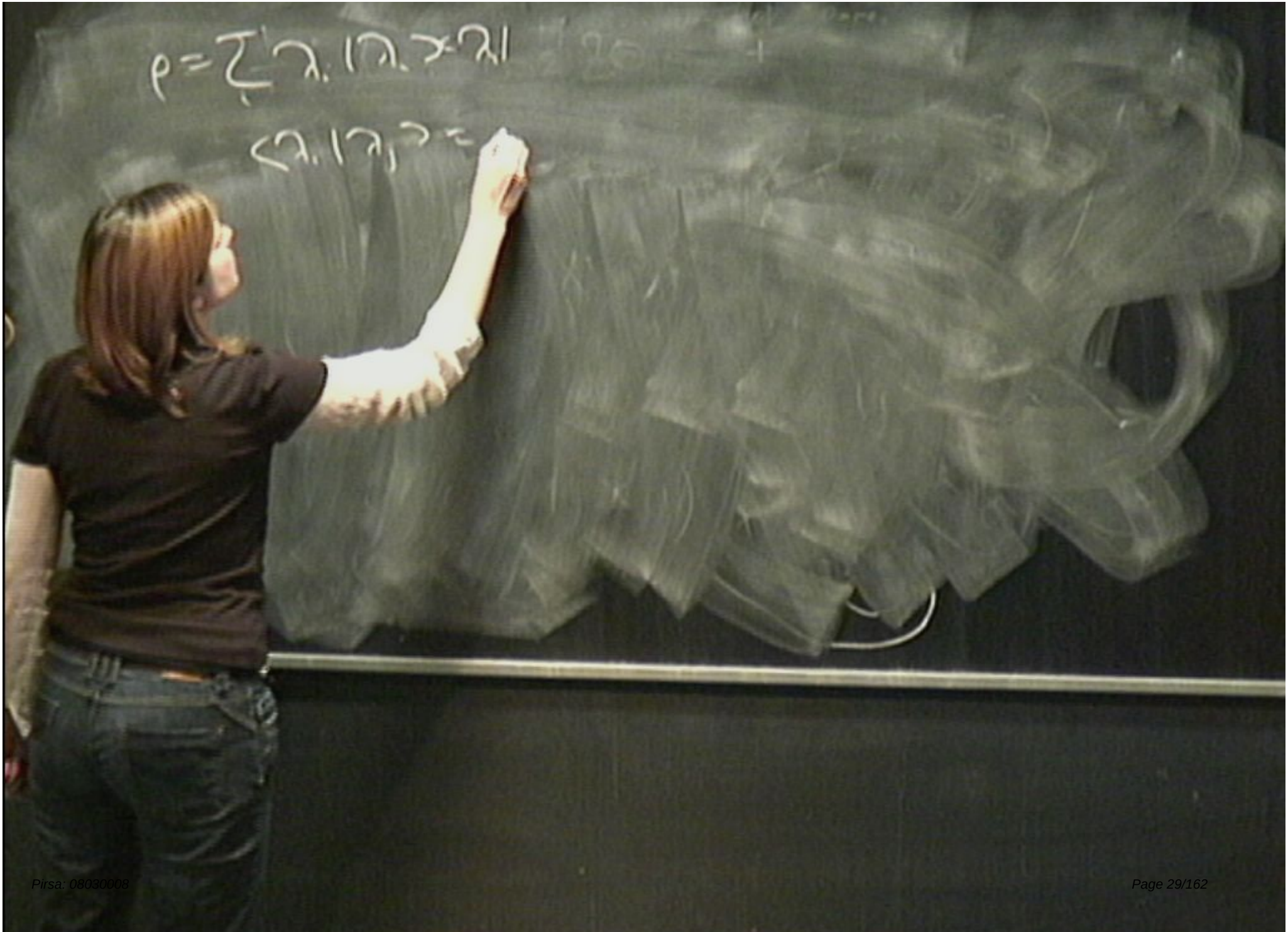
$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

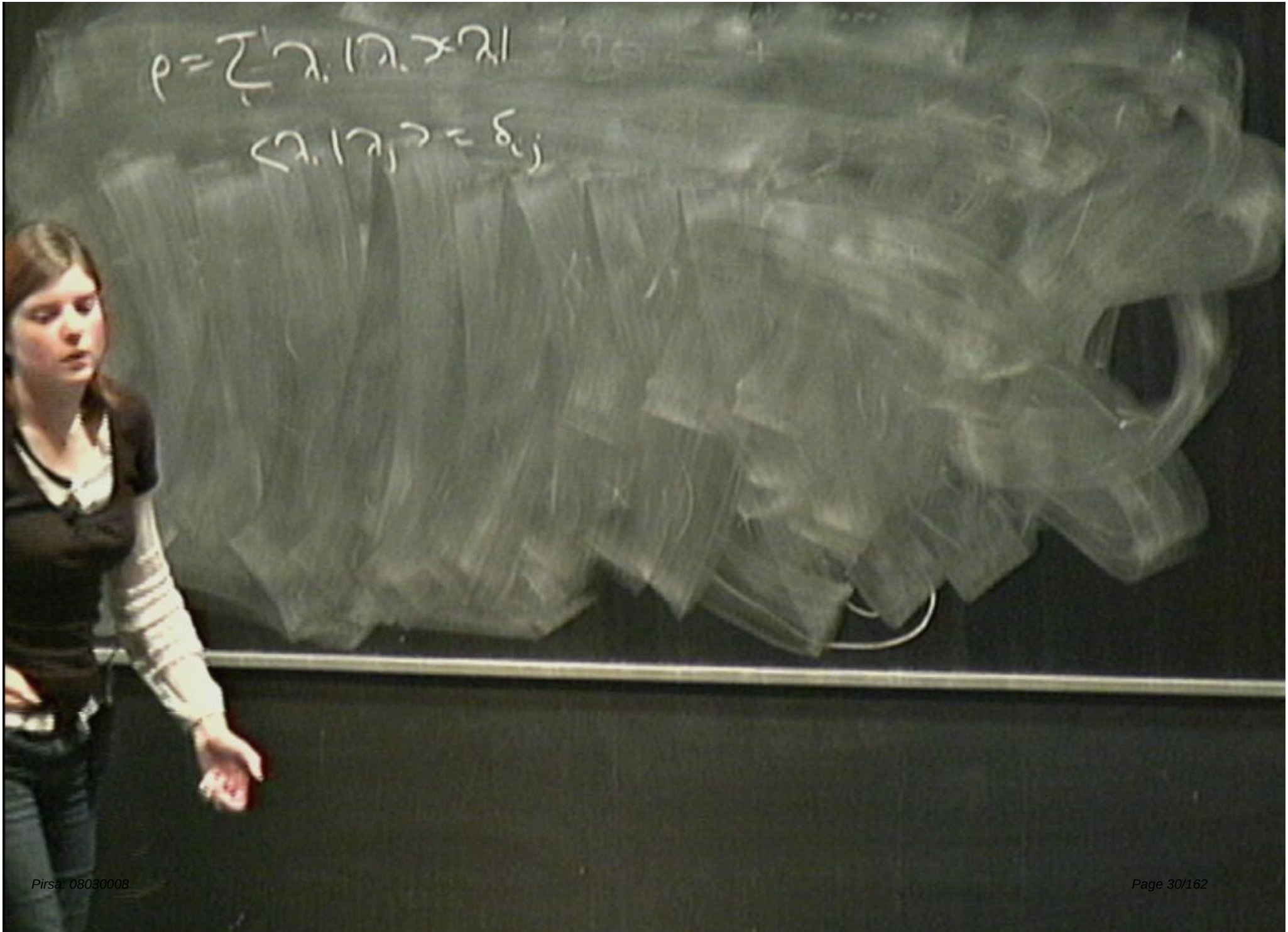
1) $\rho^\dagger = \rho$

2) $\rho \geq 0 \quad \forall\, |\alpha\rangle \qquad \langle\alpha|\rho|\alpha\rangle \geq 0$

$= \sum_i p_i |\langle\alpha|\psi_i\rangle|^2 \geq 0$

3) $\mathrm{Tr}(\rho) = 1 \qquad \mathrm{Tr}(\rho) = \sum_i p_i \langle\psi_i|\psi_i\rangle = \sum_i p_i = 1$




ρ = Σ λ_n |n⟩⟨n|
⟨n|n_j⟩ = δ_ij

$$\rho = \sum_i \lambda_i |\eta_i\rangle\langle\eta_i|$$

$$\langle\eta_i|\eta_j\rangle = \delta_{ij}$$

$$\rho = p_0 |\psi_0\rangle\langle\psi_0| + p_1 |\psi_0^\perp\rangle\langle\psi_0^\perp|$$

$$\rho = \sum_i \lambda_i |\eta_i\rangle\langle\eta_i|$$

$$\langle\eta_i|\eta_j\rangle = \delta_{ij}$$

$$\rho = \rho_0 |\psi_0\rangle\langle\psi_0| + \rho_1 |\psi_0^\perp\rangle\langle\psi_0^\perp|$$

$$|\psi_0\rangle = \cos\theta|0\rangle + e^{i\delta}\sin\theta|1\rangle$$

$$\rho = \sum_i \lambda_i |\eta_i\rangle\langle\eta_i|$$

$$\langle\eta_i|\eta_j\rangle = \delta_{ij}$$

$$\rho = p_0 |\psi_0\rangle\langle\psi_0| + p_1 |\psi_0^\perp\rangle\langle\psi_0^\perp|$$

$$|\psi_0\rangle = \cos\theta |0\rangle + e^{i\delta} \sin\theta |1\rangle$$

$$|\psi_1\rangle = -\sin\theta |0\rangle + e^{i\delta} \cos\theta |1\rangle$$

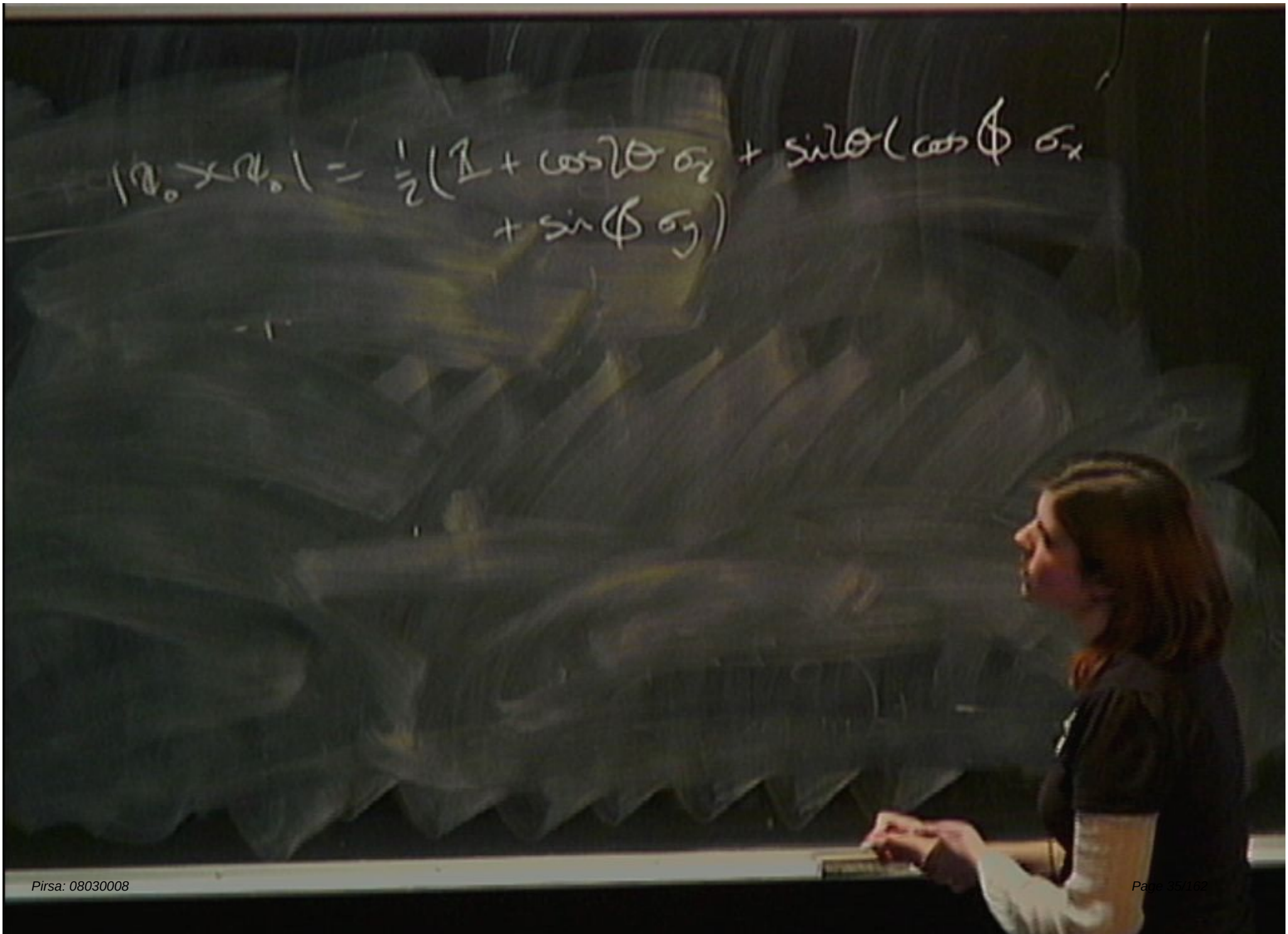
$$\rho = \sum_i \lambda_i |\eta_i\rangle\langle\eta_i|$$

$$\langle\eta_i|\eta_j\rangle = \delta_{ij}$$

$$\rho = p_0 |\psi_0\rangle\langle\psi_0| + p_1 |\psi_0^\perp\rangle\langle\psi_0^\perp|$$

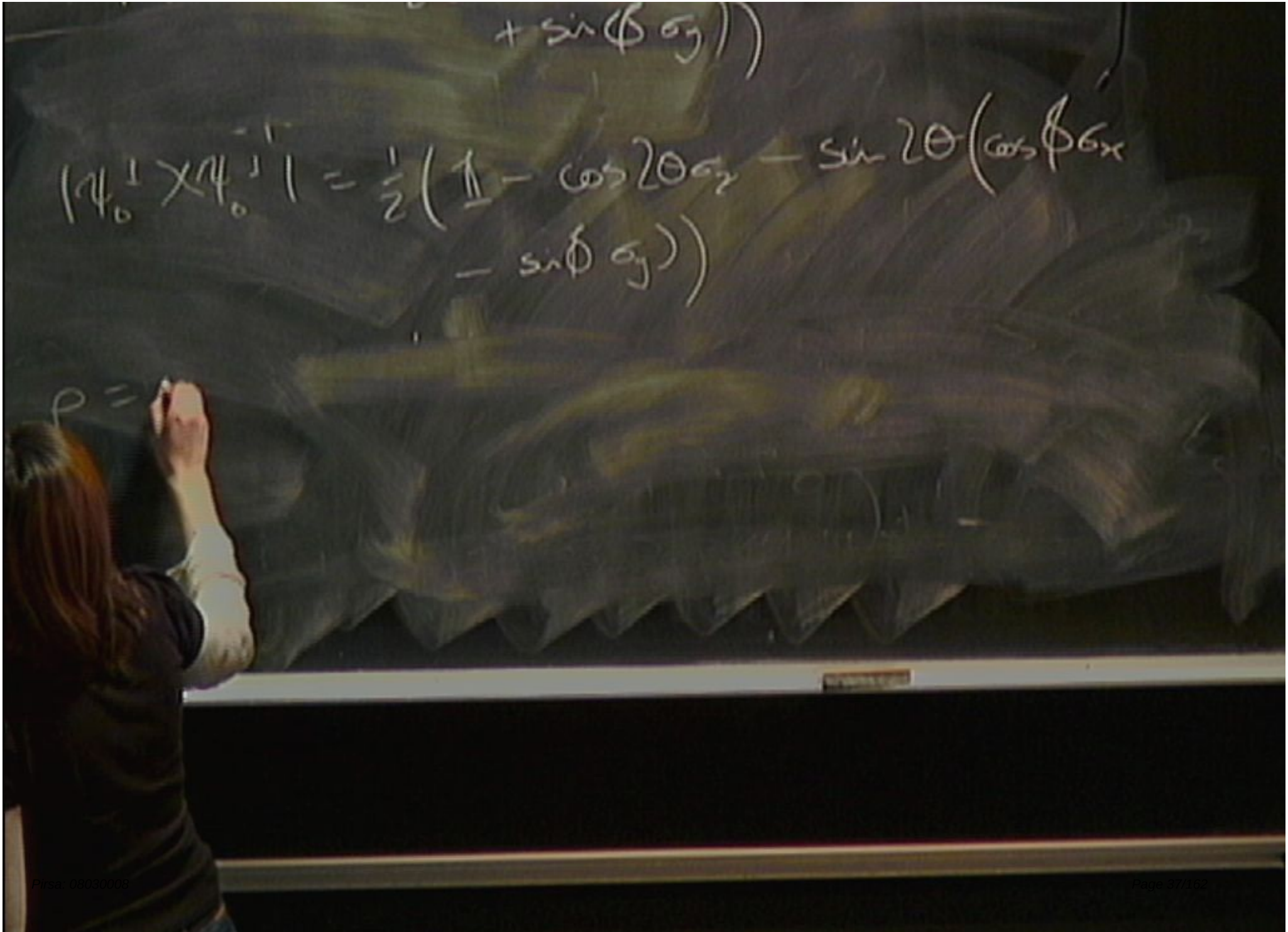
$$|\psi_0\rangle = \cos\theta\,|0\rangle + e^{i\delta}\sin\theta\,|1\rangle$$

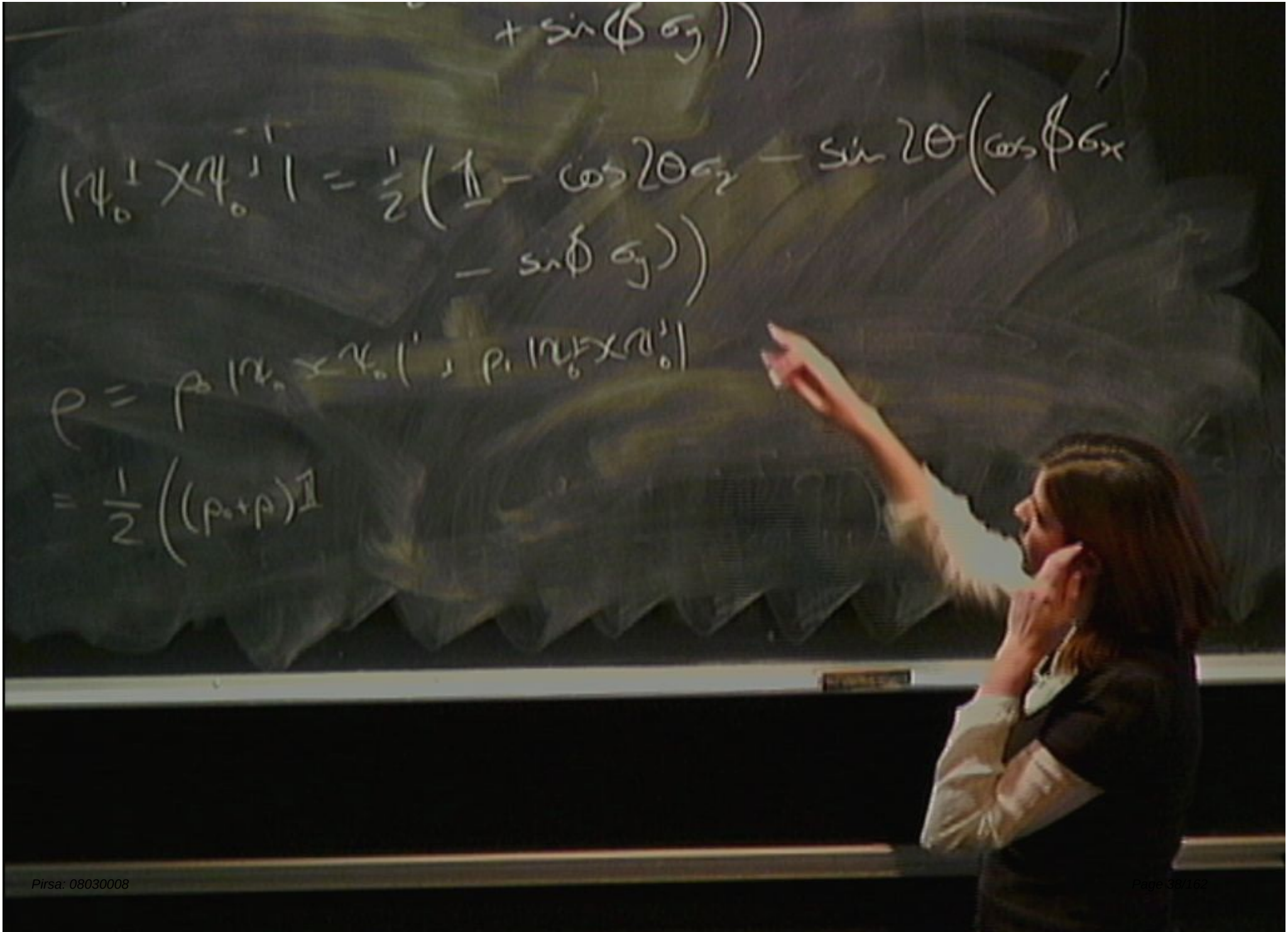
$$|\psi_0^\perp\rangle = -\sin\theta\,|0\rangle + e^{i\delta}\cos\theta\,|1\rangle$$


$|\psi_0\rangle\langle\psi_0| = \frac{1}{2}(\mathbb{1} + \cos 2\theta\, \sigma_z + \sin 2\theta(\cos\phi\, \sigma_x + \sin\phi\, \sigma_y))$

$$|\psi_0\rangle\langle\psi_0| = \frac{1}{2}(\mathbb{1} + \cos 2\theta\,\sigma_z + \sin 2\theta(\cos\phi\,\sigma_x + \sin\phi\,\sigma_y))$$

$$|\psi_0^\perp\rangle\langle\psi_0^\perp| = \frac{1}{2}(\mathbb{1} - \cos 2\theta\,\sigma_z - \sin 2\theta(\cos\phi\,\sigma_x - \sin\phi\,\sigma_y))$$


+ sin(φ σ_y))
|4_0^1 × 4_0^1| = 1/2 (1 − cos 2θ σ_z − sin 2θ (cos φ σ_x
− sin φ σ_y))
ρ =


+ sin(φ σ_y))
|η_0^1 × η_0^1| = 1/2 (1 − cos 2θ σ_z − sin 2θ (cos φ σ_x
− sin φ σ_y))
ρ = ρ_0 |η_0 × η_0| + ρ_1 |η_0^⊥ × η_0^⊥|
= 1/2 ((ρ_0 + ρ_1) I

$$|\psi_0\rangle\langle\psi_0| = \frac{1}{2}\left(\mathbb{1} + \cos 2\theta\,\sigma_z + \sin 2\theta\left(\cos\phi\,\sigma_x + \sin\phi\,\sigma_y\right)\right)$$

$$|\psi_0^\perp\rangle\langle\psi_0^\perp| = \frac{1}{2}\left(\mathbb{1} - \cos 2\theta\,\sigma_z - \sin 2\theta\left(\cos\phi\,\sigma_x - \sin\phi\,\sigma_y\right)\right)$$

$$\rho = p_0\,|\psi_0\rangle\langle\psi_0| + p_1\,|\psi_0^\perp\rangle\langle\psi_0^\perp|$$

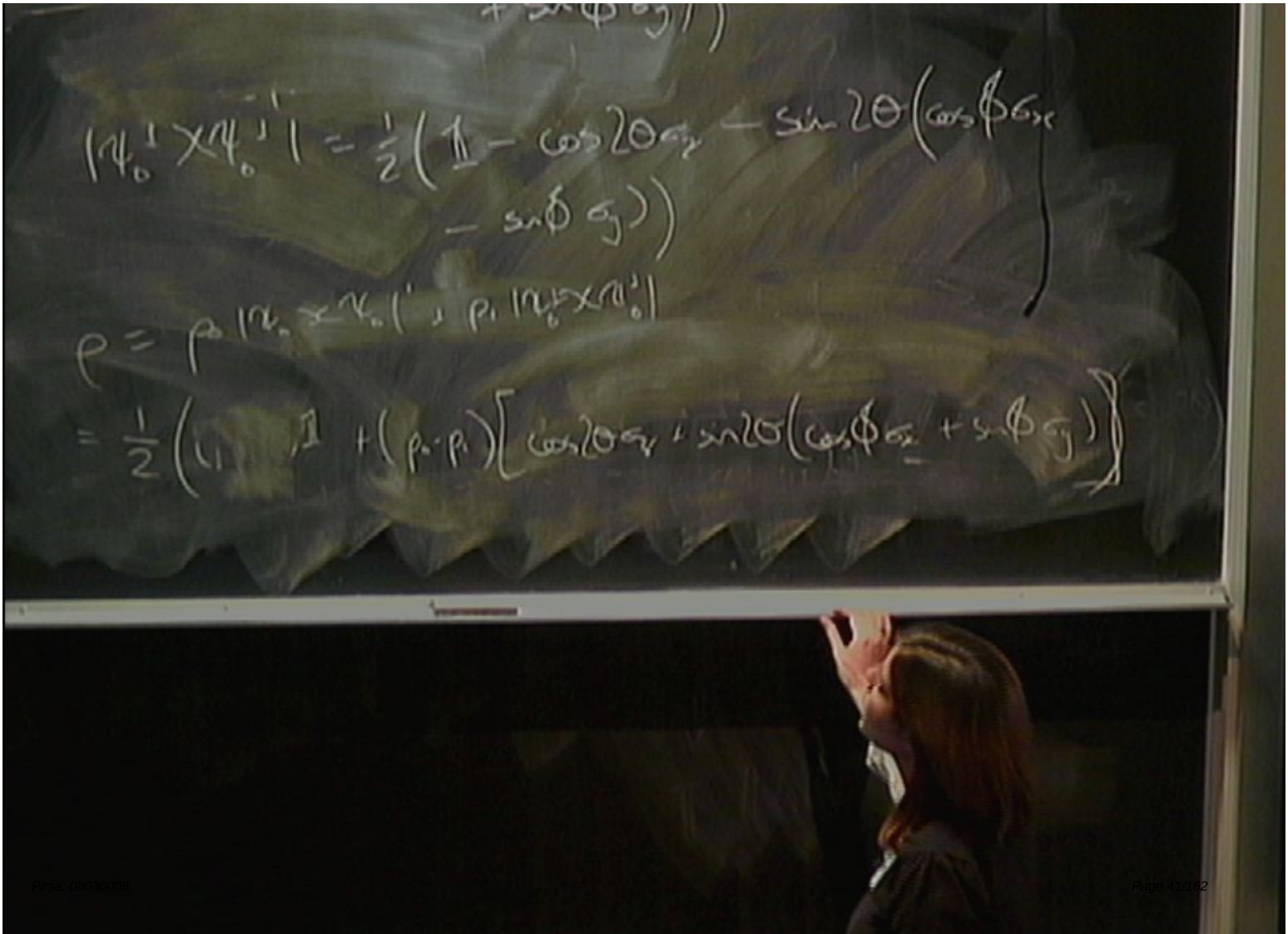
$$= \frac{1}{2}\left((p_0+p_1)\mathbb{1} + (p_0-p_1)\left[\cos 2\theta\,\sigma_z + \sin 2\theta\left(\cos\phi\,\sigma_x + \sin\right.\right.\right.$$

$$|\psi_0\rangle\langle\psi_0| = \frac{1}{2}\left(\mathbb{1} + \cos 2\theta\,\sigma_z + \sin 2\theta\left(\cos\phi\,\sigma_x + \sin\phi\,\sigma_y\right)\right)$$

$$|\psi_0^\perp\rangle\langle\psi_0^\perp| = \frac{1}{2}\left(\mathbb{1} - \cos 2\theta\,\sigma_z - \sin 2\theta\left(\cos\phi\,\sigma_x - \sin\phi\,\sigma_y\right)\right)$$

$$\rho = p_0\,|\psi_0\rangle\langle\psi_0| + p_1\,|\psi_0^\perp\rangle\langle\psi_0^\perp|$$

$$= \frac{1}{2}\left((p_0+p_1)\mathbb{1} + (p_0-p_1)\left[\cos 2\theta\,\sigma_z + \sin 2\theta\left(\cos\phi\,\sigma_x + \sin\phi\,\sigma_y\right)\right]\right)$$


$|\vec{n}_0^1 \times \vec{n}_0^2| = \frac{1}{2}(1 - \cos 2\theta_{\vec{n}} - \sin 2\theta(\cos\phi_{\vec{n}} - \sin\phi_{\vec{n}}))$
$\rho = \rho_0 |\vec{n}_0 \times \vec{n}_0| + \rho_1 |\vec{n}_0^1 \times \vec{n}_0^2|$
$= \frac{1}{2}\left(1 + (\rho_0 \cdot \rho_1)\left[\cos 2\theta_{\vec{n}} + \sin 2\theta(\cos\phi_{\vec{n}} + \sin\phi_{\vec{n}})\right]\right)$

$$|\psi_0\rangle\langle\psi_0| = \frac{1}{2}\left(\mathbb{1} + \cos 2\theta\,\sigma_z + \sin 2\theta\left(\cos\phi\,\sigma_x + \sin\phi\,\sigma_y\right)\right)$$

$$|\psi_0^\perp\rangle\langle\psi_0^\perp| = \frac{1}{2}\left(\mathbb{1} - \cos 2\theta\,\sigma_z - \sin 2\theta\left(\cos\phi\,\sigma_x - \sin\phi\,\sigma_y\right)\right)$$

$$\rho = p_0\,|\psi_0\rangle\langle\psi_0| + p_1\,|\psi_0^\perp\rangle\langle\psi_0^\perp|$$

$$= \frac{1}{2}\left(\mathbb{1} + (p_0 - p_1)\left[\cos 2\theta\,\sigma_z + \sin 2\theta\left(\cos\phi\,\sigma_x + \sin\phi\,\sigma_y\right)\right]\right)$$

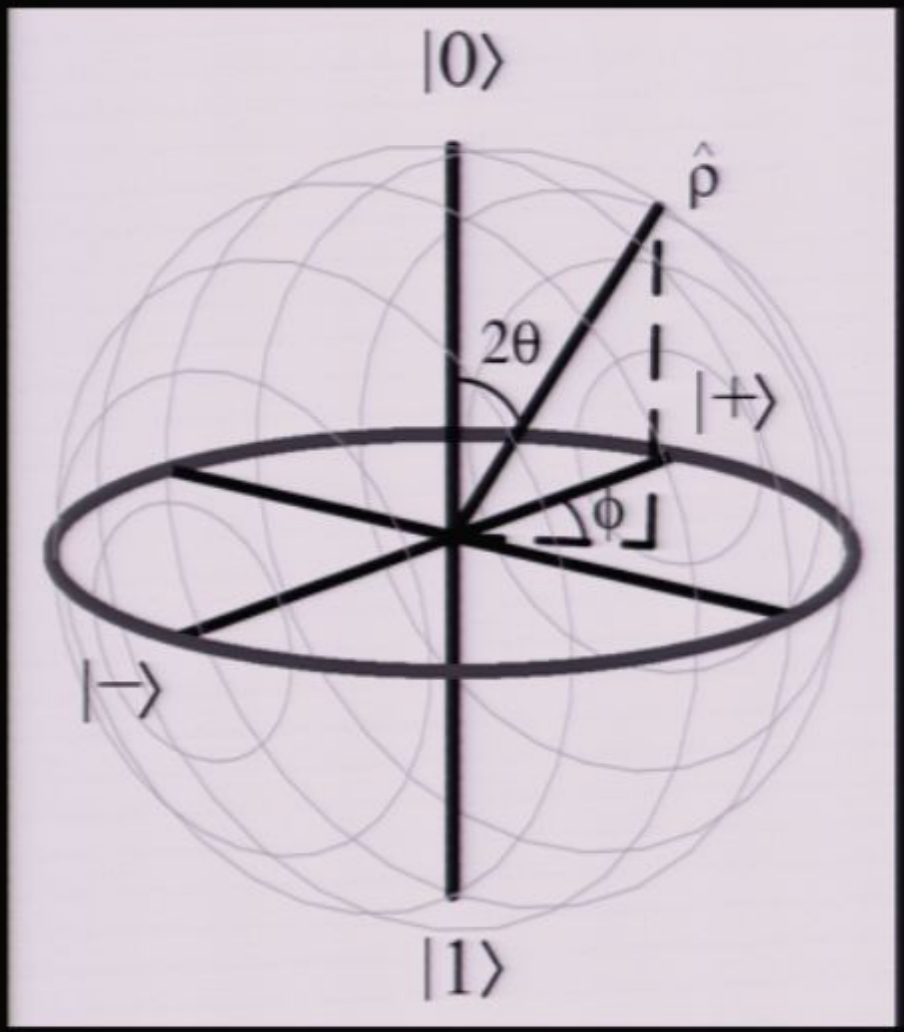
$$|\Psi_0\rangle\langle\Psi_0| = \frac{1}{2}\left(\mathbb{1} + \cos 2\theta\,\sigma_z + \sin 2\theta\left(\cos\phi\,\sigma_x + \sin\phi\,\sigma_y\right)\right)$$

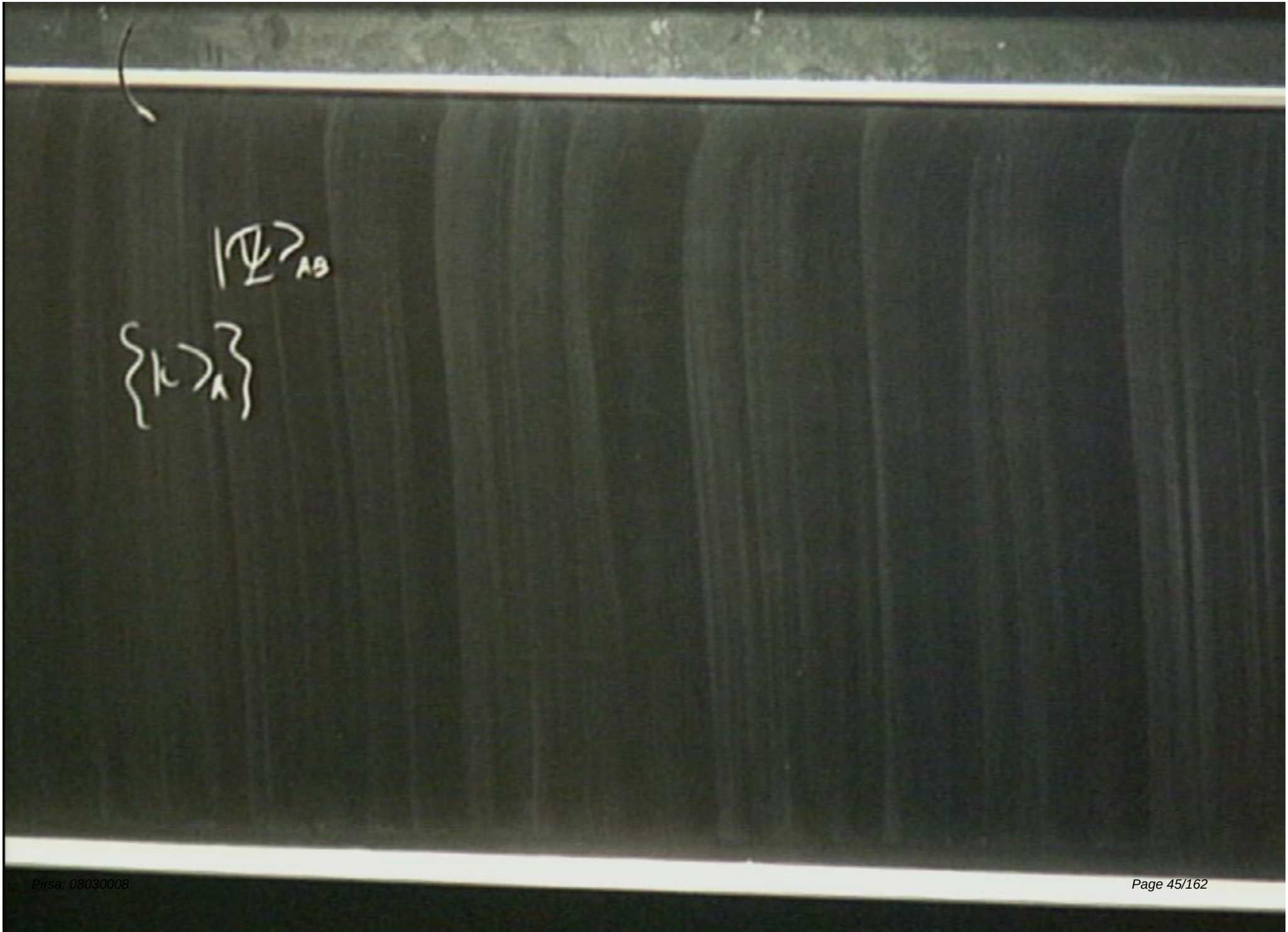
$$|\Psi_0^{\perp}\rangle\langle\Psi_0^{\perp}| = \frac{1}{2}\left(\mathbb{1} - \cos 2\theta\,\sigma_z - \sin 2\theta\left(\cos\phi\,\sigma_x + \sin\phi\,\sigma_y\right)\right)$$

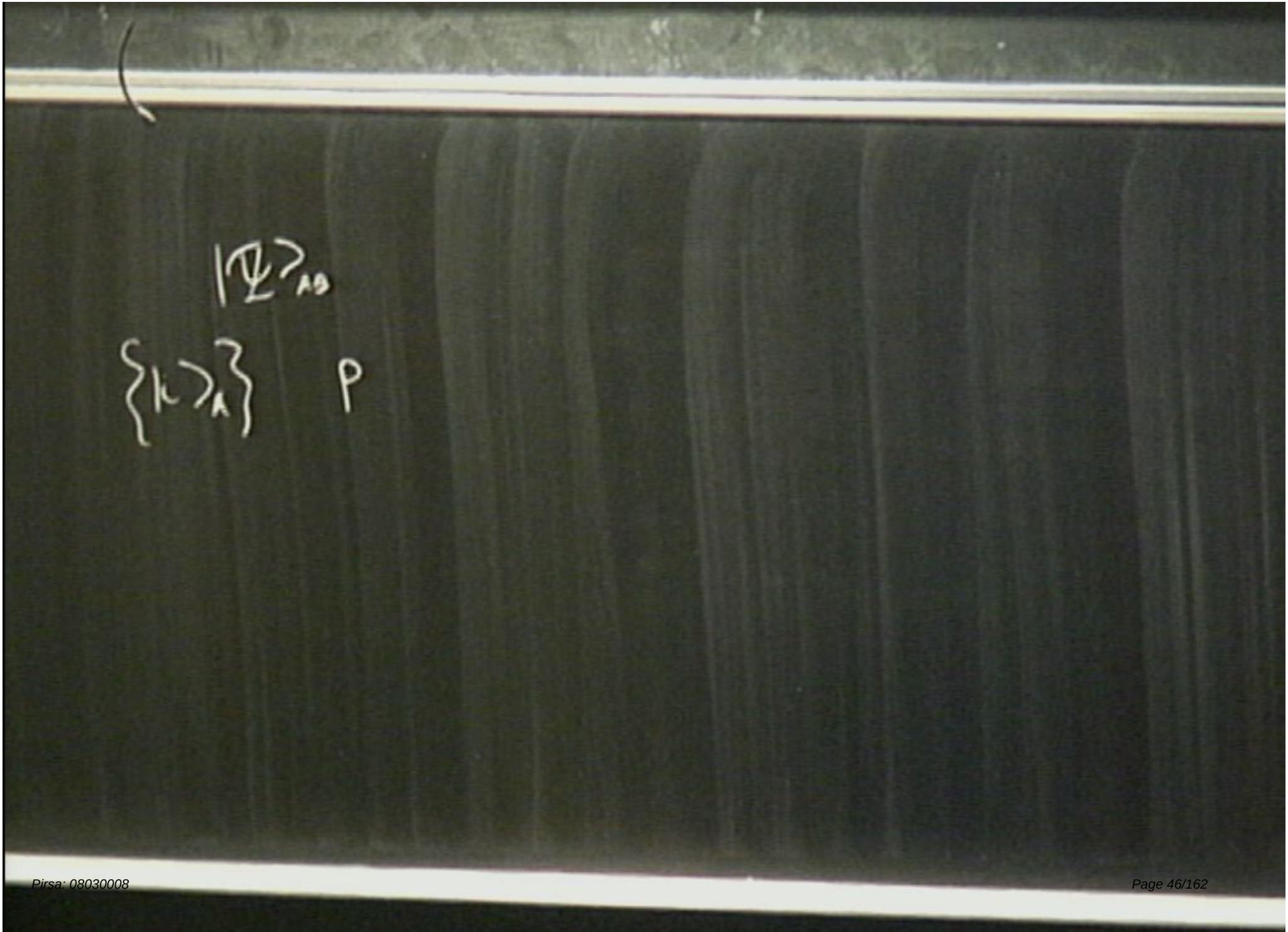
$$\rho = p_0\,|\Psi_0\rangle\langle\Psi_0| + p_1\,|\Psi_0^{\perp}\rangle\langle\Psi_0^{\perp}|$$

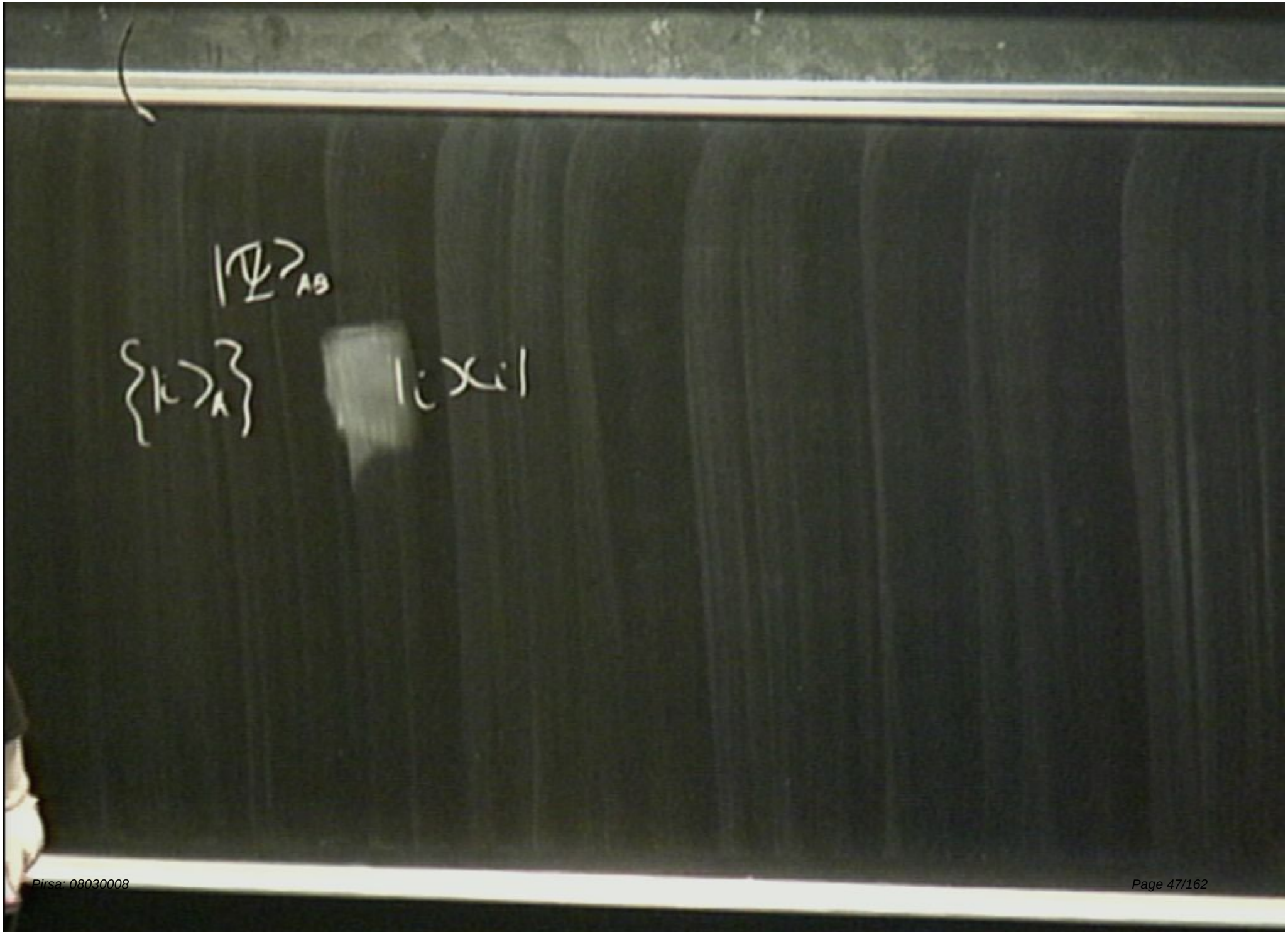
$$= \frac{1}{2}\left(\mathbb{1} + (p_0 - p_1)\left[\cos 2\theta\,\sigma_z + \sin 2\theta\left(\cos\phi\,\sigma_x + \sin\phi\,\sigma_y\right)\right]\right)$$

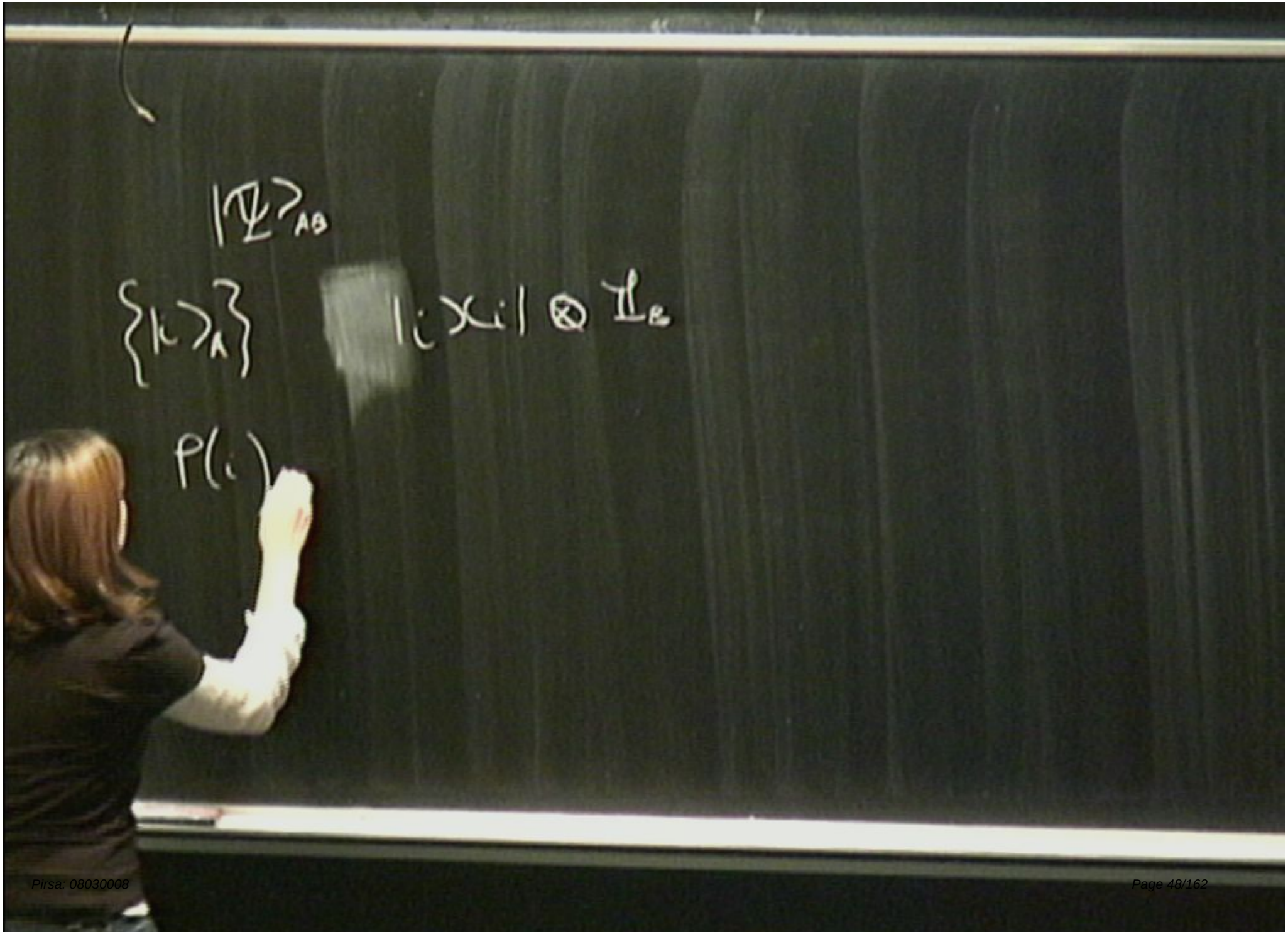
Density operators and the Bloch sphere representation of states.




$|\Psi\rangle_{AB}$
$\{|k\rangle_A\}$


$|\Psi\rangle_{AB}$
$\{|i\rangle_A\}$
P


$|\Psi\rangle_{AB}$
$\{|i\rangle_A\}$
$|i\rangle_A|x_i\rangle$


$|\Psi\rangle_{AB}$
$\{|k\rangle_A\}$
$|i\rangle\langle i| \otimes \mathbb{1}_B$
$p(i)$

$|\Psi\rangle_{AB}$

$\{|i\rangle_A\}$ $|i\rangle\langle i| \otimes \mathbb{I}_B$

$$P(i) = \mathrm{Tr}\left(\left(|\Psi\rangle\langle\Psi| \right) \left(|i\rangle\langle i| \otimes \mathbb{I}_B \right) \right)$$

$|\Psi\rangle_{AB}$

$\{|i\rangle_A\}$ $|i\rangle\langle i| \otimes \mathbb{I}_B$

$$P(i) = Tr\left(\left(|\Psi\rangle\langle\Psi|\right)\left(|i\rangle\langle i| \otimes \mathbb{I}_B\right)\right)$$

$$= Tr_A\left(Tr_B\right.$$

$|\Psi\rangle_{AB}$

$\{|i\rangle_A\}$ $|i\rangle\langle i| \otimes \mathbb{I}_B$

$$P(i) = Tr_{AB}\left(\left(|\Psi\rangle\langle\Psi|\right)\left(|i\rangle\langle i| \otimes \mathbb{I}_B\right)\right)$$

$$= Tr_A\left(Tr_B\left(|\Psi\rangle\langle\Psi|\right)\ |i\rangle\langle i|\right)$$

$|\Psi\rangle_{AB}$

$\{|i\rangle_A\}$ $\quad |i\rangle\langle i| \otimes \mathbb{I}_B$

$$P(i) = Tr_{AB}\left(\left(|\Psi\rangle\langle\Psi| \right) \left(|i\rangle\langle i| \otimes \mathbb{I}_B \right) \right)$$

$$= Tr_A\left(Tr_B\left(|\Psi\rangle\langle\Psi| \right) |i\rangle\langle i| \right)$$

$$\rho_A = Tr_B\left(|\Psi\rangle\langle\Psi| \right)$$

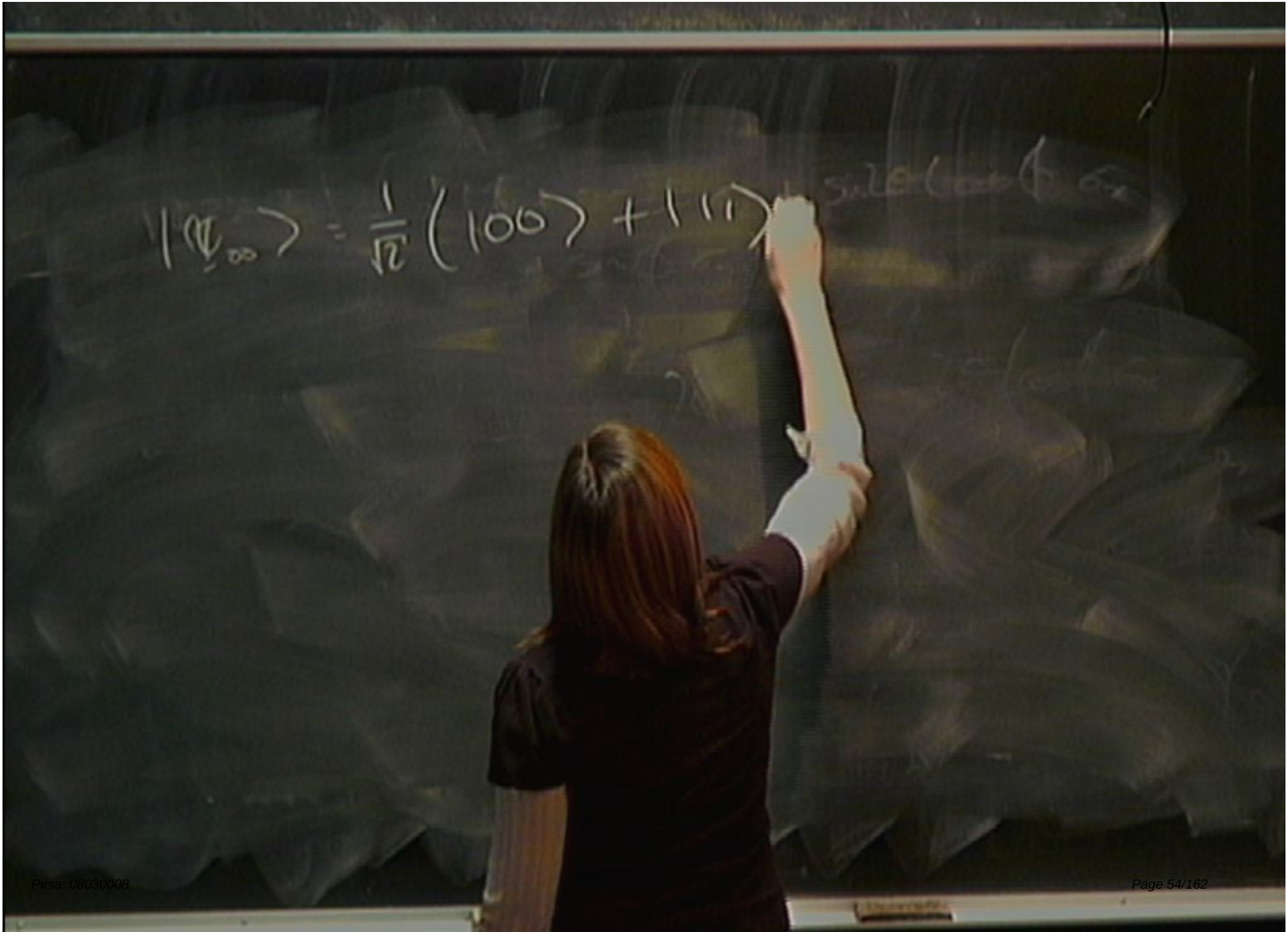
$|\Psi\rangle_{AB}$

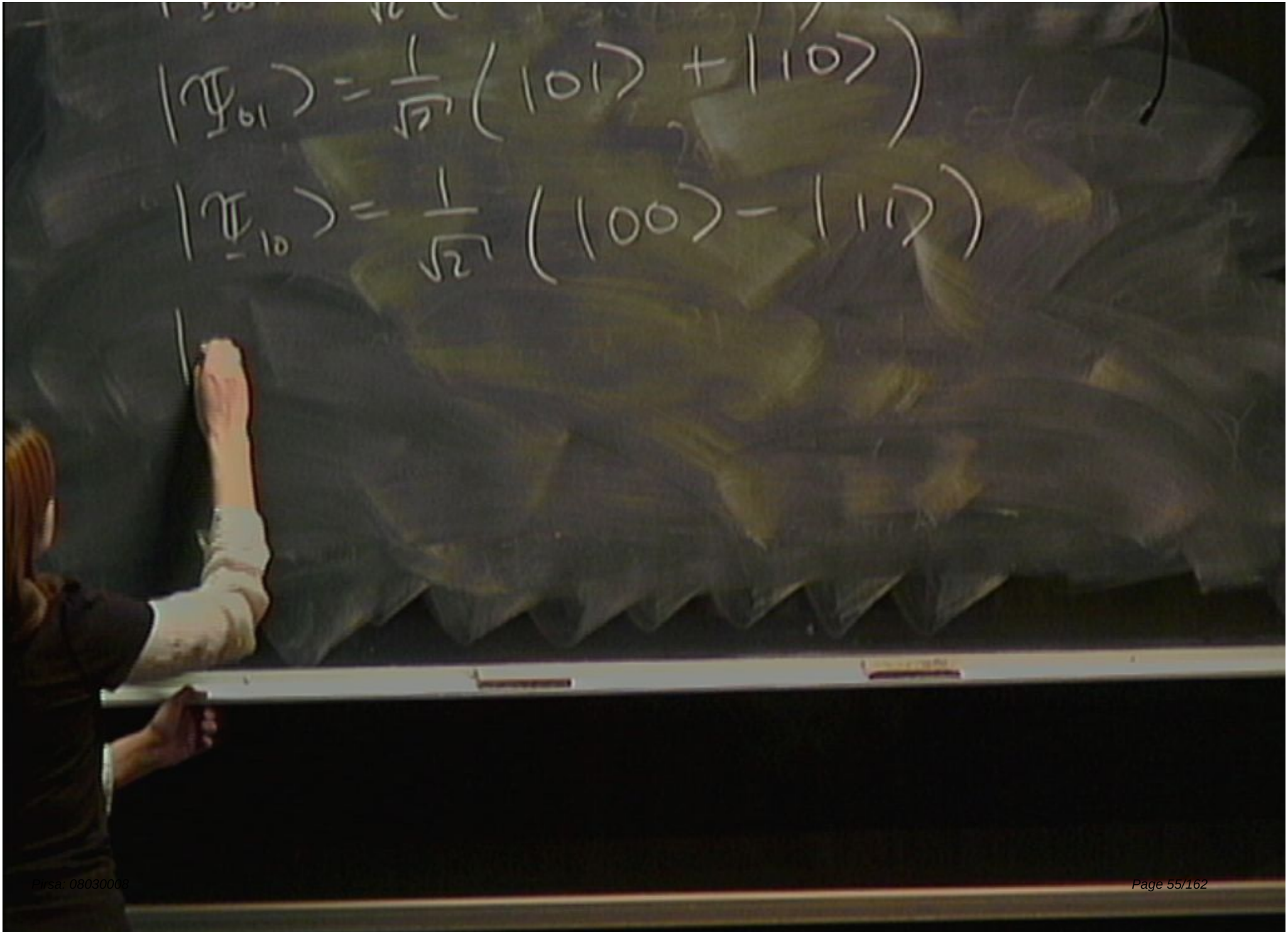
$\{|i\rangle_A\}$ $\quad |i\rangle\langle i| \otimes \mathbb{I}_B$

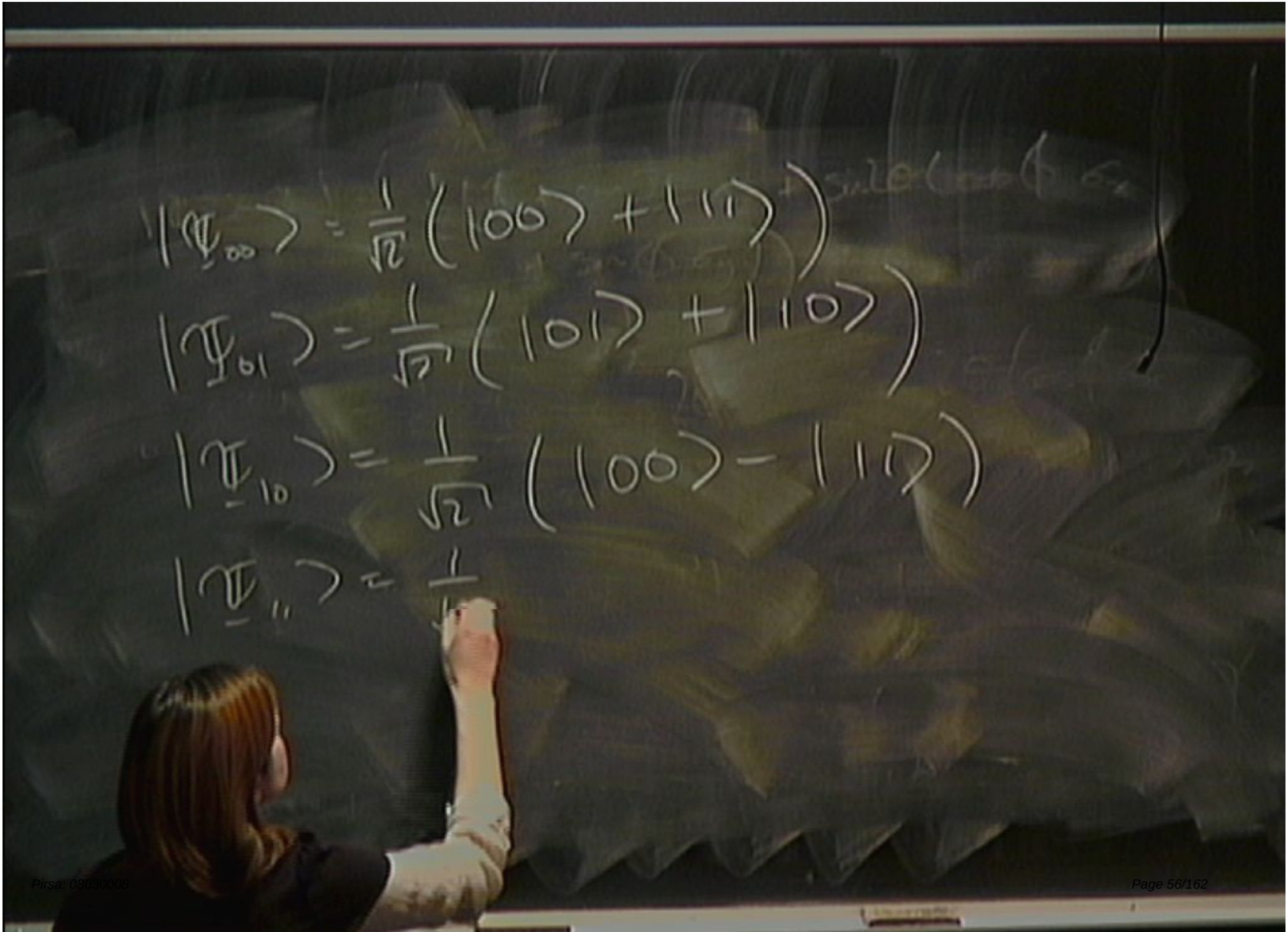
$$P(i) = Tr_{AB}\left(\left(|\Psi\rangle\langle\Psi| \right) \left(|i\rangle\langle i| \otimes \mathbb{I}_B \right) \right)$$

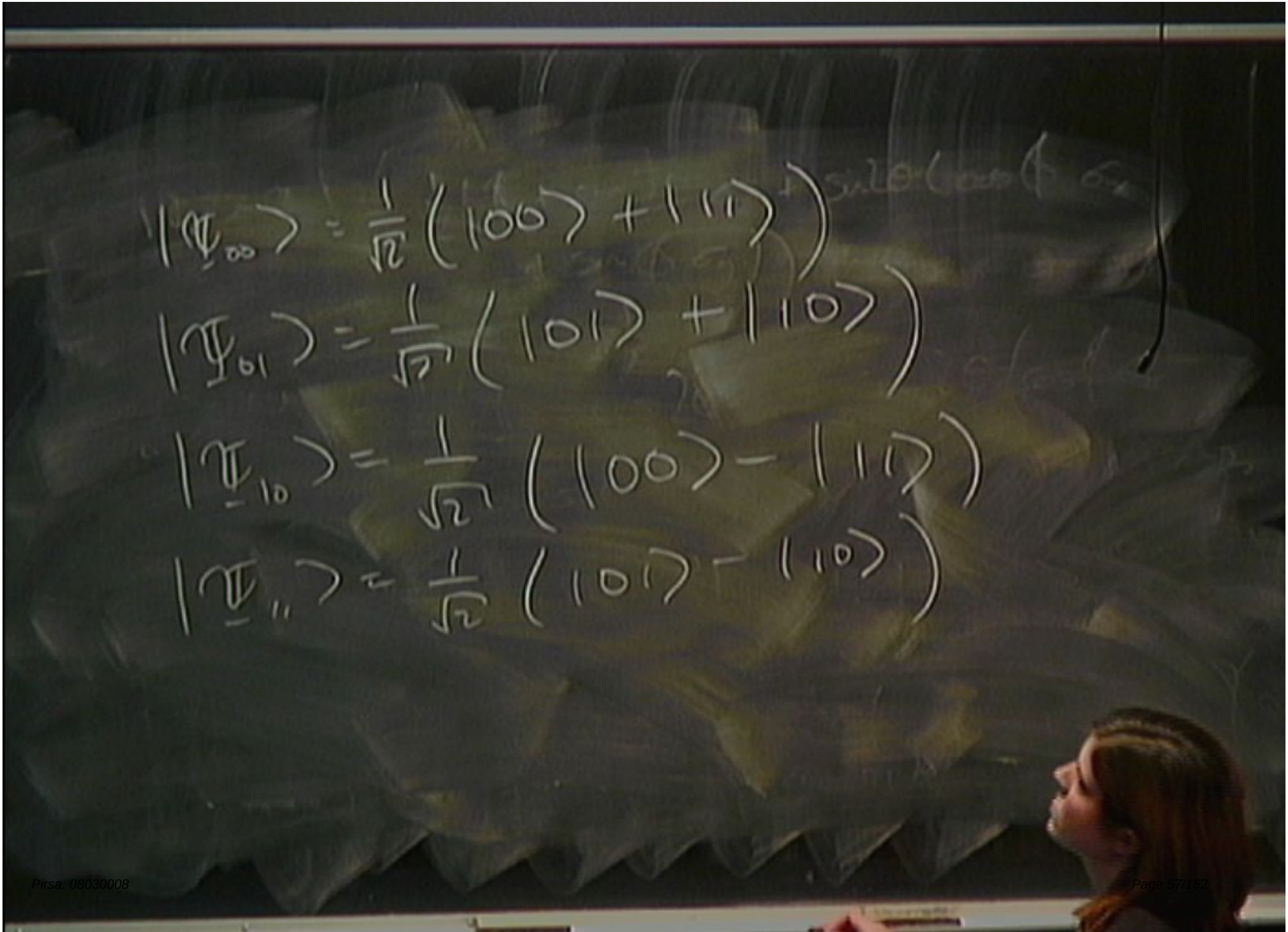
$$= Tr_A\left(Tr_B\left(|\Psi\rangle\langle\Psi| \right) |i\rangle\langle i| \right)$$

$$\rho_A = Tr_B\left(|\Psi\rangle\langle\Psi| \right)$$


$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$


$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$


$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}$


$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$|00\rangle = |0\rangle_A |0\rangle_B$$

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$|00\rangle = |0\rangle_A |0\rangle_B$$

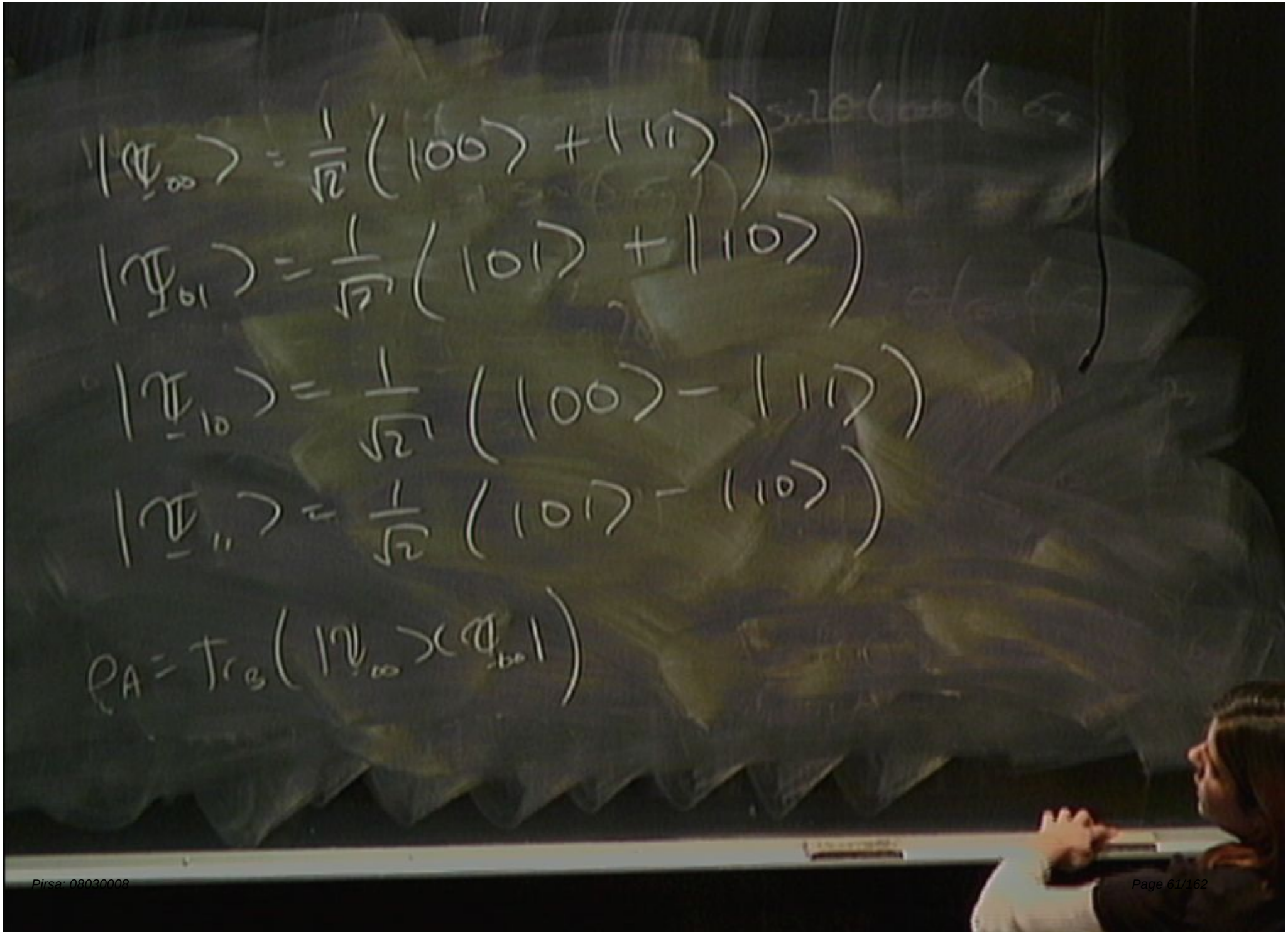
$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$|00\rangle = |0\rangle_A |0\rangle_B$$


$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$
$\rho_A = Tr_B(|\Psi_{00}\rangle\langle\Psi_{00}|)$

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

$$\rho_A = Tr_B(|\Psi_{00}\rangle\langle\Psi_{00}|) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$$

$$= \frac{1}{2}\mathbb{1}$$

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

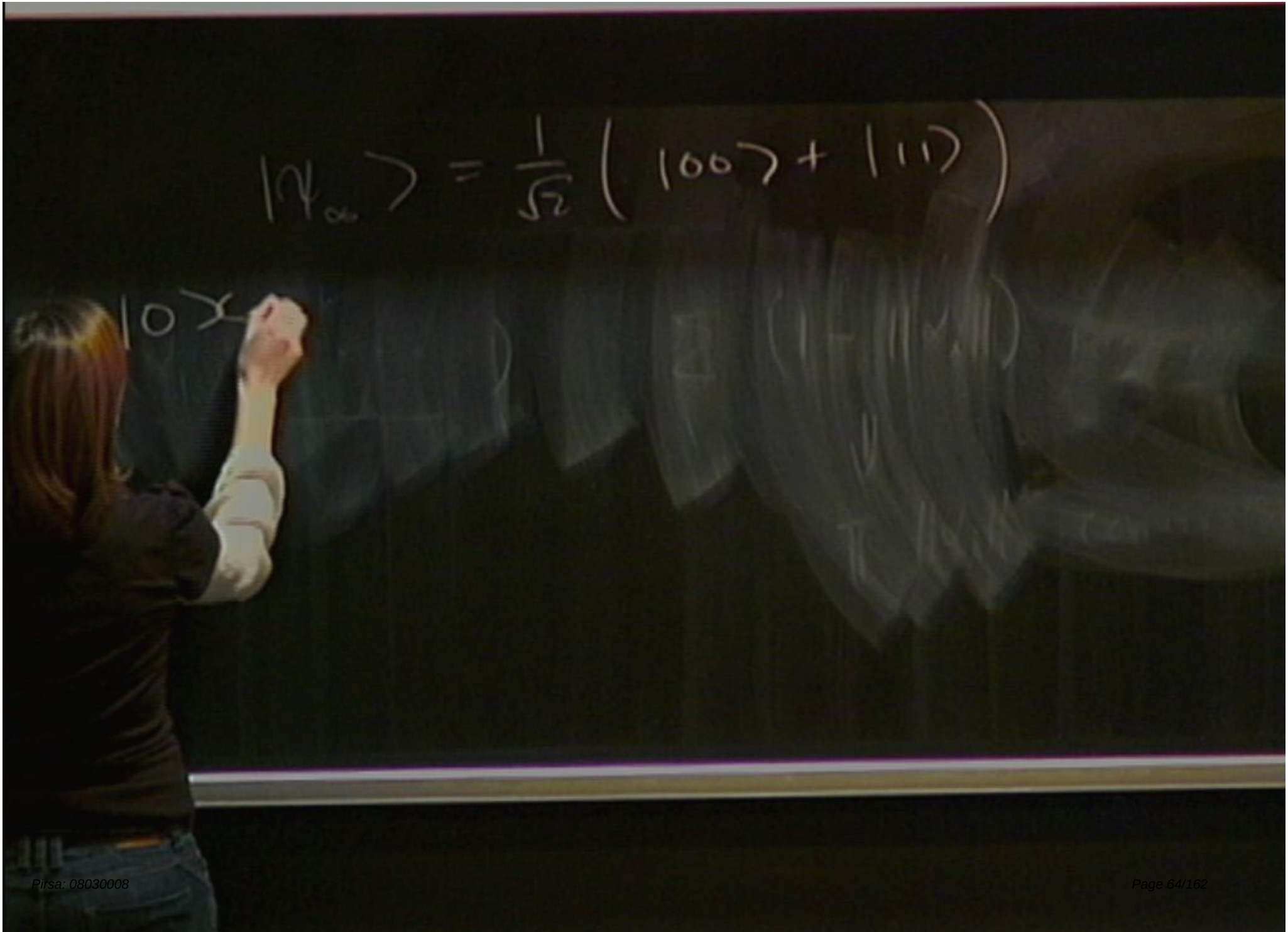
$$|\Psi_{01}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

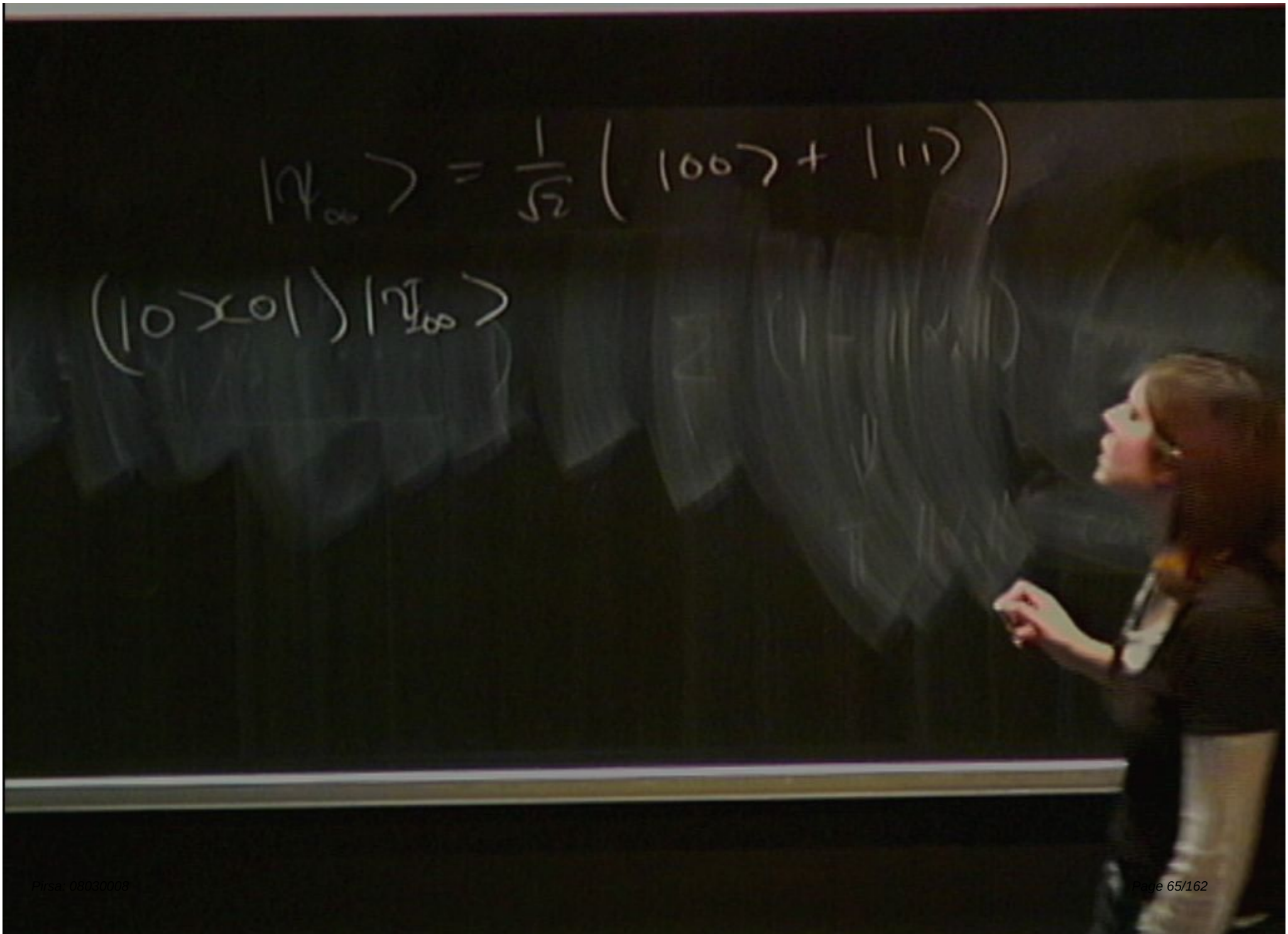
$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$|\Psi_{11}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

$$\rho_A = Tr_B\left(|\Psi_{00}\rangle\langle\Psi_{00}|\right) = \frac{1}{2}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right)$$

$$= \frac{1}{2}\mathbb{1}$$


$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
$|0\rangle$


$|\gamma_\infty\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
$(|0\rangle\langle 0|)\,|\gamma_\infty\rangle$

$$|\psi_\infty\rangle = \frac{1}{\sqrt{2}}\left(|100\rangle + |111\rangle\right)$$

$$(10\times 01)\,|\psi_\infty\rangle = \frac{1}{\sqrt{2}}\,|100\rangle$$

Quantum Communication

May share entangled states.

- **Alice**
- Sends classical information and/or quantum states to Bob.

- **Bob**
- Must make a measurement on the state sent by Alice to determine the message sent, or perform operations on his states based on the classical information sent by Alice.

Quantum Communication

May share entangled states.

- **Alice**
- Sends classical information and/or quantum states to Bob.

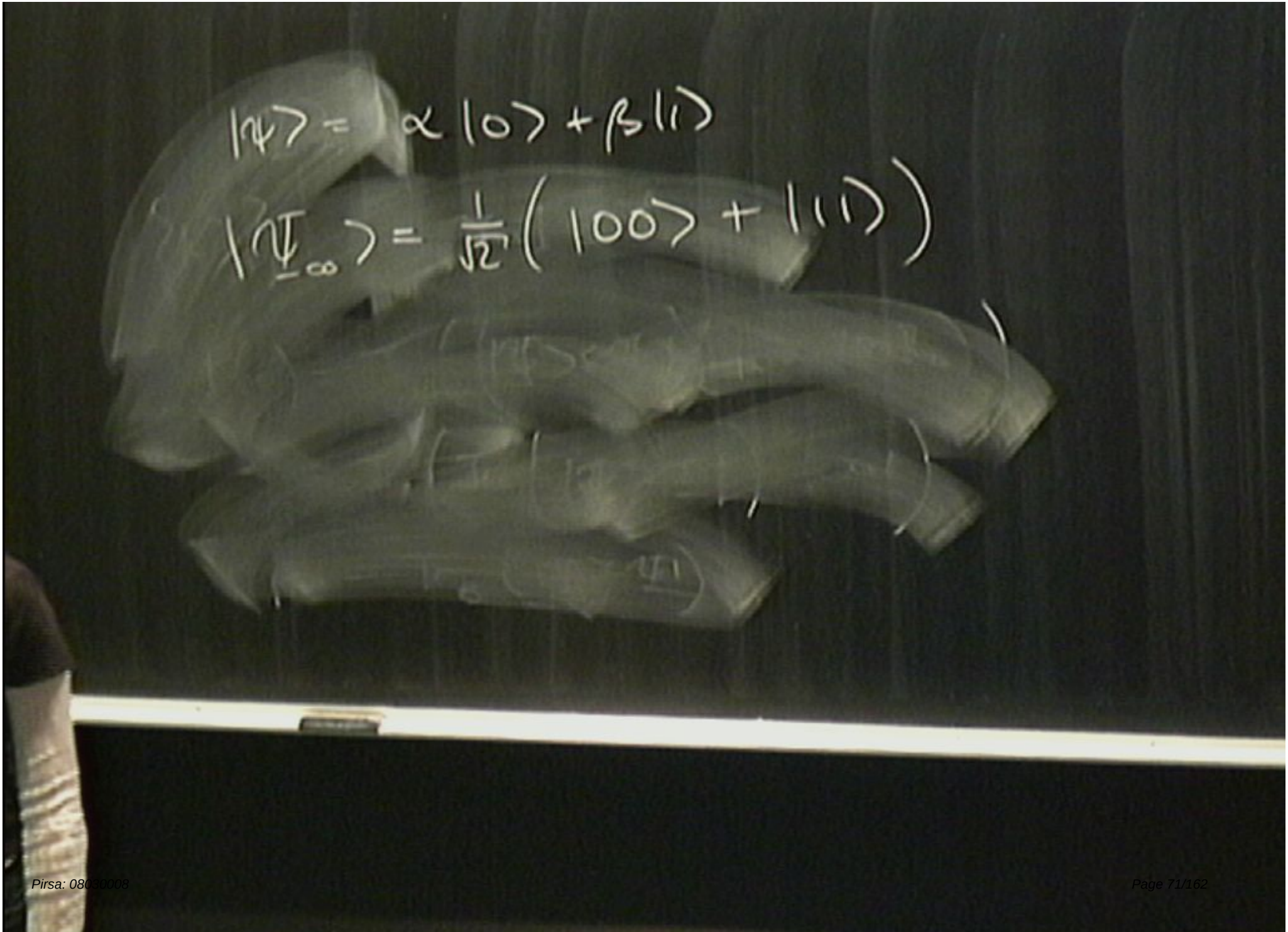
- **Bob**
- Must make a measurement on the state sent by Alice to determine the message sent, or perform operations on his states based on the classical information sent by Alice.

Superdense Coding

- Alice and Bob share a Bell state.
- By means of local operations Alice can convert the state into any of the other three Bell states.
- Alice then sends her qubit to Bob.
- Bob makes a joint measurement on the composite state to determine the operation performed by Alice, and therefore the two (classical) bits encoded.

Quantum Teleportation

- Alice has a qubit in a given state, and Alice and Bob share a Bell state.
- Alice makes a joint measurement in the Bell basis on her qubit and her half of the Bell state.
- Alice communicates the result of measurement to Bob classically.
- Based on the result of measurement Bob applies one of four unitary operators to his qubit to reproduce Alice's initial state.


$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
$|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

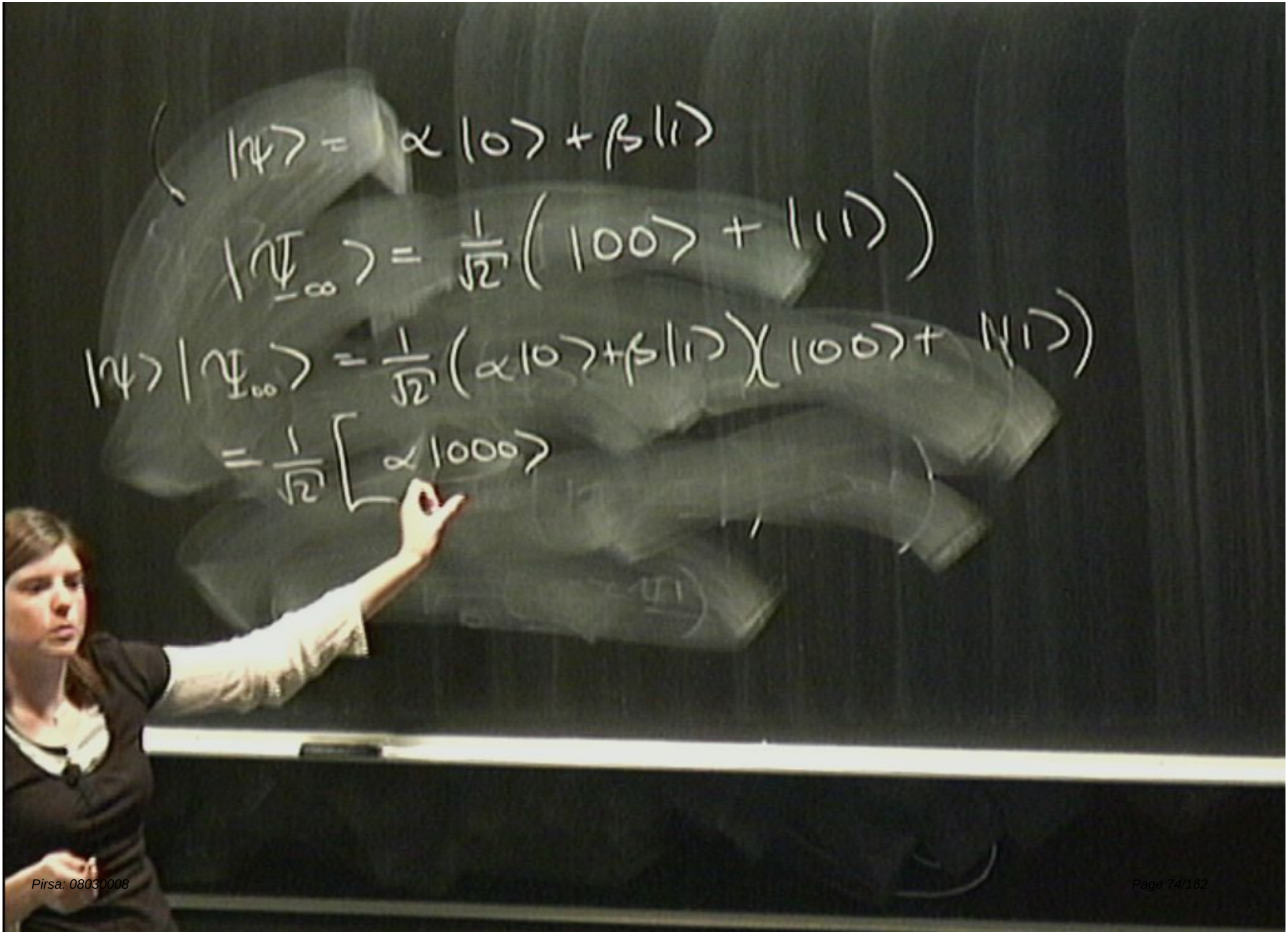
$$|\psi\rangle|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle+\beta|1\rangle\right)\left(|00\rangle+|11\rangle\right)$$

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$|\psi\rangle|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle+\beta|1\rangle)(|00\rangle+|11\rangle)$

$= \frac{1}{\sqrt{2}}[\alpha|000\rangle$


$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
$|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
$|\psi\rangle|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle+\beta|1\rangle)(|00\rangle + |11\rangle)$
$= \frac{1}{\sqrt{2}}[\alpha|000\rangle$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\psi\rangle|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle+\beta|1\rangle\right)\left(|00\rangle+|11\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left[\alpha|000\rangle + \alpha|011\rangle\right.$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\psi\rangle|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle+\beta|1\rangle\right)\left(|00\rangle+|11\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left[\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right]$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\psi\rangle|\Psi_{-\infty}\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle+\beta|1\rangle\right)\left(|00\rangle+|11\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left[\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right]$$

$$= \frac{1}{\sqrt{2}}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\psi\rangle|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle+\beta|1\rangle\right)\left(|00\rangle + |11\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left[\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right]$$

$$= \frac{1}{\sqrt{2}}\left[\right.$$

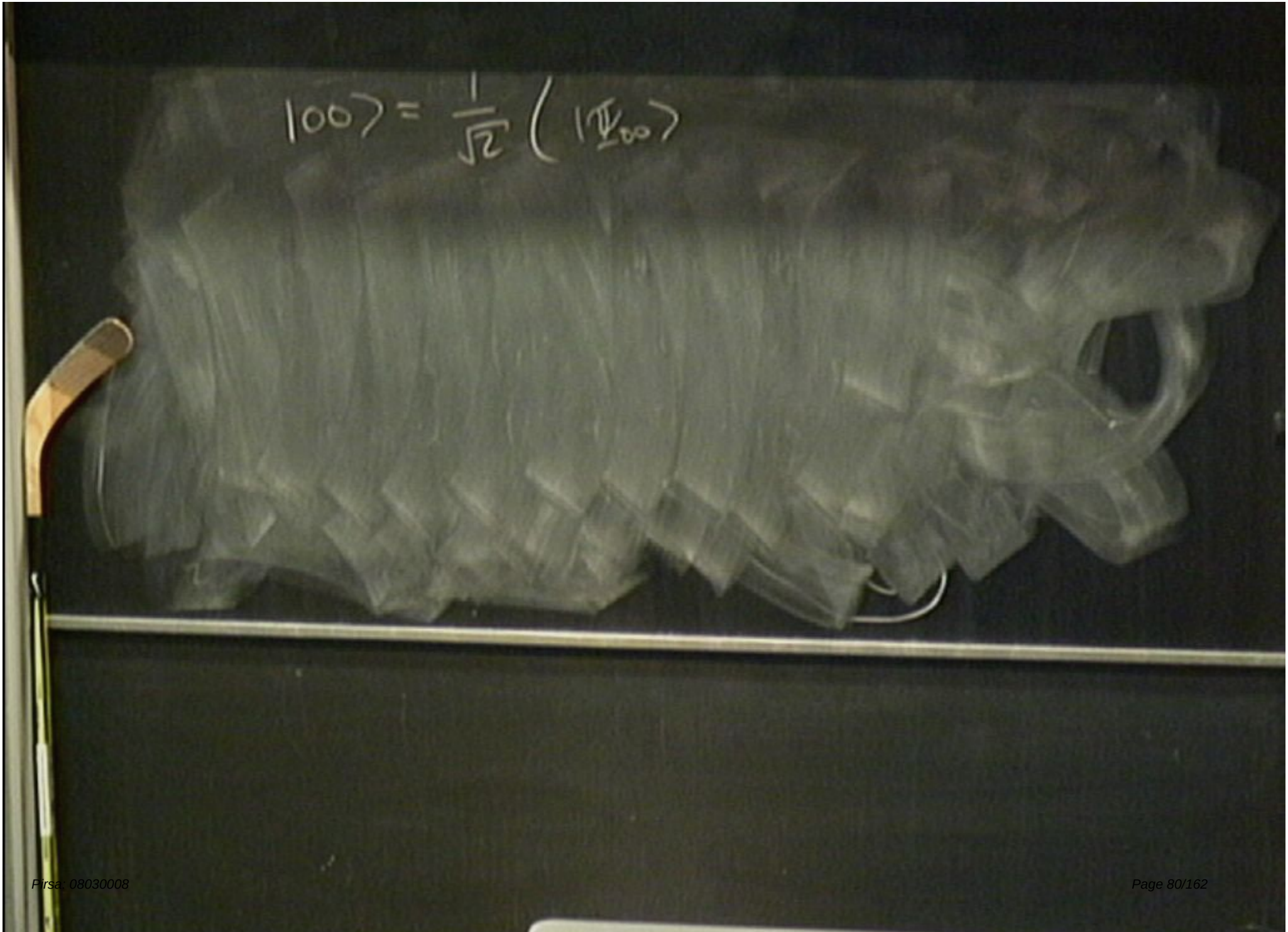
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

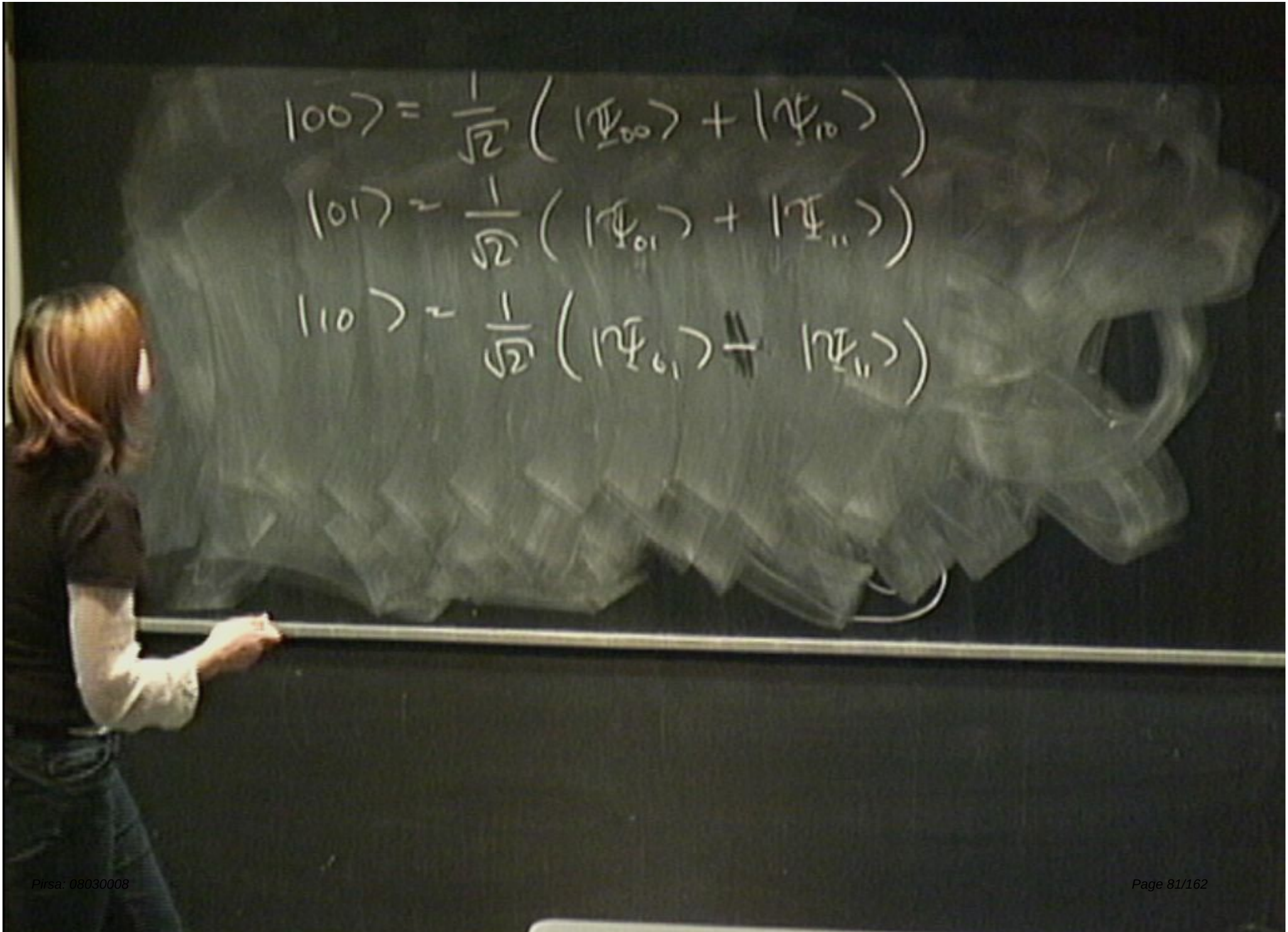
$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\psi\rangle|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle + \beta|1\rangle\right)\left(|00\rangle + |11\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left[\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right]$$

$$= \frac{1}{\sqrt{2}}\left[\left(\alpha|00\rangle + \beta|10\rangle\right)|0\rangle + \left(\alpha|01\rangle + \beta|11\rangle\right)|1\rangle\right]$$


$|00\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{00}\rangle\right.$


$|00\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{00}\rangle + |\Psi_{10}\rangle\right)$
$|01\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{01}\rangle + |\Psi_{11}\rangle\right)$
$|10\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{01}\rangle - |\Psi_{11}\rangle\right)$

$$|00\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{00}\rangle + |\Psi_{10}\rangle\right)$$

$$|01\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{01}\rangle + |\Psi_{11}\rangle\right)$$

$$|10\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{01}\rangle + |\Psi_{11}\rangle\right)$$

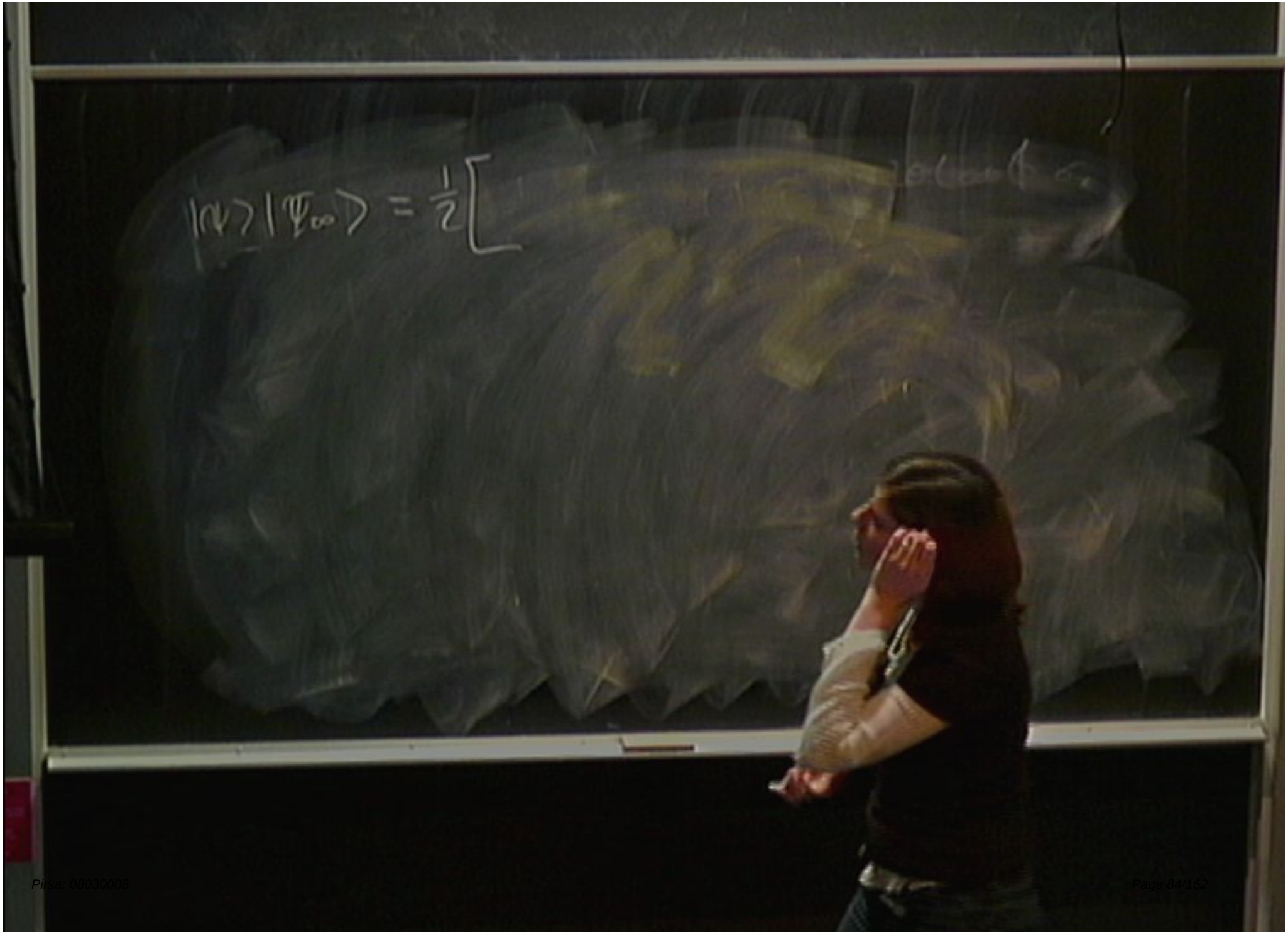
$$|11\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{01}\rangle - |\Psi_{10}\rangle\right)$$

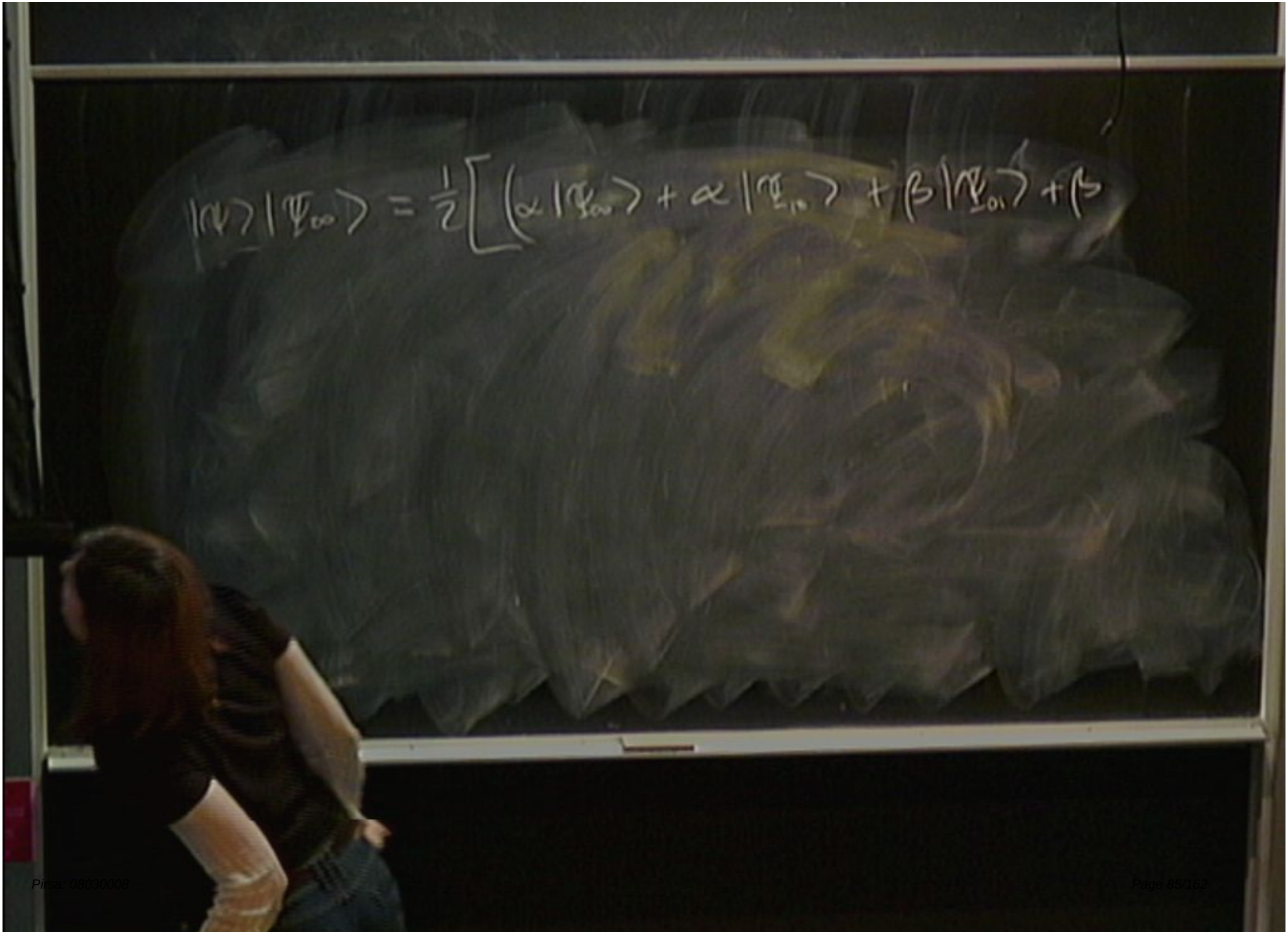
$$|00\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{00}\rangle + |\Psi_{10}\rangle\right)$$

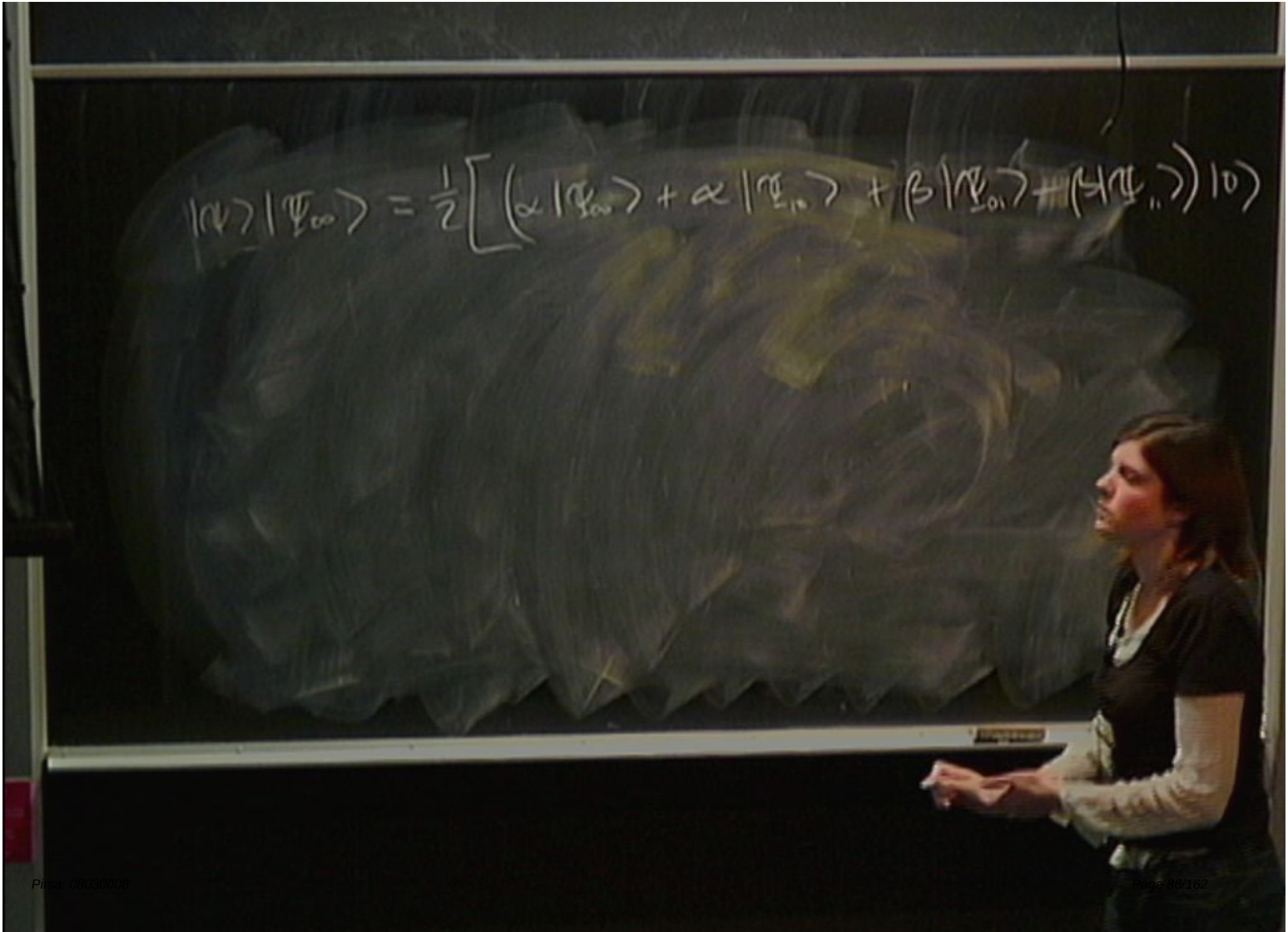
$$|01\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{01}\rangle + |\Psi_{11}\rangle\right)$$

$$|10\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{01}\rangle + |\Psi_{11}\rangle\right)$$

$$|11\rangle = \frac{1}{\sqrt{2}}\left(|\Psi_{00}\rangle - |\Psi_{10}\rangle\right)$$

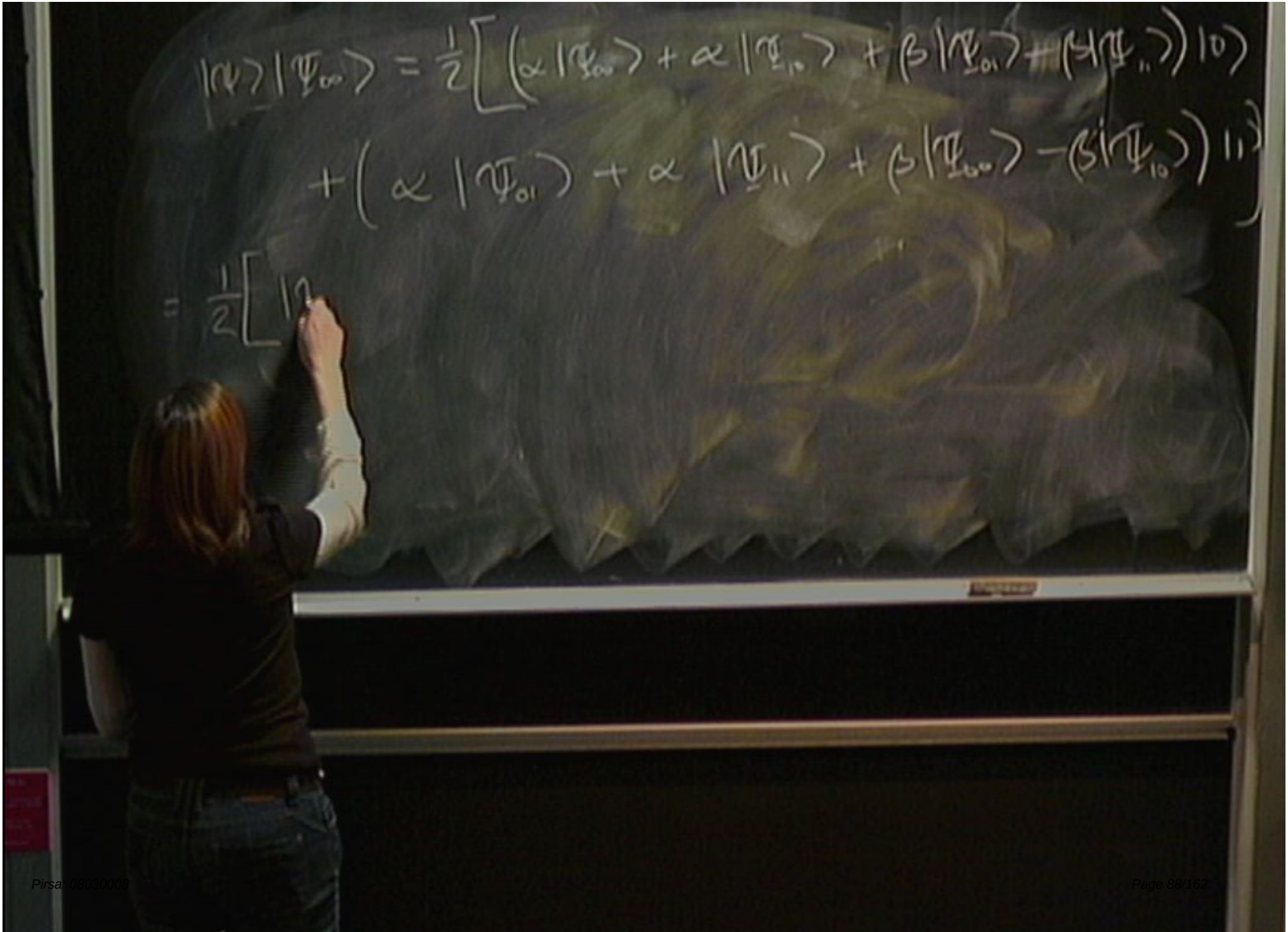

$|\psi\rangle|\Psi_{\infty}\rangle = \frac{1}{2}[$

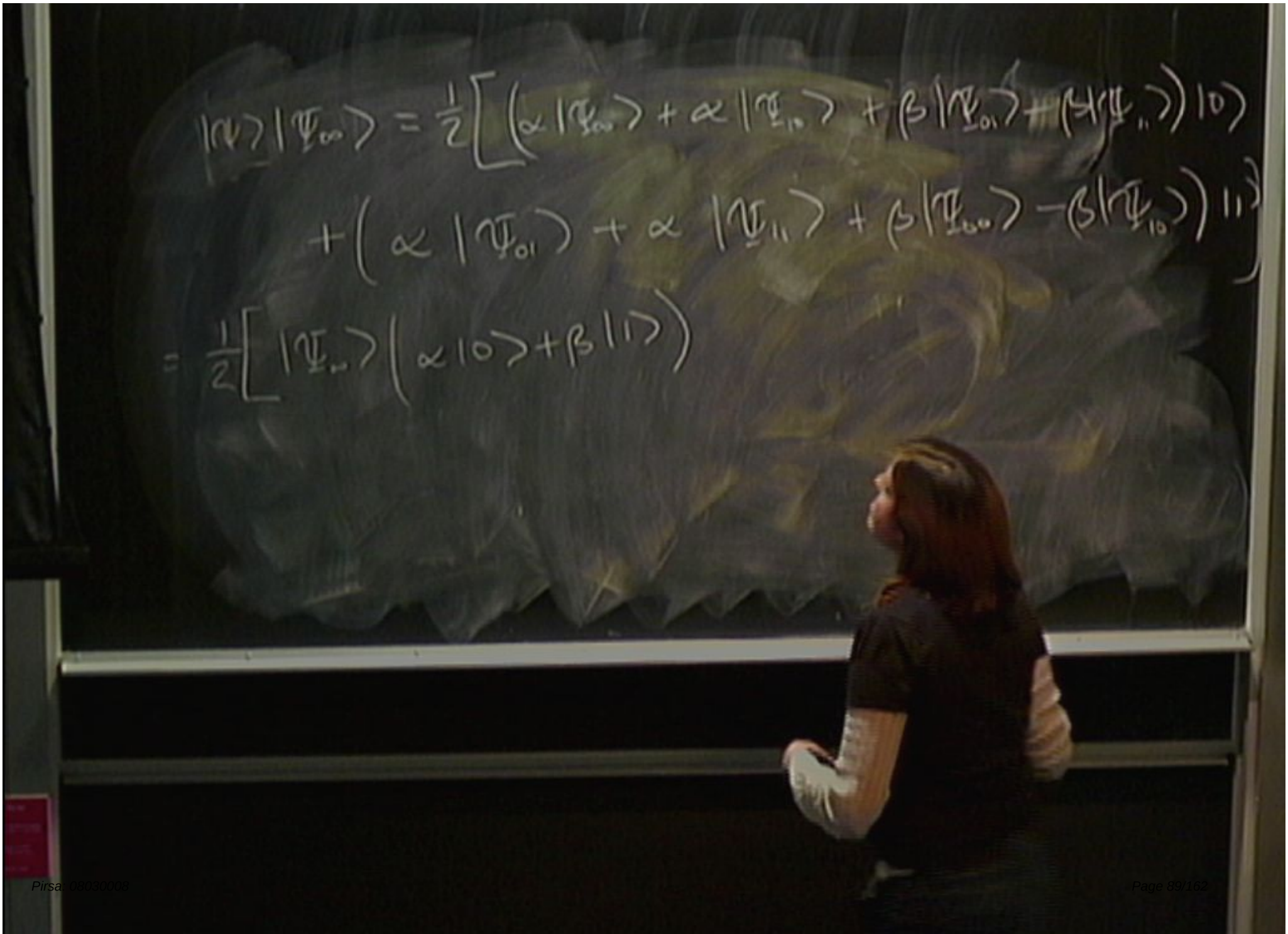

$|\psi\rangle|\Psi_{00}\rangle = \frac{1}{2}\Big[\big(\alpha|\Psi_{00}\rangle + \alpha|\Psi_{10}\rangle + \beta|\Psi_{01}\rangle + \beta$

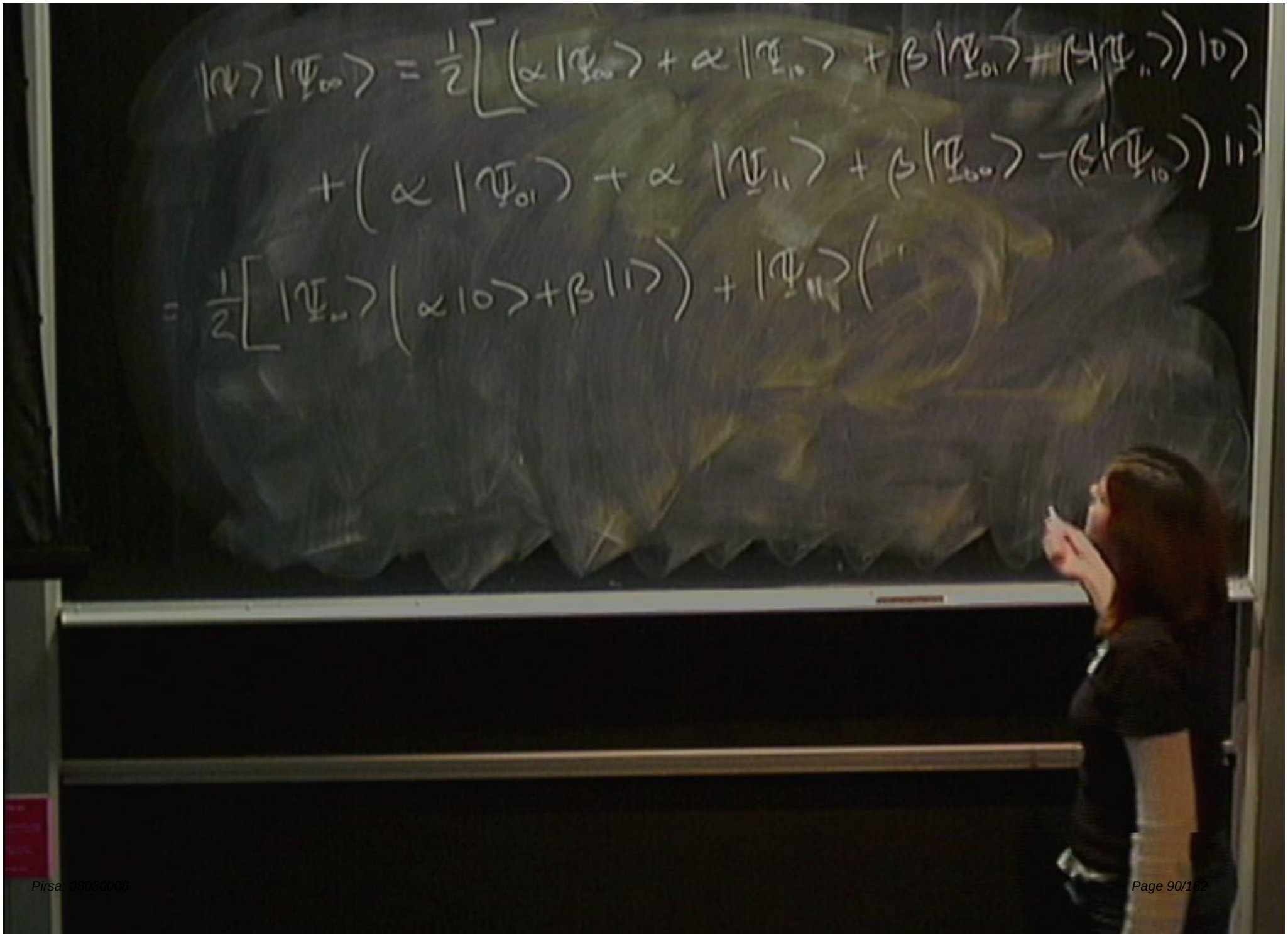

$|\psi\rangle|\Psi_{00}\rangle = \frac{1}{2}\left[\left(\alpha|\Psi_{00}\rangle + \alpha|\Psi_{10}\rangle + \beta|\Psi_{01}\rangle + (\beta|\Psi_{11}\rangle)\right)|0\rangle\right.$

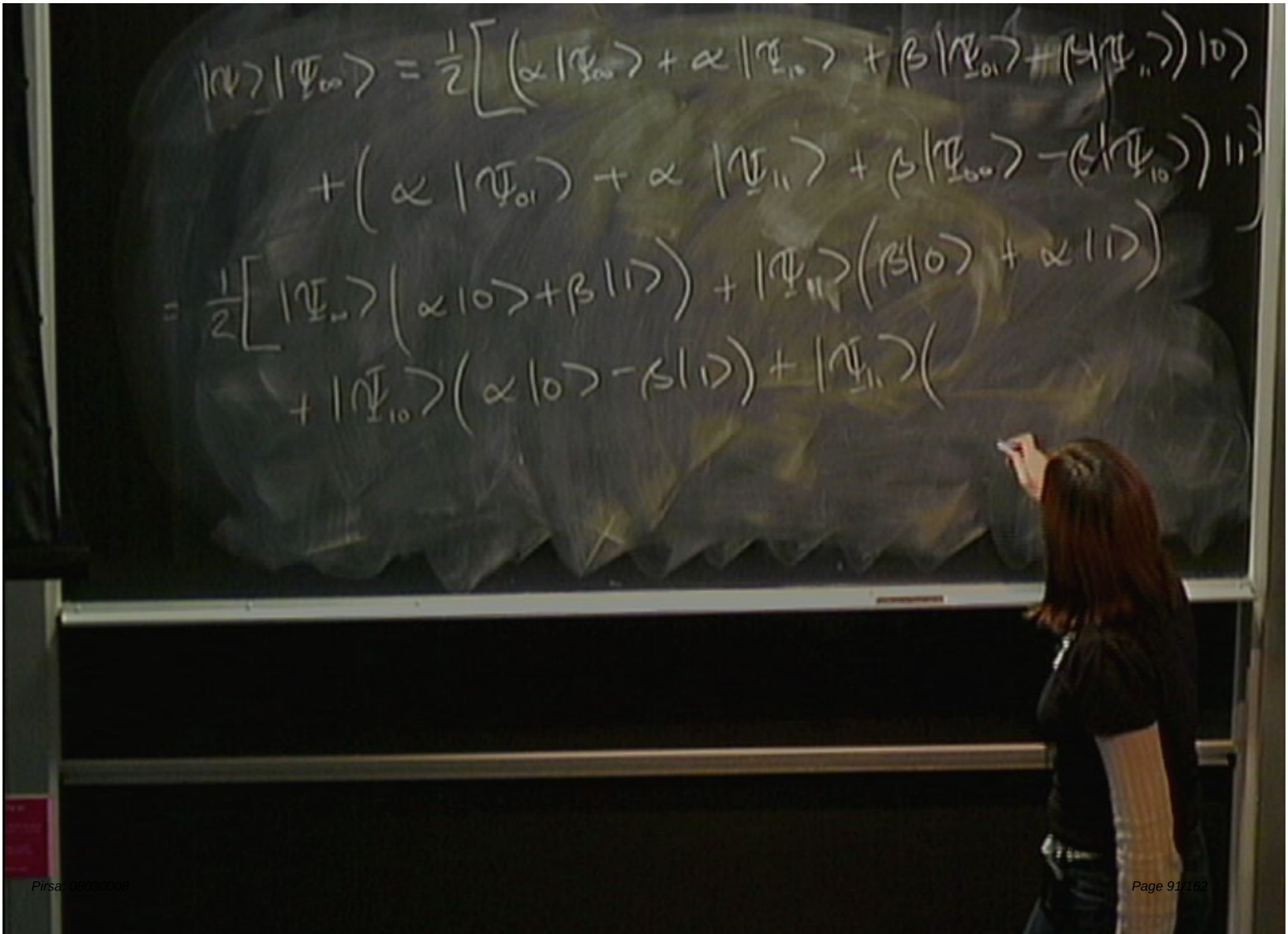
$$|\psi\rangle|\Psi_{00}\rangle = \frac{1}{2}\Big[\big(\alpha|\Psi_{00}\rangle + \alpha|\Psi_{10}\rangle + \beta|\Psi_{01}\rangle + \beta|\Psi_{11}\rangle\big)|0\rangle$$

$$+\big(\alpha|\Psi_{01}\rangle + \alpha|\Psi_{11}\rangle + \beta|\Psi_{00}\rangle - \beta|\Psi_{10}\rangle\big)|1\rangle\Big]$$


$|\psi\rangle|\Psi_{00}\rangle = \frac{1}{2}\Big[\big(\alpha|\Psi_{00}\rangle + \alpha|\Psi_{10}\rangle + \beta|\Psi_{01}\rangle + (-i|\Psi_{11}\rangle)\big)|0\rangle$
$+\big(\alpha|\Psi_{01}\rangle + \alpha|\Psi_{11}\rangle + \beta|\Psi_{00}\rangle - (\beta i|\Psi_{10}\rangle)\big)|1\rangle\Big]$
$= \frac{1}{2}\Big[|$


$|\psi\rangle|\Psi_{00}\rangle = \frac{1}{2}\Big[\big(\alpha|\Psi_{00}\rangle + \alpha|\Psi_{10}\rangle + \beta|\Psi_{01}\rangle + (\beta|\Psi_{11}\rangle)\big)|0\rangle$
$+\big(\alpha|\Psi_{01}\rangle + \alpha|\Psi_{11}\rangle + \beta|\Psi_{00}\rangle - (\beta|\Psi_{10}\rangle)\big)|1\rangle\Big]$
$= \frac{1}{2}\Big[|\Psi_{00}\rangle\big(\alpha|0\rangle + \beta|1\rangle\big)$


$|\psi\rangle|\Psi_{00}\rangle = \frac{1}{2}\Big[\big(\alpha|\Psi_{00}\rangle + \alpha|\Psi_{10}\rangle + \beta|\Psi_{01}\rangle + (\beta|\Psi_{11}\rangle)|0\rangle$
$+\big(\alpha|\Psi_{01}\rangle + \alpha|\Psi_{11}\rangle + \beta|\Psi_{00}\rangle - (\beta|\Psi_{10}\rangle)|1\rangle\Big)$
$= \frac{1}{2}\Big[|\Psi_{00}\rangle\big(\alpha|0\rangle + \beta|1\rangle\big) + |\Psi_{11}\rangle($

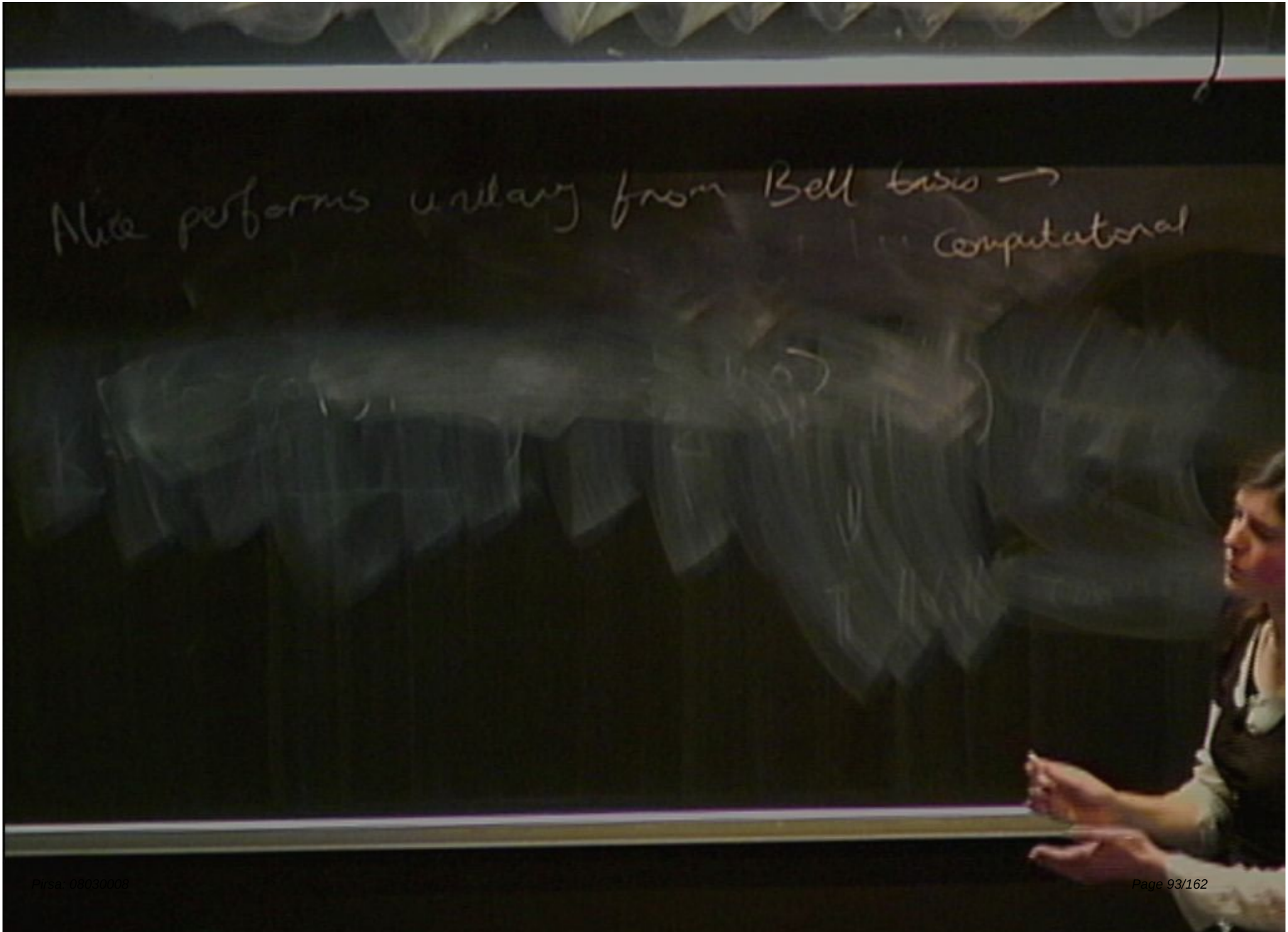

$|\psi\rangle|\Psi_{00}\rangle = \frac{1}{2}\Big[\big(\alpha|\Psi_{00}\rangle + \alpha|\Psi_{10}\rangle + \beta|\Psi_{01}\rangle + \beta|\Psi_{11}\rangle\big)|0\rangle$
$+\big(\alpha|\Psi_{01}\rangle + \alpha|\Psi_{11}\rangle + \beta|\Psi_{00}\rangle - \beta|\Psi_{10}\rangle\big)|1\rangle\Big]$
$= \frac{1}{2}\Big[|\Psi_{00}\rangle\big(\alpha|0\rangle + \beta|1\rangle\big) + |\Psi_{11}\rangle\big(\beta|0\rangle + \alpha|1\rangle\big)$
$+|\Psi_{10}\rangle\big(\alpha|0\rangle - \beta|1\rangle\big) + |\Psi_{11}\rangle($

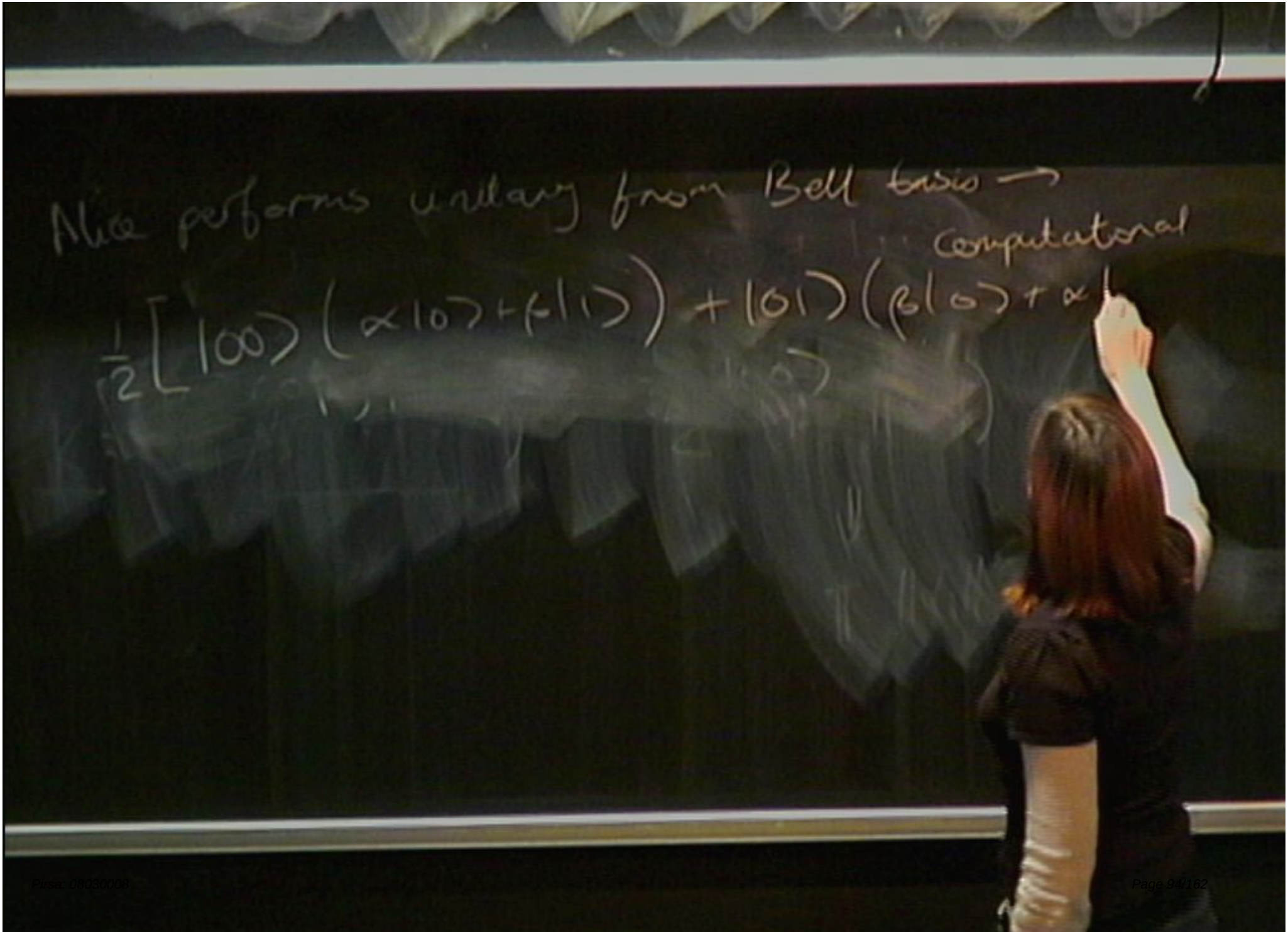
$$|\psi\rangle|\Psi_{00}\rangle = \frac{1}{2}\Big[\big(\alpha|\Psi_{00}\rangle + \alpha|\Psi_{10}\rangle + \beta|\Psi_{01}\rangle + (\beta|\Psi_{11}\rangle)\big)|0\rangle$$

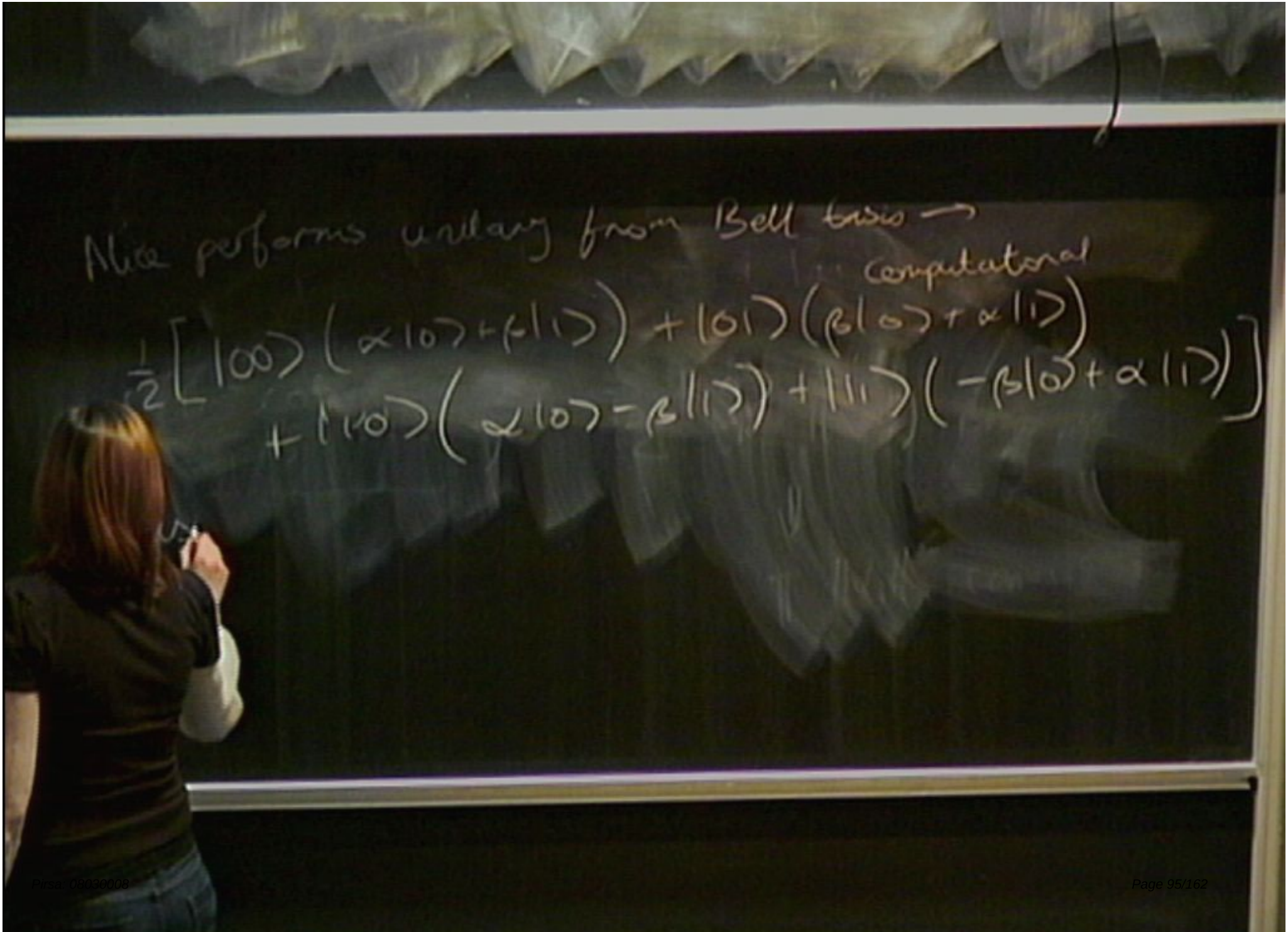
$$+\big(\alpha|\Psi_{01}\rangle + \alpha|\Psi_{11}\rangle + \beta|\Psi_{00}\rangle - (\beta|\Psi_{10}\rangle)\big)|1\rangle\Big]$$

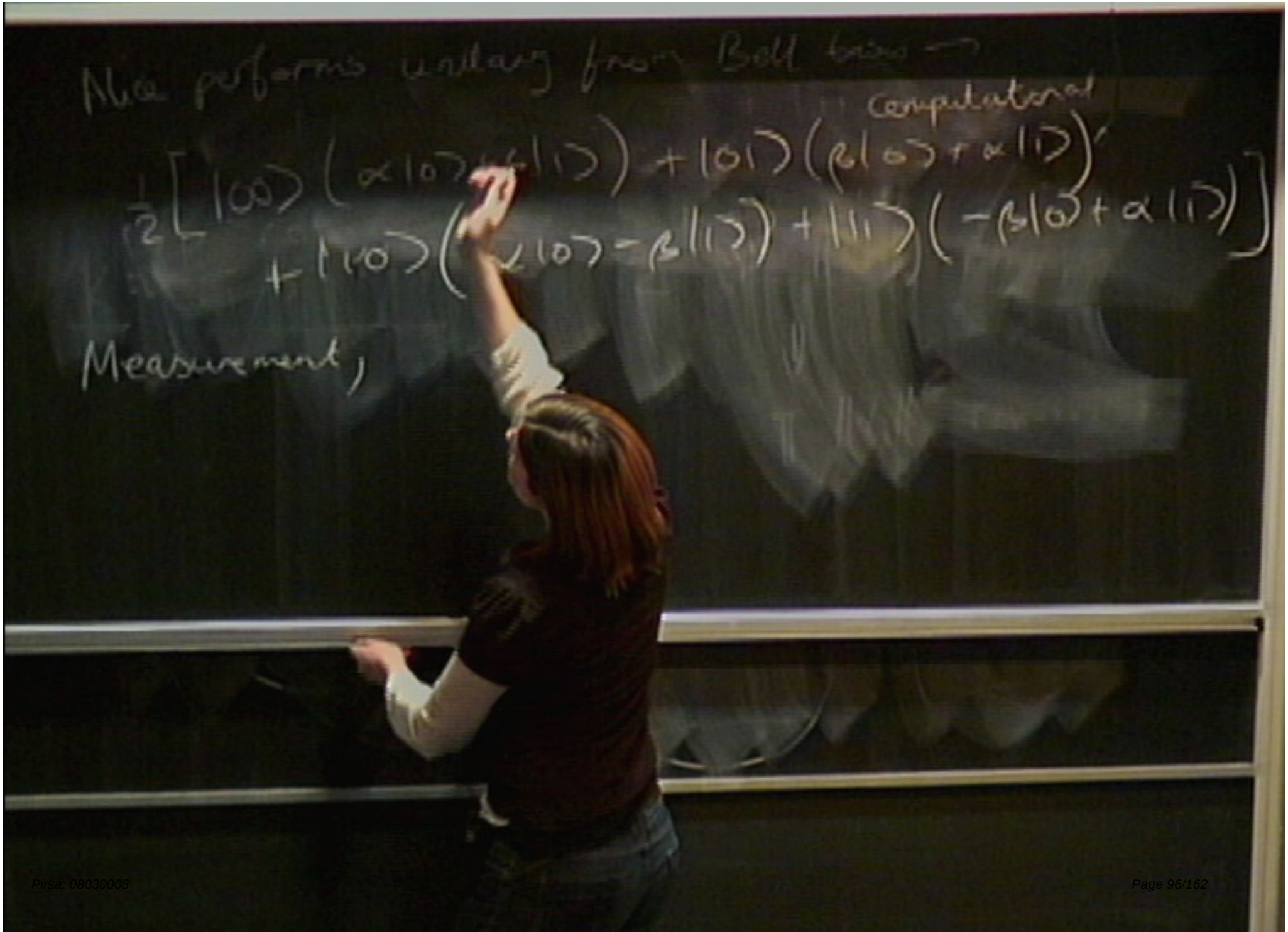
$$= \frac{1}{2}\Big[|\Psi_{00}\rangle\big(\alpha|0\rangle + \beta|1\rangle\big) + |\Psi_{11}\rangle\big(\beta|0\rangle + \alpha|1\rangle\big)$$

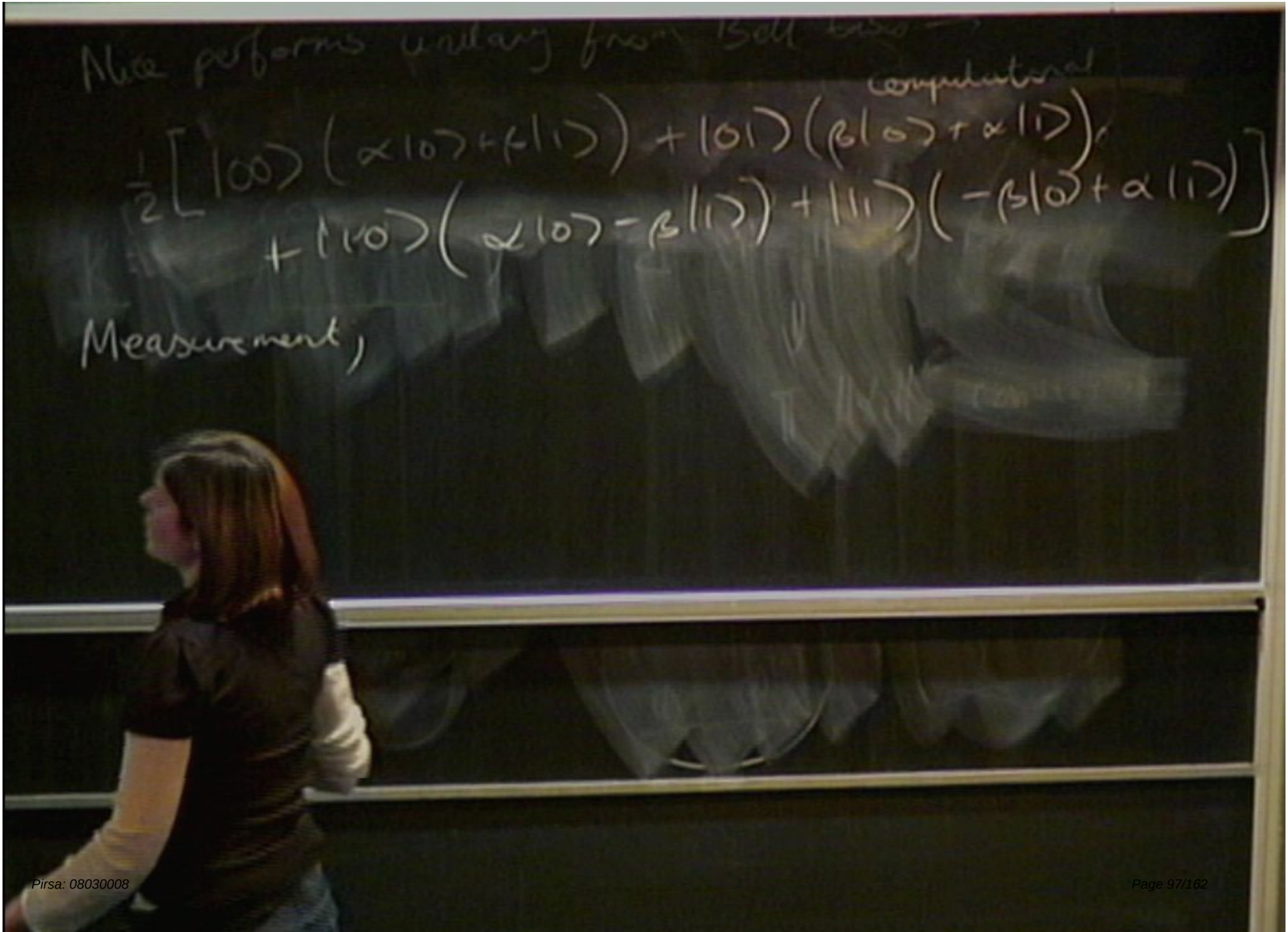
$$+|\Psi_{10}\rangle\big(\alpha|0\rangle - \beta|1\rangle\big) + |\Psi_{11}\rangle\big(-\beta|0\rangle + \alpha|1\rangle\big)\Big]$$


Alice performs unitary from Bell basis →
computational


Alice performs unitary from Bell basis →
computational
$\frac{1}{2}[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\beta|0\rangle+\alpha$


Alice performs unitary from Bell basis → computational
$\frac{1}{2}[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\beta|0\rangle+\alpha|1\rangle)$
$+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(-\beta|0\rangle+\alpha|1\rangle)]$


Alice performs unitary from Bell basis →
computational
$\frac{1}{2}[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\beta|0\rangle+\alpha|1\rangle)$
$+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(-\beta|0\rangle+\alpha|1\rangle)]$
Measurement)


Alice performs unitary from Bell basis to computational
$\frac{1}{2}[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\beta|0\rangle+\alpha|1\rangle)+$
$|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(-\beta|0\rangle+\alpha|1\rangle)]$
Measurement)

Alice performs unitary from Bell basis to computational

$$\frac{1}{2}\Big[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\beta|0\rangle+\alpha|1\rangle)$$
$$+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(-\beta|0\rangle+\alpha|1\rangle)\Big]$$

Measurement:

00	$\alpha\|0\rangle+\beta\|1\rangle$
01	$\beta\|0\rangle+\alpha\|1\rangle$
10	$\alpha\|0\rangle-\beta\|1\rangle$
11	$-\beta\|0\rangle+\alpha\|1\rangle$

Alice performs unitary from Bell basis to computational

$$\frac{1}{2}\Big[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\beta|0\rangle+\alpha|1\rangle)$$
$$+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(-\beta|0\rangle+\alpha|1\rangle)\Big]$$

Measurement:

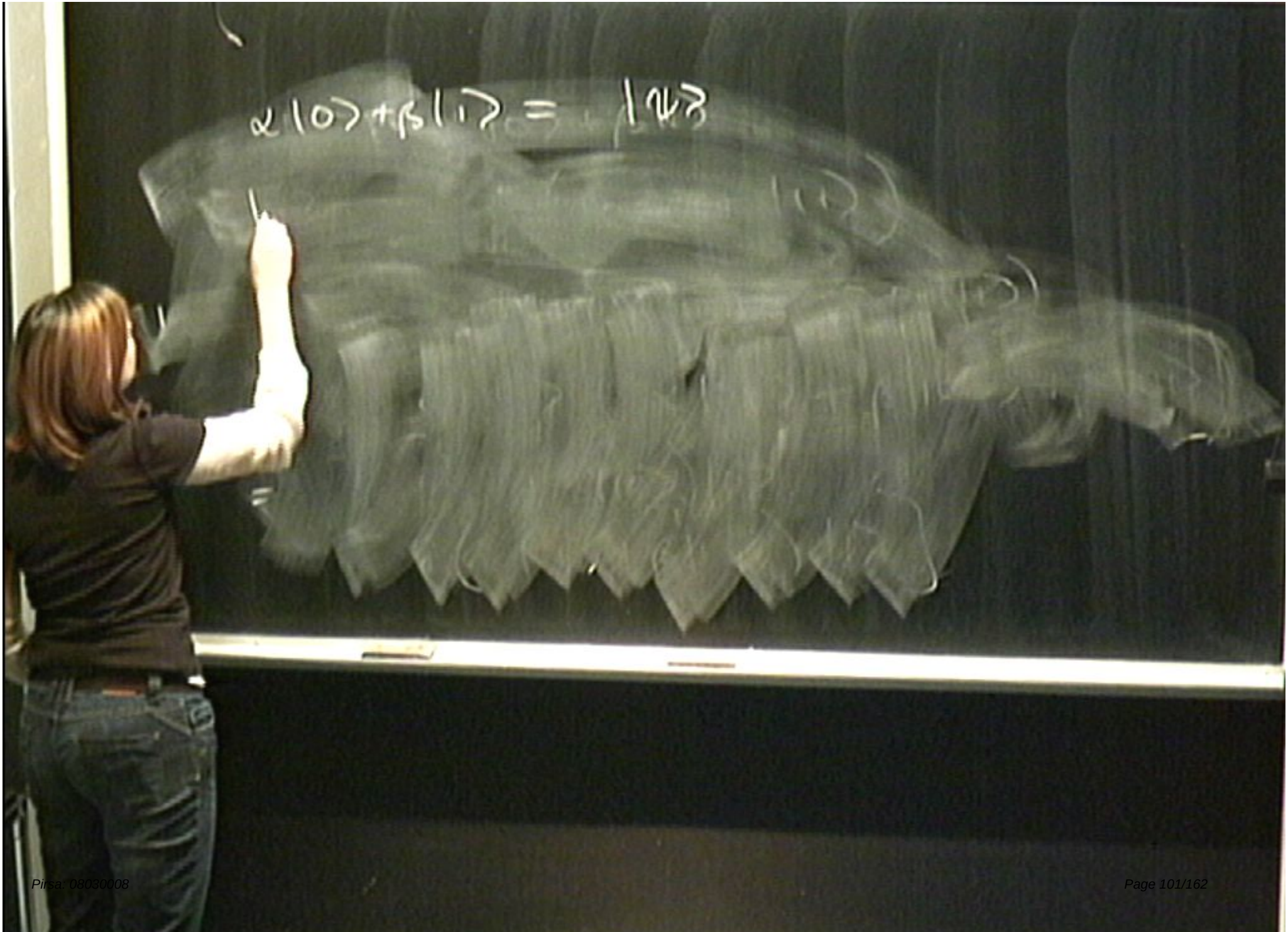
00	$\alpha\|0\rangle+\beta\|1\rangle$ ✓
01	$\beta\|0\rangle+\alpha\|1\rangle$
10	$\alpha\|0\rangle-\beta\|1\rangle$
11	$-\beta\|0\rangle+\alpha\|1\rangle$

Alice performs unitary from Bell basis → computational

$$\frac{1}{2}\Big[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\beta|0\rangle+\alpha|1\rangle)$$
$$+|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(-\beta|0\rangle+\alpha|1\rangle)\Big]$$

Measurement;

00	;	$\alpha\|0\rangle+\beta\|1\rangle$ ✓
01	;	$\beta\|0\rangle+\alpha\|1\rangle$
10	;	$\alpha\|0\rangle-\beta\|1\rangle$
11	;	$-\beta\|0\rangle+\alpha\|1\rangle$


α|0⟩+β|1⟩ = |ψ⟩

$\alpha|0\rangle + \beta|1\rangle = |\psi\rangle$

$|\psi\rangle = X(\beta|0\rangle + \alpha|1\rangle)$

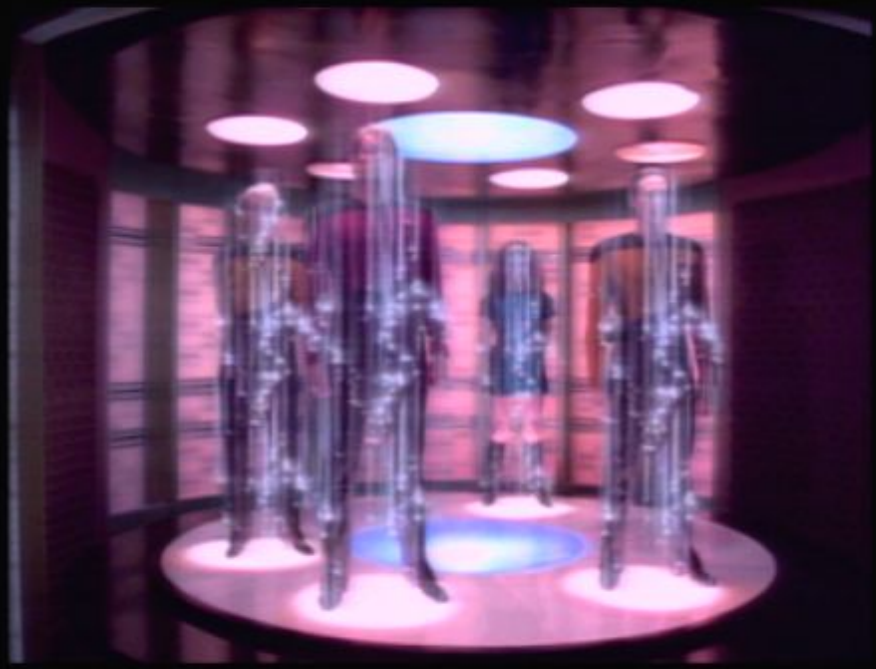
$|\psi\rangle = Z(\alpha|0\rangle - \beta|1\rangle)$

$|\psi\rangle = ZX(-\beta|0\rangle + \alpha|1\rangle)$

=

Quantum Teleportation

- Alice has a qubit in a given state, and Alice and Bob share a Bell state.
- Alice makes a joint measurement in the Bell basis on her qubit and her half of the Bell state.
- Alice communicates the result of measurement to Bob classically.
- Based on the result of measurement Bob applies one of four unitary operators to his qubit to reproduce Alice's initial state.



Quantum Teleportation

- If Alice knows the state, she needs to send an infinite amount of classical information to Bob.
- Remarkably, if she doesn't know the state, protocol still works (compare this to classical copying).
- After teleportation the state has disappeared from Alice's system and has appeared in Bob's system, therefore teleportation doesn't violate no-cloning.
- Related to dense-coding: Alice and Bob share a Bell pair and a classical channel. By making local measurements and sending two bits of classical information, Alice can send Bob enough information for him to reconstruct her initial state.
- Has uses in quantum computing –teleportation plus single qubit operations sufficient for universal quantum computation.

First Experimental Implementations

- D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, "Experimental quantum teleportation", *Nature* **390**, 575 (1997)
- D. Boschi, S. Branca, F. De Martini, L. Hardy and S. Popescu, "Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels", *Physical Review Letters* **80**, 1121 (1998)
- A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble and E. S. Polzik, "Unconditional Quantum Teleportation", *Science* **282**, 706 (1998)
- M. A. Nielsen, E. Knill and R. Laflamme, "Complete quantum teleportation using nuclear magnetic resonance", *Nature* **396**, 52 (1998)

Cryptography – The Caesar Cipher

MEET ME AT EIGHT

+5 ↓

RJJY RJ FY JNLMY

- 5 ↓

MEET ME AT EIGHT

- Not difficult to break.

Cryptography – The Vernam Cipher

Message:

01111100010100011100000

Key:

10001101000111010100001

Encryption: ⬇ XOR

11110001010011001000001

Key:

10001101000111010100001

Decryption: ⬇ XOR

01111100010100011100000

Cryptography – The Vernam Cipher

Message:

01111100010100011100000

Key:

10001101000111010100001

Encryption: ⬇ XOR

11110001010011001000001

Key:

10001101000111010100001

Decryption: ⬇ XOR

01111100010100011100000

Private Key Cryptography

- Alice and Bob must share a secret key
- Key can only be used once
- Problem of communicating securely becomes the problem of distributing (and storing) keys securely.
- Alice and Bob do not know if an eavesdropper Eve has gained access to the key.

Cryptography – The Vernam Cipher

Message:

01111100010100011100000

Key:

10001101000111010100001

Encryption: ⬇ XOR

11110001010011001000001

Key:

10001101000111010100001

Decryption: ⬇ XOR

01111100010100011100000

Private Key Cryptography

- Alice and Bob must share a secret key
- Key can only be used once
- Problem of communicating securely becomes the problem of distributing (and storing) keys securely.
- Alice and Bob do not know if an eavesdropper Eve has gained access to the key.

Public Key Cryptography

- Bob publishes the public key f, making it available to anybody.
- Alice encodes her information using the public key and sends it to Bob.
- Bob has a secret key, f^{-1}, which he uses to decrypt the message.
- f chosen so that given knowledge of f, f^{-1} is difficult to find.
- In principle an eavesdropper has access to the public key f, and the encrypted information.
- Security based on computational complexity of f^{-1}.

Private Key Cryptography

- Alice and Bob must share a secret key
- Key can only be used once
- Problem of communicating securely becomes the problem of distributing (and storing) keys securely.
- Alice and Bob do not know if an eavesdropper Eve has gained access to the key.

Public Key Cryptography

- Bob publishes the public key f, making it available to anybody.
- Alice encodes her information using the public key and sends it to Bob.
- Bob has a secret key, f^{-1}, which he uses to decrypt the message.
- f chosen so that given knowledge of f, f^{-1} is difficult to find.
- In principle an eavesdropper has access to the public key f, and the encrypted information.
- Security based on computational complexity of f^{-1}.

Public Key Cryptography - RSA

- Bob chooses two large prime numbers p and q, and computes pq=N.
- Bob chooses at random a number d that is co-prime with (p-1)(q-1).
- Bob computes e, such that

$$ed|_{\text{mod } (p-1)(q-1)} = 1.$$

- The pair (e,N) forms the public key, the pair (d,N) forms the private key.
- Alice encodes a message m < N as follows:

$$f(m) = m^e|_{\text{mod } N}$$

- Bob decodes the message by applying his secret key

$$f^{-1}(f(m)) = (f(m))^d|_{\text{mod } N} = m^{ed}|_{\text{mod } N} = m$$

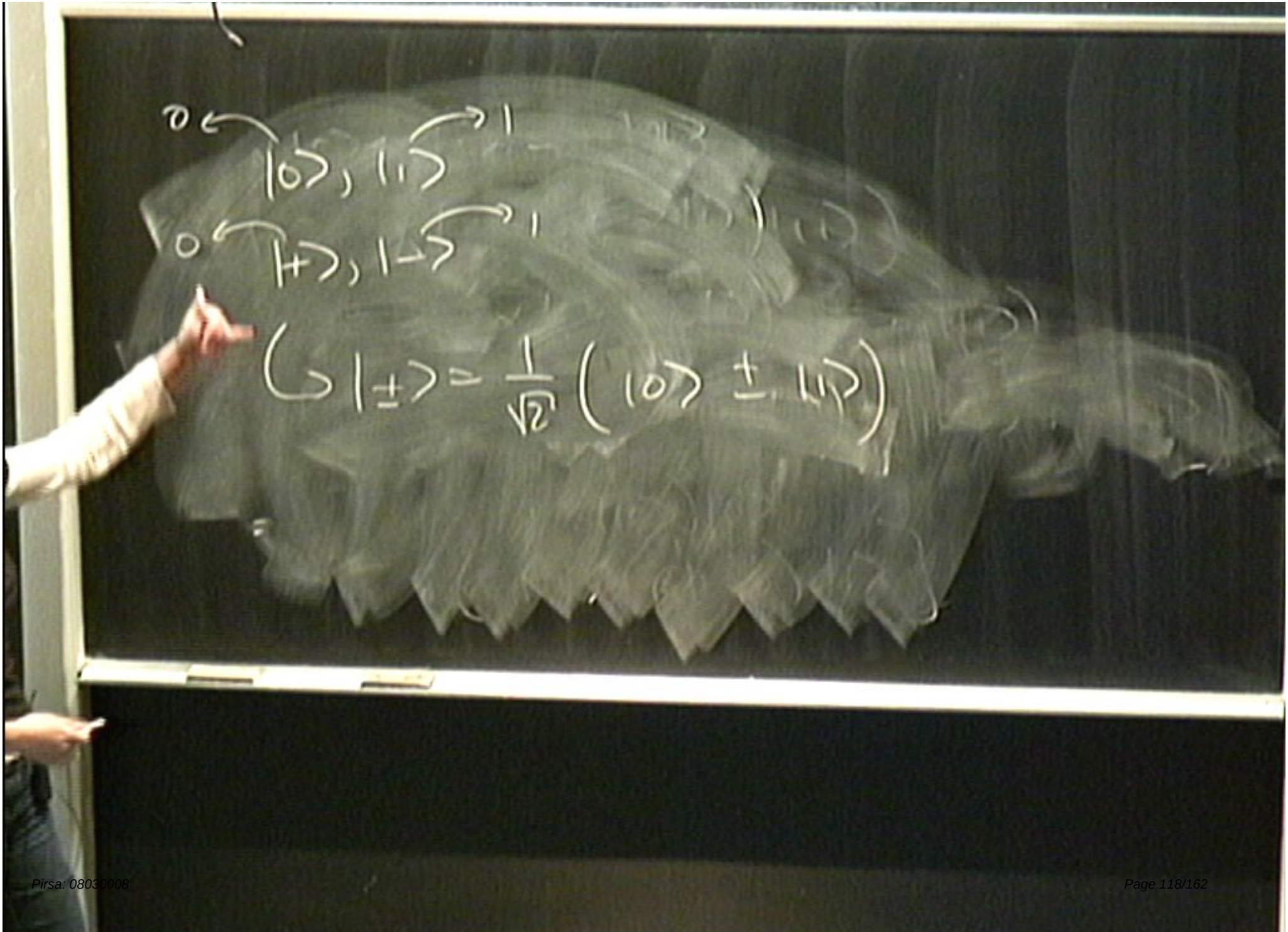
Quantum Key Distribution: BB84 Protocol

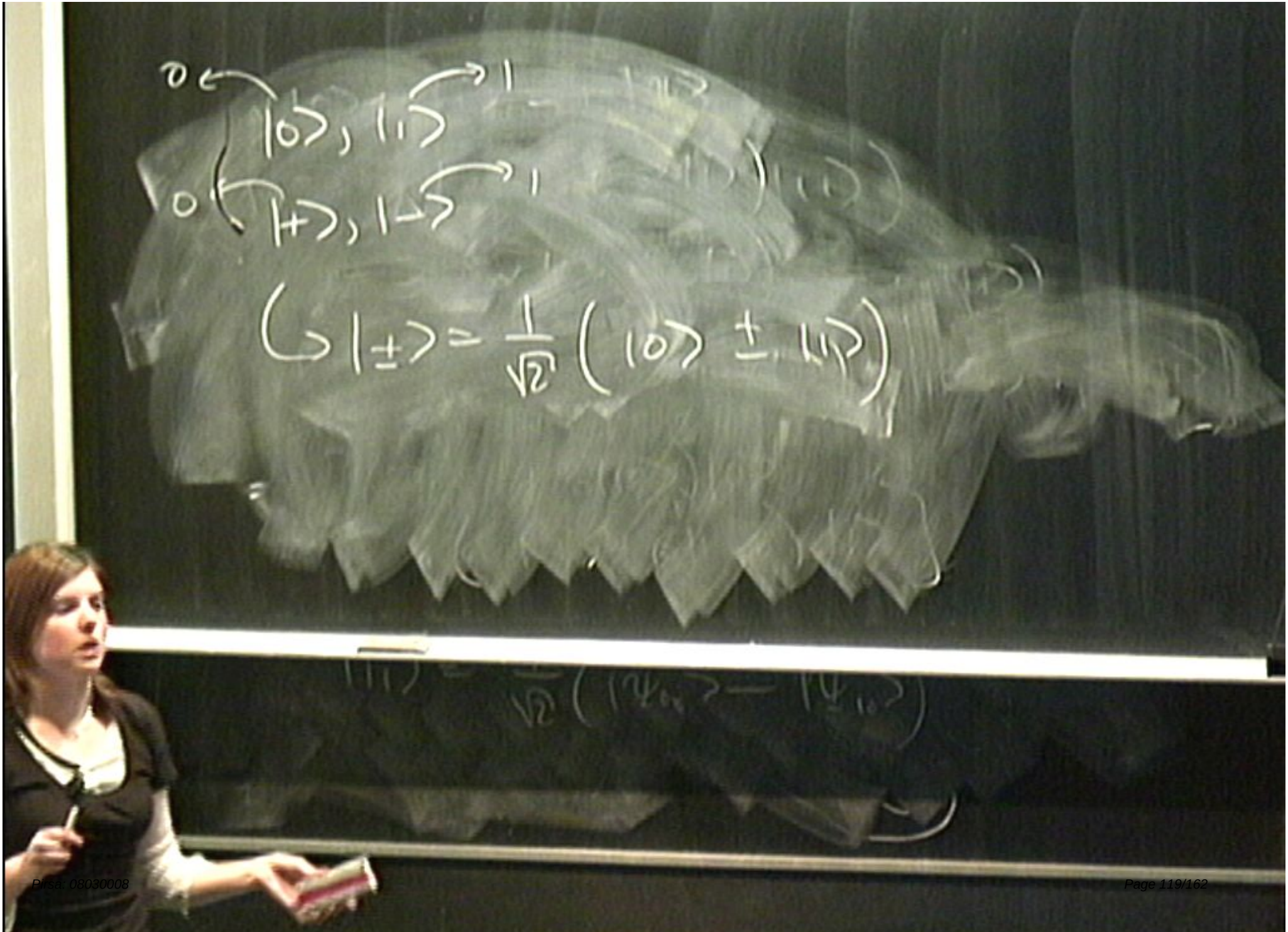
- Alice chooses at random in which basis to encode her information, and sends a quantum state to Bob.
- Bob chooses at random in which basis to measure.
- Basis reconciliation: over a public classical channel, Alice and Bob announce the bases.
- Whenever they both chose the same basis, they keep the corresponding bit. This forms a shared bit string, and they discard all other bits.
- Alice and Bob check a subset of their shared bit string.
- An eavesdropper introduces errors into the shared bit string and thus can be detected.

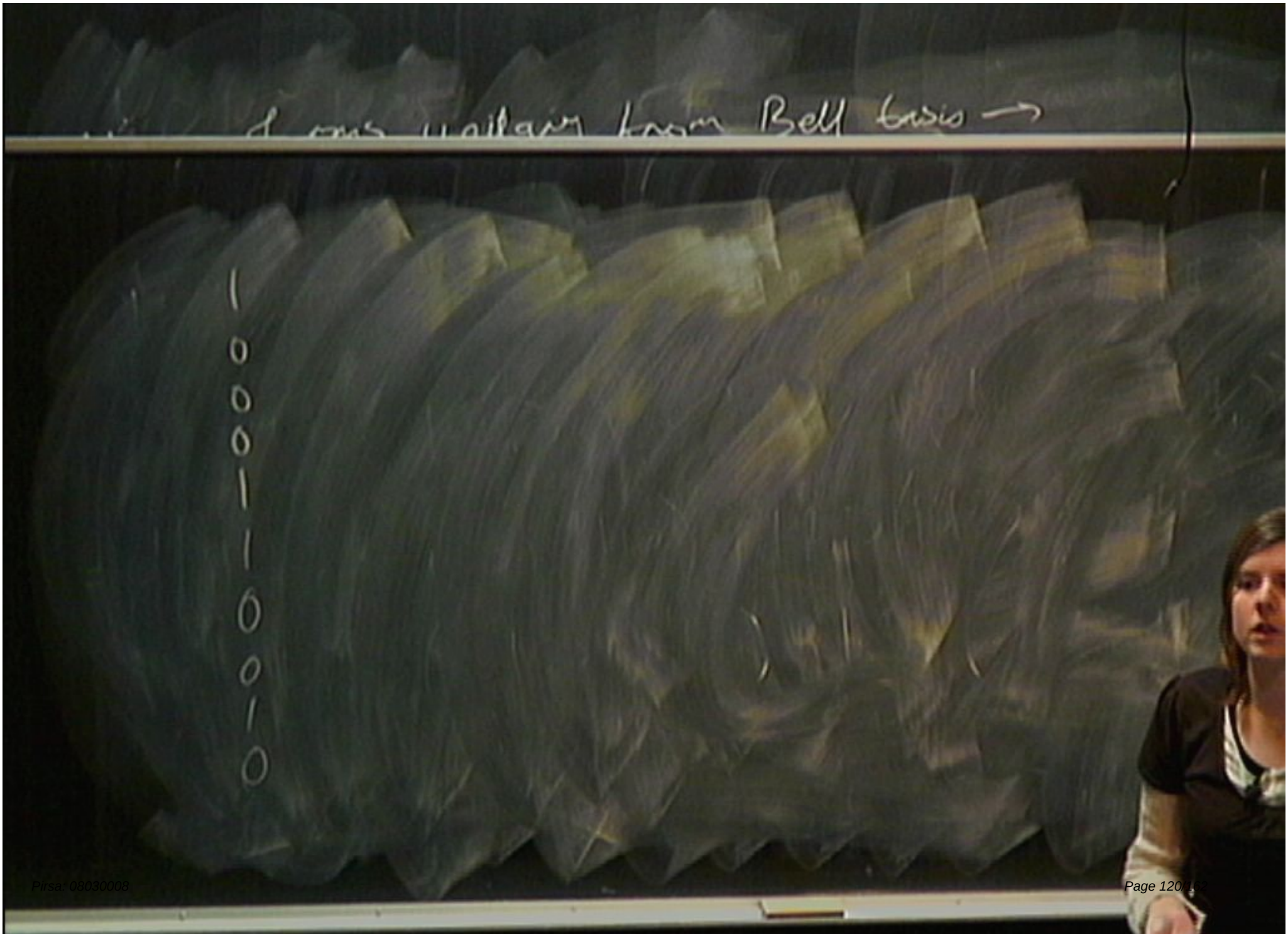
$|0\rangle, |1\rangle$

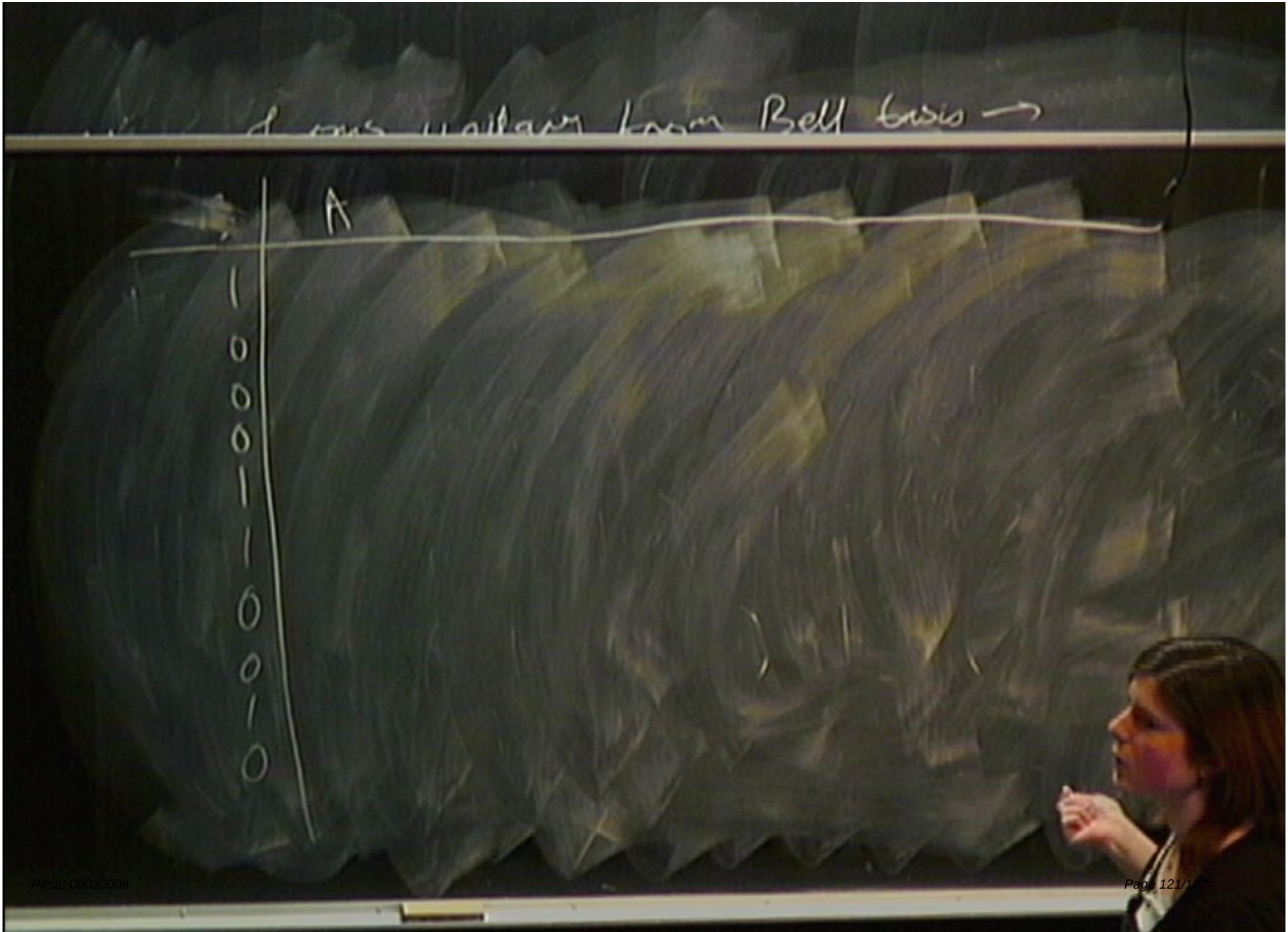
$|+\rangle, |-\rangle$

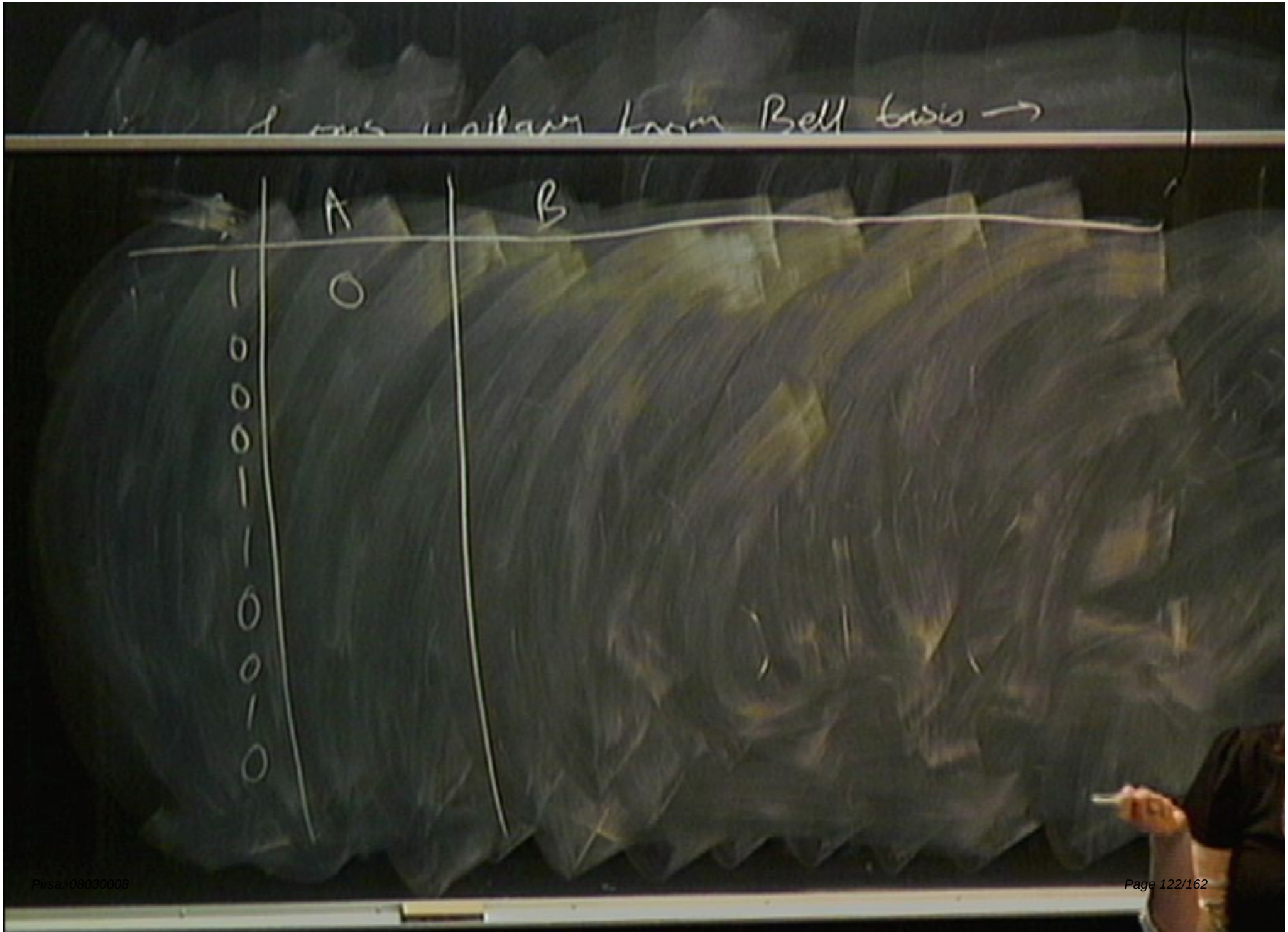
$\Rightarrow |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

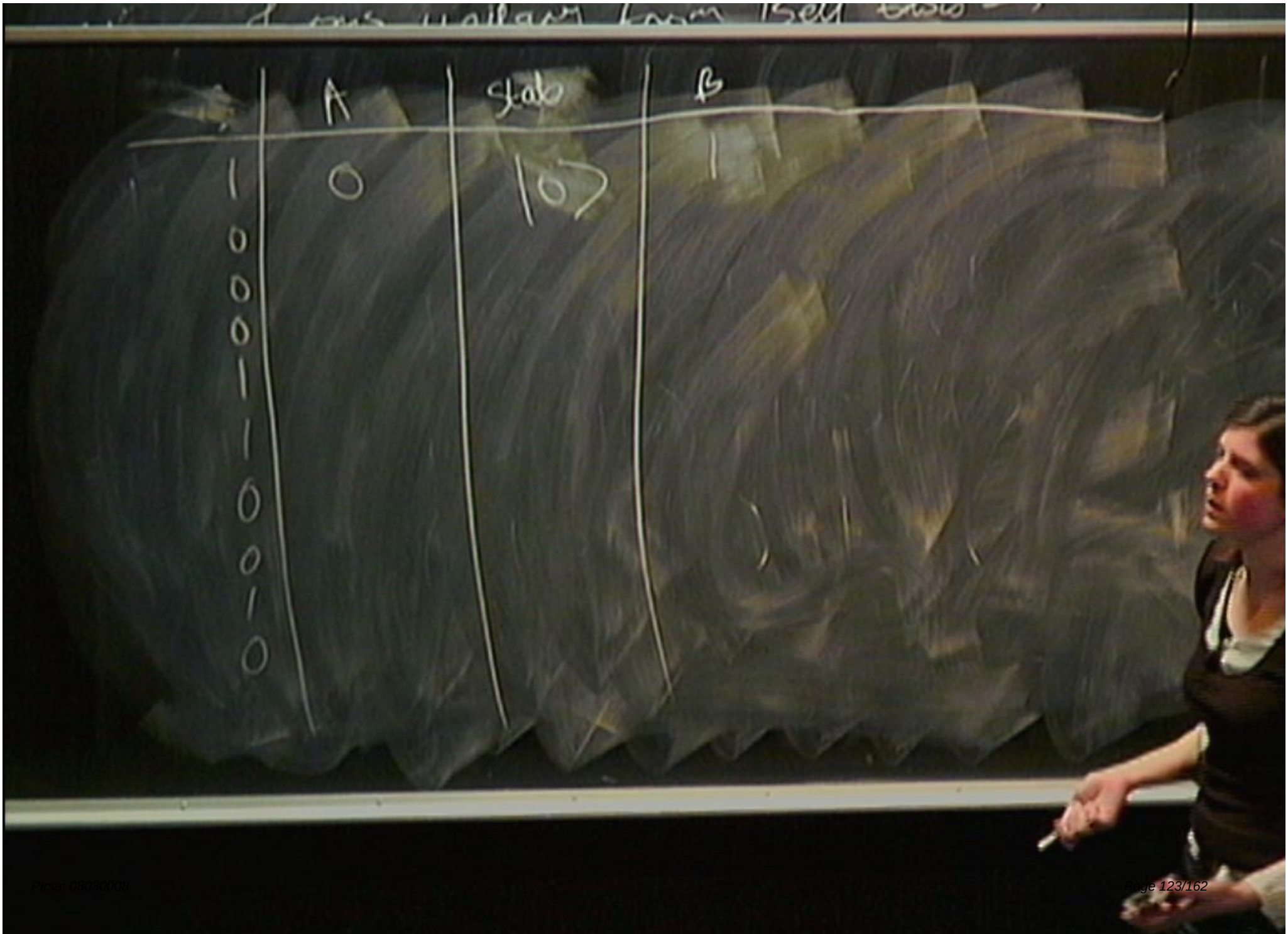

0 ← |0⟩, |1⟩ → 1
0 ← |+⟩, |−⟩ → 1
$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

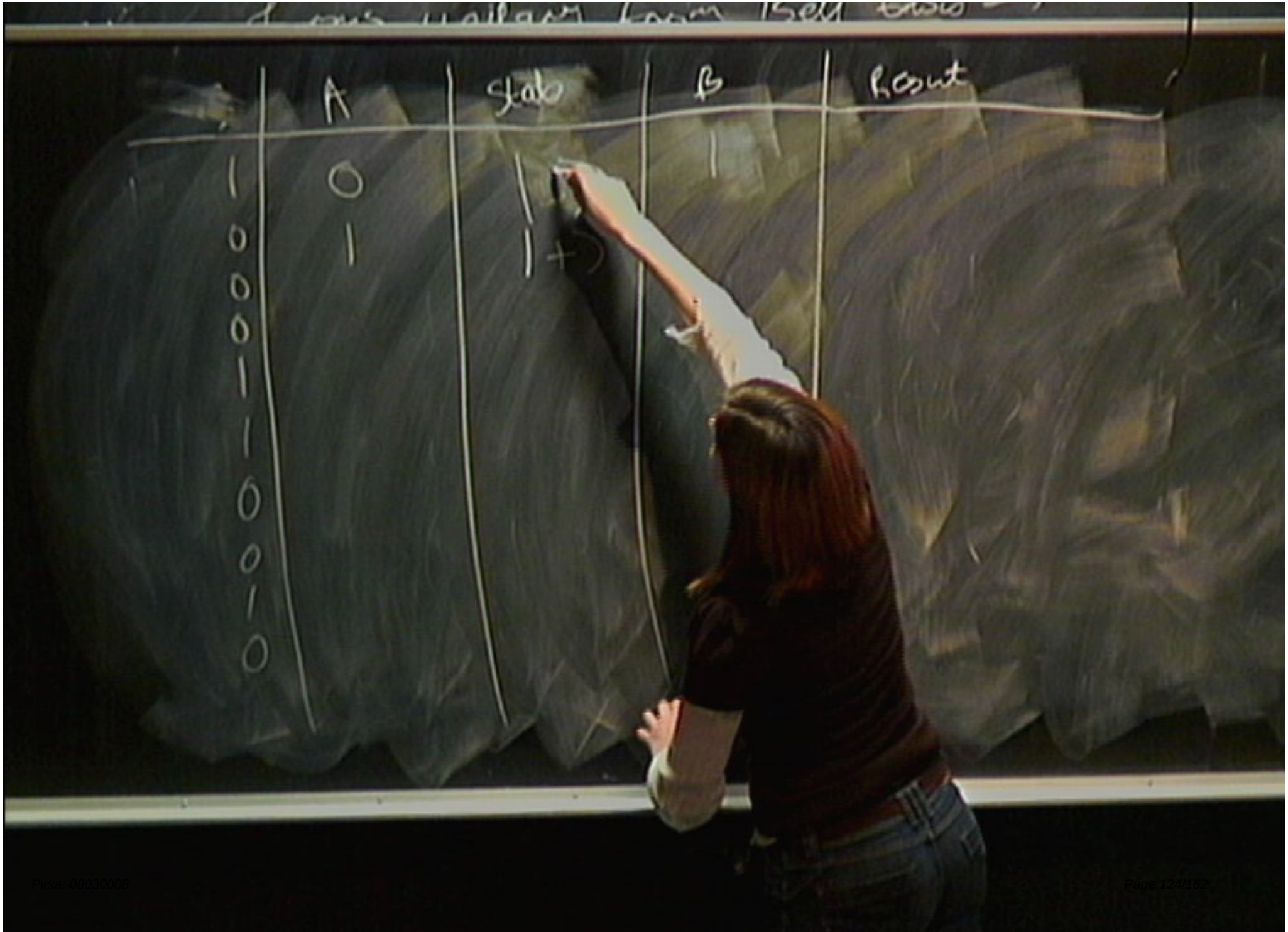

0 ← |0⟩, |1⟩ → 1
0 ← |+⟩, |−⟩ → 1
$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

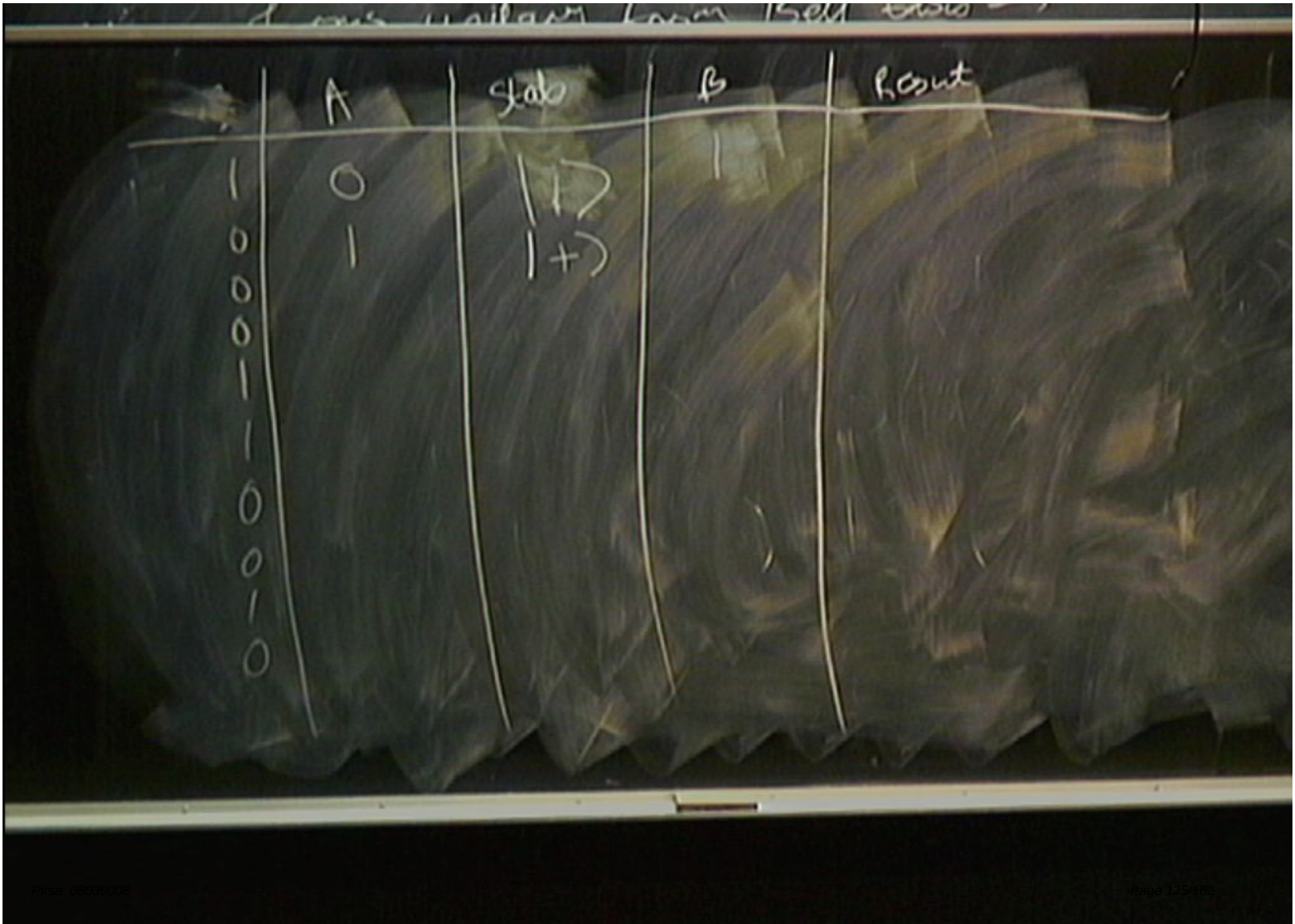

1
0
0
1
1
0
0
1
0

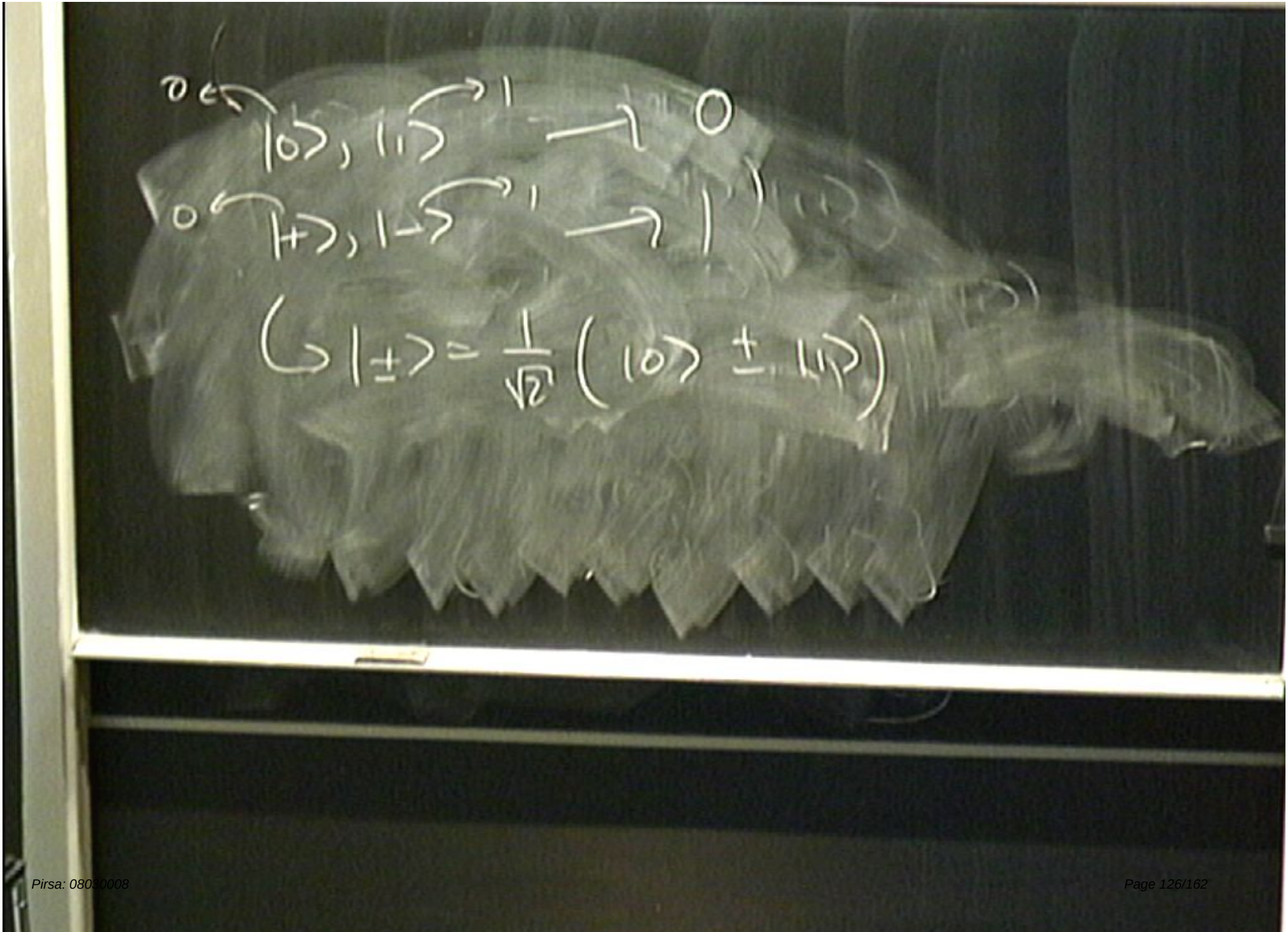

Bell basis
1 0 0 1 1 0 0 1 0


A
B
0
0
0
0
1
1
0
0
1
0


A
Slab
B
|0⟩
|1⟩


A
Slab
B
Rout

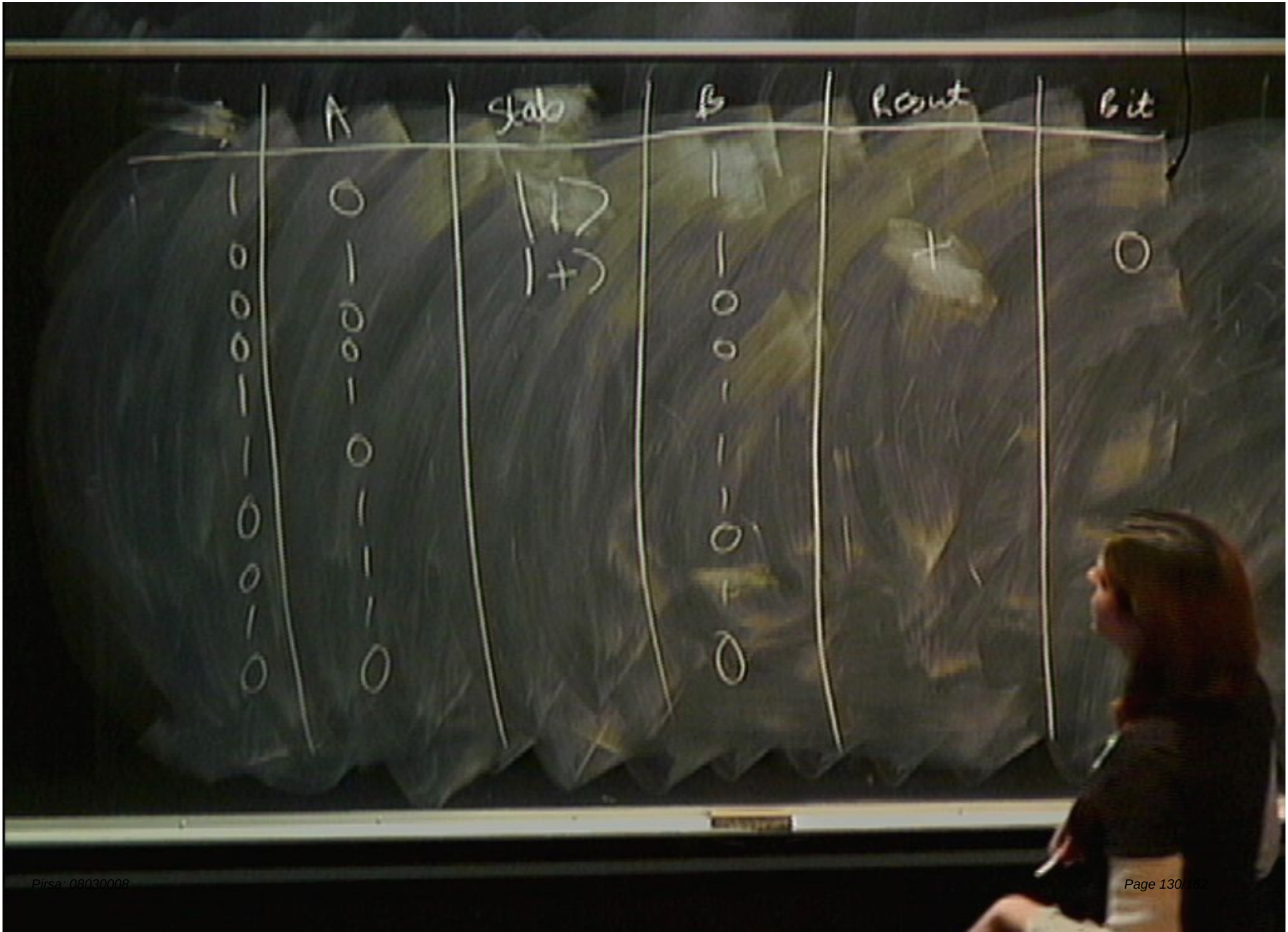

A
Slab
B
Rout
1
0
0
0
1
1
0
0
1
0
|1⟩
|+⟩


0 ← |0⟩, |1⟩ → 1 → 0
0 ← |+⟩, |−⟩ → 1 → 1
$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

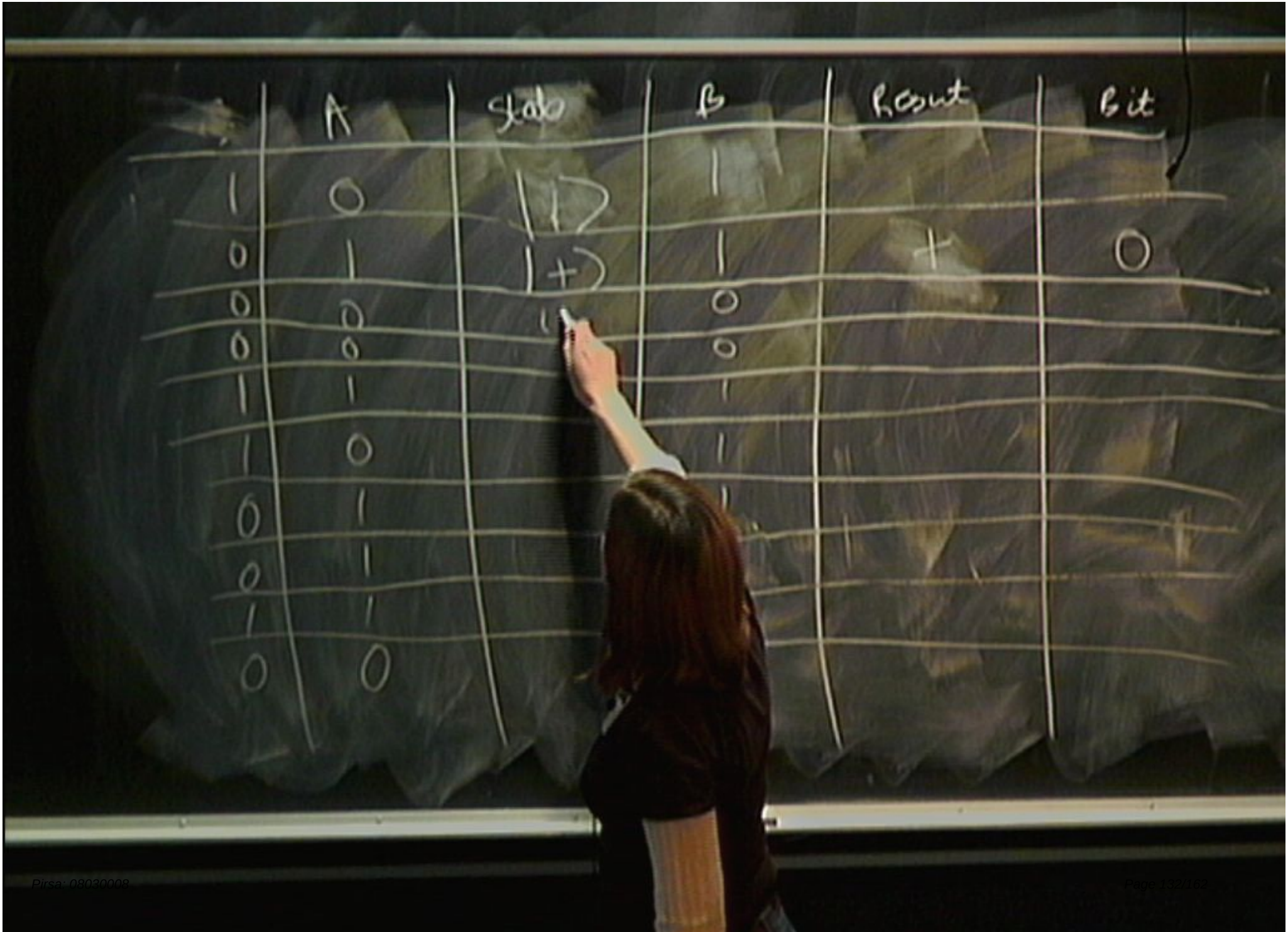

A
Slab
B
Rout
1 0 0 0 1 1 0 0 1 0
0
1
|1>
|+>
1
1
0


A
Slab
B
Result
Bit
1
0
1
0
0
0
1
1
0
0
1
0
1
0
1
+
0

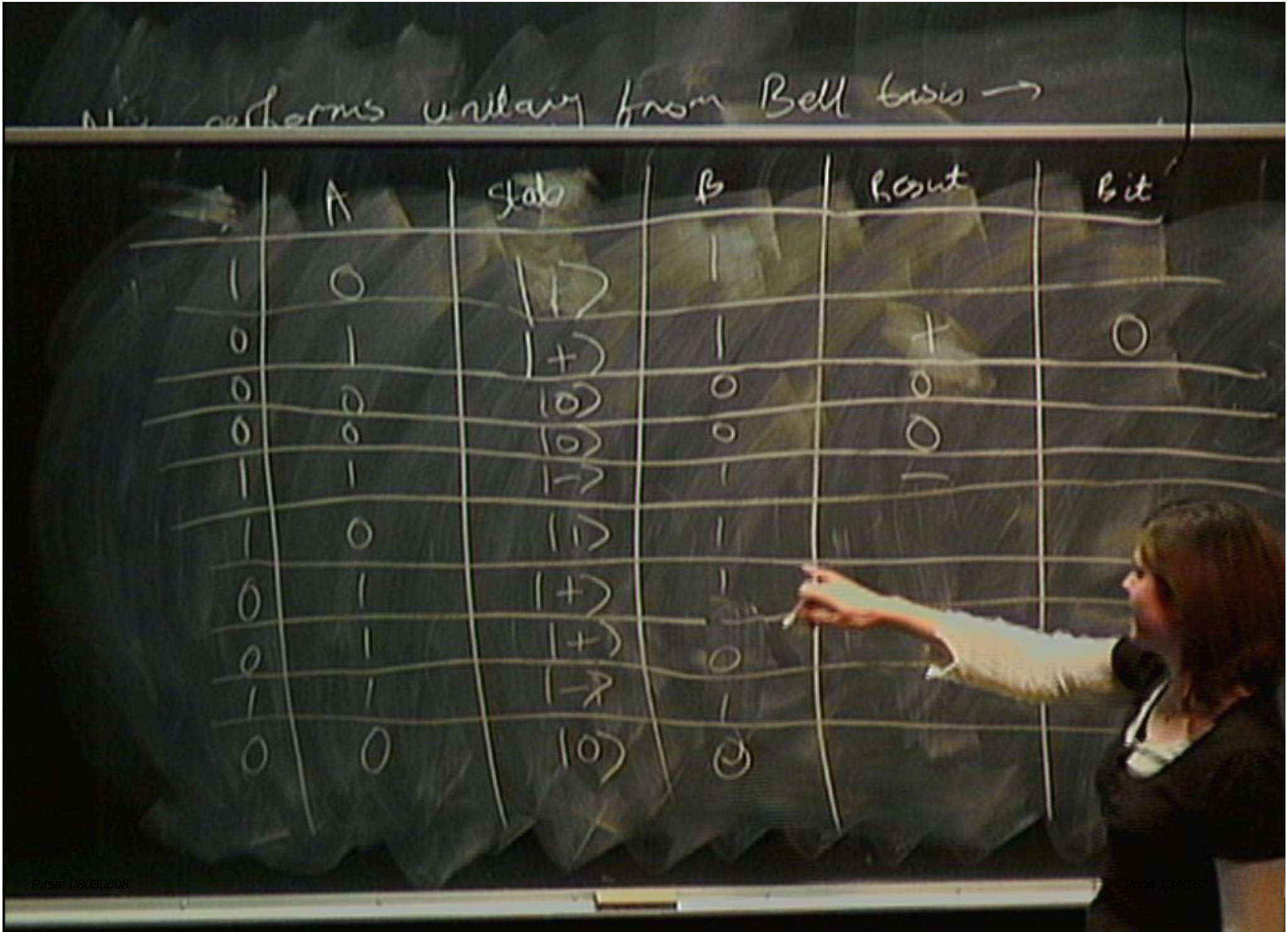

A
Slab
B
Rout
Bit
0
1
+
0


A
Sabo
B
Result
Bit


A
Sdab
B
Bout
Bit


A
Sabo
B
Rout
Bit


A
Sum
B
Bout
Bit

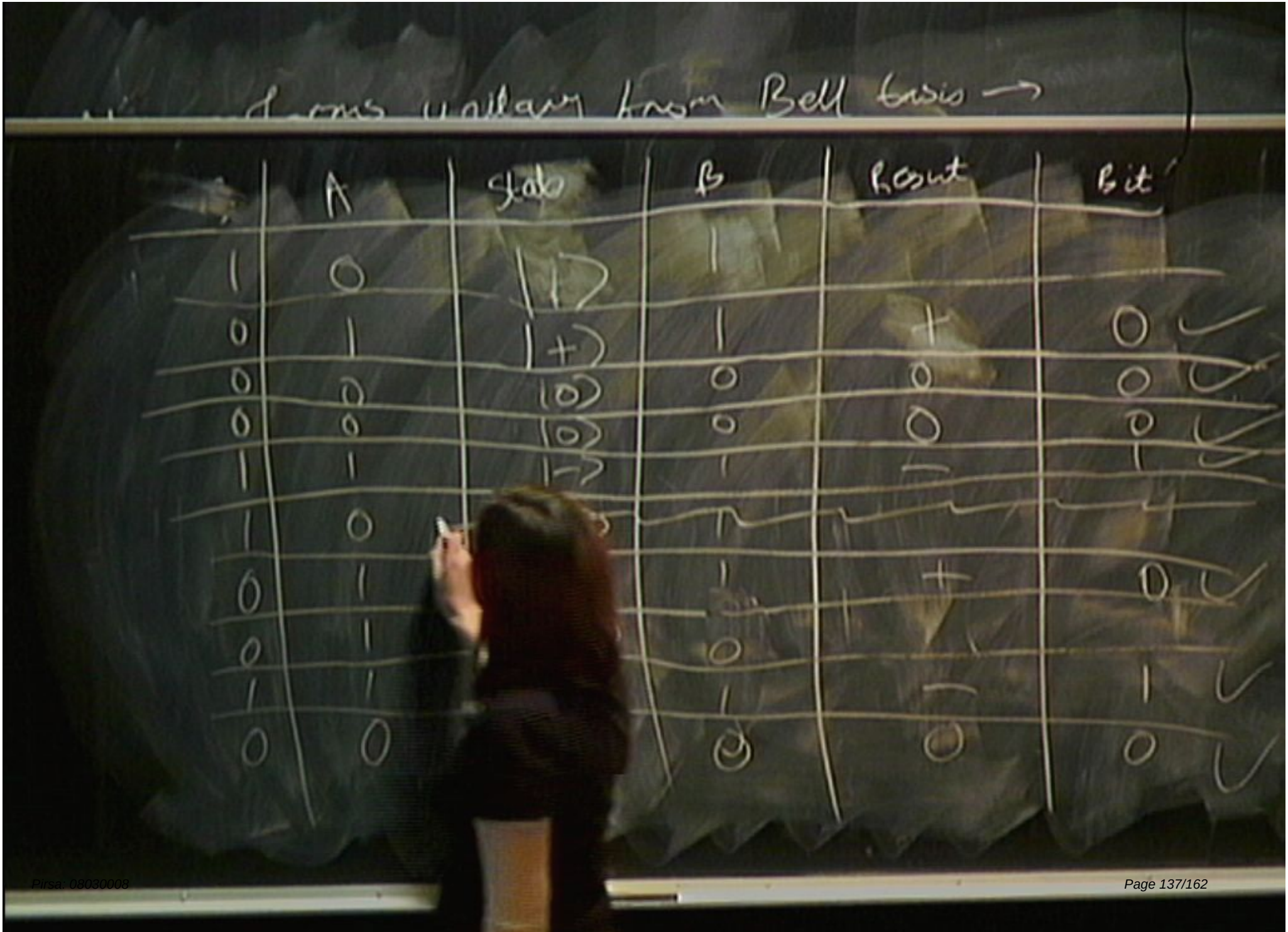

Bell basis →
A
Stab
B
Rout
Bit

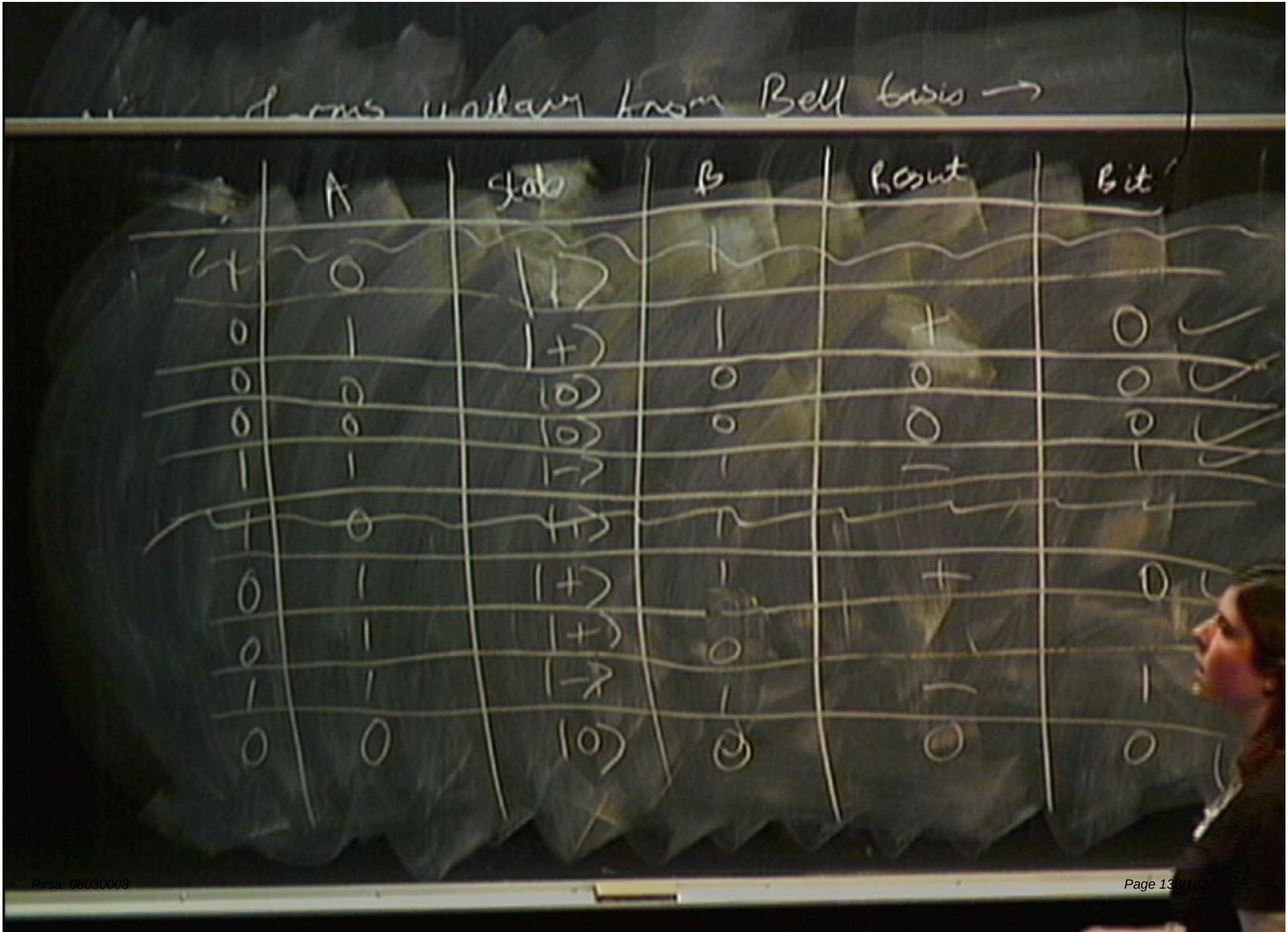
No collapse unless from Bell basis →

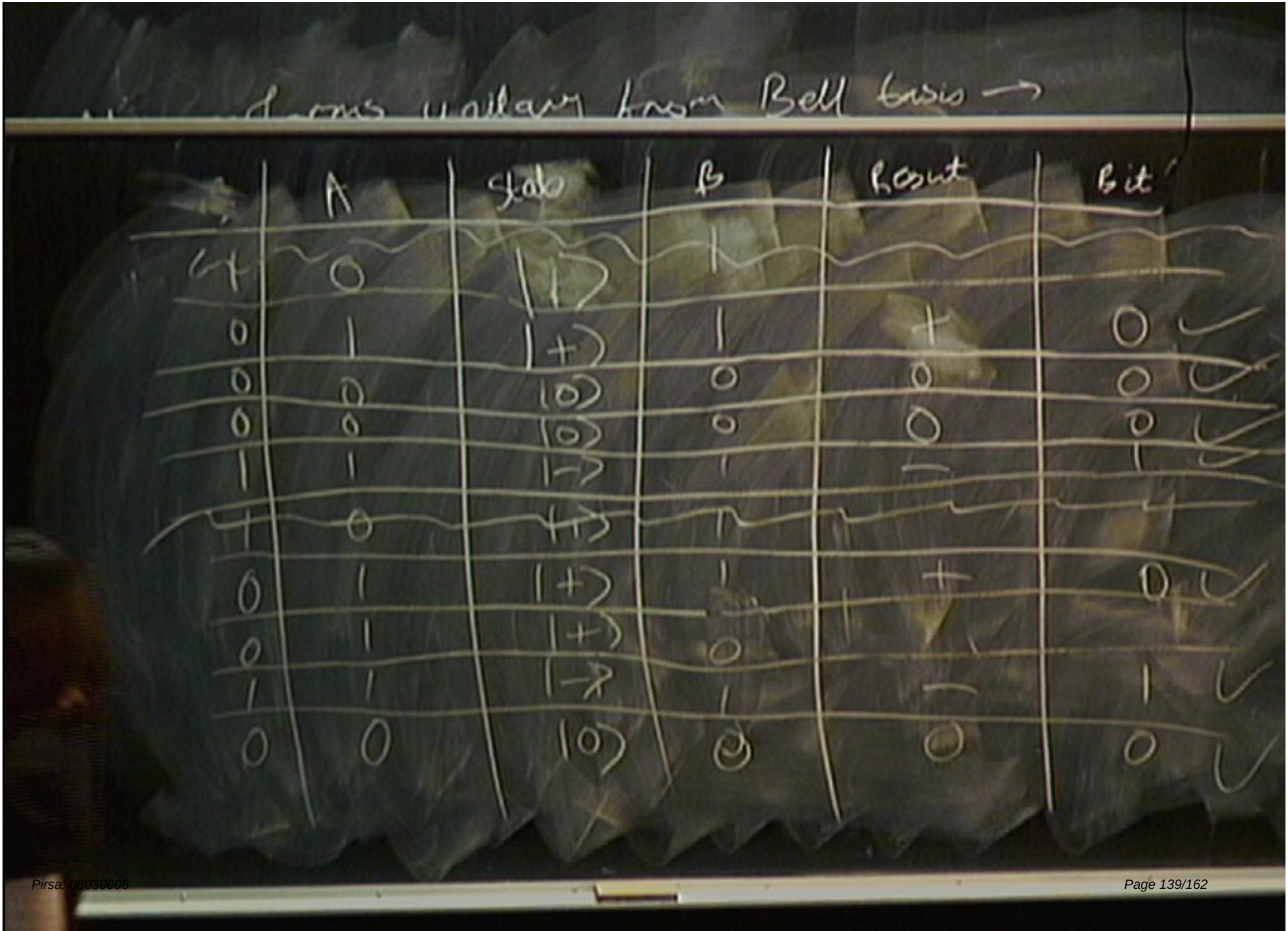
	A	state	B	Result	Bit
1	0	$\|1\rangle$	1		
0	1	$\|+\rangle$	1	+	0
0	0	$\|0\rangle$	0	0	0
0	0	$\|0\rangle$	0	0	0
1	-	$\|-\rangle$	1	-	1
1	0	$\|1\rangle$	1		
0	1	$\|+\rangle$	1	+	1
0	1	$\|+\rangle$	0	+	1
1	1	$\|-\rangle$	1	-	1
0	0	$\|0\rangle$	0	0	

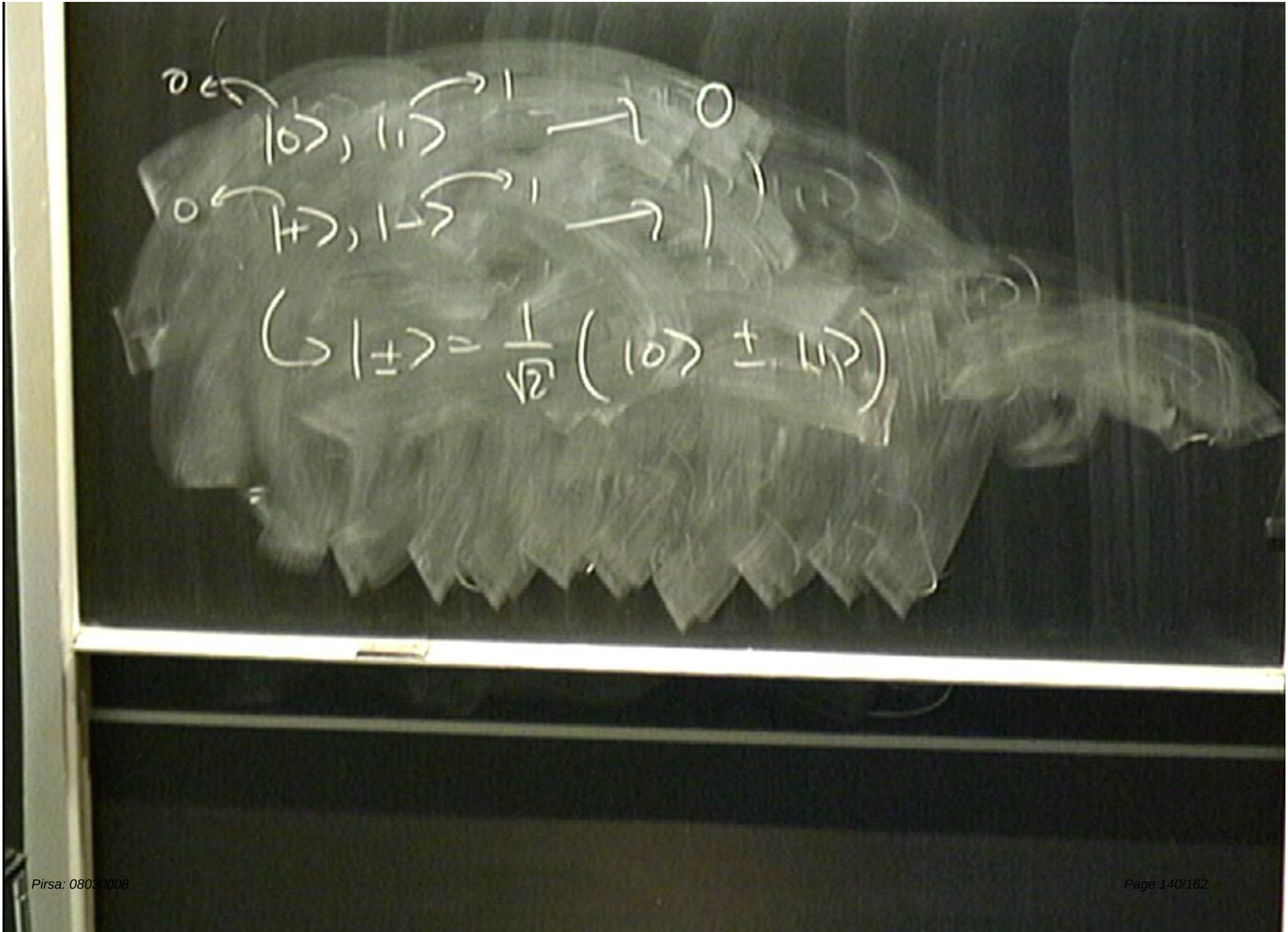
... outcomes obtain from Bell basis →

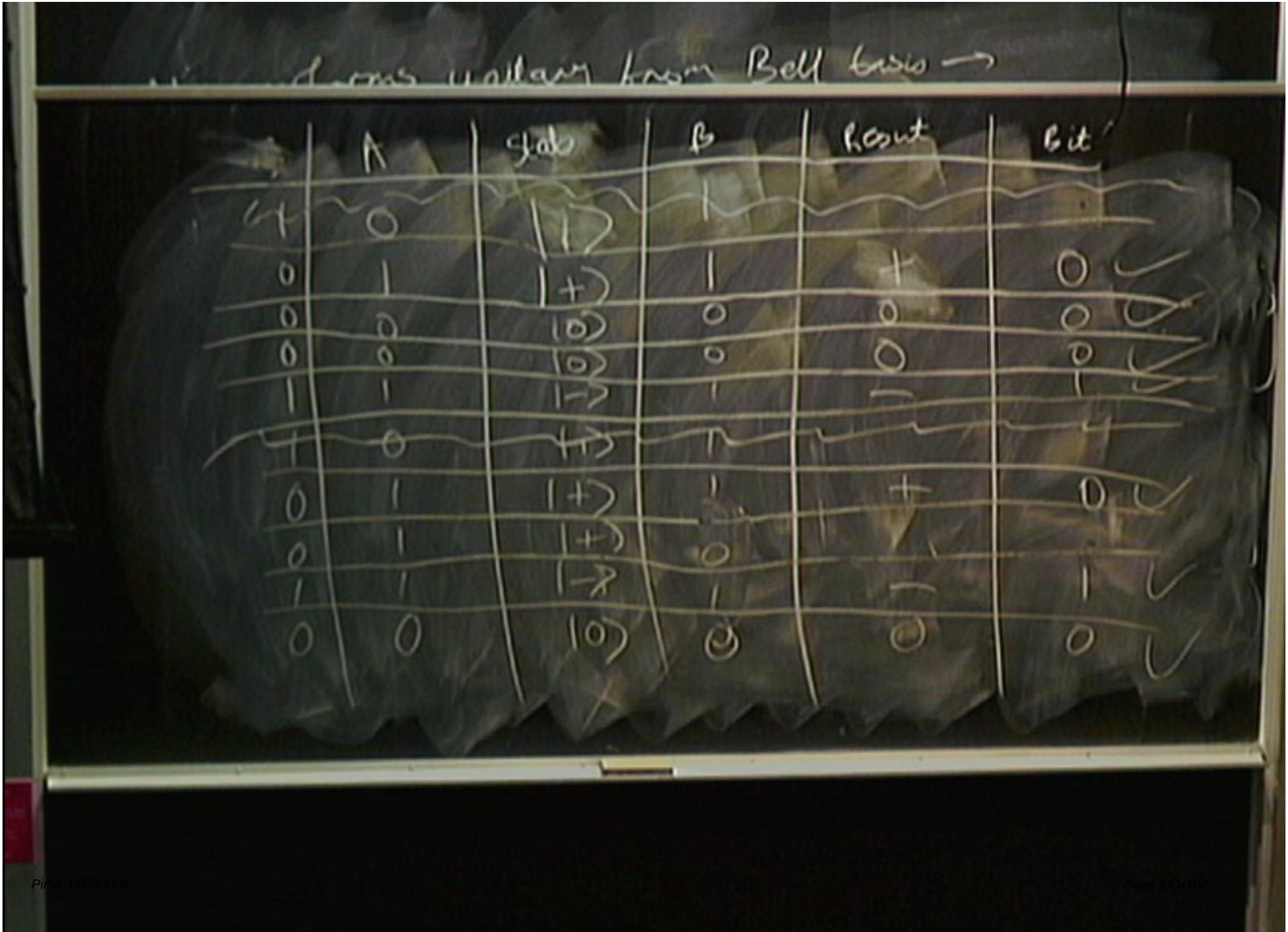
	A	state	B	Rout	Bit
1	0	$\|1\rangle$	1		
0	1	$\|+\rangle$	1	+	0
0	0	$\|0\rangle$	0	0	0
0	0	$\|0\rangle$	0	0	0
1	1	$\|-\rangle$	1	−	1
1	0	$\|1\rangle$	1		
0	1	$\|+\rangle$	1	+	1
0	1	$\|+\rangle$	0		
1	1	$\|-\rangle$	1	−	1
0	0	$\|0\rangle$	0	0	0

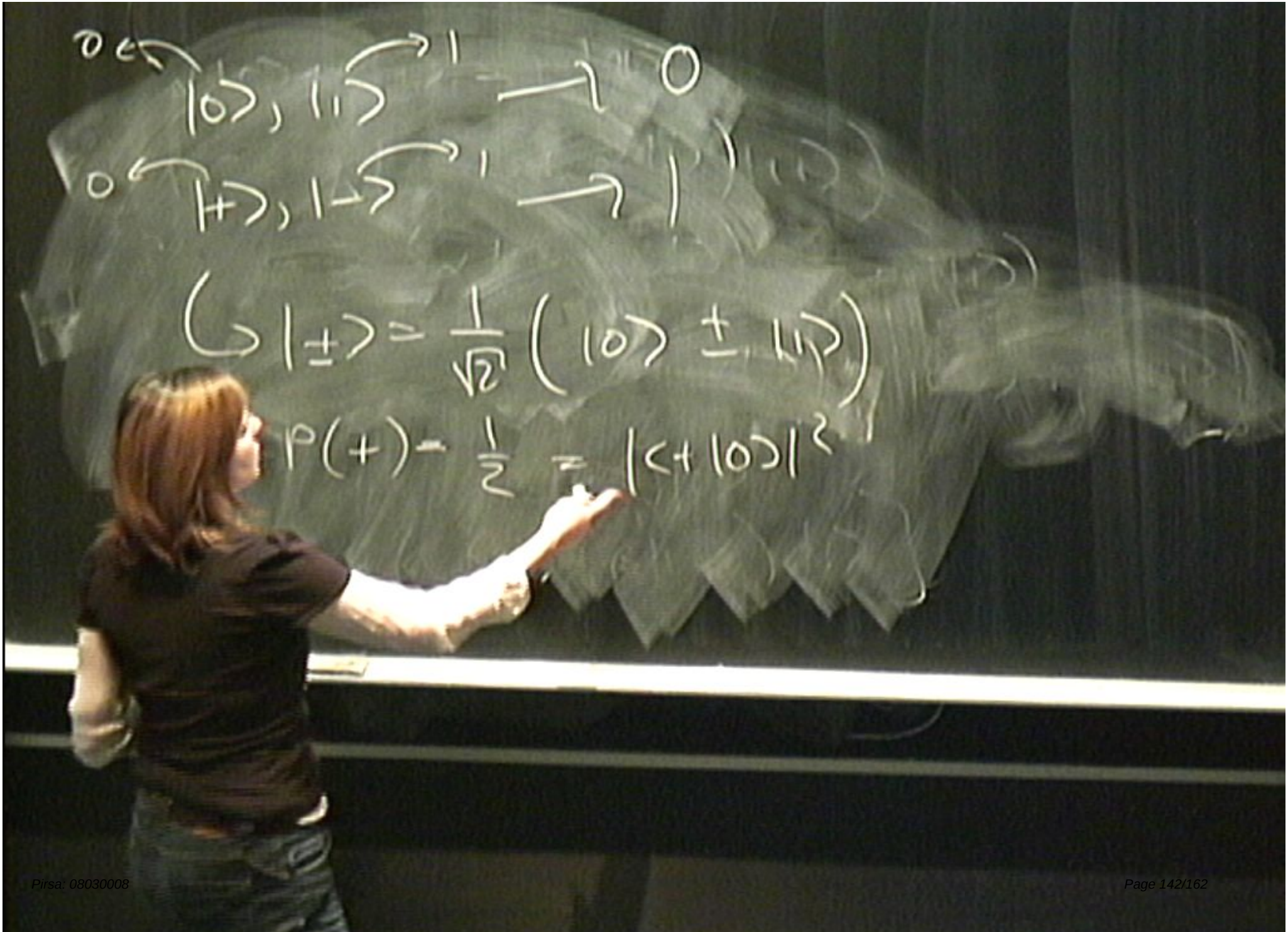

Bell basis →
A
State
B
Result
Bit

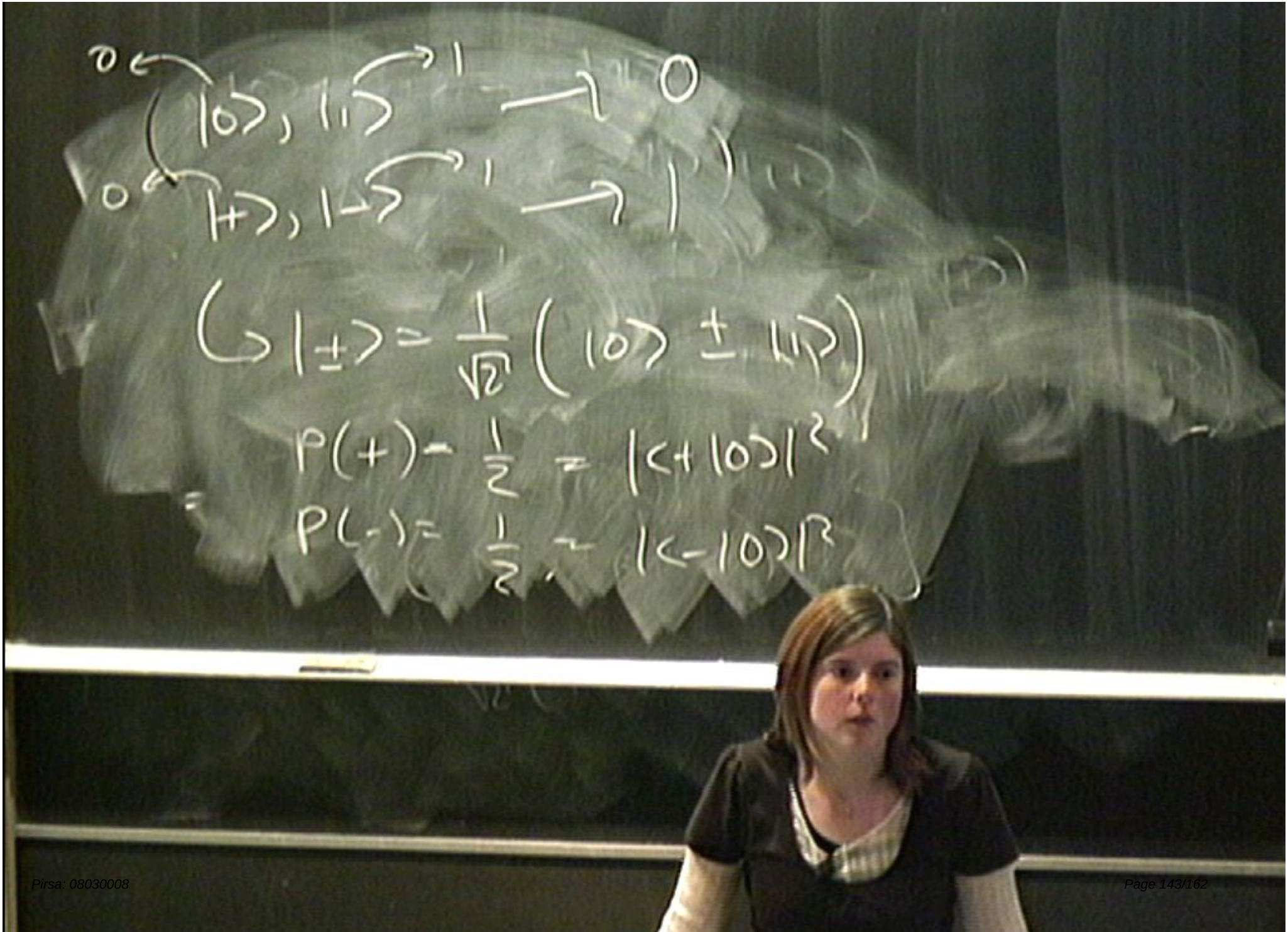

Bell basis →
A
state
B
Result
Bit
Pirsa: 08030008
Page 138/162


Bell basis →
A
state
B
Result
Bit


0 ← |0⟩, |1⟩ → 1 → 0
0 ← |+⟩, |−⟩ → 1 → 1
↳ |±⟩ = 1/√2 (|0⟩ ± |1⟩)

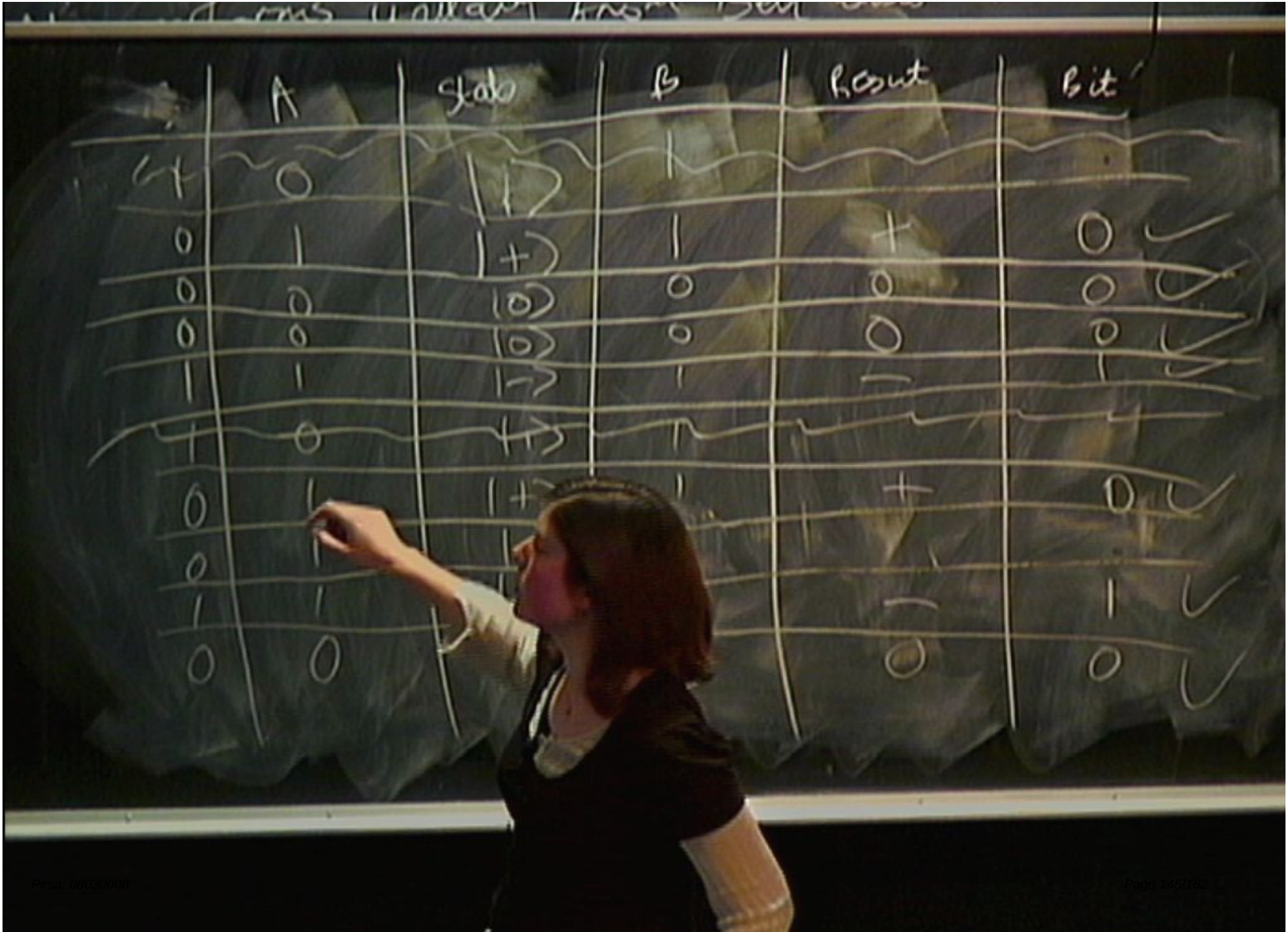

Bell basis →
A
Label
B
Result
Bit


0 ← |0⟩, |1⟩ → 1 → 0
0 ← |+⟩, |−⟩ → 1 → 1
|±⟩ = 1/√2 (|0⟩ ± |1⟩)
P(+) = 1/2 = |⟨+|0⟩|²


0 ← |0⟩, |1⟩ → 1 → 0
0 ← |+⟩, |−⟩ → 1 → 1
↳ |±⟩ = 1/√2 (|0⟩ ± |1⟩)
P(+) = 1/2 = |⟨+|0⟩|²
P(−) = 1/2 = |⟨−|0⟩|²

Quantum Key Distribution: BB84 Protocol

- Alice chooses at random in which basis to encode her information, and sends a quantum state to Bob.
- Bob chooses at random in which basis to measure.
- Basis reconciliation: over a public classical channel, Alice and Bob announce the bases.
- Whenever they both chose the same basis, they keep the corresponding bit. This forms a shared bit string, and they discard all other bits.
- Alice and Bob check a subset of their shared bit string.
- An eavesdropper introduces errors into the shared bit string and thus can be detected.


A
Sum
B
Bout
Bit

Quantum Key Distribution: BB84 Protocol

- Alice chooses at random in which basis to encode her information, and sends a quantum state to Bob.
- Bob chooses at random in which basis to measure.
- Basis reconciliation: over a public classical channel, Alice and Bob announce the bases.
- Whenever they both chose the same basis, they keep the corresponding bit. This forms a shared bit string, and they discard all other bits.
- Alice and Bob check a subset of their shared bit string.
- An eavesdropper introduces errors into the shared bit string and thus can be detected.

Quantum key Distribution: E91 Protocol

- Alice and Bob share Bell states (from a common source, or e.g. Alice creates entangled states and sends one of each pair to Bob).
- Alice and Bob each choose at random whether to measure the x,y or z directions of spin.
- Basis reconciliation; Alice and Bob announce the bases used, and divide their bits into two groups –those in which they used the same basis and those in which they used different bases.
- In the subset in which they used different bases they check that their results give maximum violation of Bell's inequality. If they do not they conclude there was some noise or eavesdropping on the channel.
- The remaining bits form the private shared key.
- This protocol may be useful in the future for key storage.

Error Correction and Privacy Amplification

- In any experimental implementation there will always be errors introduced in the channel.
- Assume that all errors are due to Eve.
- If the error rate is too high, abort the protocol and try again.
- If the error rate is acceptable, use error correction and privacy amplification to distill a secure key.

Error Correction and Privacy Amplification

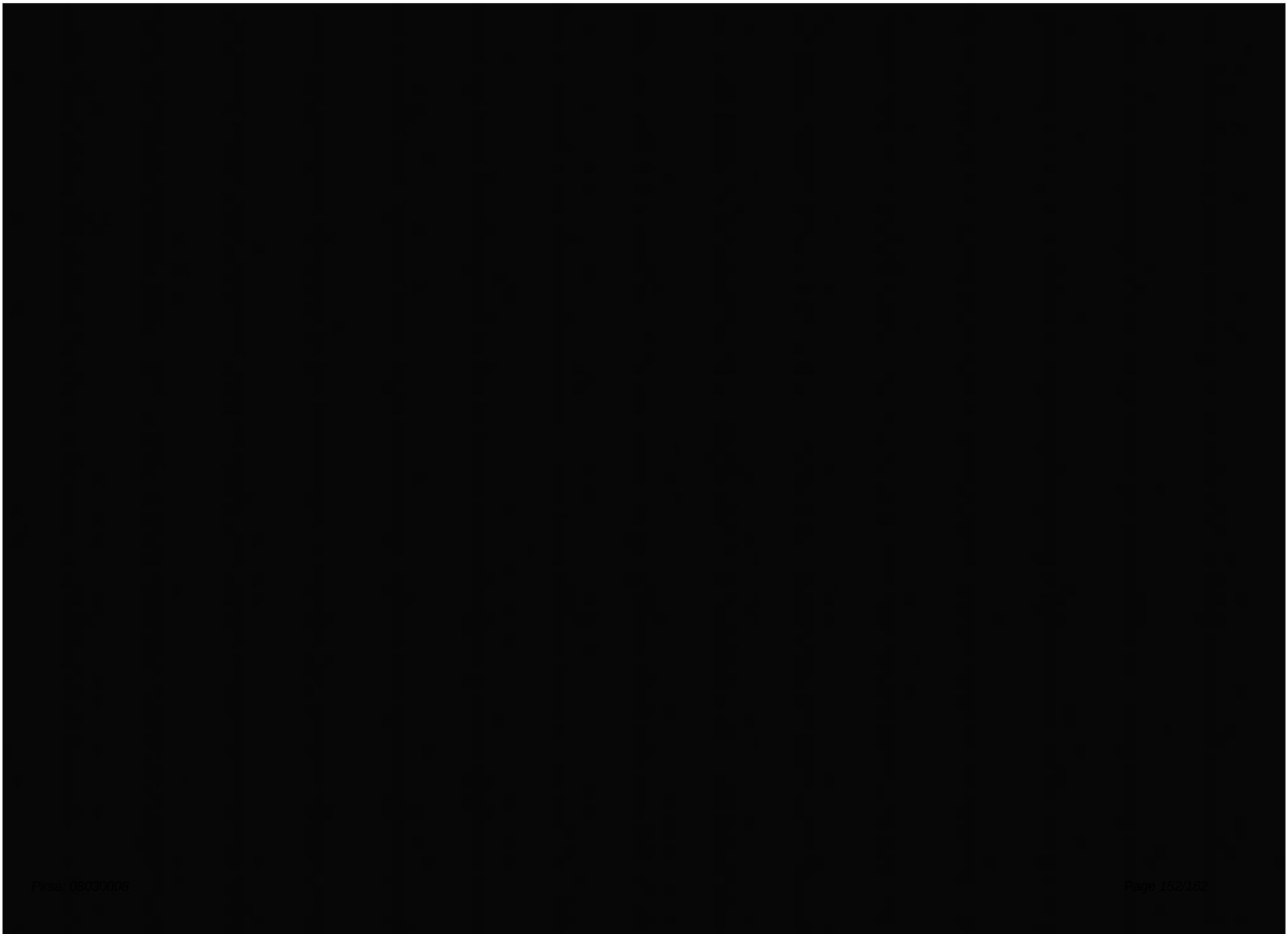
- In any experimental implementation there will always be errors introduced in the channel.
- Assume that all errors are due to Eve.
- If the error rate is too high, abort the protocol and try again.
- If the error rate is acceptable, use error correction and privacy amplification to distill a secure key.

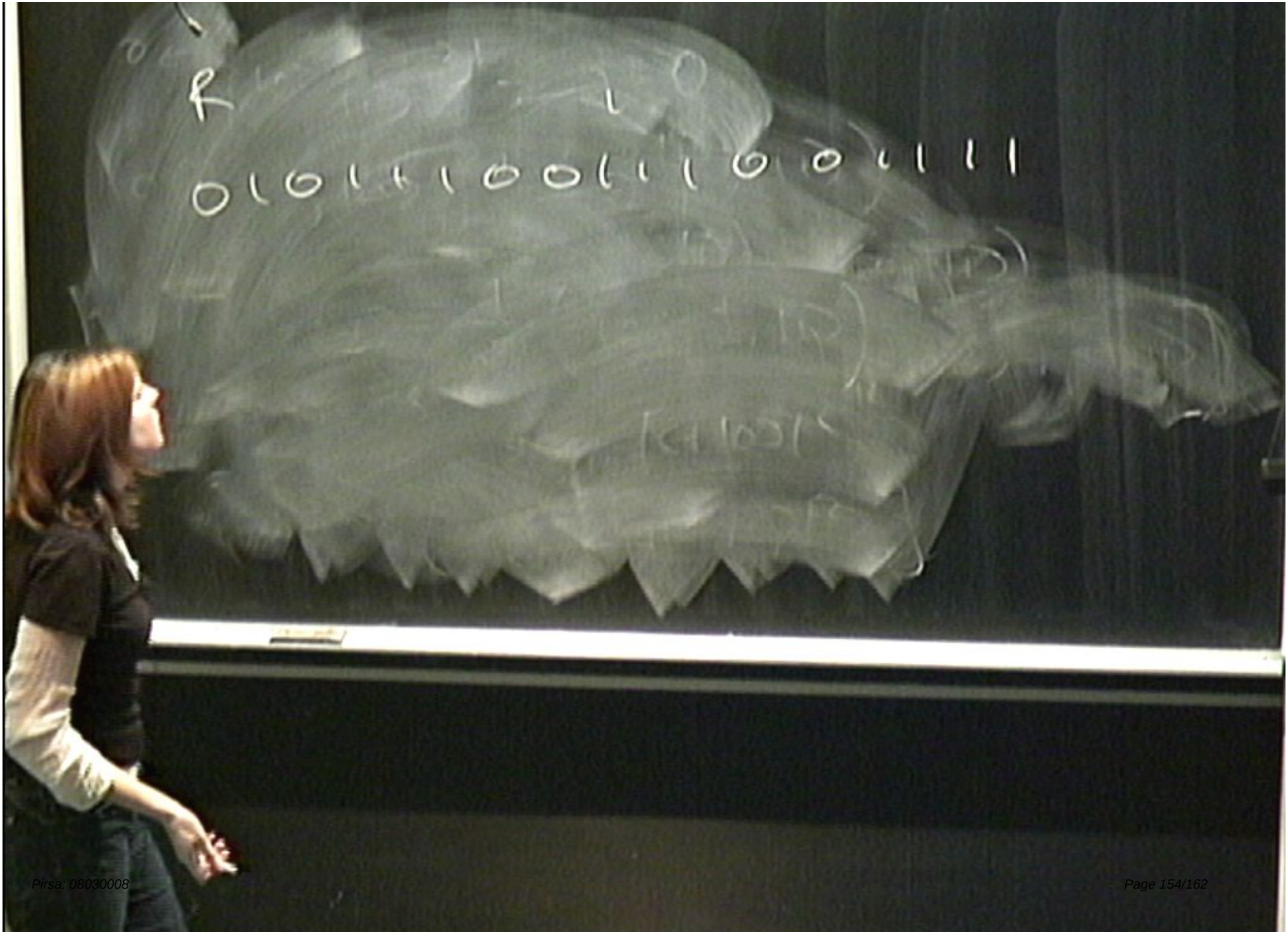
Experimental Implementations

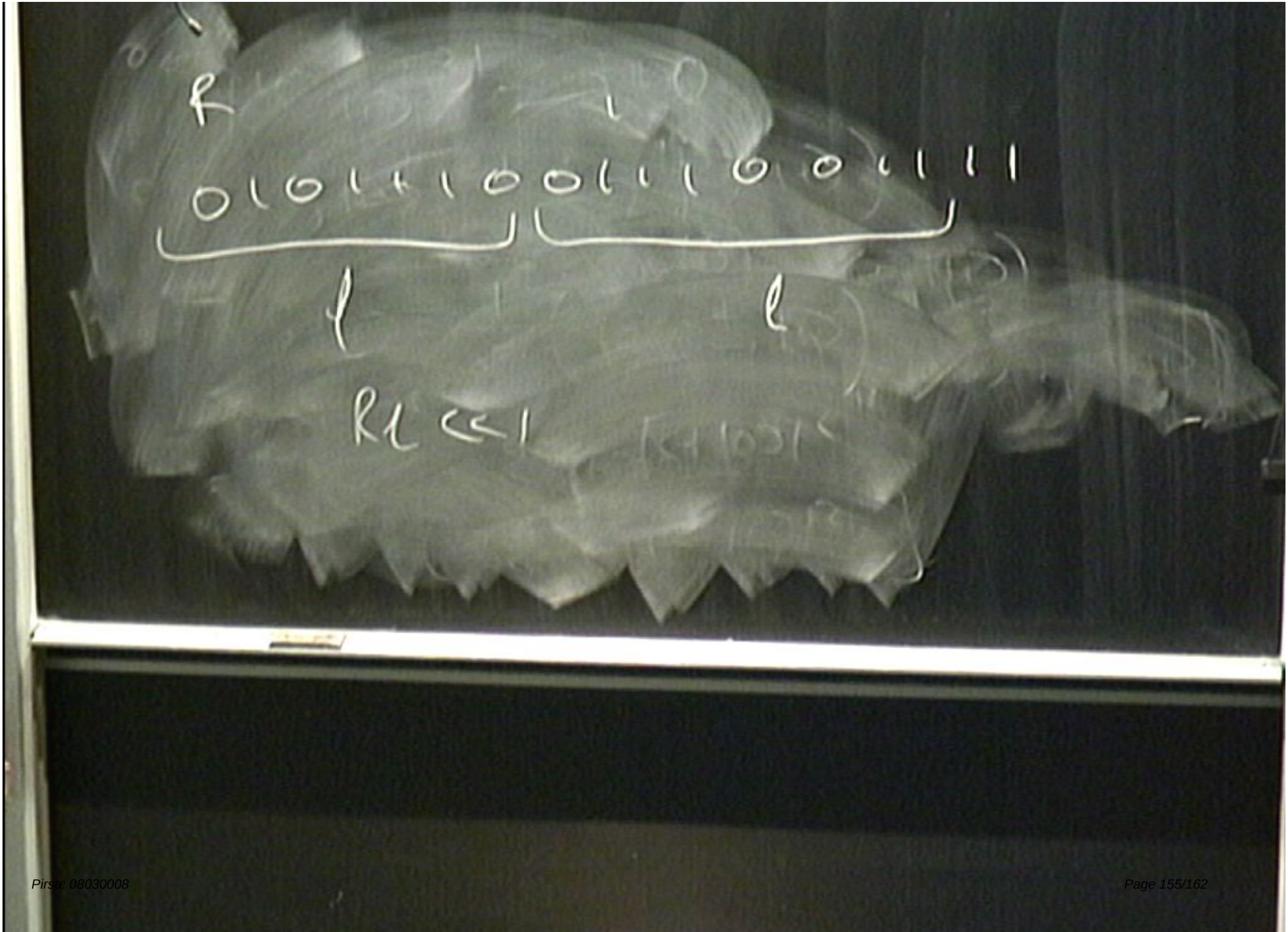
- See Gisin et al, 2002 for a review of the development of QKD.
- Fibre based: over 148.7 km in Los Alamos (2006).
- Free-space: 144km, between two of the Canary Islands (2006).
- First bank transfer using quantum cryptography took place in Austria in 2004!
- Some companies now offering commercial QKD systems. May be the first commercial use of quantum information theory.

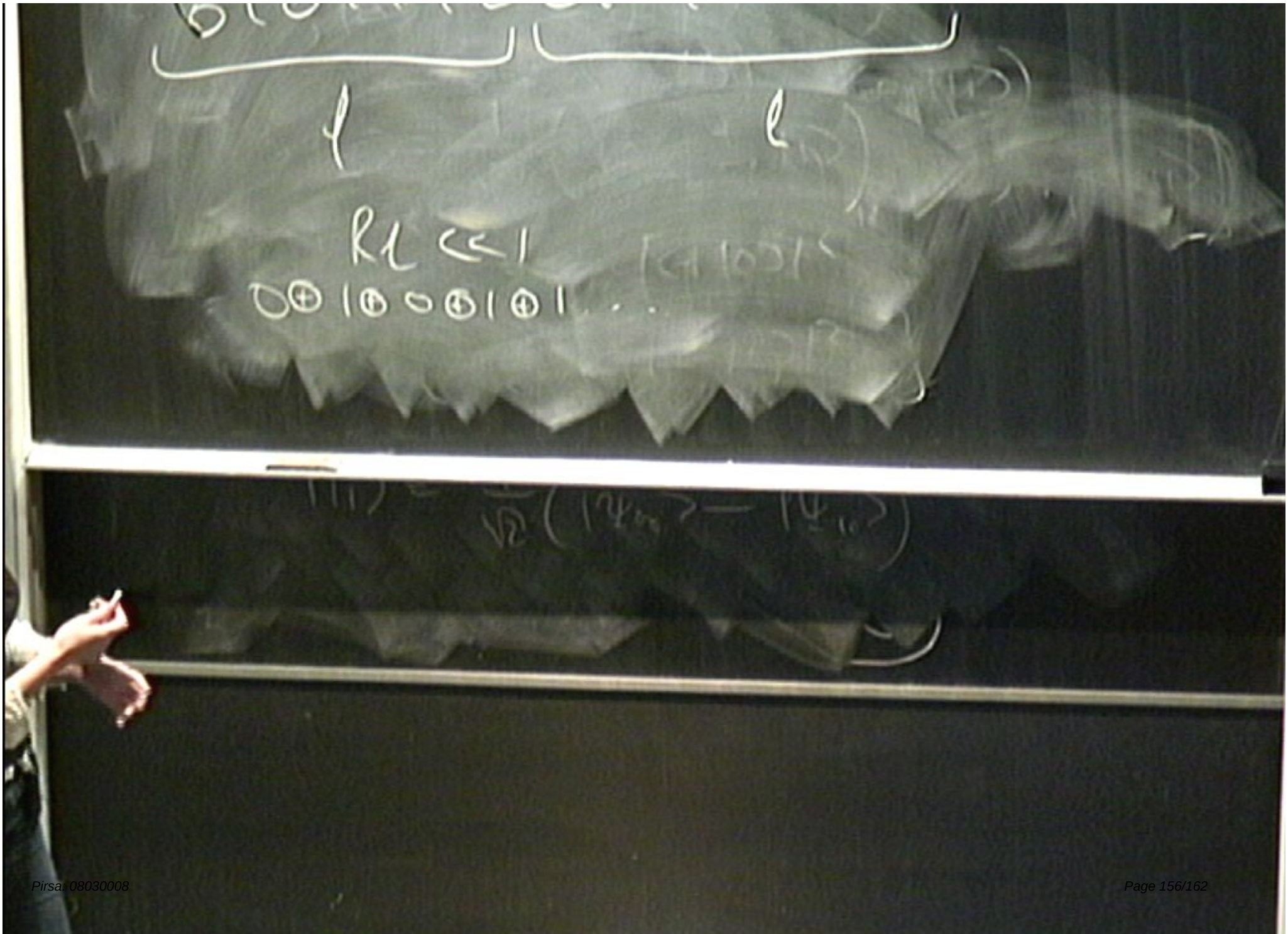
Error Correction and Privacy Amplification

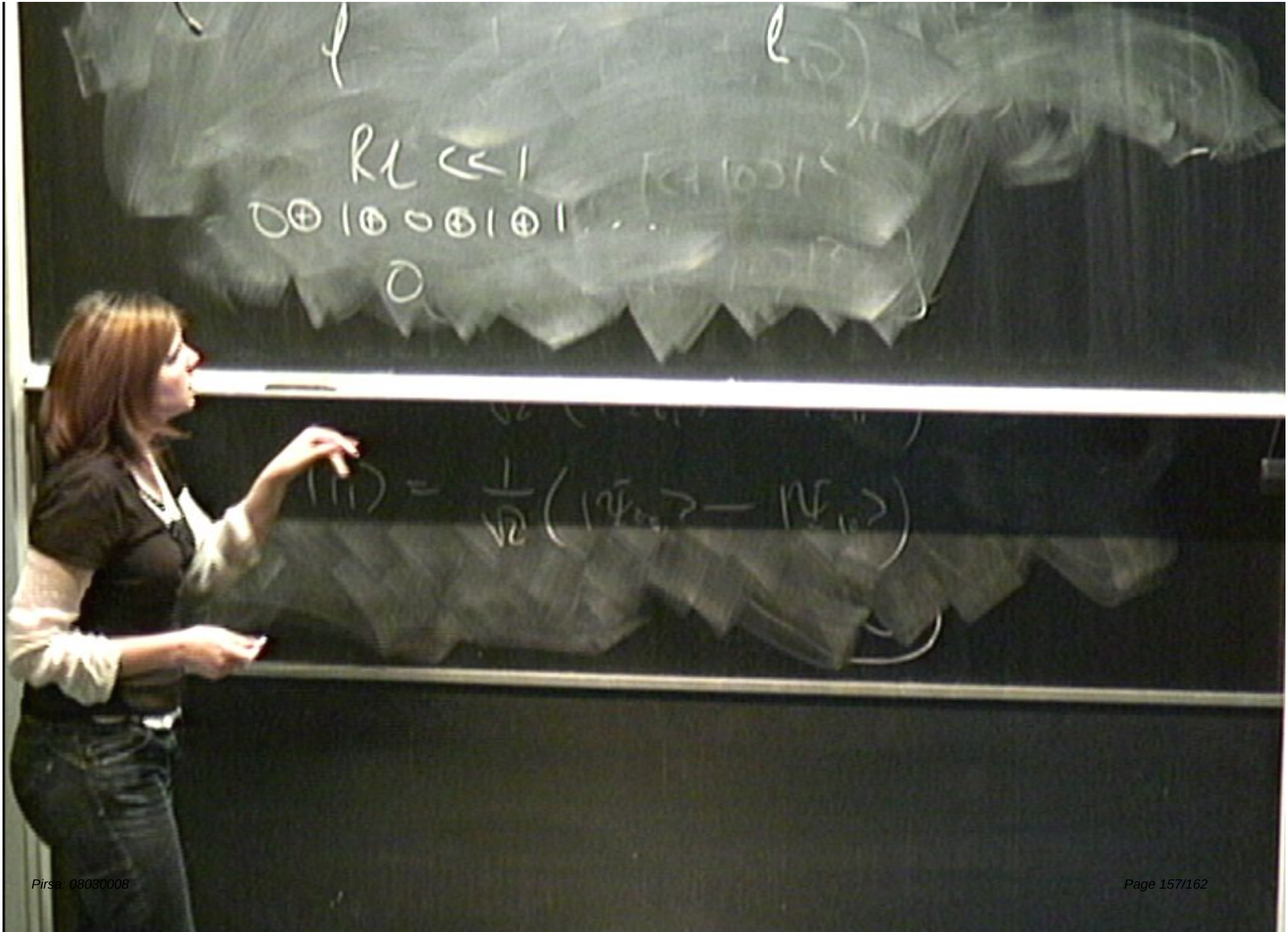
- In any experimental implementation there will always be errors introduced in the channel.
- Assume that all errors are due to Eve.
- If the error rate is too high, abort the protocol and try again.
- If the error rate is acceptable, use error correction and privacy amplification to distill a secure key.

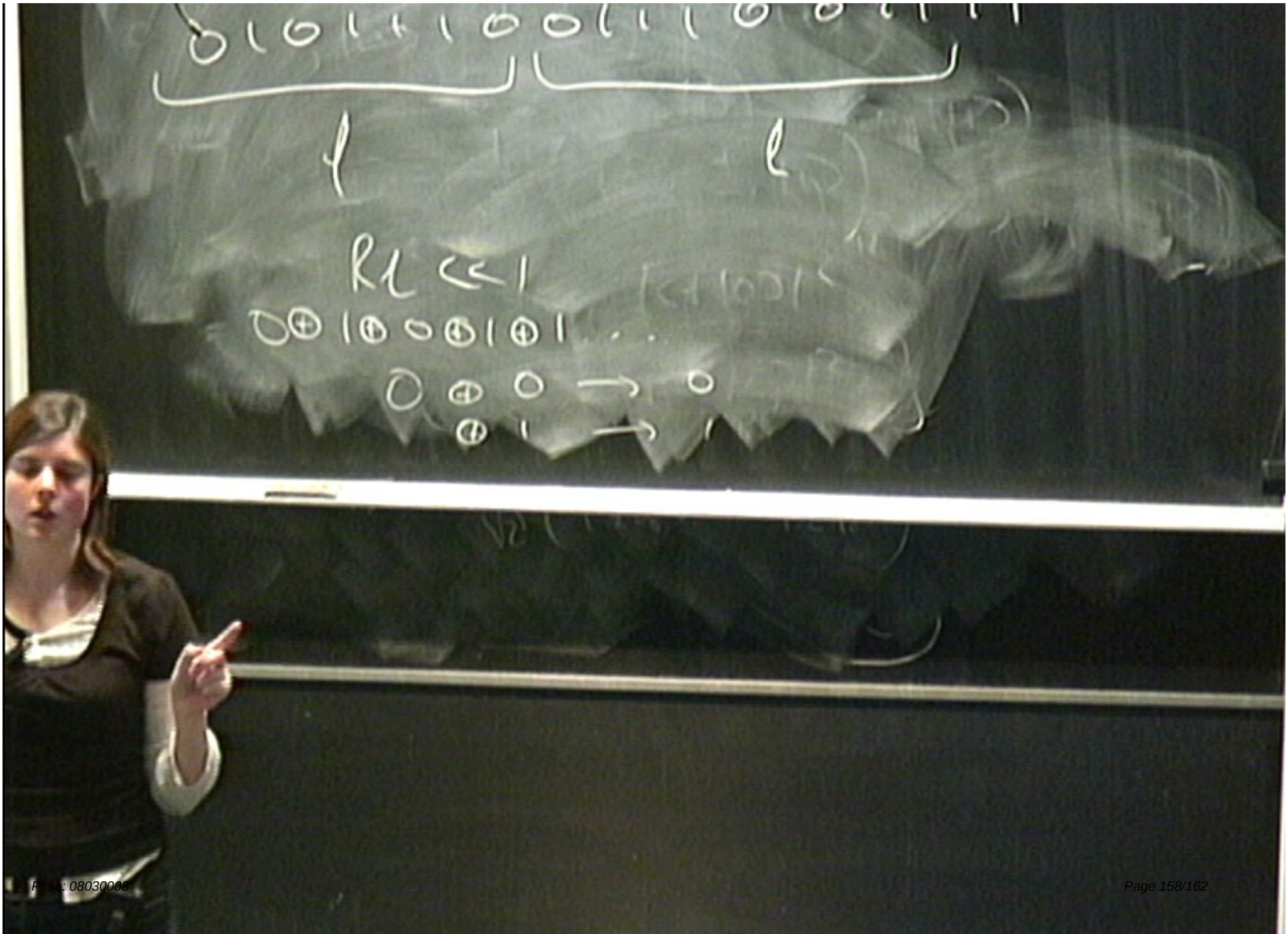


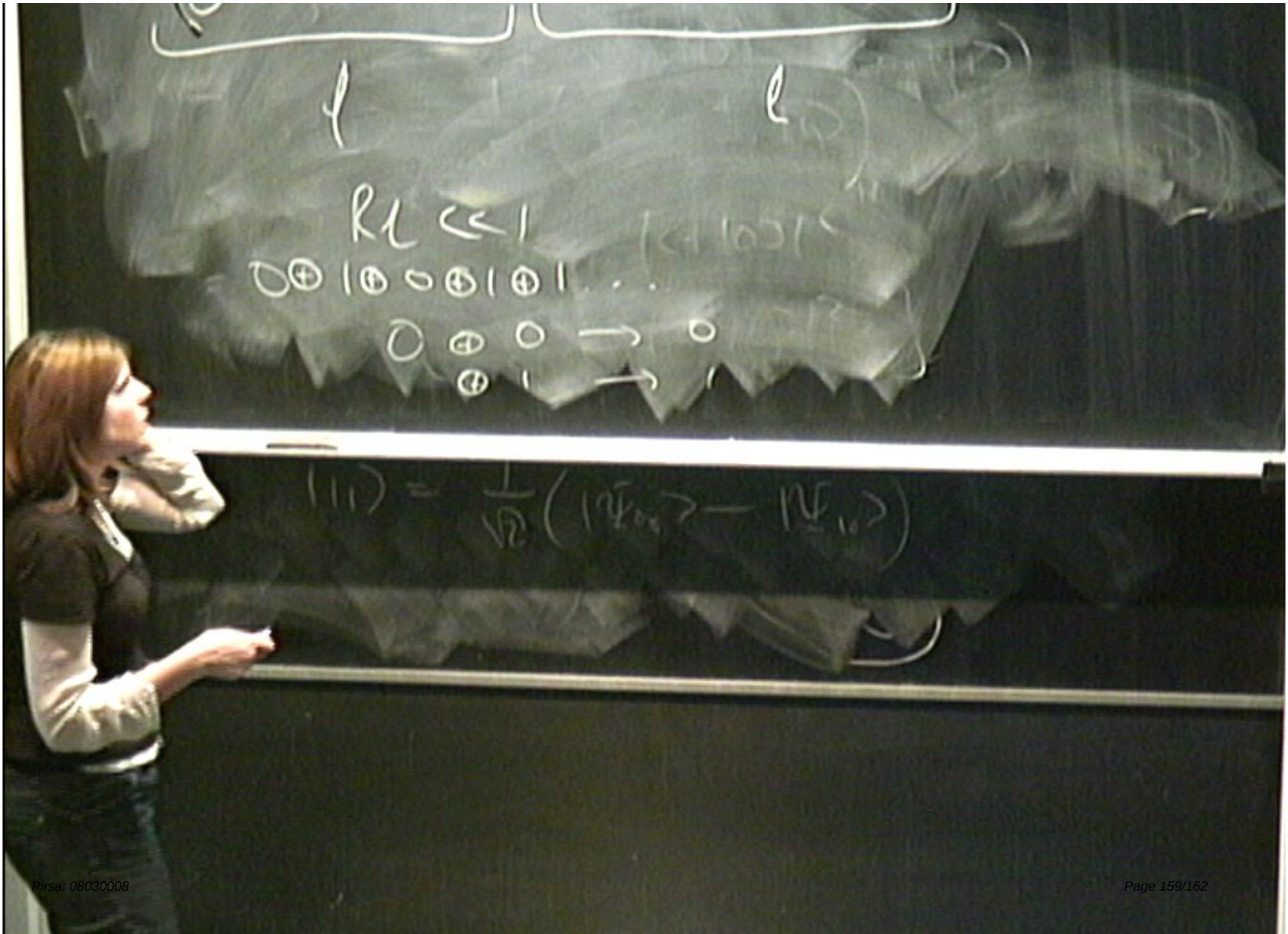


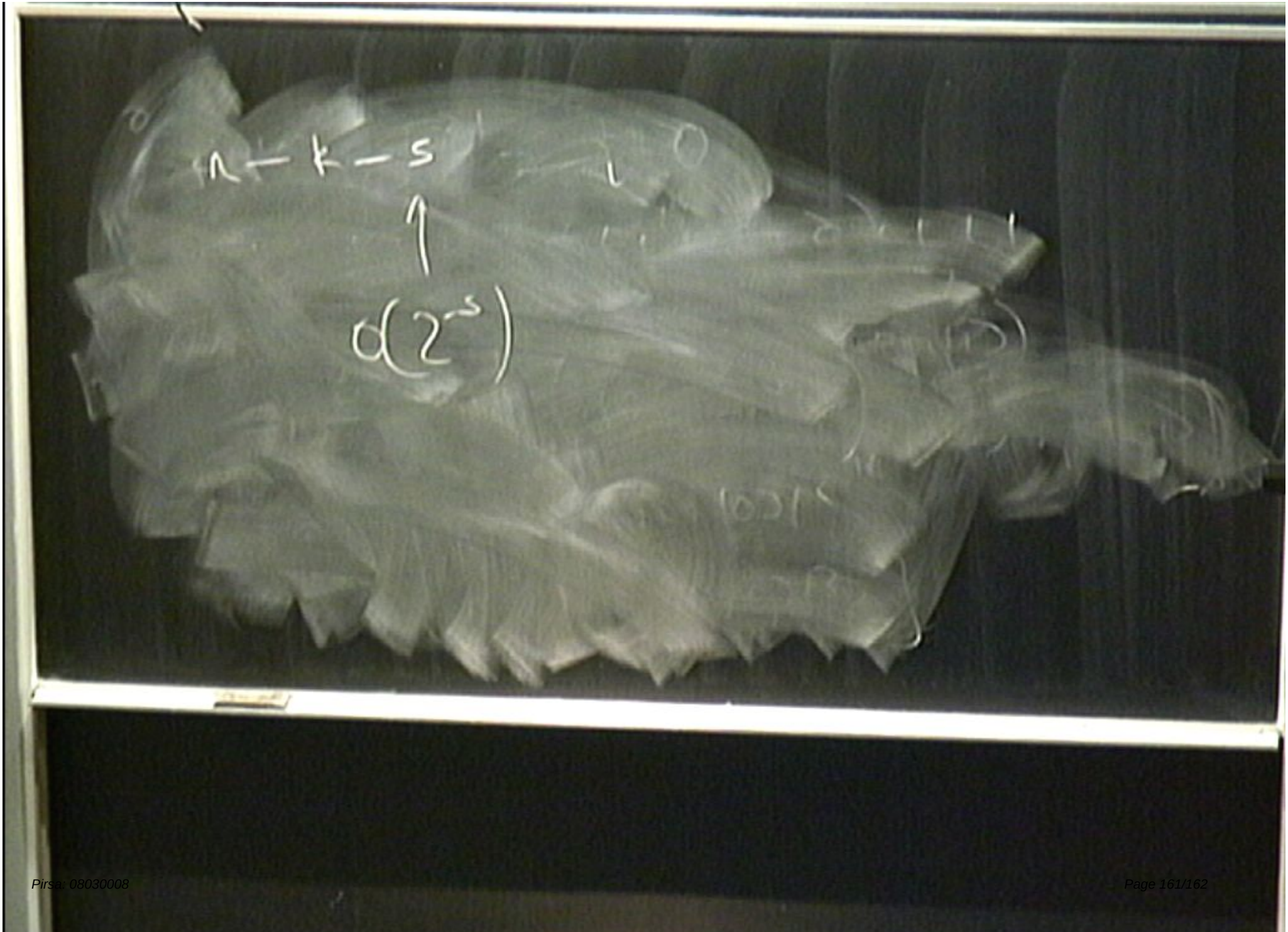

R
l
l
l
Rl << 1


l
l
Rl << 1
0 1 0 0 0 1 0 1 . .


Rl << 1
0 ⊕ 1 0 ⊕ 0 ⊕ 1 ⊕ 1 . .
0
(|↑↓⟩ − |↓↑⟩)




$R\ell \ll 1$
$|1\rangle = \frac{1}{\sqrt{2}}(|\Psi_{0,1}\rangle - |\Psi_{1,0}\rangle)$


n − k − s
d(2^-s)

Experimental Implementations

- See Gisin et al, 2002 for a review of the development of QKD.
- Fibre based: over 148.7 km in Los Alamos (2006).
- Free-space: 144km, between two of the Canary Islands (2006).
- First bank transfer using quantum cryptography took place in Austria in 2004!
- Some companies now offering commercial QKD systems. May be the first commercial use of quantum information theory.