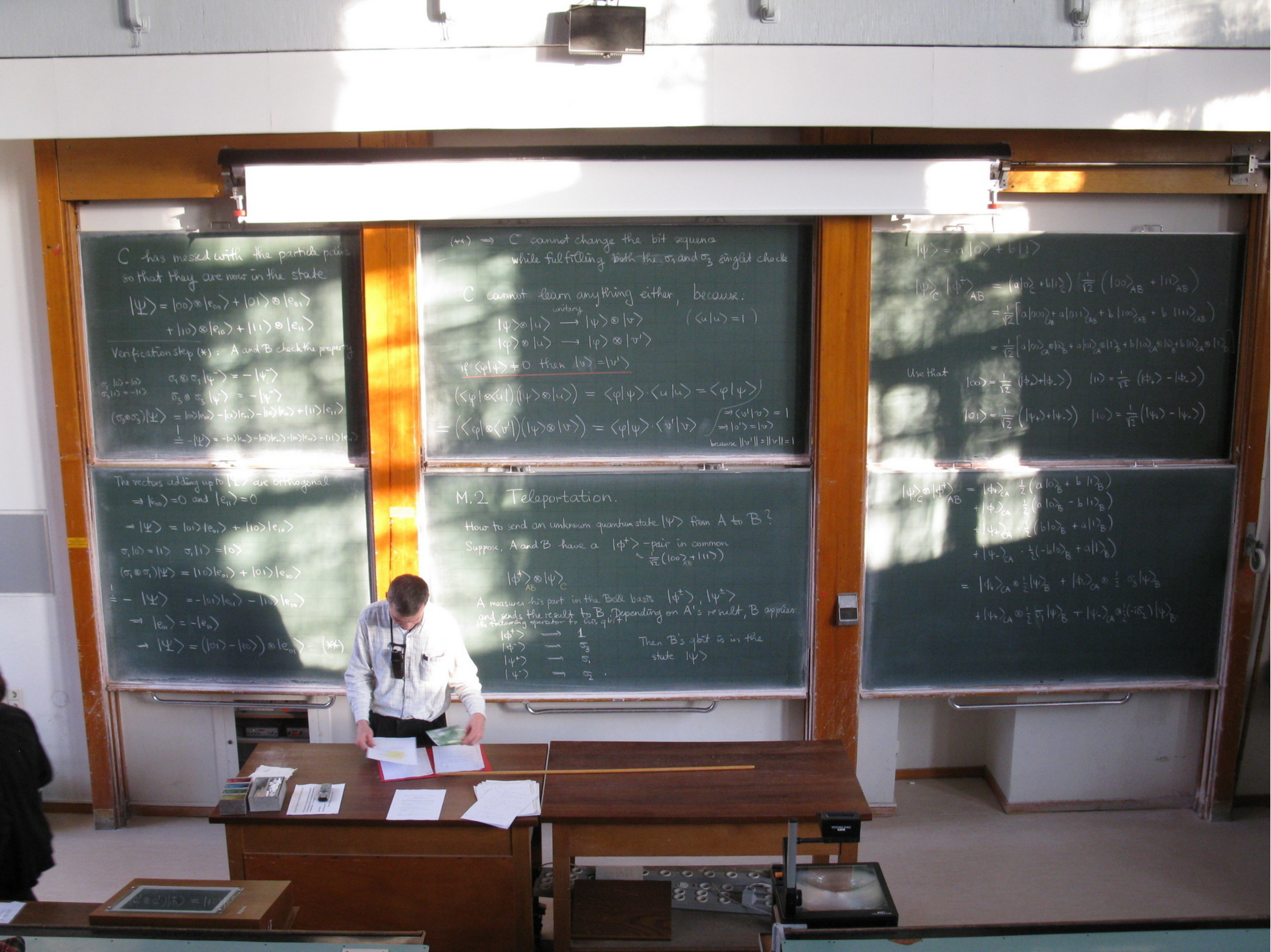

density matrix $\rho = \rho^+ \geq 0$, $\mathrm{Tr}\,\rho = 1$.
special case: pure state
(↔ a vector in Hilbert space)
$\rho_\psi = P_\psi = |\psi\rangle\langle\psi|$
$\rightarrow \rho_\psi^2 = \rho_\psi$ (projection)
in general, $\rho^2 < \rho$ if $\rho$ is not pure.
DM useful whenever $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$
regardless of the dimensions of $\mathcal{H}_1$ and $\mathcal{H}_2$.
Today. $\mathcal{H}_1 = \mathcal{H}_2 \cong \mathbb{C}^2$
1 2 $|\psi^-\rangle$
Def. Bell states
$|\phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$
$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ singlet state
These vectors are orthonormal in $\mathbb{C}^2 \otimes \mathbb{C}^2$
(exercise!)
They are all entangled states.
The density matrix for measurements on qbit 1 is
$\rho_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
(maximal entropy)
e.g. for $|\psi^-\rangle$ $A = A^+ \in M_2(\mathbb{C})$
$\langle\psi^-| A \otimes 1 |\psi^-\rangle = \frac{1}{2}\left(\langle 01| - \langle 10|\right)(A \otimes 1)\left(|01\rangle - |10\rangle\right)$
$= \frac{1}{2}\big(\langle 01|A\otimes 1|01\rangle - \langle 01|A\otimes 1|10\rangle - \langle 10|A\otimes 1|01\rangle$
$+ \langle 10|A\otimes 1|10\rangle\big)$
$= \frac{1}{2}\left(\langle 0|A|0\rangle + \langle 1|A|1\rangle\right) = \frac{1}{2}(A_{00} + A_{11})$
$\langle 01|A\otimes 1|10\rangle = \langle 0|A|1\rangle \cdot \underbrace{\langle 1|0\rangle}_{0} = 0$
$\langle 0|\otimes\langle 1|( \quad )|1\rangle\otimes|0\rangle$
$= \frac{1}{2}\mathrm{Tr}(A) = \mathrm{Tr}(A \cdot \frac{1}{2} 1)$
$|\psi^-\rangle$ has the following properties.
$(\vec{\sigma} \otimes 1)|\psi^-\rangle = -(1 \otimes \vec{\sigma})|\psi^-\rangle$
$\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ vector of Pauli matrices, and $|0\rangle \leftrightarrow \binom{1}{0}$ $|1\rangle \leftrightarrow \binom{0}{1}$
more generally
$\langle\psi^-| \vec{a}\cdot\vec{\sigma} \otimes \vec{b}\cdot\vec{\sigma} |\psi^-\rangle = -\vec{a}\cdot\vec{b}$. $\forall \vec{a}, \vec{b} \in \mathbb{R}^3$.
M. Cryptography and Teleportation
M.1 Cryptography, here: key exchange
Angela ⟶ Barack
$T \rightarrow M \rightarrow T = M \oplus_2 S$
one-time pad:
a sequence of bits S
known only to A
and B
$M = T \oplus_2 S$
eavesdropper
Cheney
Protocol: set up a source of particle pairs
in the $|\psi^-\rangle$ state.
A and B perform measurements of $\sigma_1$ and $\sigma_3$
(1 and 3 are chosen randomly, with prob' $\frac{1}{2}$)
A and B make public on which of the particles they measured
$\sigma_1$ or $\sigma_3$, but do not reveal the result of the measurement.
A and B select the subsequence where they measured
the same $\sigma_i$
A and B pick another subsequence randomly,
to check if someone listened.
The remaining sequence is M



C has messed with the particle pairs so that they are now in the state
$|\Psi\rangle = |00\rangle \otimes |e_{00}\rangle + |01\rangle \otimes |e_{01}\rangle + |10\rangle \otimes |e_{10}\rangle + |11\rangle \otimes |e_{11}\rangle$
Verification step (*): A and B check the property
$\sigma_3 |0\rangle = |0\rangle$
$\sigma_3 |1\rangle = -|1\rangle$
$\sigma_1 \otimes \sigma_1 |\psi^-\rangle = -|\psi^-\rangle$
$\sigma_3 \otimes \sigma_3 |\psi^-\rangle = -|\psi^-\rangle$
$(\sigma_3 \otimes \sigma_3)|\Psi\rangle = |00\rangle|e_{00}\rangle - |01\rangle|e_{01}\rangle - |10\rangle|e_{10}\rangle + |11\rangle|e_{11}\rangle$
$\overset{!}{=} -|\Psi\rangle = -|00\rangle|e_{00}\rangle - |01\rangle|e_{01}\rangle - |10\rangle|e_{10}\rangle - |11\rangle|e_{11}\rangle$
The vectors adding up to $|\Psi\rangle$ are orthogonal
$\Rightarrow |e_{00}\rangle = 0$ and $|e_{11}\rangle = 0$
$\Rightarrow |\Psi\rangle = |01\rangle|e_{01}\rangle + |10\rangle|e_{10}\rangle$
$\sigma_1|0\rangle = |1\rangle \quad \sigma_1|1\rangle = |0\rangle$
$(\sigma_1 \otimes \sigma_1)|\Psi\rangle = |10\rangle|e_{01}\rangle + |01\rangle|e_{10}\rangle$
$\overset{!}{=} -|\Psi\rangle = -|01\rangle|e_{01}\rangle - |10\rangle|e_{10}\rangle$
$\Rightarrow |e_{01}\rangle = -|e_{10}\rangle$
$\Rightarrow |\Psi\rangle = (|01\rangle - |10\rangle) \otimes |e_{01}\rangle$ (**)
(**) $\Rightarrow$ C cannot change the bit sequence
while fulfilling ~~both the~~ $\sigma_1$ and $\sigma_3$ singlet check
C cannot learn anything either, because:
$|\psi\rangle \otimes |u\rangle \xrightarrow{\text{unitary}} |\psi\rangle \otimes |v\rangle \qquad (\langle u|u\rangle = 1)$
$|\varphi\rangle \otimes |u\rangle \longrightarrow |\varphi\rangle \otimes |v'\rangle$
if $\langle\varphi|\psi\rangle \neq 0$ then $|v\rangle = |v'\rangle$
$(\langle\varphi| \otimes \langle u|)(|\psi\rangle \otimes |u\rangle) = \langle\varphi|\psi\rangle \cdot \langle u|u\rangle = \langle\varphi|\psi\rangle$
$= (\langle\varphi| \otimes \langle v'|)(|\psi\rangle \otimes |v\rangle) = \langle\varphi|\psi\rangle \cdot \langle v'|v\rangle$
$\Rightarrow \langle v'|v\rangle = 1$
$\Rightarrow |v'\rangle = |v\rangle$
because $\|v'\| = \|v\| = 1$
M.2 Teleportation.
How to send an unknown quantum state $|\psi\rangle$ from A to B?
Suppose, A and B have a $|\phi^+\rangle$-pair in common
$\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle)$
$|\phi^+\rangle_{AB} \otimes |\psi\rangle_C$
A measures his part in the Bell basis $|\phi^\pm\rangle$, $|\psi^\pm\rangle$
and sends the result to B. Depending on A's result, B applies the following operator to his qbit
$|\phi^+\rangle \longrightarrow 1$
$|\phi^-\rangle \longrightarrow \sigma_3$
$|\psi^+\rangle \longrightarrow \sigma_1$
$|\psi^-\rangle \longrightarrow \sigma_2$.
Then B's qbit is in the state $|\psi\rangle$
$|\psi\rangle = a|0\rangle + b|1\rangle$
$|\psi\rangle_C |\phi^+\rangle_{AB} = (a|0\rangle_C + b|1\rangle_C) \frac{1}{\sqrt{2}} (|00\rangle_{AB} + |11\rangle_{AB})$
$= \frac{1}{\sqrt{2}} [a|000\rangle_{CAB} + a|011\rangle_{CAB} + b|100\rangle_{CAB} + b|111\rangle_{CAB})$
$= \frac{1}{\sqrt{2}} [a|00\rangle_{CA} \otimes |0\rangle_B + a|01\rangle_{CA} \otimes |1\rangle_B + b|10\rangle_{CA} \otimes |0\rangle_B + b|11\rangle_{CA} \otimes |1\rangle_B]$
Use that
$|00\rangle = \frac{1}{\sqrt{2}}(|\phi_+\rangle + |\phi_-\rangle) \qquad |11\rangle = \frac{1}{\sqrt{2}}(|\phi_+\rangle - |\phi_-\rangle)$
$|01\rangle = \frac{1}{\sqrt{2}}(|\psi_+\rangle + |\psi_-\rangle) \qquad |10\rangle = \frac{1}{\sqrt{2}}(|\psi_+\rangle - |\psi_-\rangle)$
$|\psi\rangle_C \otimes |\phi^+\rangle_{AB} = |\phi_+\rangle_{CA} \frac{1}{2}(a|0\rangle_B + b|1\rangle_B)$
$+ |\phi_-\rangle_{CA} \cdot \frac{1}{2}(a|0\rangle_B - b|1\rangle_B)$
$+ |\psi_+\rangle_{CA} \cdot \frac{1}{2}(b|0\rangle_B + a|1\rangle_B)$
$+ |\psi_-\rangle_{CA} \cdot \frac{1}{2}(-b|0\rangle_B + a|1\rangle_B)$
$= |\phi_+\rangle_{CA} \otimes \frac{1}{2}|\psi\rangle_B + |\phi_-\rangle_{CA} \otimes \frac{1}{2} \sigma_3 |\psi\rangle_B$
$+ |\psi_+\rangle_{CA} \otimes \frac{1}{2} \sigma_1 |\psi\rangle_B + |\psi_-\rangle_{CA} \otimes \frac{1}{2}(-i\sigma_2)|\psi\rangle_B$.