Title: Quantum Information Theory #1

Date: Mar 11, 2008 06:30 PM

URL: http://pirsa.org/08030004

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

Quantum Information
Lecture 1: Bit vs. Qubit

Sarah Croke

Perimeter Institute (Office: 252)

scroke@perimeterinstitute.ca

"We never experiment with just one electron or atom or (small) molecule. In thought-experiments we sometimes assume that we do; this invariably entails ridiculous consequences… we are not experimenting with single particles, any more than we can raise Ichthyosauria in the zoo."

Schrödinger, *Brit J Phil Sci*, **3**, 233 (1952)

References

- M.A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000)
- J. Preskill, Lecture Notes, http://www.theory.caltech.edu/%7Epreskill/ph219/index.html#lecture
- P. Kaye, R. Laflamme and M. Mosca, *An Introduction to Quantum Computing*, Oxford University Press (2007)
- G. Benenti, G. Casati and G. Strini, *Principles of Quantum Computation and Information*, World Scientific
  - *Volume I: Basic Concepts* (2004)
  - *Volume II: Basic Tools and Special Topics* (2007)
- J. J. Sakurai, *Modern Quantum Mechanics*, Addison Wesley (1993)

Outline

- Lecture 1: Bit vs. Qubit
  - Why quantum information theory?
  - The difference between a bit and a quantum bit
  - Two-level quantum systems
- Lecture 2: Quantum Communication
- Lecture 3: Quantum Computing
- Lecture 4: Horizons

Outline

- Lecture 1: Bit vs. Qubit
- Lecture 2: Quantum Communication
  - Quantum teleportation
  - Quantum key distribution, BB84 and E91 protocols
  - Entanglement as a resource
- Lecture 3: Quantum Computing
- Lecture 4: Horizons

Outline

- Lecture 1: Bit vs. Qubit
- Lecture 2: Quantum Communication
- Lecture 3: Quantum Computing
  - Quantum circuit diagrams
  - Quantum algorithms: Deutsch-Josza, Grover's search algorithm.
- Lecture 4: Horizons

Outline

- Lecture 1: Bit vs. Qubit
- Lecture 2: Quantum Communication
- Lecture 3: Quantum Computing
- Lecture 4: Horizons
  - Decoherence, scalability
  - What information processing tasks can be performed with quantum systems but not classical ones?

Information is physical!!!

- R. Landauer, *Physics Today* **44**, 5, p.23 (1993), S. Lloyd, Nature 406, 1047 (2000)
- States of a (physical) system used to store and manipulate information.

- Processing that information depends on the physical system in which it is encoded.
- Quantum information theory – information is encoded in quantum systems.

Why Quantum Information Theory?

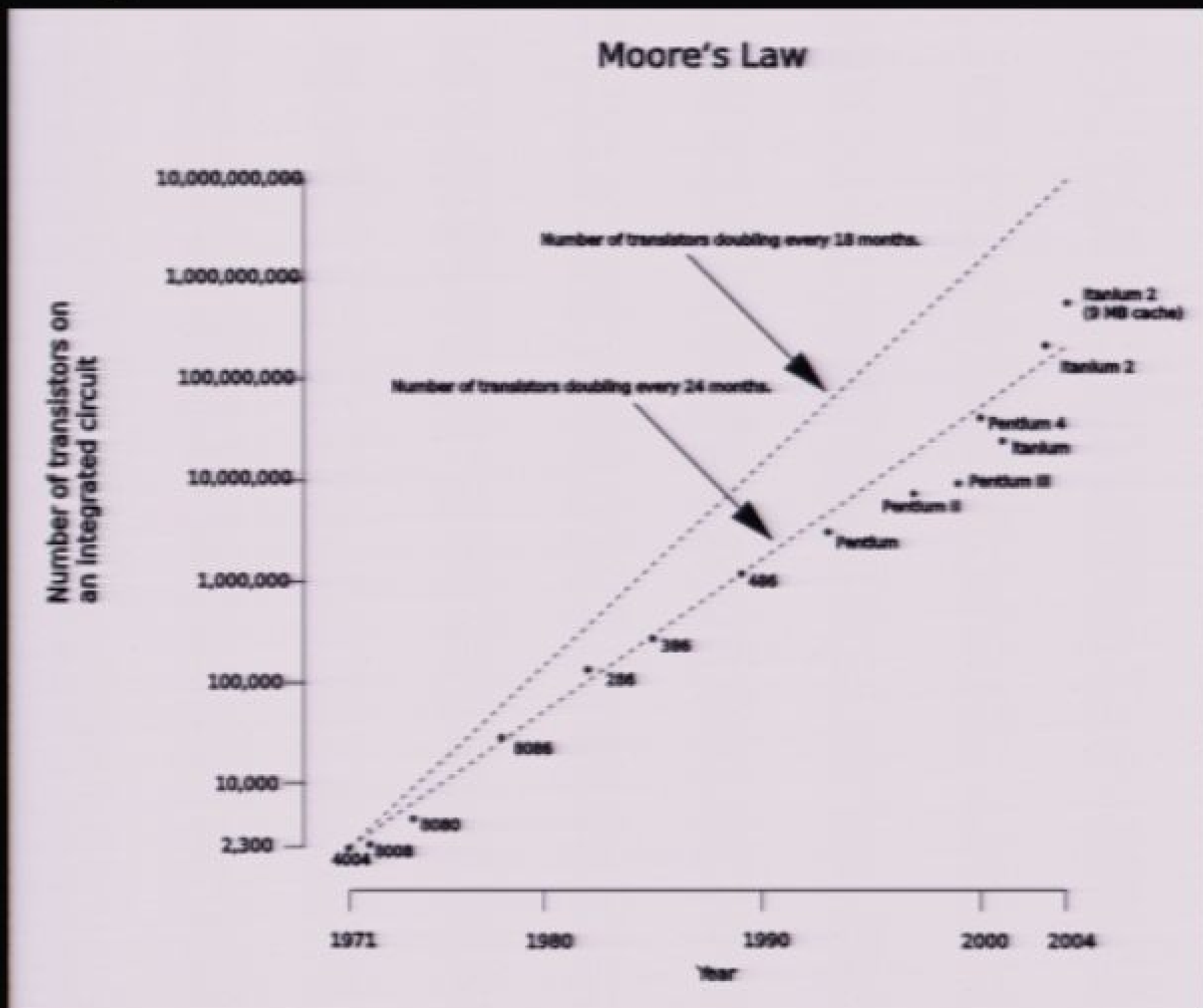


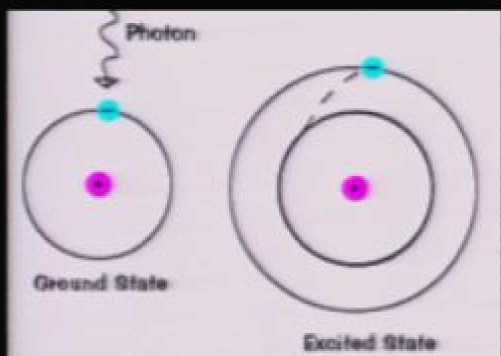
Image from www.wikipedia.org

Why Quantum Information Theory?

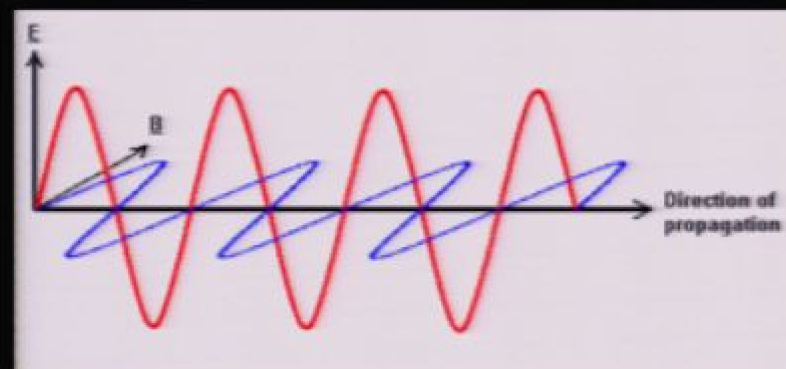
- Quantum systems cannot be efficiently simulated by classical computers (Benioff, Feynman, 1980s).
- What else can we do with quantum systems that is not possible classically?
  - Dense coding, teleportation.
  - Quantum key distribution provably secure against attack by eavesdroppers.
  - Quantum algorithms which offer speed-up over classical algorithms.

Two-level Systems

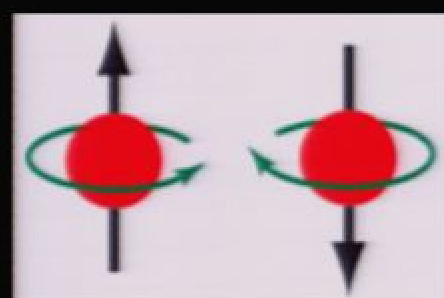
- Two-level atom



- Polarisation of light



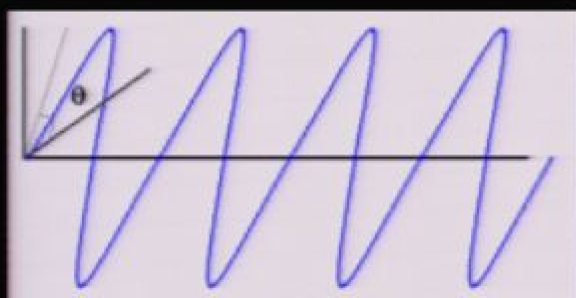
- Spin-1/2 particles



Polarisation of Light

- Linear Polarisation

$$\cos\theta|h\rangle + \sin\theta|v\rangle$$

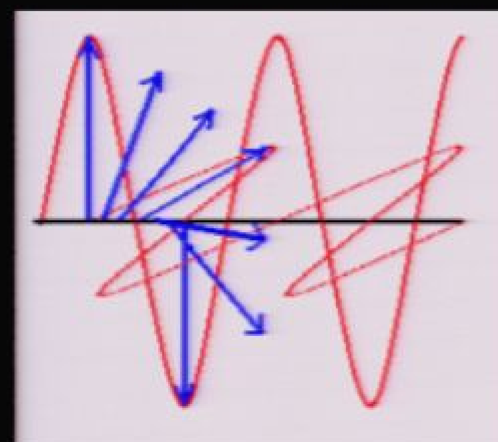


- Elliptical Polarisation –in general complex amplitudes

$$\cos\theta|h\rangle + e^{i\delta}\sin\theta|v\rangle$$

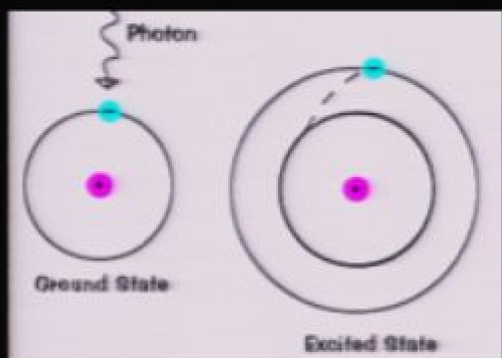
- Circular Polarisation

$$\frac{1}{\sqrt{2}}(|h\rangle \pm i|v\rangle)$$

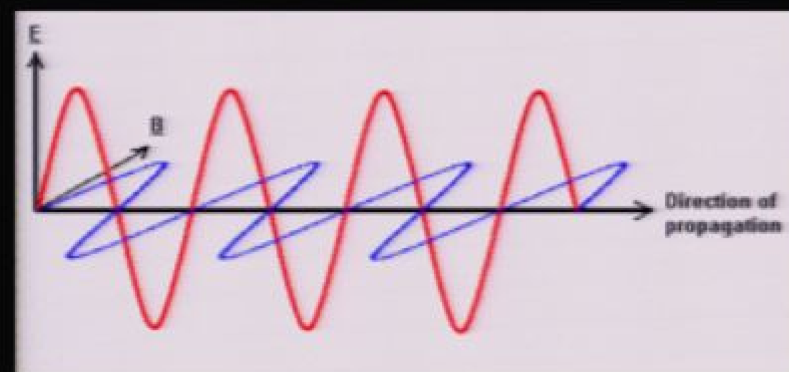


Two-level Systems

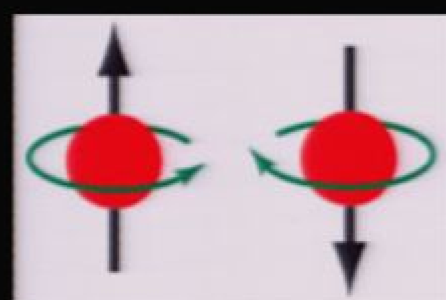
- Two-level atom



- Polarisation of light



- Spin-1/2 particles

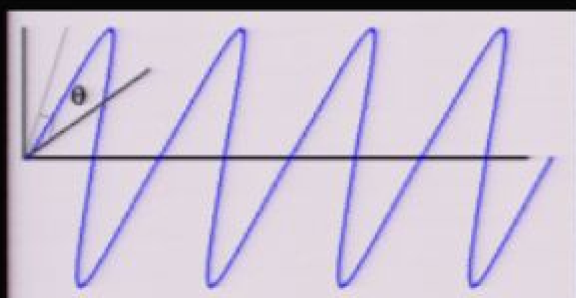


$$\bar{\underline{E}}(t) = \bar{E}(0)\, e^{i(kz - \omega t)}$$

Polarisation of Light

- Linear Polarisation

$$\cos\theta|h\rangle + \sin\theta|v\rangle$$

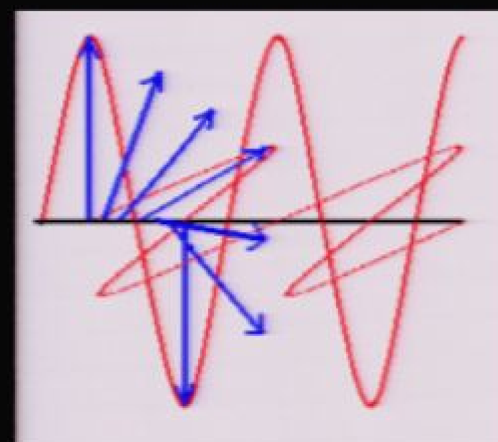


- Elliptical Polarisation –in general complex amplitudes

$$\cos\theta|h\rangle + e^{i\delta}\sin\theta|v\rangle$$

- Circular Polarisation

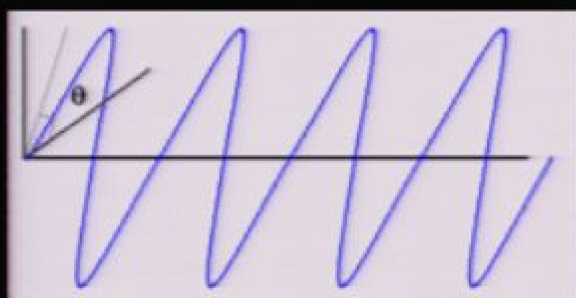
$$\frac{1}{\sqrt{2}}(|h\rangle \pm i|v\rangle)$$



Polarisation of Light

- Linear Polarisation

$$\cos\theta|h\rangle + \sin\theta|v\rangle$$

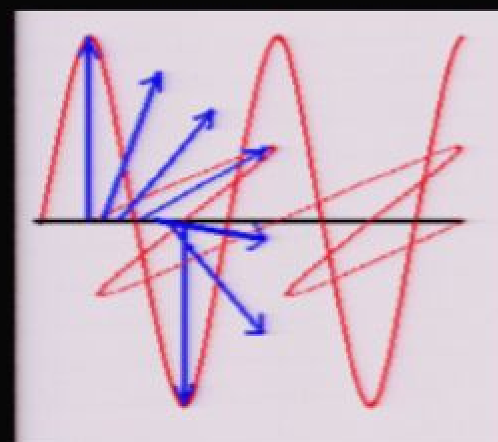


- Elliptical Polarisation –in general complex amplitudes

$$\cos\theta|h\rangle + e^{i\delta}\sin\theta|v\rangle$$

- Circular Polarisation

$$\frac{1}{\sqrt{2}}(|h\rangle \pm i|v\rangle)$$



$$\underline{\bar{E}}(t) = \bar{E}(0)\, e^{i(kz-\omega t)}$$

$$= E\left(\underline{x}\, e^{i(kz-\omega t)} + \underline{y}\, e^{i(kz-\omega t+\pi/2)}\right)$$

$$\underline{E}(t) = \underline{E}(0)\, e^{i(kz-\omega t)}$$

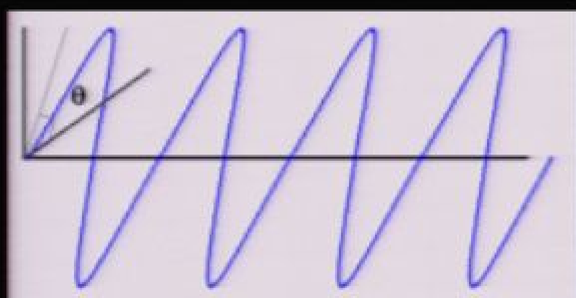
$$= E\left(\underline{x}\, e^{i(kz-\omega t)} + \underline{y}\, e^{i(kz-\omega t+\pi/2)} \right)$$

$$= E(\underline{x} + i\underline{y})\, e^{i(kz-\omega t)}$$

Polarisation of Light

- Linear Polarisation

  $$\cos\theta|h\rangle + \sin\theta|v\rangle$$

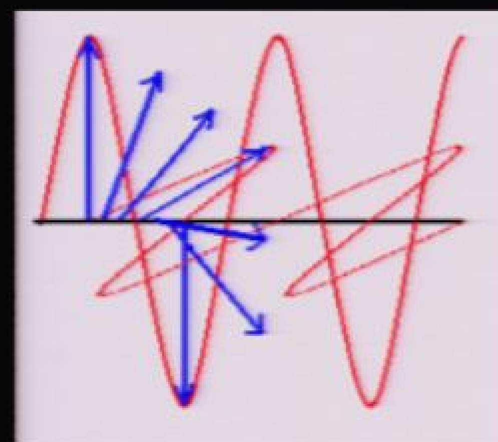


- Elliptical Polarisation –in general complex amplitudes

  $$\cos\theta|h\rangle + e^{i\delta}\sin\theta|v\rangle$$

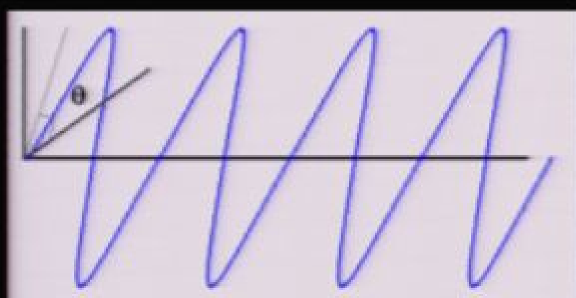
- Circular Polarisation

  $$\frac{1}{\sqrt{2}}(|h\rangle \pm i|v\rangle)$$



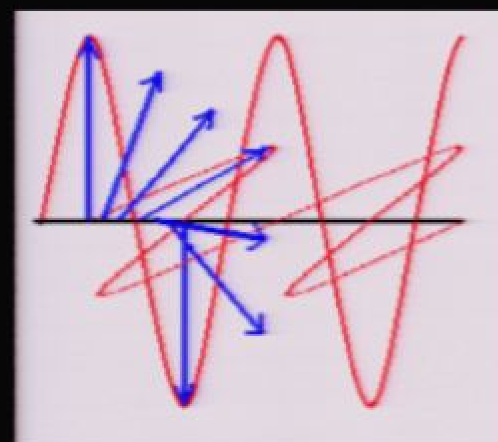
Polarisation of Light

- Linear Polarisation
  $$\cos\theta|h\rangle + \sin\theta|v\rangle$$



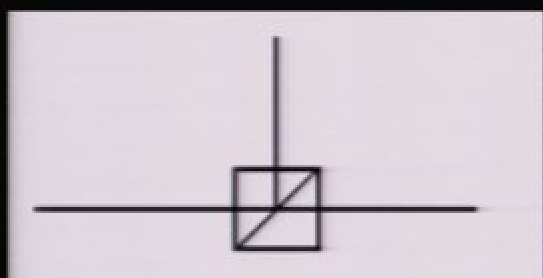
- Elliptical Polarisation –in general complex amplitudes
  $$\cos\theta|h\rangle + e^{i\delta}\sin\theta|v\rangle$$

- Circular Polarisation
  $$\frac{1}{\sqrt{2}}(|h\rangle \pm i|v\rangle)$$

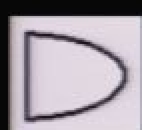


Optical Components

- Polarising beam splitter (PBS) –transmits one polarisation, reflects the other



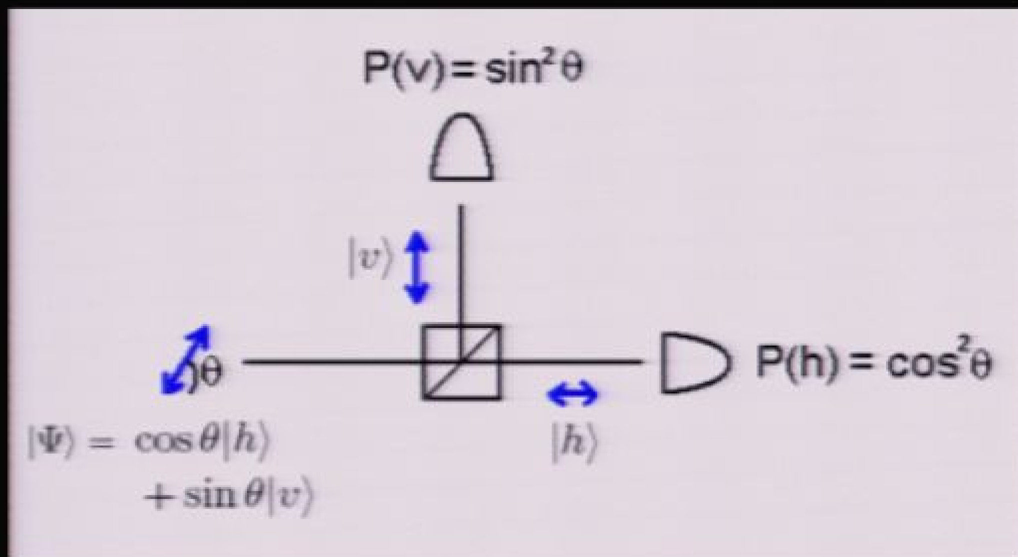
- Photo-detector (PD) –detects light



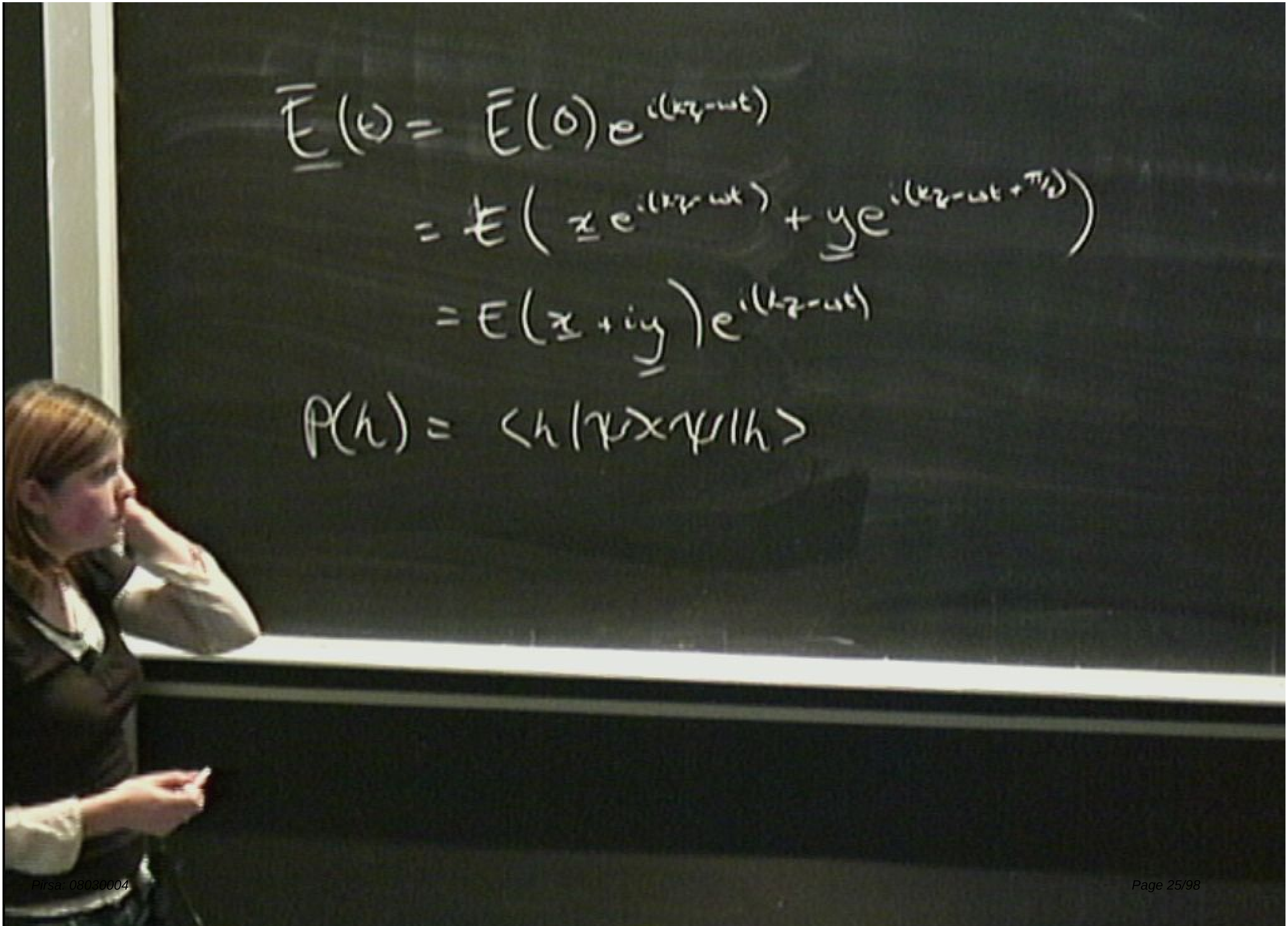
- Half-wave plate (HWP) – introduces a phase difference of $\pm\pi$ between orthogonal polarisations
- $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\alpha/2$: $\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$
- Quarter-wave plate (QWP) – introduces a phase of $\pm\pi/2$ between orthogonal polarisations

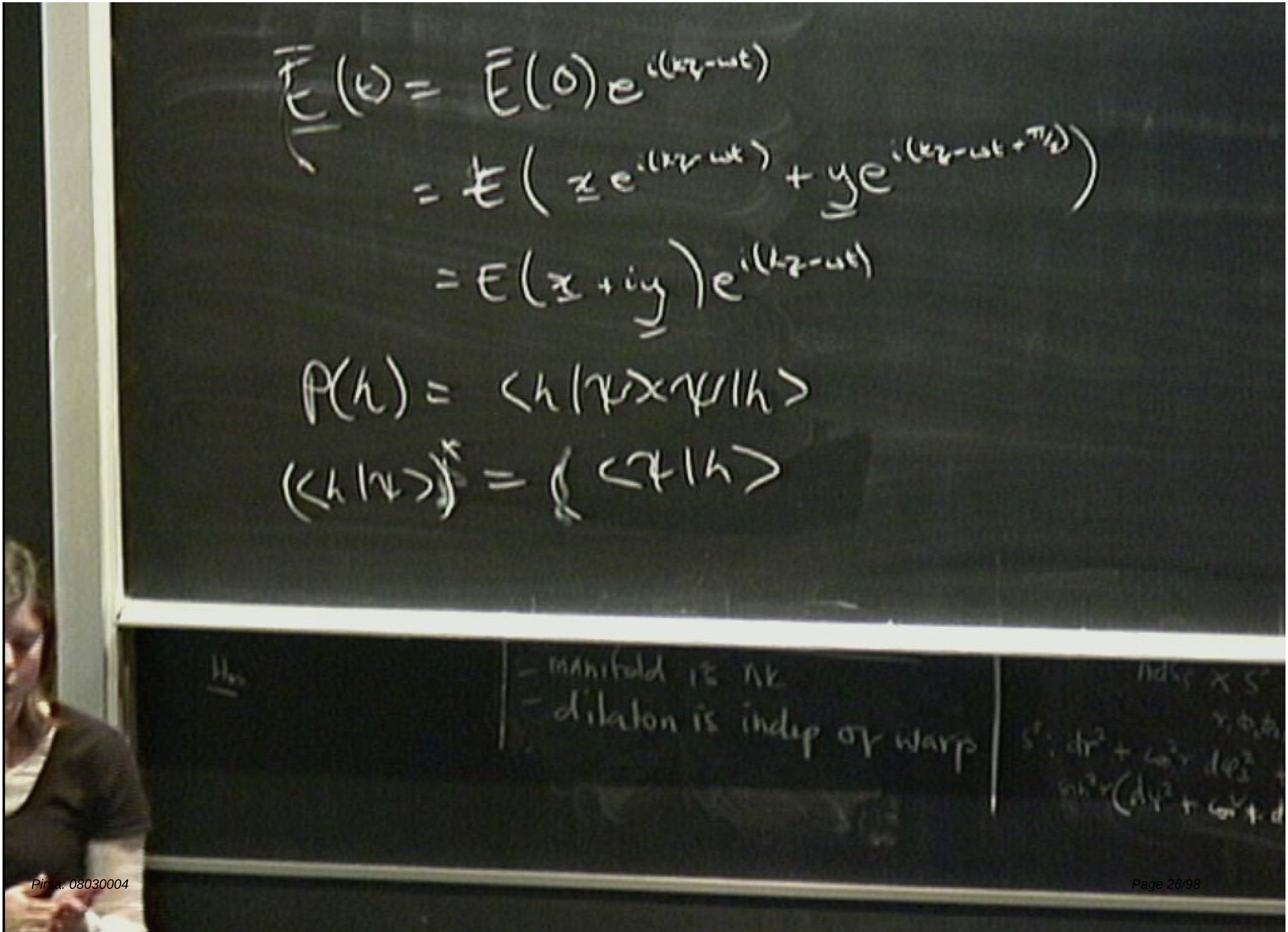
  $\begin{pmatrix} 1 & 0 \\ 0 & \pm i \end{pmatrix}$
- $\beta/2$: $\frac{1}{\sqrt{2}}\begin{pmatrix} \cos\beta - i & \sin\beta \\ \sin\beta & -\cos\beta - i \end{pmatrix}$

Polarisation Measurements

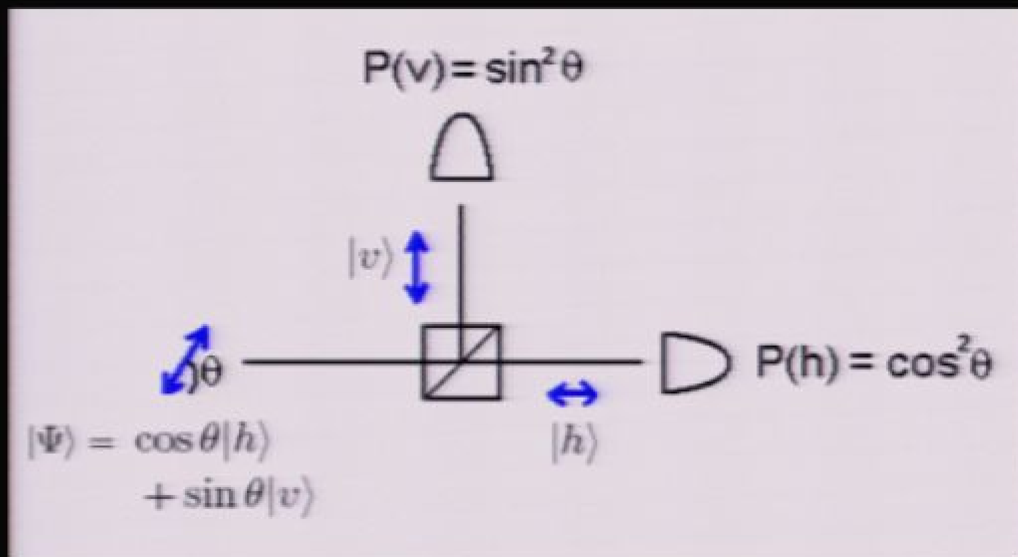


- $P(h) = |\langle\Psi|h\rangle|^2$, $P(v) = |\langle\Psi|v\rangle|^2$
- Measurement transforms state to $|h\rangle$ or $|v\rangle$
- Measurement completely specified by operators $|h\rangle\langle h|$, $|v\rangle\langle v|$


$\underline{\bar{E}}(t) = \bar{E}(0)\, e^{i(kz-\omega t)}$
$= E\left(\underline{x}\, e^{i(kz-\omega t)} + \underline{y}\, e^{i(kz-\omega t+\pi/2)} \right)$
$= E(\underline{x} + i\underline{y})\, e^{i(kz-\omega t)}$
$P(h) = \langle h|\psi\rangle\langle\psi|h\rangle$


E(t) = E(0) e^{i(kz-ωt)}
= E(x e^{i(kz-ωt)} + y e^{i(kz-ωt+π/2)})
= E(x + iy) e^{i(kz-ωt)}
P(h) = <h|ψ><ψ|h>
(<h|ψ>)* = <ψ|h>
- manifold is ...
- dilaton is indep of warp

Polarisation Measurements



- $P(h) = |\langle\Psi|h\rangle|^2$, $P(v) = |\langle\Psi|v\rangle|^2$
- Measurement transforms state to $|h\rangle$ or $|v\rangle$
- Measurement completely specified by operators $|h\rangle\langle h|$, $|v\rangle\langle v|$

Properties of Measurement Operators

- Von Neumann measurement:

$$|h\rangle\langle h| + |v\rangle\langle v| = \hat{\mathrm{I}} \quad (1)$$

$$(|h\rangle\langle h|)^\dagger = |h\rangle\langle h| \quad (2)$$

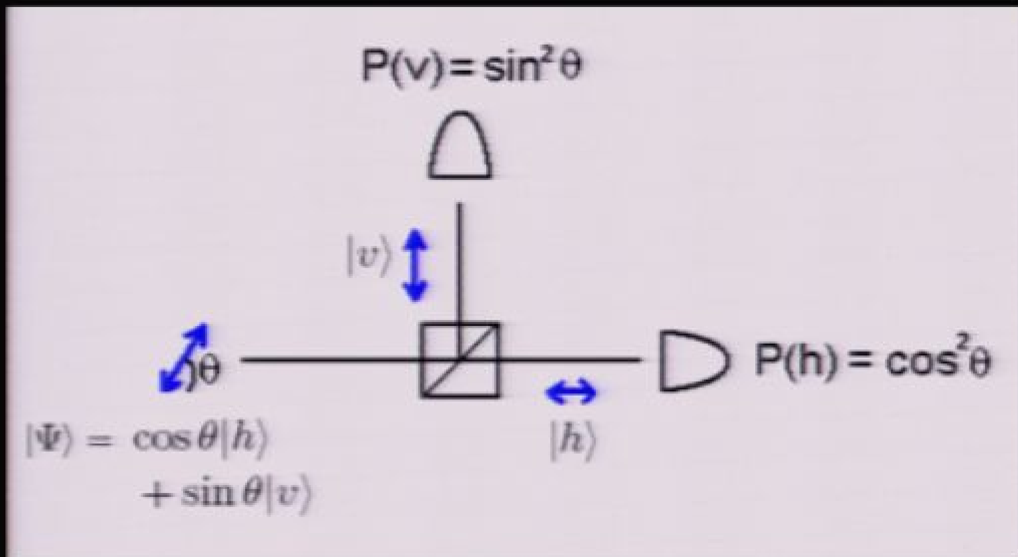
$$|h\rangle\langle h| \geq 0 \quad (3)$$

$$|h\rangle\langle h|v\rangle\langle v| = 0 \quad (4)$$

- Where, by (3) we mean:

$$\langle\Psi|(|h\rangle\langle h|)|\Psi\rangle \geq 0 \;\; \forall \;\; |\Psi\rangle$$

Polarisation Measurements



- $P(h) = |\langle\Psi|h\rangle|^2$, $P(v) = |\langle\Psi|v\rangle|^2$
- Measurement transforms state to $|h\rangle$ or $|v\rangle$
- Measurement completely specified by operators $|h\rangle\langle h|$, $|v\rangle\langle v|$

Properties of Measurement Operators

- Von Neumann measurement:

$$\begin{aligned} |h\rangle\langle h| + |v\rangle\langle v| &= \hat{\mathrm{I}} && (1) \\ (|h\rangle\langle h|)^\dagger &= |h\rangle\langle h| && (2) \\ |h\rangle\langle h| &\geq 0 && (3) \\ |h\rangle\langle h|v\rangle\langle v| &= 0 && (4) \end{aligned}$$

- Where, by (3) we mean:

$$\langle\Psi|(|h\rangle\langle h|)|\Psi\rangle \geq 0 \;\; \forall \;\; |\Psi\rangle$$

Properties of Measurement Operators

- Von Neumann measurement:

$$|h\rangle\langle h| + |v\rangle\langle v| = \hat{\mathrm{I}} \quad (1)$$

$$(|h\rangle\langle h|)^\dagger = |h\rangle\langle h| \quad (2)$$

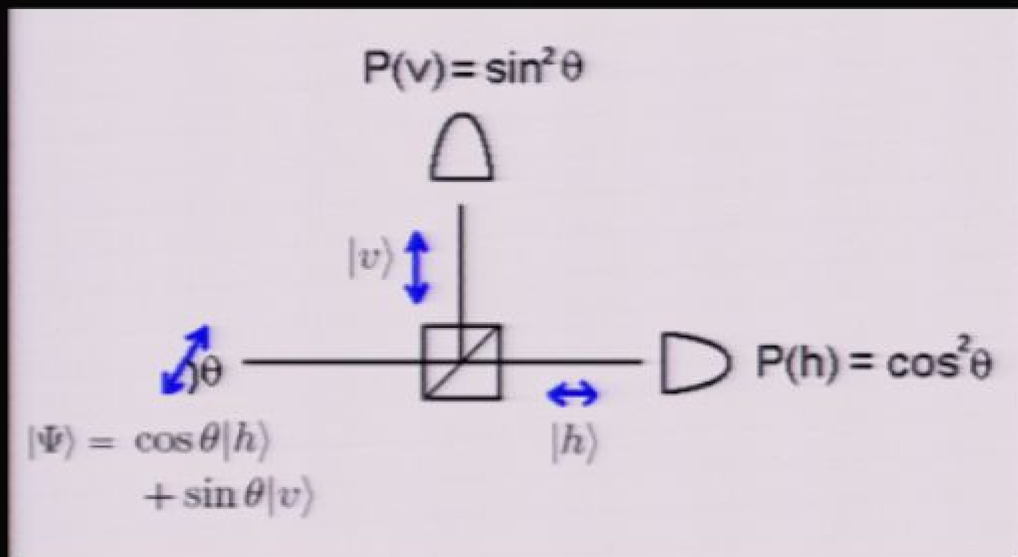
$$|h\rangle\langle h| \geq 0 \quad (3)$$

$$|h\rangle\langle h|v\rangle\langle v| = 0 \quad (4)$$

- Where, by (3) we mean:

$$\langle\Psi|(|h\rangle\langle h|)|\Psi\rangle \geq 0 \;\; \forall \;\; |\Psi\rangle$$

Polarisation Measurements



- $P(h) = |\langle\Psi|h\rangle|^2$, $P(v) = |\langle\Psi|v\rangle|^2$
- Measurement transforms state to $|h\rangle$ or $|v\rangle$
- Measurement completely specified by operators

  $|h\rangle\langle h|$, $|v\rangle\langle v|$

Properties of Measurement Operators

- Von Neumann measurement:

$$|h\rangle\langle h| + |v\rangle\langle v| = \hat{\mathrm{I}} \quad (1)$$

$$(|h\rangle\langle h|)^\dagger = |h\rangle\langle h| \quad (2)$$

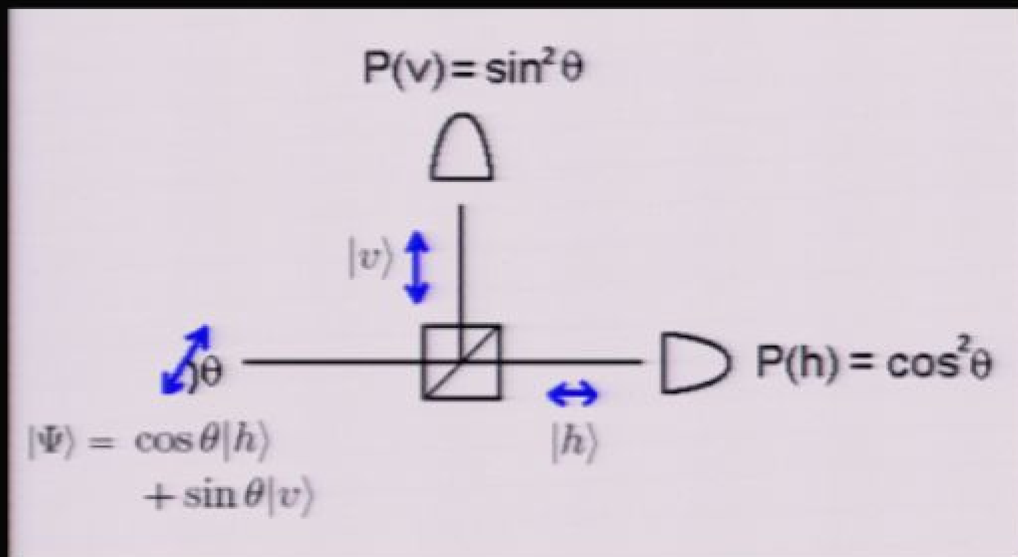
$$|h\rangle\langle h| \geq 0 \quad (3)$$

$$|h\rangle\langle h|v\rangle\langle v| = 0 \quad (4)$$

- Where, by (3) we mean:

$$\langle\Psi|(|h\rangle\langle h|)|\Psi\rangle \geq 0 \;\; \forall \;\; |\Psi\rangle$$

Polarisation Measurements



- $P(h) = |\langle\Psi|h\rangle|^2$, $P(v) = |\langle\Psi|v\rangle|^2$
- Measurement transforms state to $|h\rangle$ or $|v\rangle$
- Measurement completely specified by operators $|h\rangle\langle h|$, $|v\rangle\langle v|$

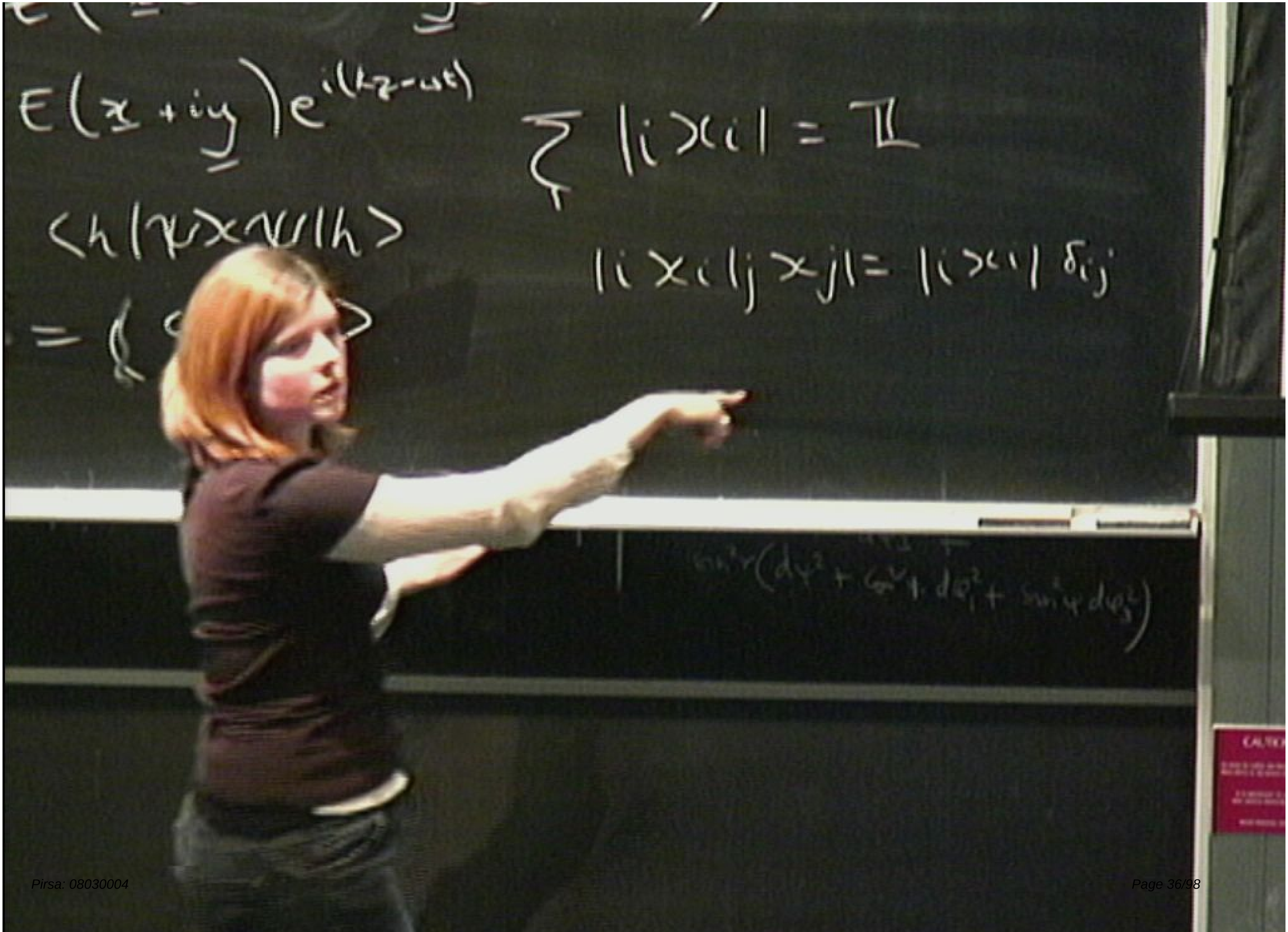
Properties of Measurement Operators

- Von Neumann measurement:

$$
\begin{aligned}
|h\rangle\langle h| + |v\rangle\langle v| &= \hat{\mathrm{I}} \qquad (1)\\
(|h\rangle\langle h|)^{\dagger} &= |h\rangle\langle h| \qquad (2)\\
|h\rangle\langle h| &\geq 0 \qquad (3)\\
|h\rangle\langle h|v\rangle\langle v| &= 0 \qquad (4)
\end{aligned}
$$

- Where, by (3) we mean:

$$\langle\Psi|(|h\rangle\langle h|)|\Psi\rangle \geq 0 \;\; \forall \;\; |\Psi\rangle$$


E(x + iy)e^{i(kz-ωt)}
Σ |i⟩⟨i| = 𝟙
⟨h|ψ⟩⟨ψ|h⟩
|i⟩⟨i|j⟩⟨j| = |i⟩⟨i| δ_ij

$$|i\, x_i|\, |j\, x_j| = |i\, x_i|\, \delta_{ij}$$

Dirac Bra-Ket Notation

- States represented as normalised state kets $|\Psi\rangle$ in a complex, linear vector space;
- For every ket $|\Psi\rangle$ there is a corresponding bra $\langle\Psi|$ in the dual space
- The vector space has an inner product $\langle\alpha|\beta\rangle$, which satisfies $\langle\alpha|\beta\rangle = (\langle\beta|\alpha\rangle)^*$
- Outer products $|\alpha\rangle\langle\beta|$ form operators on the vector space.
- Hermitian conjugate: $(|\alpha\rangle\langle\beta|)^\dagger = |\beta\rangle\langle\alpha|$
- Hermitian operators: $\hat{A}^\dagger = \hat{A}$
- Unitary operators preserve inner products:

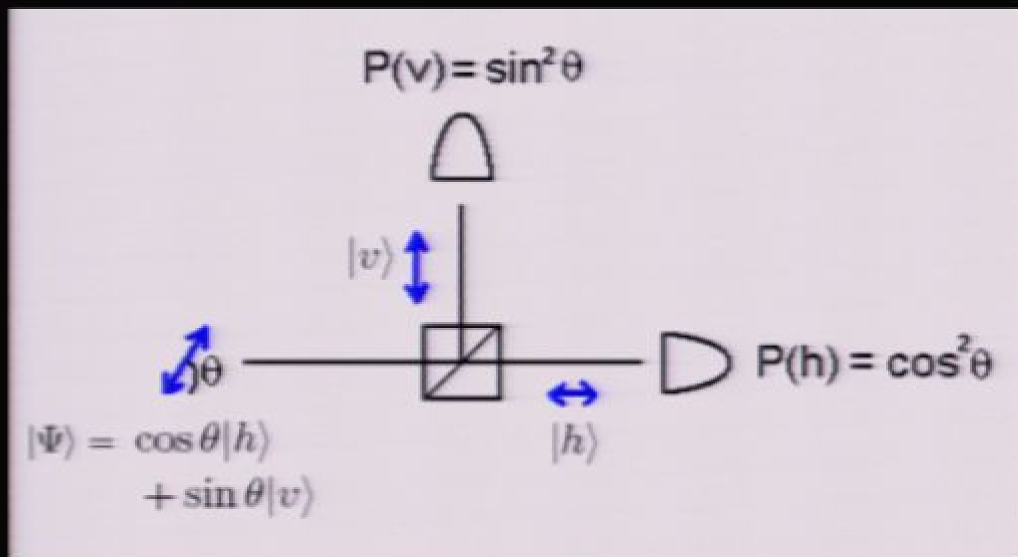
$$\hat{U}^\dagger\hat{U} = \hat{U}\hat{U}^\dagger = \hat{\mathbb{1}}$$

Dirac Bra-Ket Notation

- States represented as normalised state kets $|\Psi\rangle$ in a complex, linear vector space;
- For every ket $|\Psi\rangle$ there is a corresponding bra $\langle\Psi|$ in the dual space
- The vector space has an inner product $\langle\alpha|\beta\rangle$, which satisfies $\langle\alpha|\beta\rangle = (\langle\beta|\alpha\rangle)^*$
- Outer products $|\alpha\rangle\langle\beta|$ form operators on the vector space.
- Hermitian conjugate: $(|\alpha\rangle\langle\beta|)^\dagger = |\beta\rangle\langle\alpha|$
- Hermitian operators: $\hat{A}^\dagger = \hat{A}$
- Unitary operators preserve inner products:

$$\hat{U}^\dagger\hat{U} = \hat{U}\hat{U}^\dagger = \hat{1}$$

Polarisation Measurements



- $P(h) = |\langle\Psi|h\rangle|^2$, $P(v) = |\langle\Psi|v\rangle|^2$
- Measurement transforms state to $|h\rangle$ or $|v\rangle$
- Measurement completely specified by operators $|h\rangle\langle h|$, $|v\rangle\langle v|$

Properties of Measurement Operators

- Von Neumann measurement:

$$|h\rangle\langle h| + |v\rangle\langle v| = \hat{\mathrm{I}} \quad (1)$$

$$(|h\rangle\langle h|)^{\dagger} = |h\rangle\langle h| \quad (2)$$

$$|h\rangle\langle h| \geq 0 \quad (3)$$

$$|h\rangle\langle h|v\rangle\langle v| = 0 \quad (4)$$

- Where, by (3) we mean:

$$\langle\Psi|(|h\rangle\langle h|)|\Psi\rangle \geq 0 \;\; \forall \;\; |\Psi\rangle$$

Dirac Bra-Ket Notation

- States represented as normalised state kets $|\Psi\rangle$ in a complex, linear vector space;
- For every ket $|\Psi\rangle$ there is a corresponding bra $\langle\Psi|$ in the dual space
- The vector space has an inner product $\langle\alpha|\beta\rangle$, which satisfies $\langle\alpha|\beta\rangle = (\langle\beta|\alpha\rangle)^*$
- Outer products $|\alpha\rangle\langle\beta|$ form operators on the vector space.
- Hermitian conjugate: $(|\alpha\rangle\langle\beta|)^\dagger = |\beta\rangle\langle\alpha|$
- Hermitian operators: $\hat{A}^\dagger = \hat{A}$
- Unitary operators preserve inner products:

$$\hat{U}^\dagger\hat{U} = \hat{U}\hat{U}^\dagger = \hat{1}$$

Properties of Measurement Operators

- Von Neumann measurement:

$$|h\rangle\langle h| + |v\rangle\langle v| = \hat{I} \quad (1)$$

$$(|h\rangle\langle h|)^\dagger = |h\rangle\langle h| \quad (2)$$

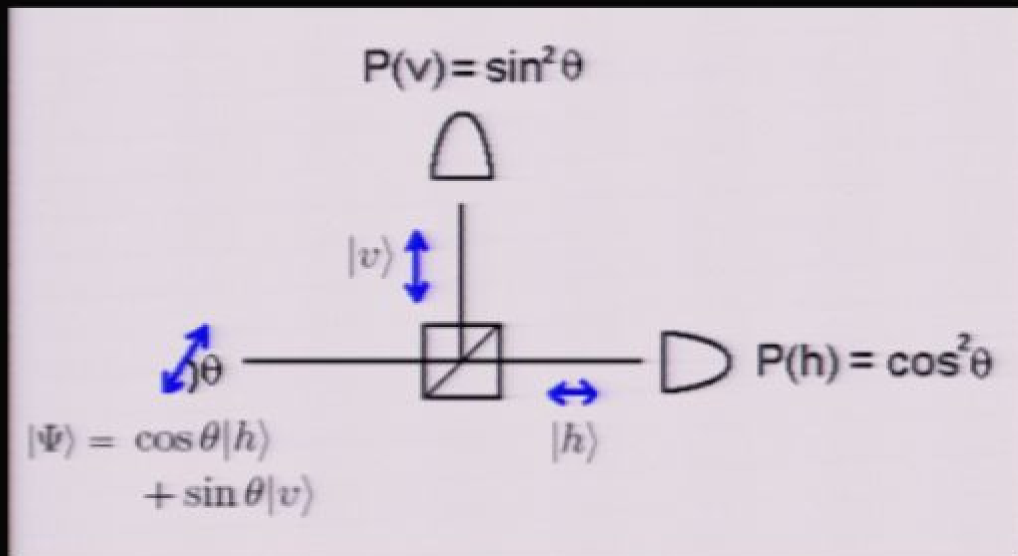
$$|h\rangle\langle h| \geq 0 \quad (3)$$

$$|h\rangle\langle h|v\rangle\langle v| = 0 \quad (4)$$

- Where, by (3) we mean:

$$\langle\Psi|(|h\rangle\langle h|)|\Psi\rangle \geq 0 \;\; \forall \;\; |\Psi\rangle$$

Polarisation Measurements

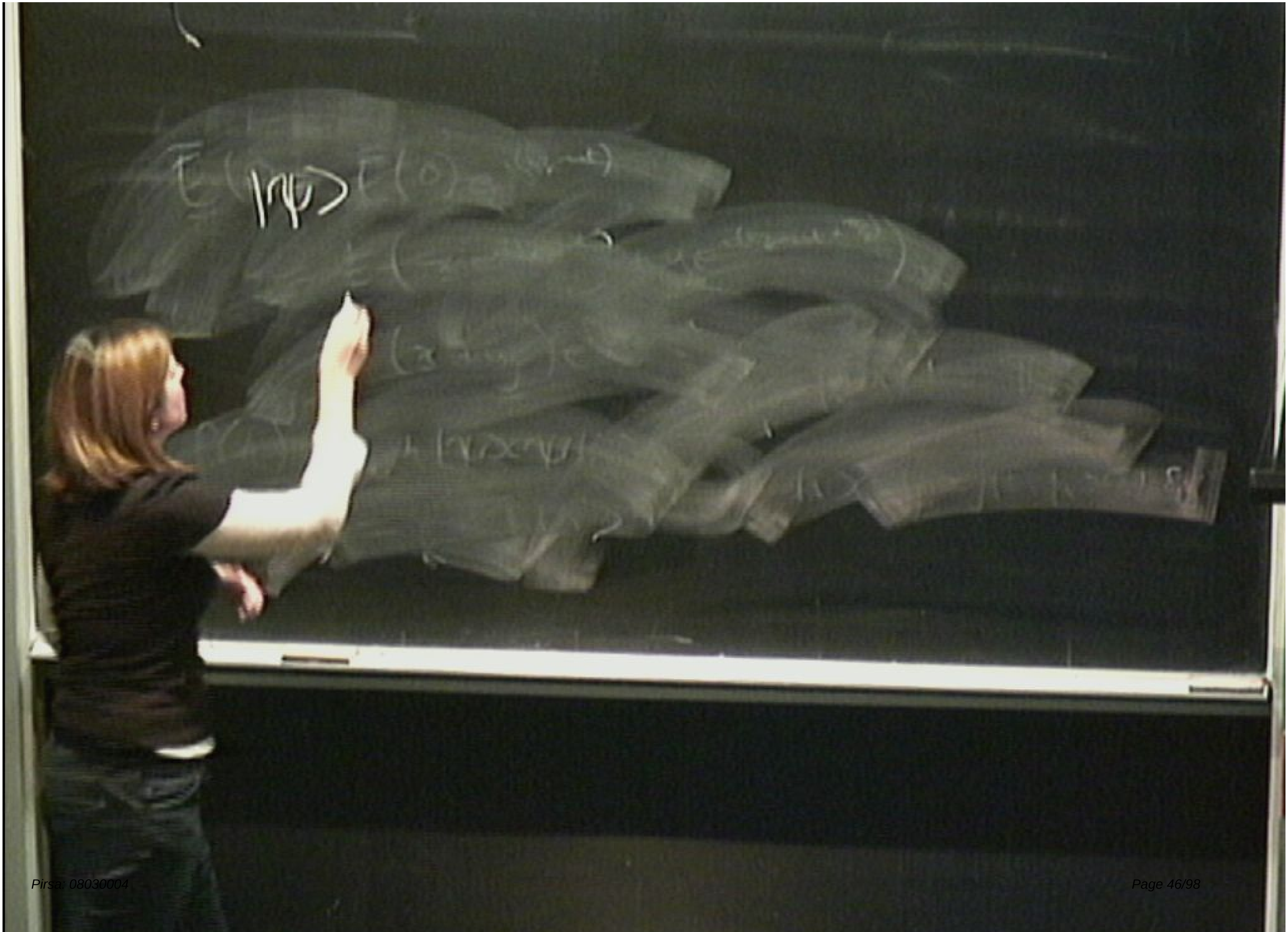


- $P(h) = |\langle\Psi|h\rangle|^2$, $P(v) = |\langle\Psi|v\rangle|^2$
- Measurement transforms state to $|h\rangle$ or $|v\rangle$
- Measurement completely specified by operators $|h\rangle\langle h|$, $|v\rangle\langle v|$

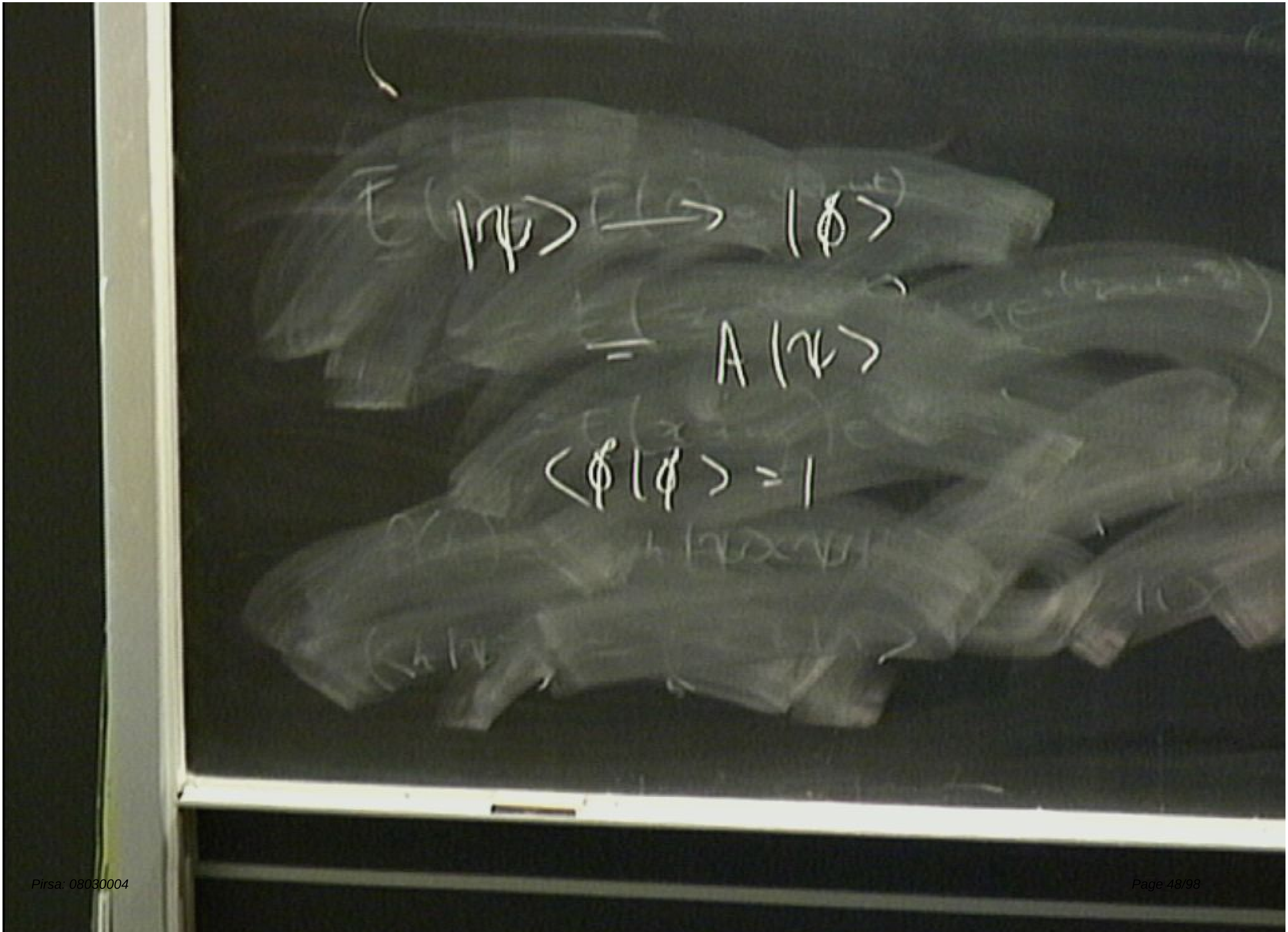
Dirac Bra-Ket Notation

- States represented as normalised state kets $|\Psi\rangle$ in a complex, linear vector space;
- For every ket $|\Psi\rangle$ there is a corresponding bra $\langle\Psi|$ in the dual space
- The vector space has an inner product $\langle\alpha|\beta\rangle$, which satisfies $\langle\alpha|\beta\rangle = (\langle\beta|\alpha\rangle)^*$
- Outer products $|\alpha\rangle\langle\beta|$ form operators on the vector space.
- Hermitian conjugate: $(|\alpha\rangle\langle\beta|)^\dagger = |\beta\rangle\langle\alpha|$
- Hermitian operators: $\hat{A}^\dagger = \hat{A}$
- Unitary operators preserve inner products:

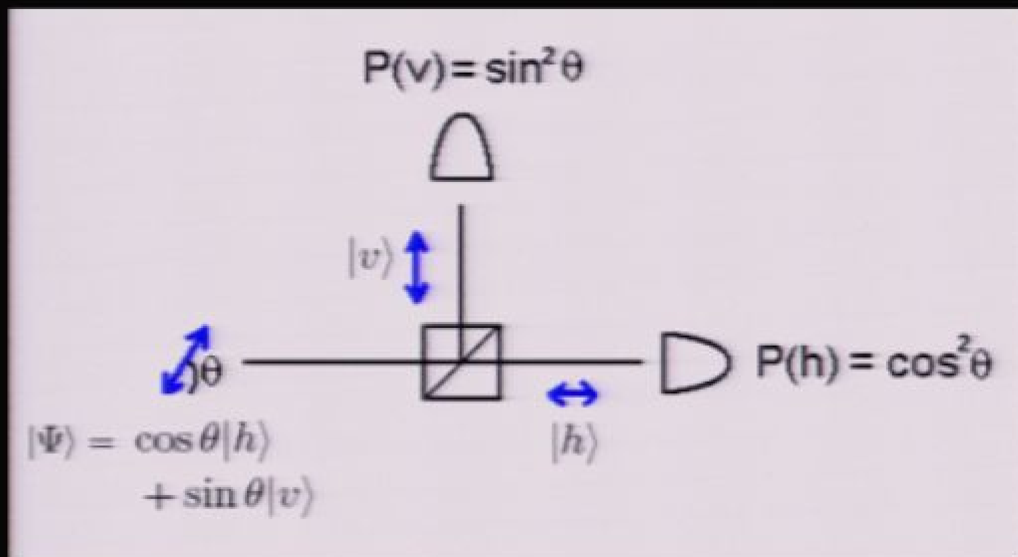
$$\hat{U}^\dagger\hat{U} = \hat{U}\hat{U}^\dagger = \hat{1}$$




|ψ⟩ ⟶ |φ⟩


|ψ⟩ → |φ⟩
= A |ψ⟩
⟨φ|φ⟩ = 1

Polarisation Measurements



- $P(h) = |\langle\Psi|h\rangle|^2$, $P(v) = |\langle\Psi|v\rangle|^2$
- Measurement transforms state to $|h\rangle$ or $|v\rangle$
- Measurement completely specified by operators $|h\rangle\langle h|$, $|v\rangle\langle v|$

Transformation of states

- Unitary evolution

$$|\psi(t)\rangle = \hat{U}(t)|\psi(0)\rangle$$

- Schrödinger equation

$$\begin{aligned}
\frac{\partial}{\partial t}|\psi(t)\rangle &= -\frac{i}{\hbar}\hat{H}|\psi(t)\rangle \\
\frac{\partial}{\partial t}\hat{U}(t)|\psi(0)\rangle &= -\frac{i}{\hbar}\hat{H}\hat{U}(t)|\psi(0)\rangle \\
\frac{\partial}{\partial t}\hat{U}(t) &= -\frac{i}{\hbar}\hat{H}\hat{U}(t)
\end{aligned}$$

Transformation of states

- Unitary evolution

$$|\psi(t)\rangle = \hat{U}(t)|\psi(0)\rangle$$

- Schrödinger equation

$$\frac{\partial}{\partial t}|\psi(t)\rangle = -\frac{i}{\hbar}\hat{H}|\psi(t)\rangle$$

$$\frac{\partial}{\partial t}\hat{U}(t)|\psi(0)\rangle = -\frac{i}{\hbar}\hat{H}\hat{U}(t)|\psi(0)\rangle$$

$$\frac{\partial}{\partial t}\hat{U}(t) = -\frac{i}{\hbar}\hat{H}\hat{U}(t)$$

Quantum Mechanics in Finite-Dimensions

- States represented as normalised state kets in a complex, linear vector space; $|\Psi\rangle$
- Von Neumann measurement along orthogonal directions $\{|i\rangle\}$
- Probability of obtaining result i:

$$P(i|\Psi) = |\langle\Psi|i\rangle|^2$$

- For a closed system, evolution is unitary

$$|\psi(t)\rangle = \hat{U}(t)|\psi(0)\rangle$$

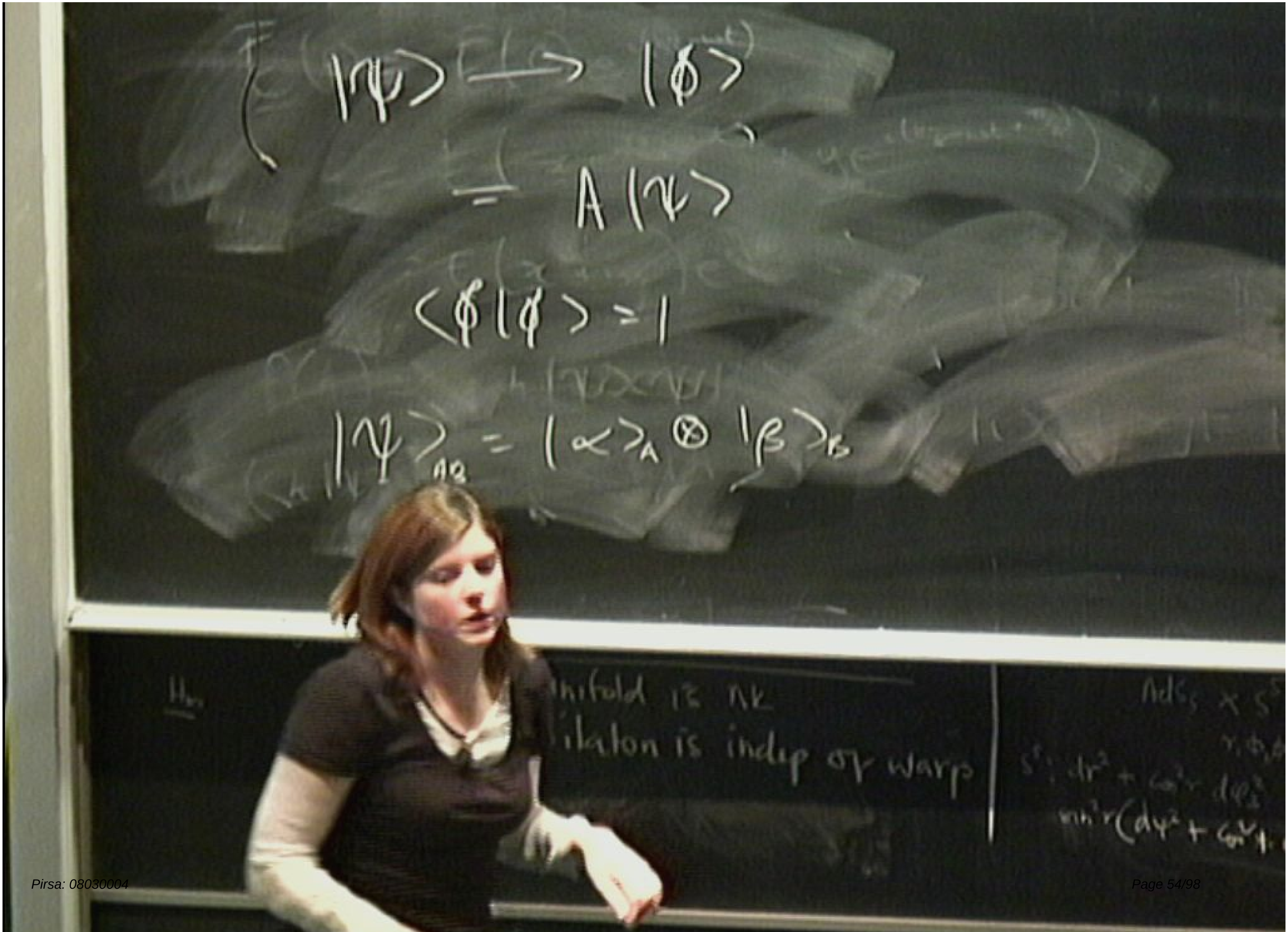
- Perfect discrimination is possible, in principle, between mutually orthogonal states.

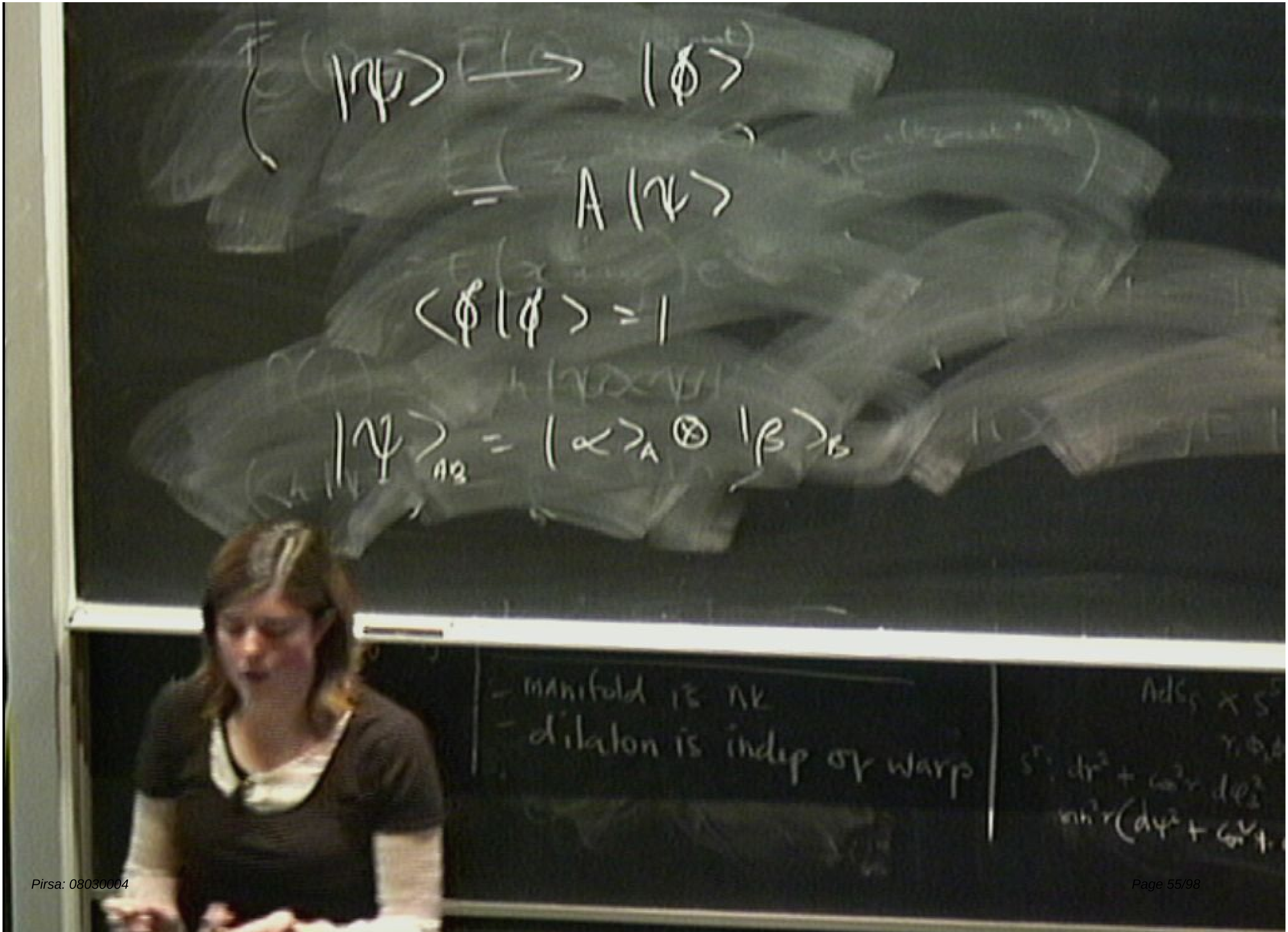
Entanglement

- Composite systems; Can write the state of a joint system as $|\Psi\rangle_{AB} = |\alpha\rangle_A |\beta\rangle_B$
- The superposition principle states that superposition states are also allowed, at least in principle

$$|\Psi\rangle_{AB} = a_0|\alpha_0\rangle_A|\beta_0\rangle_B + a_1|\alpha_1\rangle_A|\beta_1\rangle_B$$

- These states cannot be written as a product state, and arise due to some interaction of the systems; after the interaction the systems remain correlated.


$|\psi\rangle \longrightarrow |\phi\rangle$
$= A|\psi\rangle$
$\langle\phi|\phi\rangle = 1$
$|\psi\rangle_{AB} = |\alpha\rangle_A \otimes |\beta\rangle_B$
ilaton is indep of warp
$AdS_5 \times S^5$


|ψ⟩ ⟶ |φ⟩
= A|ψ⟩
⟨φ|φ⟩ = 1
|ψ⟩_AB = |α⟩_A ⊗ |β⟩_B
- manifold is RK
- dilaton is indep of warp
AdS_5 × S^5

Entanglement

- Composite systems; Can write the state of a joint system as $|\Psi\rangle_{AB} = |\alpha\rangle_A|\beta\rangle_B$
- The superposition principle states that superposition states are also allowed, at least in principle

$$|\Psi\rangle_{AB} = a_0|\alpha_0\rangle_A|\beta_0\rangle_B + a_1|\alpha_1\rangle_A|\beta_1\rangle_B$$

- These states cannot be written as a product state, and arise due to some interaction of the systems; after the interaction the systems remain correlated.

Entanglement

- Composite systems; Can write the state of a joint system as $|\Psi\rangle_{AB} = |\alpha\rangle_A |\beta\rangle_B$
- The superposition principle states that superposition states are also allowed, at least in principle

$$|\Psi\rangle_{AB} = a_0 |\alpha_0\rangle_A |\beta_0\rangle_B + a_1 |\alpha_1\rangle_A |\beta_1\rangle_B$$

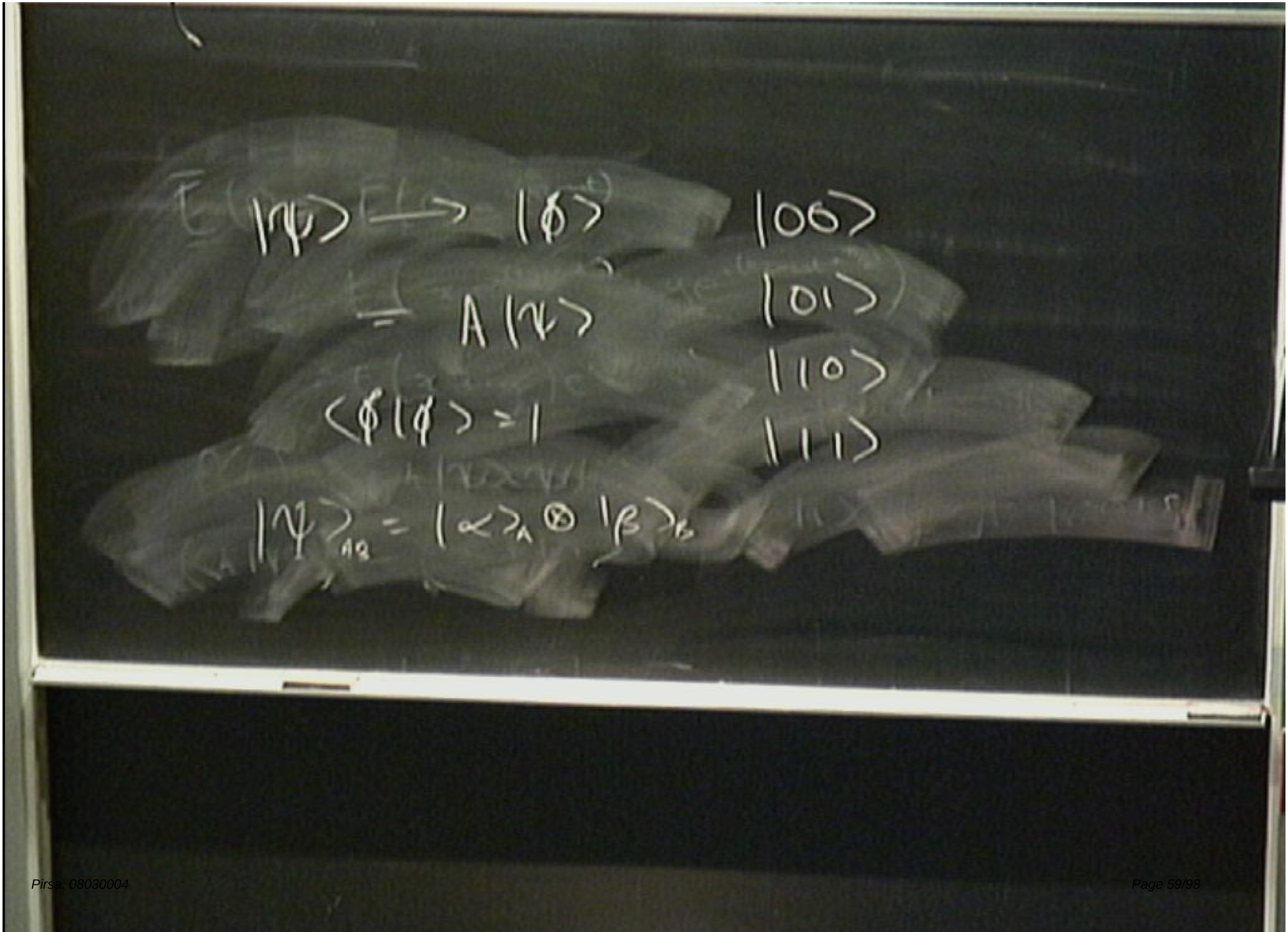
- These states cannot be written as a product state, and arise due to some interaction of the systems; after the interaction the systems remain correlated.

Entanglement

- The Bell states are given by

$$
\begin{aligned}
|\Psi_{00}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \\
|\Psi_{01}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \\
|\Psi_{10}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) \\
|\Psi_{11}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)
\end{aligned}
$$

and are said to be maximally entangled. Note that these states are mutually orthogonal.


|ψ⟩ ⟶ |φ⟩
A|ψ⟩
⟨φ|φ⟩ = 1
|ψ⟩AB = |α⟩A ⊗ |β⟩B
|00⟩
|01⟩
|10⟩
|11⟩

Entanglement

- The Bell states are given by

$$
\begin{aligned}
|\Psi_{00}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \\
|\Psi_{01}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \\
|\Psi_{10}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) \\
|\Psi_{11}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)
\end{aligned}
$$

and are said to be maximally entangled. Note that these states are mutually orthogonal.

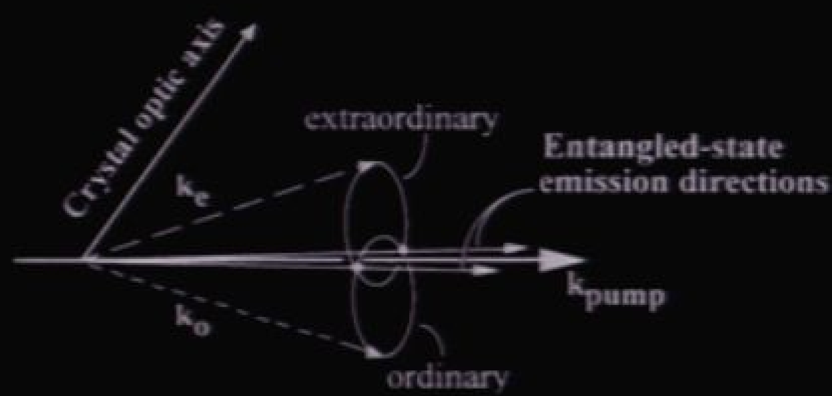
Entanglement

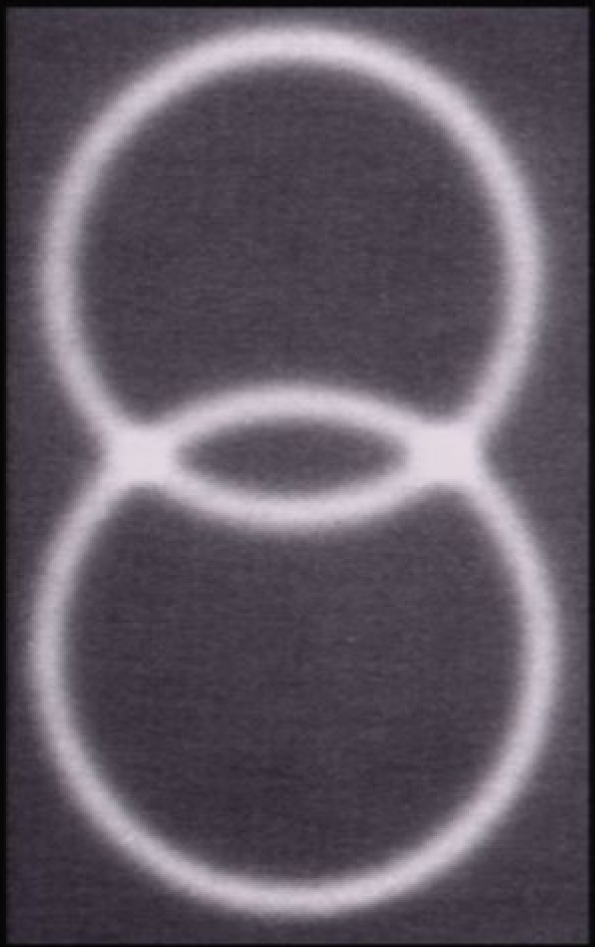
- The Bell states are given by

$$
\begin{aligned}
|\Psi_{00}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \\
|\Psi_{01}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \\
|\Psi_{10}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) \\
|\Psi_{11}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)
\end{aligned}
$$

and are said to be maximally entangled. Note that these states are mutually orthogonal.

Parametric Down Conversion (Type II)





P.Kwiat et al, PRL 75, 4337 (1995)

No-cloning Theorem

- Arbitrary quantum states cannot be cloned
- Proof is due to the linearity of quantum mechanics
  - Suppose there exists an operator $\hat{V}$ such that

$$\begin{aligned} \hat{V}|0\rangle_A|\psi\rangle_B &= |0\rangle_A|0\rangle_B \\ \hat{V}|1\rangle_A|\psi\rangle_B &= |1\rangle_A|1\rangle_B \end{aligned}$$

  - Consider the action of this operator on a superposition state

$$\begin{aligned} \hat{V}\left(\alpha_0|0\rangle_A + \alpha_1|1\rangle_A\right)|\psi\rangle_B &= \alpha_0|0\rangle_A|0\rangle_B + \alpha_1|1\rangle_A|1\rangle_B \\ &\neq \left(\alpha_0|0\rangle_A + \alpha_1|1\rangle_A\right)\left(\alpha_0|0\rangle_B + \alpha_1|1\rangle_B\right) \end{aligned}$$

Super-dense coding

- Suppose Alice and Bob share the entangled state

$$|\Psi_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

- Alice can convert the shared state into any one of the other Bell states

$$\begin{aligned}
|\Psi_{00}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \\
|\Psi_{01}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \\
|\Psi_{10}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) \\
|\Psi_{11}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)
\end{aligned}$$

using only local operations

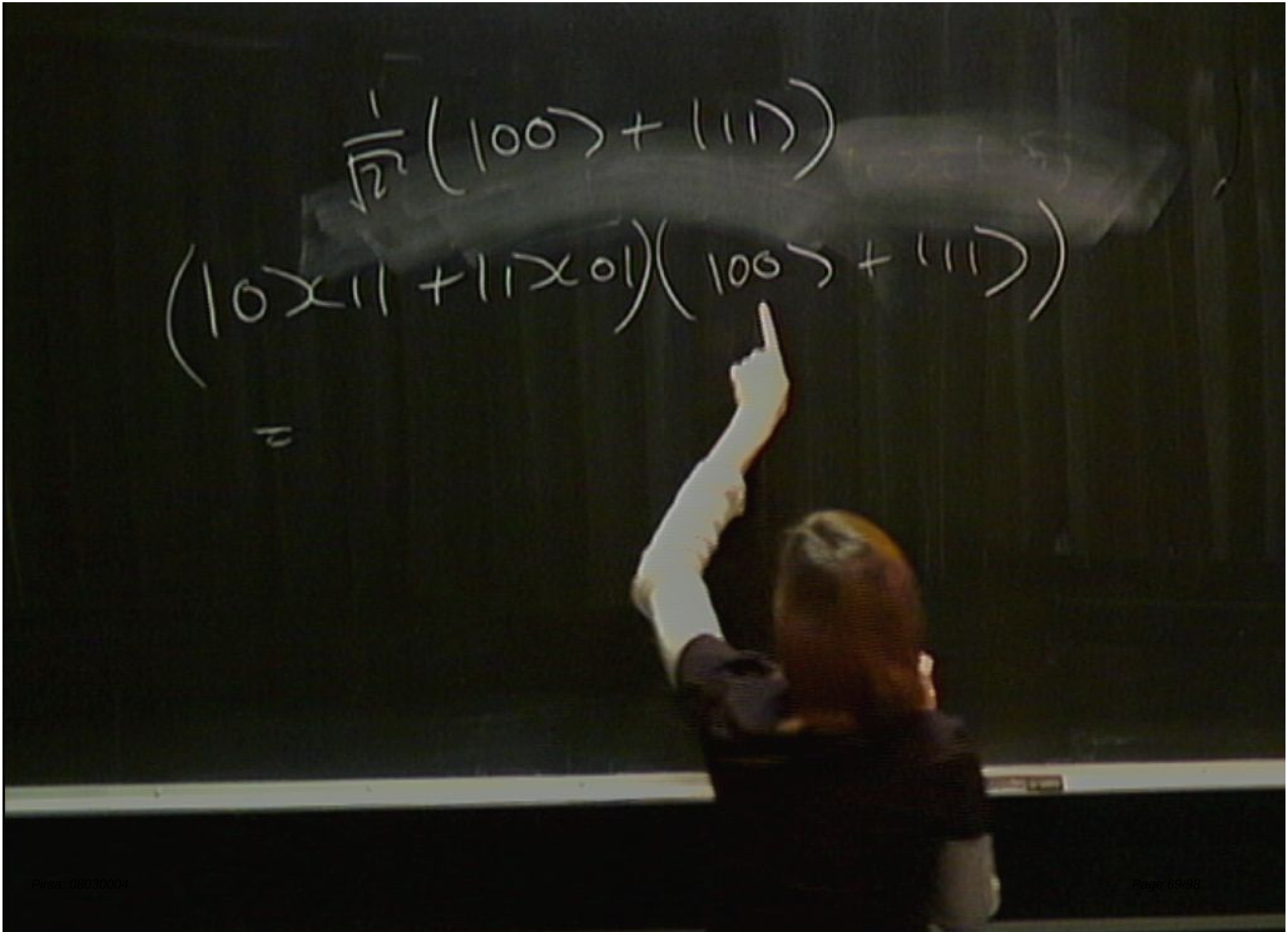
$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

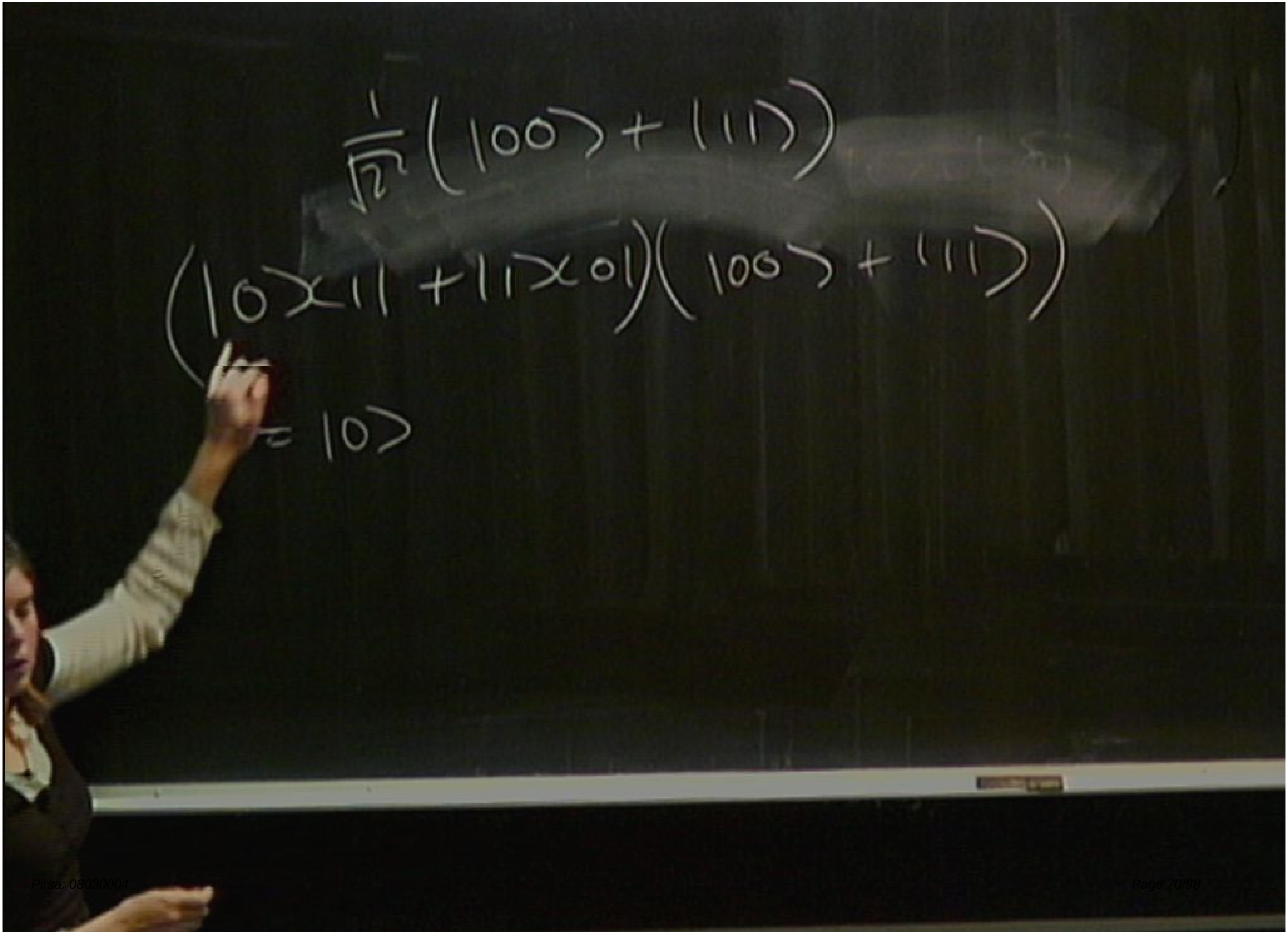
$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

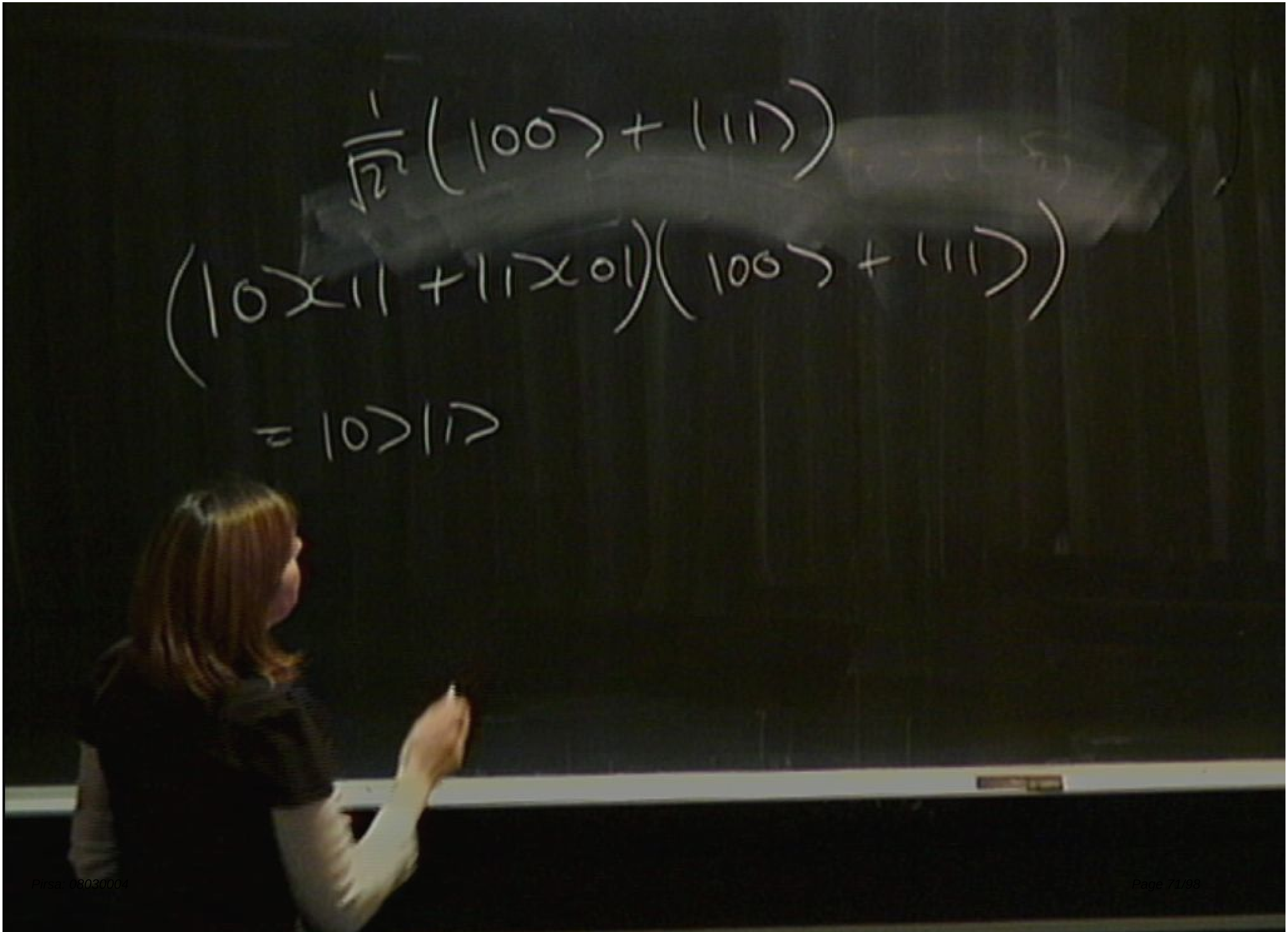
$$\left(|0\rangle\langle 11| + |1\rangle\langle 01|\right)$$

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

$$\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right)\left(|00\rangle + |11\rangle\right)$$


1/√2 (|00⟩ + |11⟩)
(|0⟩⟨1| + |1⟩⟨0|)(|00⟩ + |11⟩)
=

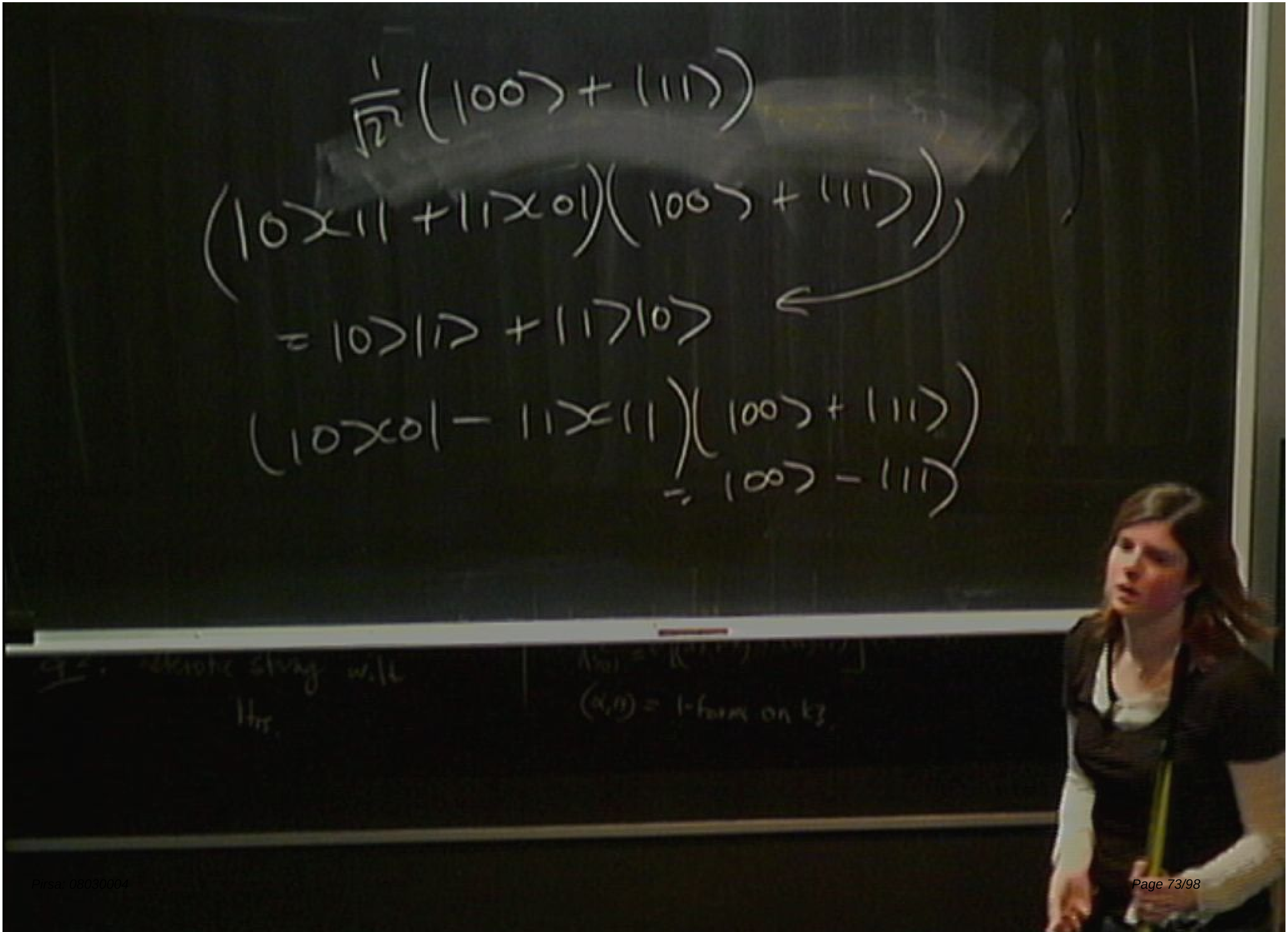

1/√2 (|00⟩ + |11⟩)
(|10⟩⟨11| + |11⟩⟨01|)(|00⟩ + |11⟩)
= |10⟩


1/√2 (|00⟩ + |11⟩)
(|0⟩⟨11| + |1⟩⟨01|)(|00⟩ + |11⟩)
= |0⟩|1⟩

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

$$\left(|10\rangle\langle 11| + |11\rangle\langle 01|\right)\left(|00\rangle + |11\rangle\right)$$

$$= |0\rangle|1\rangle + |1\rangle|0\rangle$$


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

Super-dense coding

- To encode the message "00", Alice applies the identity operator (i.e. does nothing) to her qubit.
- Similarly, to encode the messages "01", "10", or "11", Alice applies one of the operators

$$
\begin{aligned}
\hat{U}_{01} &= \hat{X} = |0\rangle_{A\,A}\langle 1| + |1\rangle_{A\,A}\langle 0| \\
\hat{U}_{10} &= \hat{Z} = |0\rangle_{A\,A}\langle 0| - |1\rangle_{A\,A}\langle 1| \\
\hat{U}_{11} &= \hat{Z}\hat{X} = |1\rangle_{A\,A}\langle 0| - |1\rangle_{A\,A}\langle 0|
\end{aligned}
$$

- Alice then sends her qubit to Bob, who measures in the Bell basis to determine the message.
- Alice can encode two bits of information by sending only one qubit.

Super-dense coding

- To encode the message "00", Alice applies the identity operator (i.e. does nothing) to her qubit.
- Similarly, to encode the messages "01", "10", or "11", Alice applies one of the operators

$$\hat{U}_{01} = \hat{X} = |0\rangle_{A\,A}\langle 1| + |1\rangle_{A\,A}\langle 0|$$
$$\hat{U}_{10} = \hat{Z} = |0\rangle_{A\,A}\langle 0| - |1\rangle_{A\,A}\langle 1|$$
$$\hat{U}_{11} = \hat{Z}\hat{X} = |1\rangle_{A\,A}\langle 0| - |1\rangle_{A\,A}\langle 0|$$

- Alice then sends her qubit to Bob, who measures in the Bell basis to determine the message.
- Alice can encode two bits of information by sending only one qubit.

Super-dense coding

- Suppose Alice and Bob share the entangled state

$$|\Psi_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

- Alice can convert the shared state into any one of the other Bell states

$$\begin{aligned}
|\Psi_{00}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \\
|\Psi_{01}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \\
|\Psi_{10}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) \\
|\Psi_{11}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)
\end{aligned}$$

using only local operations

Super-dense coding

- To encode the message "00", Alice applies the identity operator (i.e. does nothing) to her qubit.
- Similarly, to encode the messages "01", "10", or "11", Alice applies one of the operators

$$\begin{aligned} \hat{U}_{01} &= \hat{X} = |0\rangle_{A\,A}\langle 1| + |1\rangle_{A\,A}\langle 0| \\ \hat{U}_{10} &= \hat{Z} = |0\rangle_{A\,A}\langle 0| - |1\rangle_{A\,A}\langle 1| \\ \hat{U}_{11} &= \hat{Z}\hat{X} = |1\rangle_{A\,A}\langle 0| - |1\rangle_{A\,A}\langle 0| \end{aligned}$$

- Alice then sends her qubit to Bob, who measures in the Bell basis to determine the message.
- Alice can encode two bits of information by sending only one qubit.

Super-dense coding

- Suppose Alice and Bob share the entangled state

$$|\Psi_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

- Alice can convert the shared state into any one of the other Bell states

$$\begin{aligned}
|\Psi_{00}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \\
|\Psi_{01}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) \\
|\Psi_{10}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B) \\
|\Psi_{11}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)
\end{aligned}$$

using only local operations

Super-dense coding

- To encode the message "00", Alice applies the identity operator (i.e. does nothing) to her qubit.
- Similarly, to encode the messages "01", "10", or "11", Alice applies one of the operators

$$\hat{U}_{01} = \hat{X} = |0\rangle_{A\,A}\langle 1| + |1\rangle_{A\,A}\langle 0|$$
$$\hat{U}_{10} = \hat{Z} = |0\rangle_{A\,A}\langle 0| - |1\rangle_{A\,A}\langle 1|$$
$$\hat{U}_{11} = \hat{Z}\hat{X} = |1\rangle_{A\,A}\langle 0| - |1\rangle_{A\,A}\langle 0|$$

- Alice then sends her qubit to Bob, who measures in the Bell basis to determine the message.
- Alice can encode two bits of information by sending only one qubit.

Deutsch algorithm

- Suppose I have a black box which acts as follows

$$|x\rangle|y\rangle \;\rightarrow\; |x\rangle|y \oplus f(x)\rangle$$

  for some binary function f. I want to know whether f(0) and f(1) are the same or different.
- Classically, need to evaluate both f(0) and f(1)
- What about quantum mechanically? The superposition principle means that I can evaluate both at the same time.

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|0\rangle \;\rightarrow\; \frac{1}{\sqrt{2}}\left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle\right)$$

Deutsch algorithm

- Suppose both the target and the control are superposition states

$$\frac{1}{2}\left(|0\rangle+|1\rangle\right)\left(|0\rangle-|1\rangle\right) \rightarrow \frac{1}{2}\Big((-1)^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle\Big)\left(|0\rangle-|1\rangle\right)$$

- If f(0) and f(1) are equal, the control qubit is in state

$$\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$$

- If they are different, the control qubit is in the orthogonal state $\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$

Deutsch algorithm

- Suppose I have a black box which acts as follows

$$|x\rangle|y\rangle \;\rightarrow\; |x\rangle|y \oplus f(x)\rangle$$

  for some binary function f. I want to know whether f(0) and f(1) are the same or different.
- Classically, need to evaluate both f(0) and f(1)
- What about quantum mechanically? The superposition principle means that I can evaluate both at the same time.

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|0\rangle \;\rightarrow\; \frac{1}{\sqrt{2}}\left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle\right)$$

Deutsch algorithm

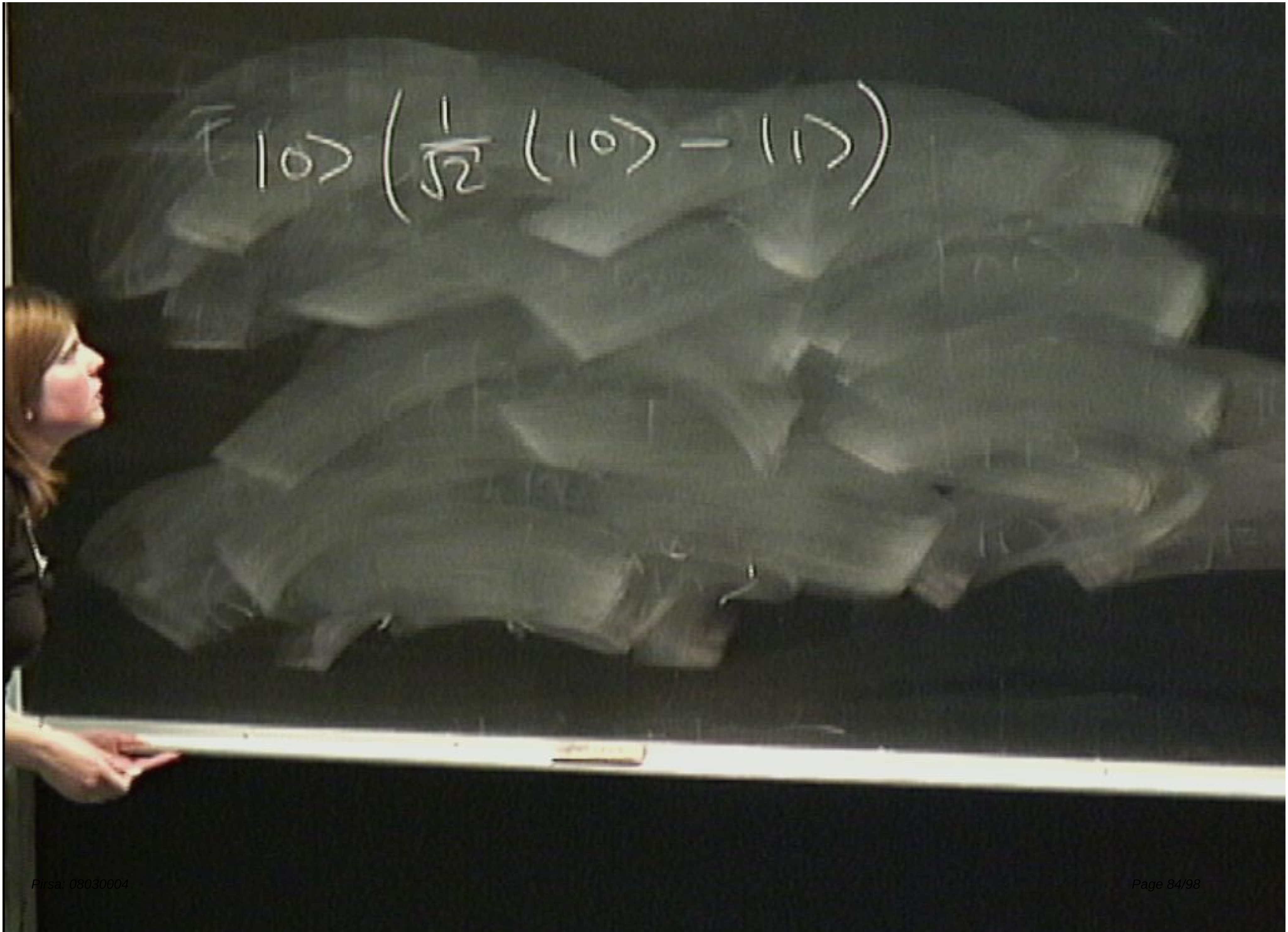
- Suppose both the target and the control are superposition states

$$\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \rightarrow \frac{1}{2}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)(|0\rangle - |1\rangle)$$

- If f(0) and f(1) are equal, the control qubit is in state

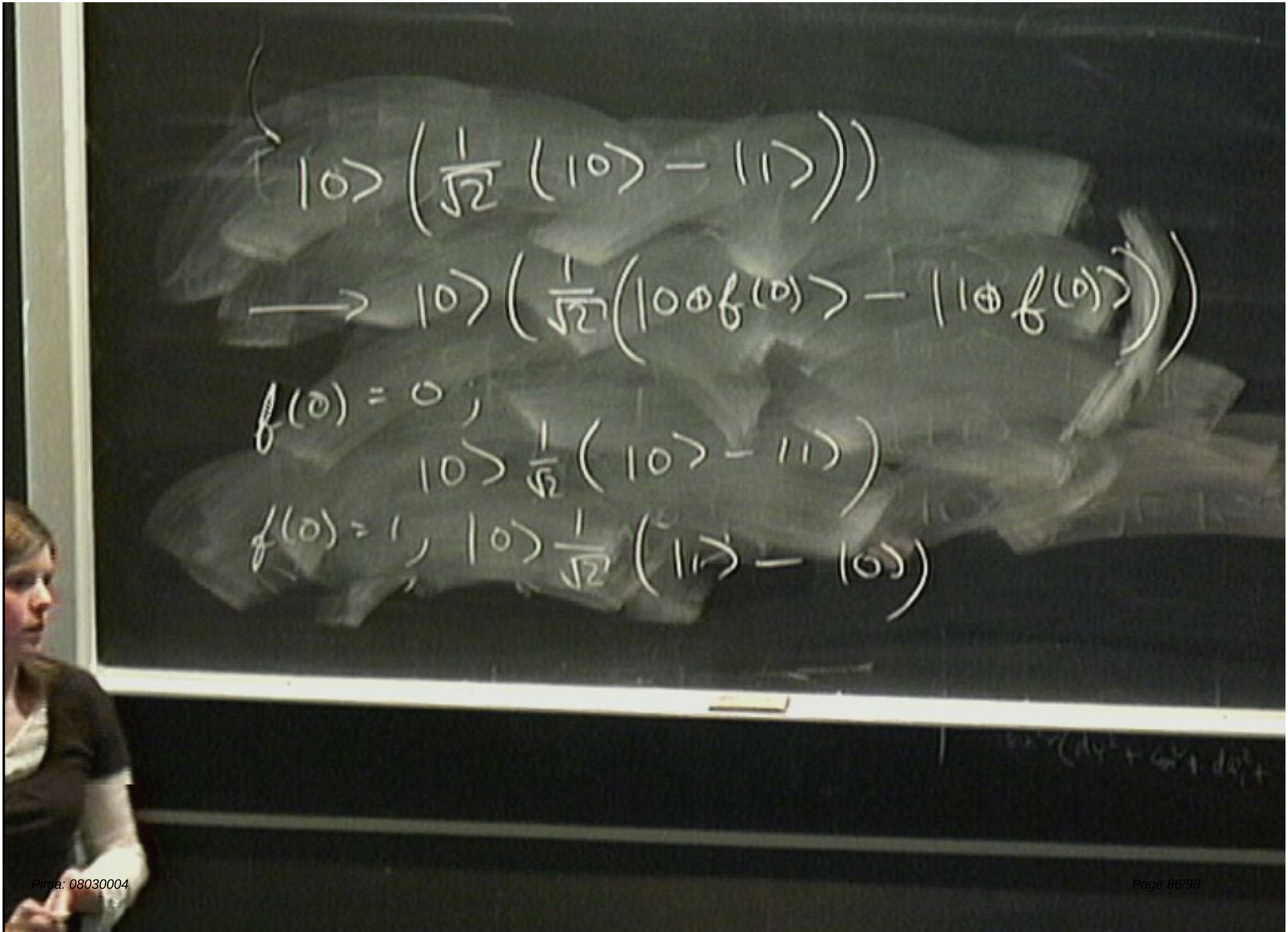
$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

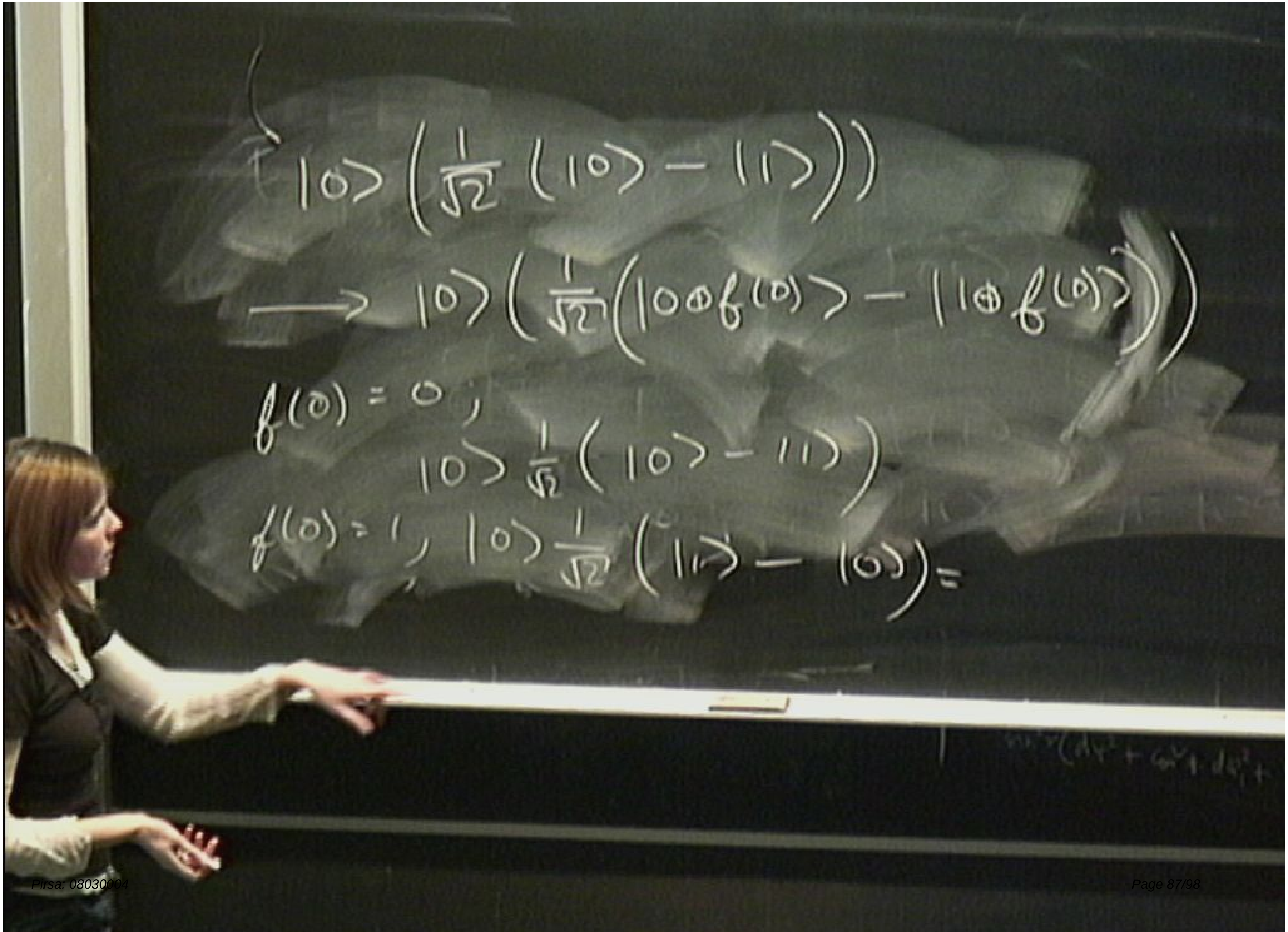
- If they are different, the control qubit is in the orthogonal state $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$


F |0⟩ (1/√2 (|0⟩ − |1⟩))

$$F|0\rangle\left(\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right)$$

$$\longrightarrow |0\rangle\left(\frac{1}{\sqrt{2}}\left(|0+f(0)\rangle - |1+f(0)\rangle\right)\right)$$


$|0\rangle \left(\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right)$
$\longrightarrow |0\rangle \left(\frac{1}{\sqrt{2}} \left(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle \right) \right)$
$f(0) = 0,$
$|0\rangle \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$
$f(0) = 1, \; |0\rangle \frac{1}{\sqrt{2}} (|1\rangle - |0\rangle)$


|0⟩ (1/√2 (|0⟩ − |1⟩))
→ |0⟩ (1/√2 (|0⊕f(0)⟩ − |1⊕f(0)⟩))
f(0) = 0 ;
|0⟩ 1/√2 (|0⟩ − |1⟩)
f(0) = 1 , |0⟩ 1/√2 (|1⟩ − |0⟩) =

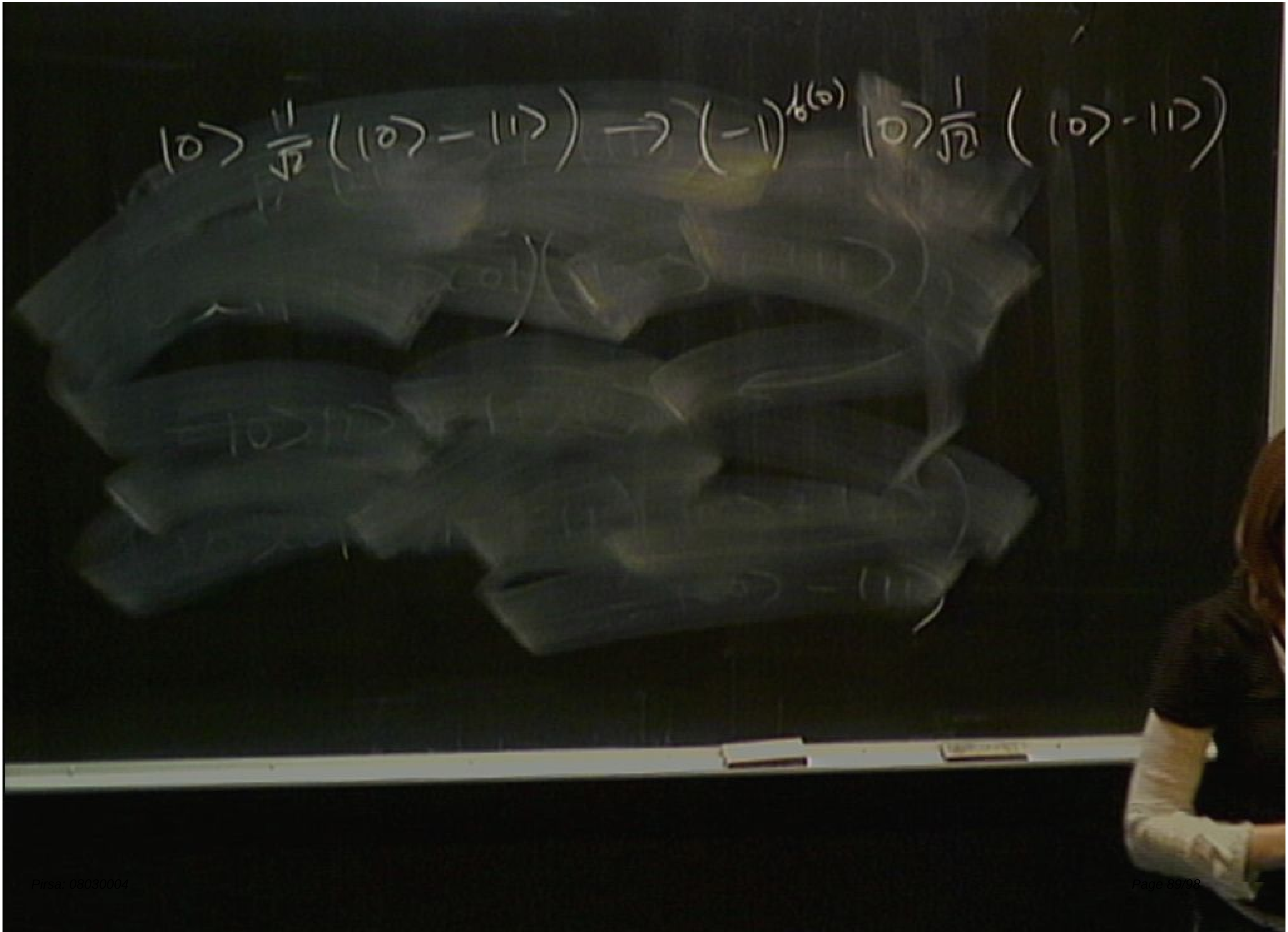
$$|0\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right)$$

$$\longrightarrow |0\rangle\left(\frac{1}{\sqrt{2}}\left(|0\oplus f(0)\rangle - |1\oplus f(0)\rangle\right)\right)$$

$f(0) = 0$;

$$|0\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$f(0) = 1$, $|0\rangle\frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -|0\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$


|0> 1/√2 (|0> − |1>) → (−1)^f(0) |0> 1/√2 (|0> − |1>)

$$|0\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow (-1)^{f(0)} |0\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|1\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow (-1)^{f(1)} |0\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|0\rangle \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \longrightarrow (-1)^{f(0)}\, |0\rangle \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$|1\rangle \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \longrightarrow (-1)^{f(1)}\, |0\rangle \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$|0\rangle \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \to (-1)^{f(0)} |0\rangle \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$|1\rangle \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \to (-1)^{f(1)} |0\rangle \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right)$$

$$= \frac{1}{2}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)\left(|0\rangle - |1\rangle\right)$$

Deutsch algorithm

- Suppose both the target and the control are superposition states

$$\frac{1}{2}\left(|0\rangle + |1\rangle\right)\left(|0\rangle - |1\rangle\right) \rightarrow \frac{1}{2}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)\left(|0\rangle - |1\rangle\right)$$

- If f(0) and f(1) are equal, the control qubit is in state

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

- If they are different, the control qubit is in the orthogonal state $\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$

Summary: Classical vs Quantum Information

- Classical information stored as "0"s and "1"s – "bit"
- e.g punch cards, charge in a capacitor, current flowing, magnetic storage

- Quantum information: two-level system "qubit" $|0\rangle, |1\rangle$
- Superposition principle: $\alpha|0\rangle + \beta|1\rangle$ also allowed
- Quantum parallelism

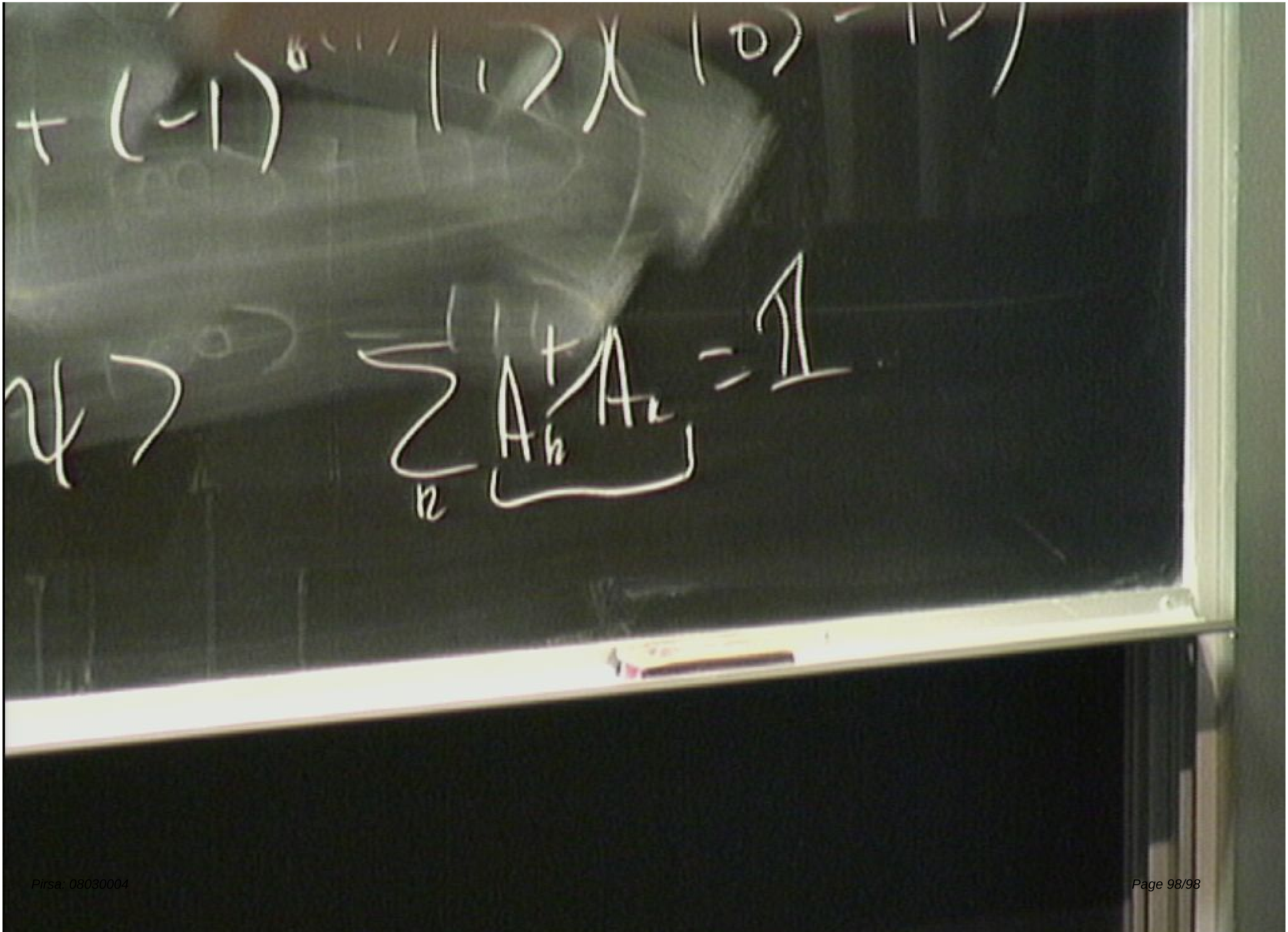
Summary: Quantum Information

- No-cloning theorem.
- Entanglement, that is quantum correlations, can be used as a resource in quantum information.
- The superposition principle allows quantum parallelism in information processing, it is sometimes possible to use this to investigate global properties of a function efficiently.

Summary: Quantum Information

- No-cloning theorem.
- Entanglement, that is quantum correlations, can be used as a resource in quantum information.
- The superposition principle allows quantum parallelism in information processing, it is sometimes possible to use this to investigate global properties of a function efficiently.

(α,β) = 1-forms on


$\sum_k A_k^\dagger A_k = \mathbb{1}$