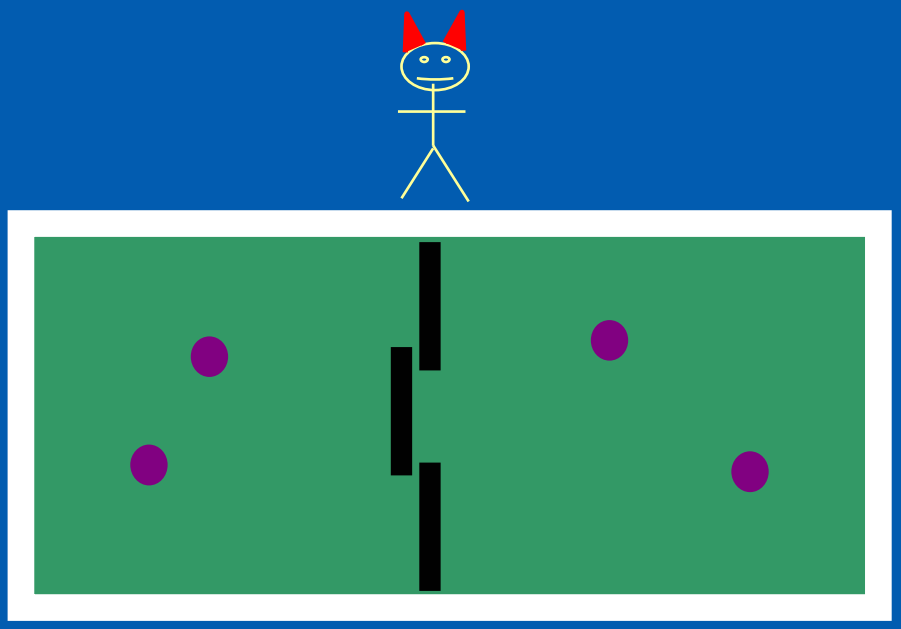
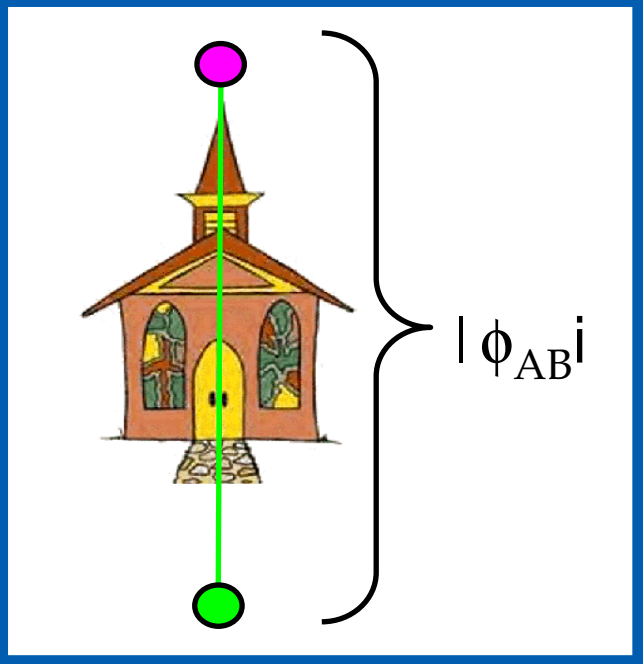
The power of forgetting

Patrick Hayden (McGill Computer Science)

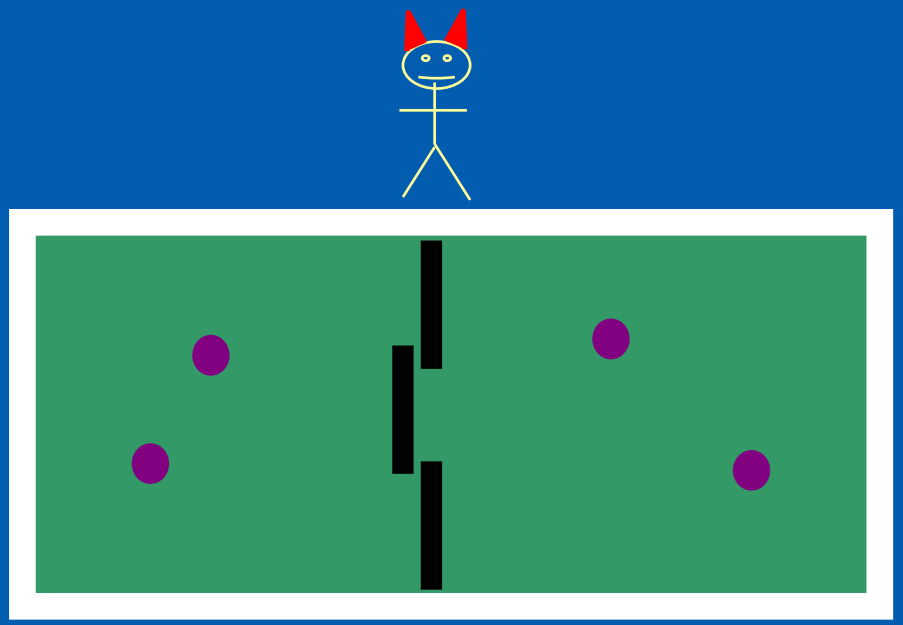




Overview

- Maxwell's demon
- Erasure in quantum information
  - Entanglement-assisted capacity
  - Capacities of broadcast channels
- Consequences for "real" physical systems
  - Random dynamics

Maxwell's Demon



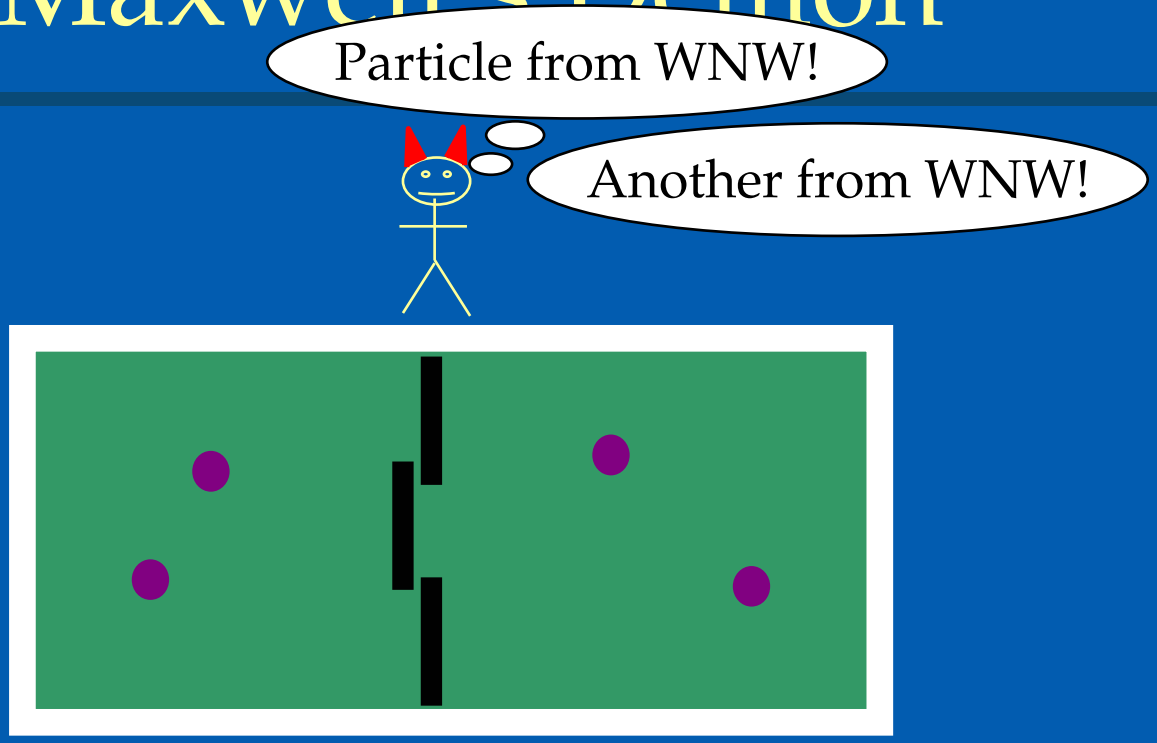
Gas originally at equilibrium. Demon inserts partition.

Demon uses door to allow particles to move left to right, but not right to left.

Entropy decreases.

What gives? Stumped Maxwell, von Neumann, Brillouin, Szilard...

Maxwell's Demon



Watch again...

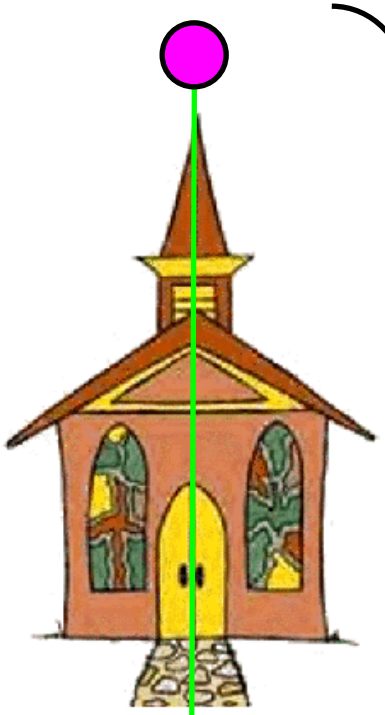
Demon must process information about incoming particles.

Finite memory: he must eventually start *forgetting*.

Landauer's principle restores global increase of entropy.

[Bennett 82]

Church of the Larger Hilbert Space



$|\phi_{AB}\rangle$

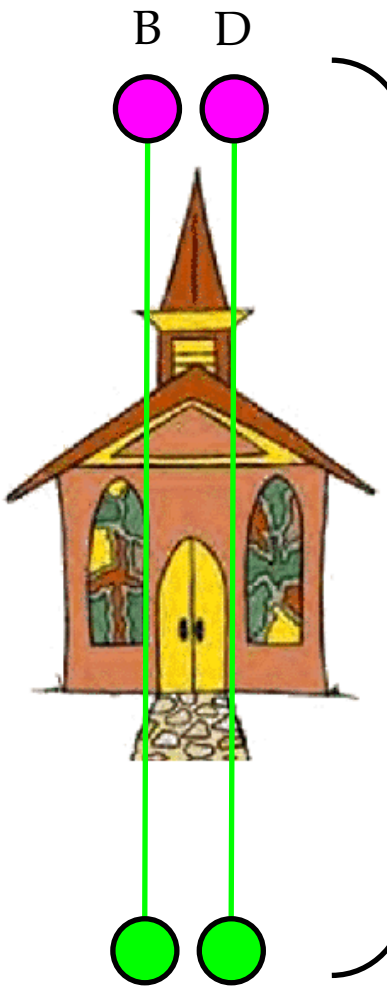
ρ_A

When faced with a mixed state ρ_A, we can always imagine that A is part of a larger system A - B on which the state is *pure*.

Purifications are essentially *unique*. (Up to local unitary transformations of the purifying space.)

$Tr_B\ |\phi_{AB}\rangle\langle\phi_{AB}| = \rho_A$

Purification and correlation



$|\phi_{AB}\rangle\,|\psi_{BD}\rangle$

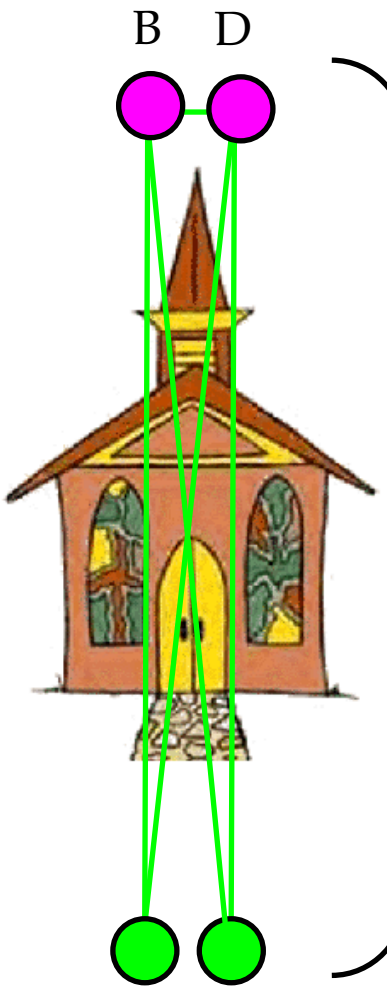
$\rho_A \otimes \sigma_C$

$\mathrm{Tr}_{BD}\, \phi_{AB} \otimes \psi_{CD} = \rho_A \otimes \sigma_C$

Moral: When faced with a mixed state ρ_A, we can always imagine that A is part of a larger system A - B on which the state is *pure.*

Purifications are essentially *unique.* (Up to local unitary transformations of the purifying space.)

Purification and correlation



ρ_A - σ_C

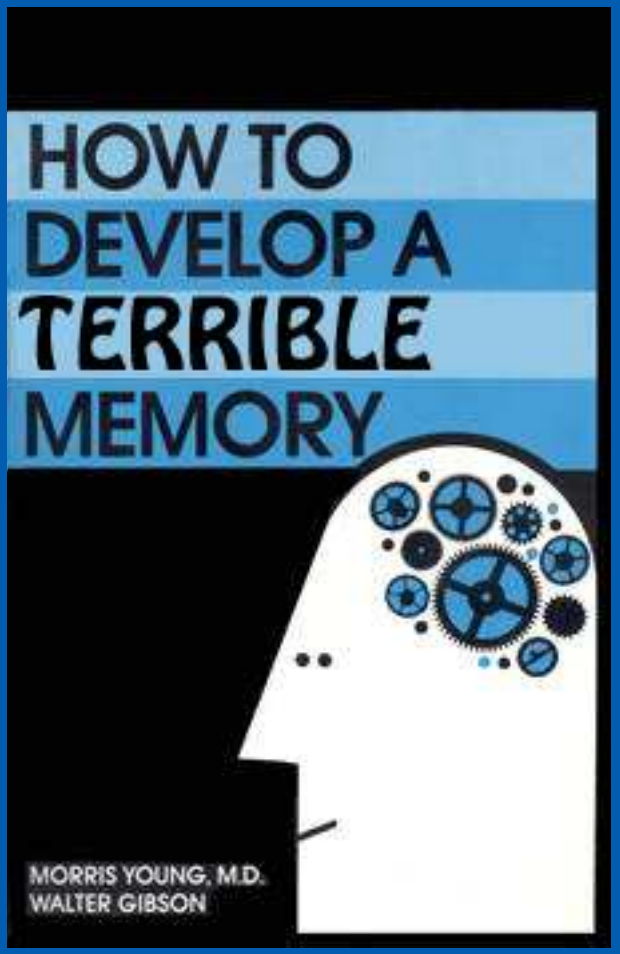
$|\psi_{ABCD}\rangle = (id_{AC} \otimes U_{BD})|\phi_{ABCD}\rangle$

$\mathrm{Tr}_{BD}\, \xi_{ABCD} = \rho_A$ - σ_C

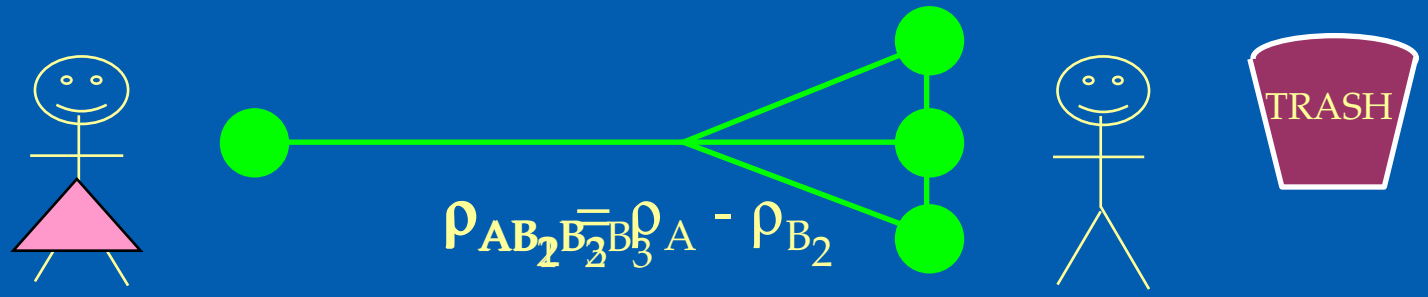
Moral: When faced with a mixed state ρ_A, we can always imagine that A is part of a larger system A - B on which the state is *pure.*

Purifications are essentially *unique.* (Up to local unitary transformations of the purifying space.)

The art of forgetting



The art of forgetting (aka privacy amplification)



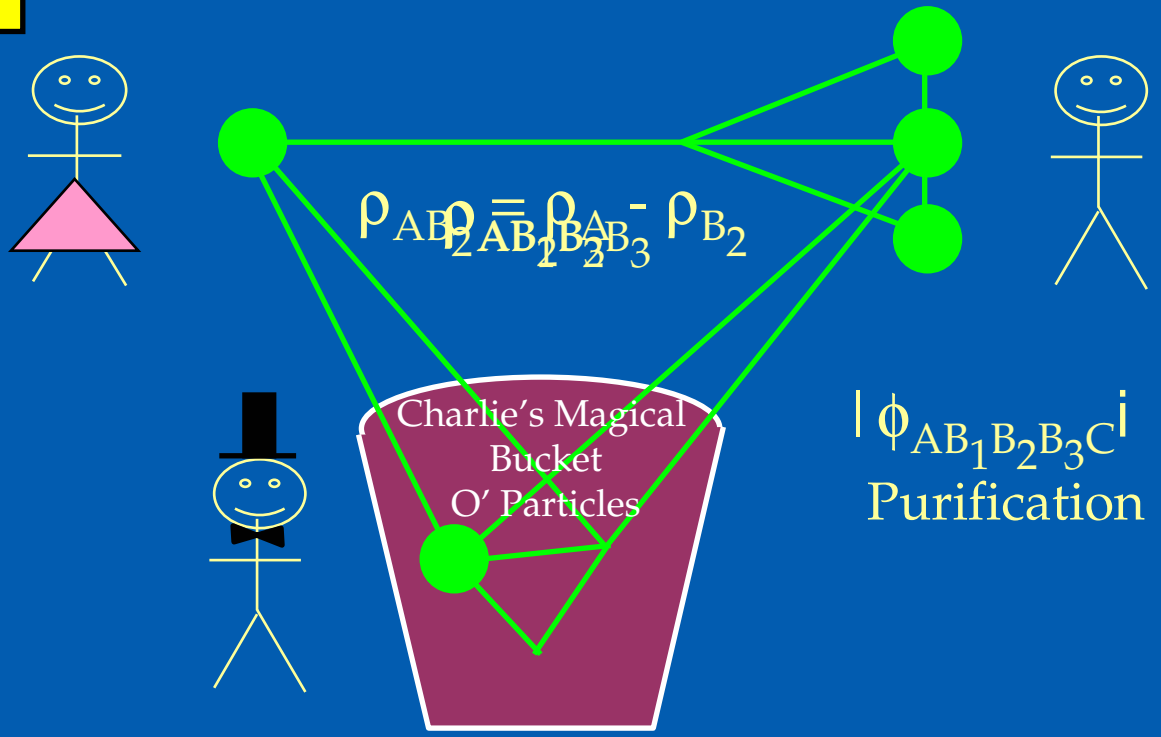
How can Bob unilaterally destroy his correlation with Alice?

What is the minimal number of particles he must discard before the remaining state is uncorrelated?

In this case, by discarding 2 particles, Bob succeeded in eliminating all correlations with Alice's particle

The benefits of forgetting: Applied theology

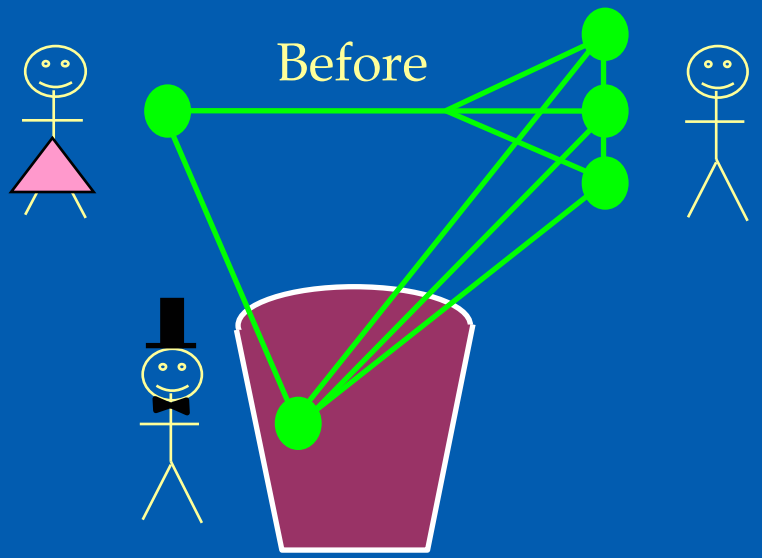
Watch again:



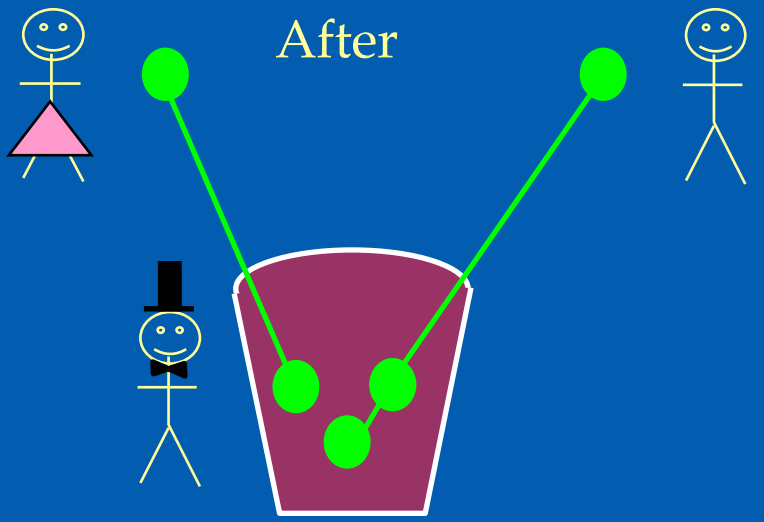
All purifications equivalent up to a unitary transformation in Charlie's lab.

Charlie holds **uncorrelated** purifications of **both** Alice's particle and Bob's remaining particles.

The benefits of forgetting: Applied theology



$|\phi_{AB_1B_2B_3C}\rangle$



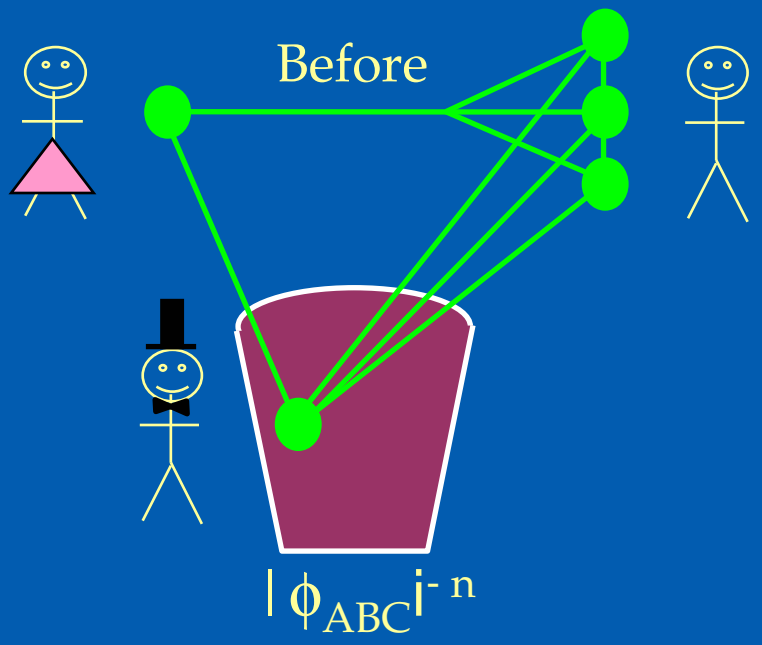
$|\psi_{AC_1}\rangle|\xi_{B_2C_2C_3}\rangle$

Alice never did anything) Her density operator $\phi_A = \psi_A$ is unchanged

Originally, her purification is held by both Bob and Charlie.
Afterwards, entirely by Charlie.

Bob **transferred** his Alice entanglement to Charlie
and **distilled** entanglement with Charlie, just by discarding particles!

Time for some formulas: How much does Bob need to send?



Uncertainty: von Neumann entropy

$$H(A)_\rho = H(\rho_A) = -\,\mathrm{tr}[\,\rho_A \log \rho_A\,]$$

Correlation: mutual information

$$I(A;B)_\rho = H(A)_\rho + H(B)_\rho - H(AB)_\rho$$

$$I(A;B)_\rho = \begin{cases} 0 \text{ if and only if } \rho_{AB} = \rho_A \otimes \rho_B \\ m \text{ for } m \text{ pairs of correlated bits} \\ 2m \text{ for } m \text{ singlets (maximal)} \end{cases}$$

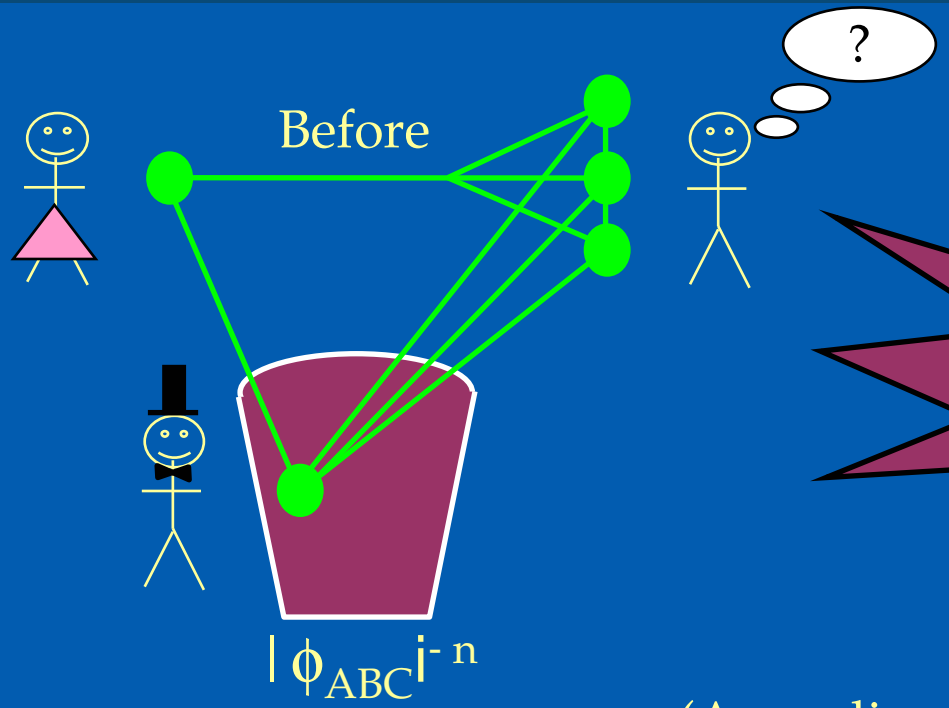
Initial mutual information: $n\, I(A;B)_\phi$

Final mutual information: ε

Each qubit Bob discards has the potential to eliminate at most 2 bits of correlation

Bob should (ideally) send around $nI(A;B)_\phi/2$ qubits to Charlie.

How does Bob choose *which* qubits?



At random

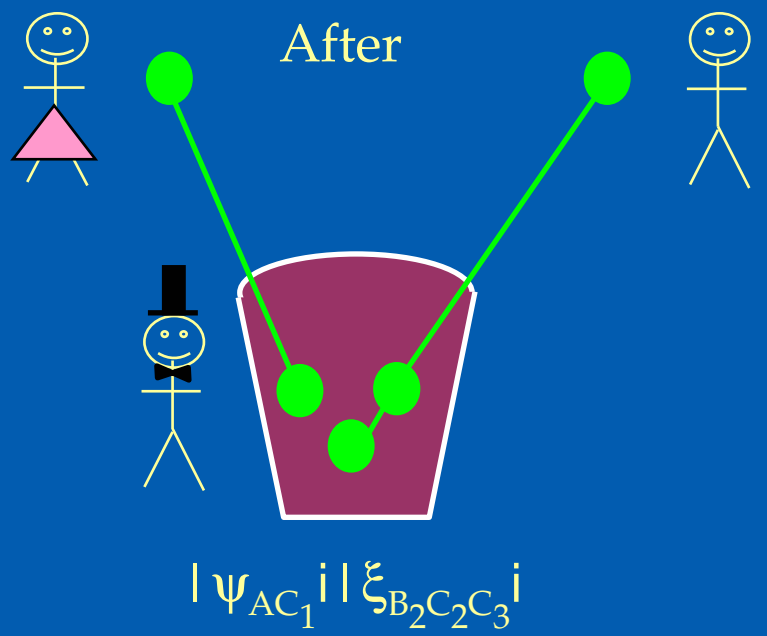
(According to the unitarily invariant measure on the high-probability subspace of $B^{\otimes n}$.)

Bob can ignore the correlation structure of his state!

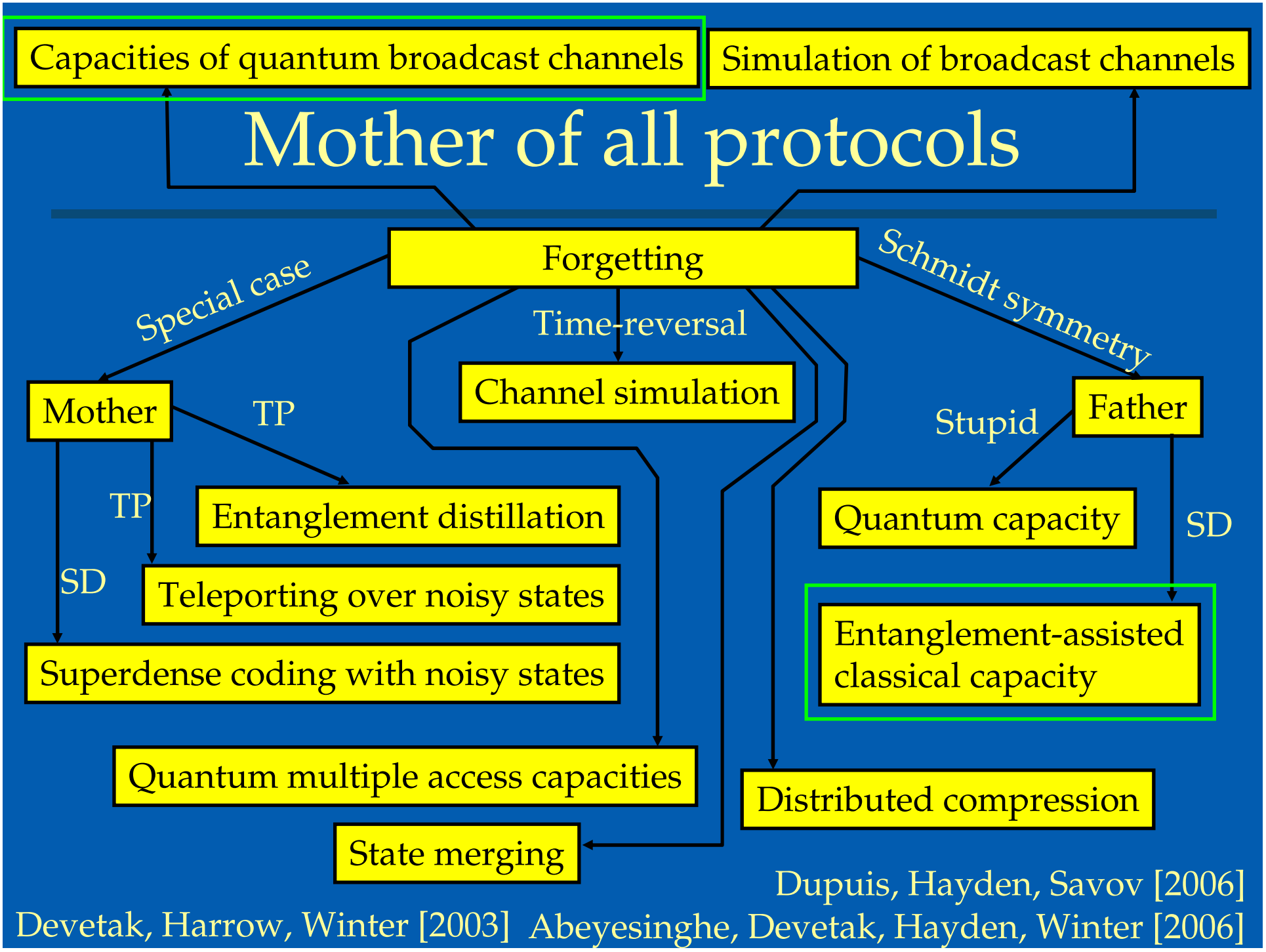
Final accounting

Investment:
Bob sends Charlie ~$n[I(A;B)_\phi]/2$ qubits

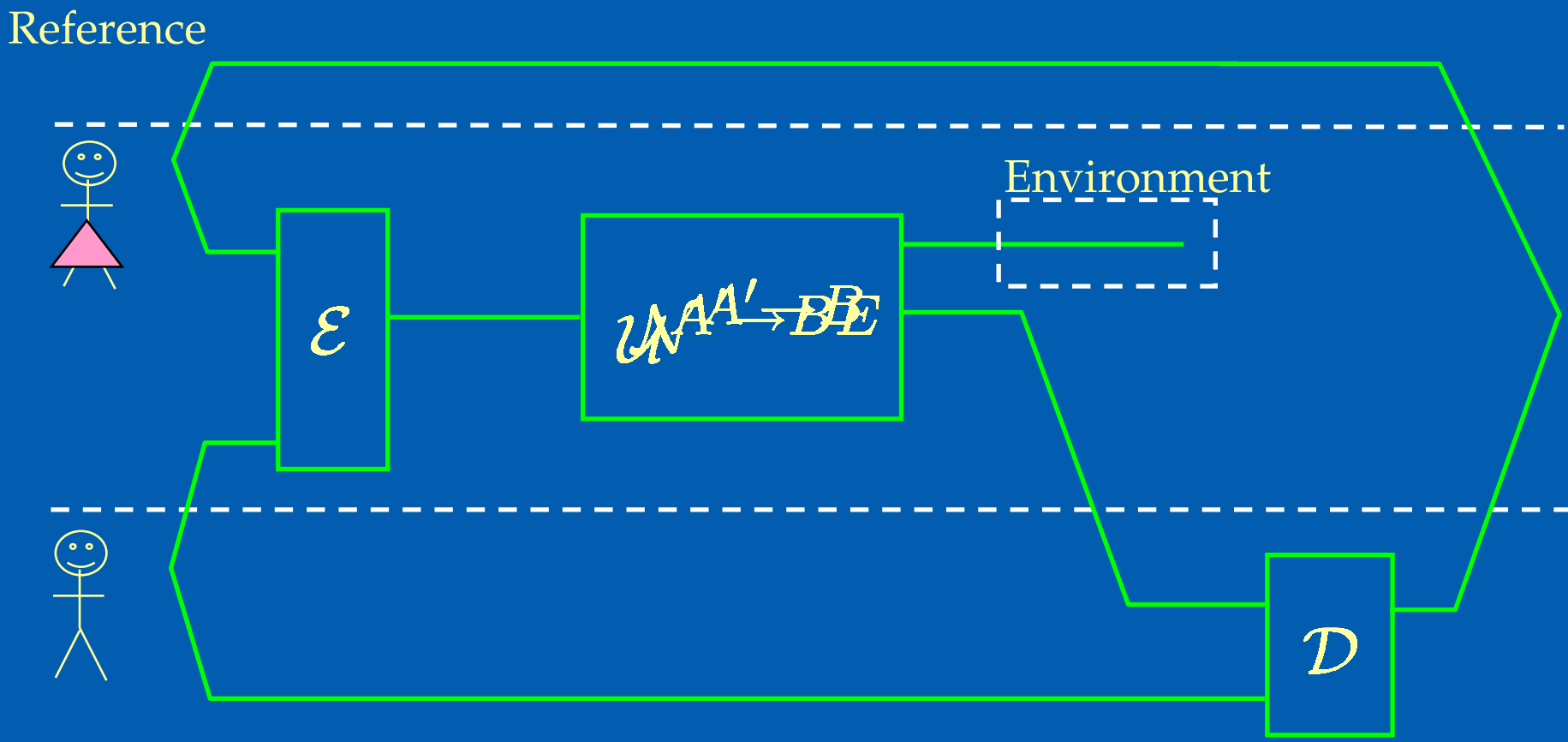
Rewards:
1) Charlie holds Alice's purification
2) B and C establish ??? singlets



OK – but what good is it?

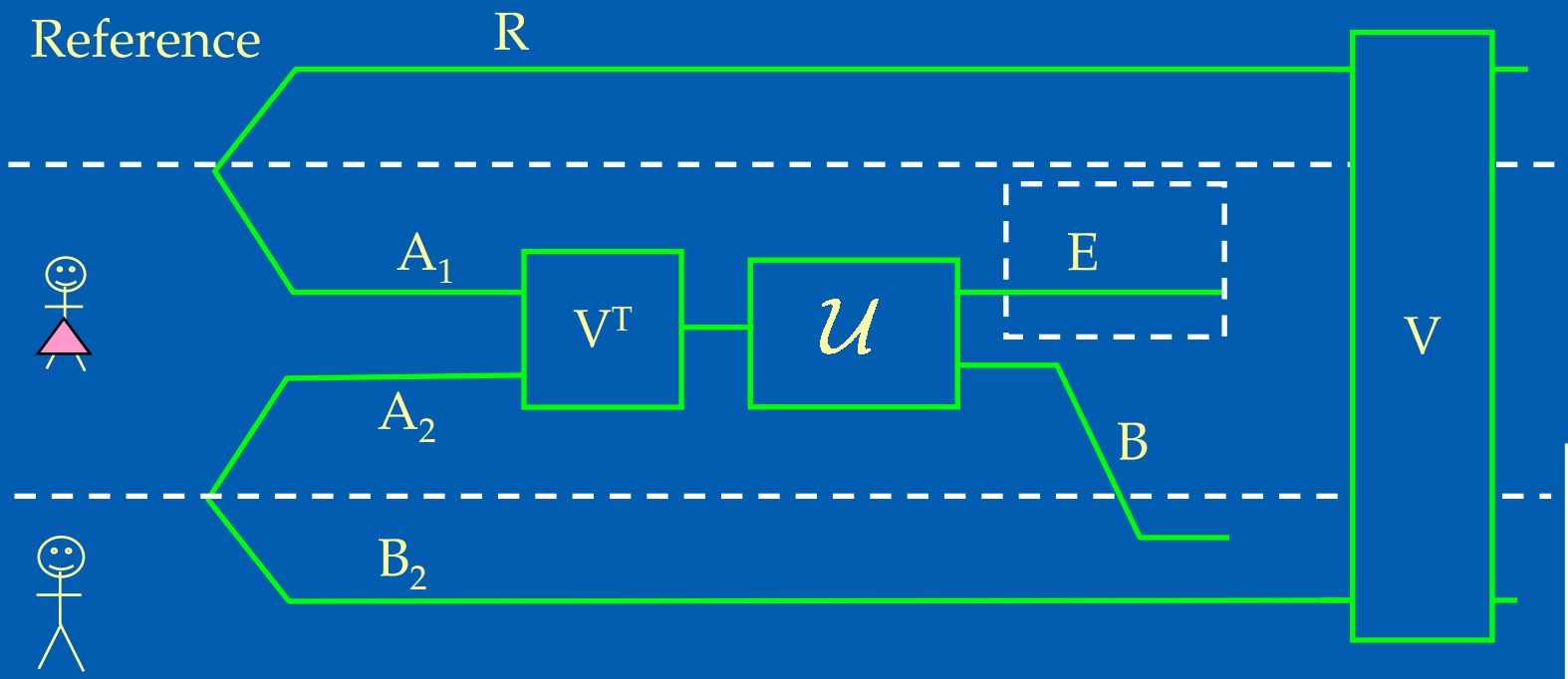

Capacities of quantum broadcast channels
Simulation of broadcast channels
Mother of all protocols
Forgetting
Special case
Time-reversal
Schmidt symmetry
Mother
TP
Channel simulation
Father
Stupid
TP
Entanglement distillation
Quantum capacity
SD
SD
Teleporting over noisy states
Entanglement-assisted classical capacity
Superdense coding with noisy states
Quantum multiple access capacities
Distributed compression
State merging
Dupuis, Hayden, Savov [2006]
Devetak, Harrow, Winter [2003]
Abeyesinghe, Devetak, Hayden, Winter [2006]

Entanglement-assisted communication



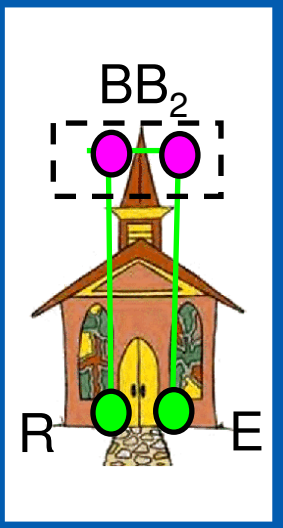
Objective is to transfer Alice's reference entanglement to Bob

Reduction to forgetting

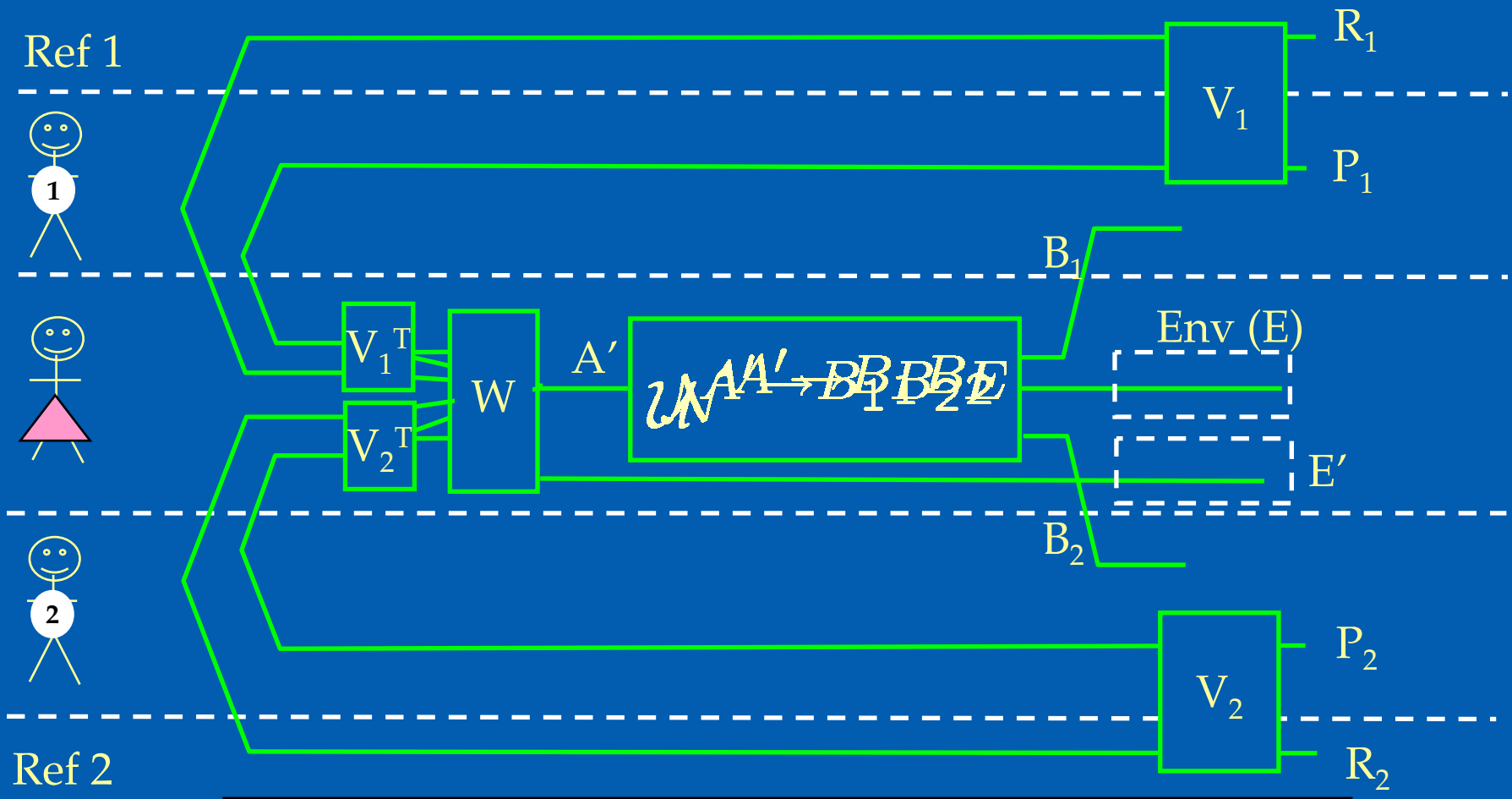


Who needs to do the forgetting?
It is sufficient to ensure that there is product state on R-E

Imagine: apply a random unitary V to RB_2.
Result: For sufficiently large B_2, product state on R-E !



Quantum broadcast channels



Who needs to do the forgetting?

Sufficient: product states on R_1- EP_2R_2 and R_2- EP_1R_1

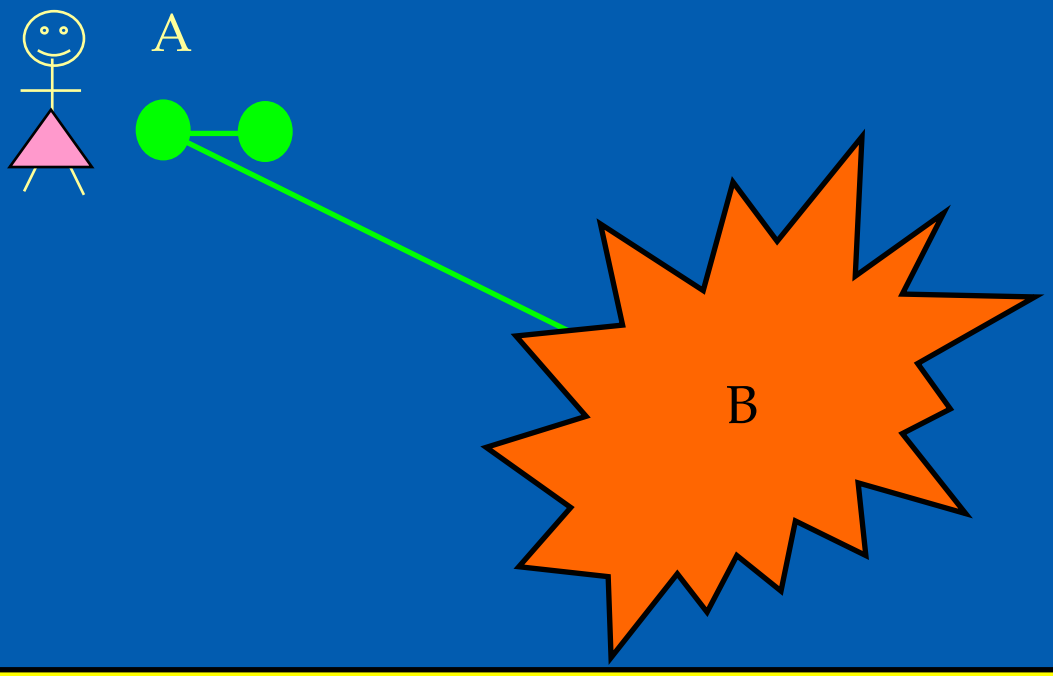
Broadcast channels: result

Given any state $U^{A' \to B_1 B_2 E} |\phi^{A_1 A_2 A'}\rangle$, any rate pair (Q_1, Q_2) of entanglement transmission to Alice and Bob is achievable provided:

$$\begin{aligned} Q_1 &\leq \frac{1}{2} I(A_1; B_1) \\ Q_2 &\leq \frac{1}{2} I(A_2; B_2) \\ Q_2 + Q_2 &\leq \frac{1}{2} \left[I(A_1; B_1) + I(A_2; B_2) - I(A_1; A_2) \right] \end{aligned}$$

Same form as *Marton's region*: conjectured optimal for classical channels

Random dynamics and information leakage



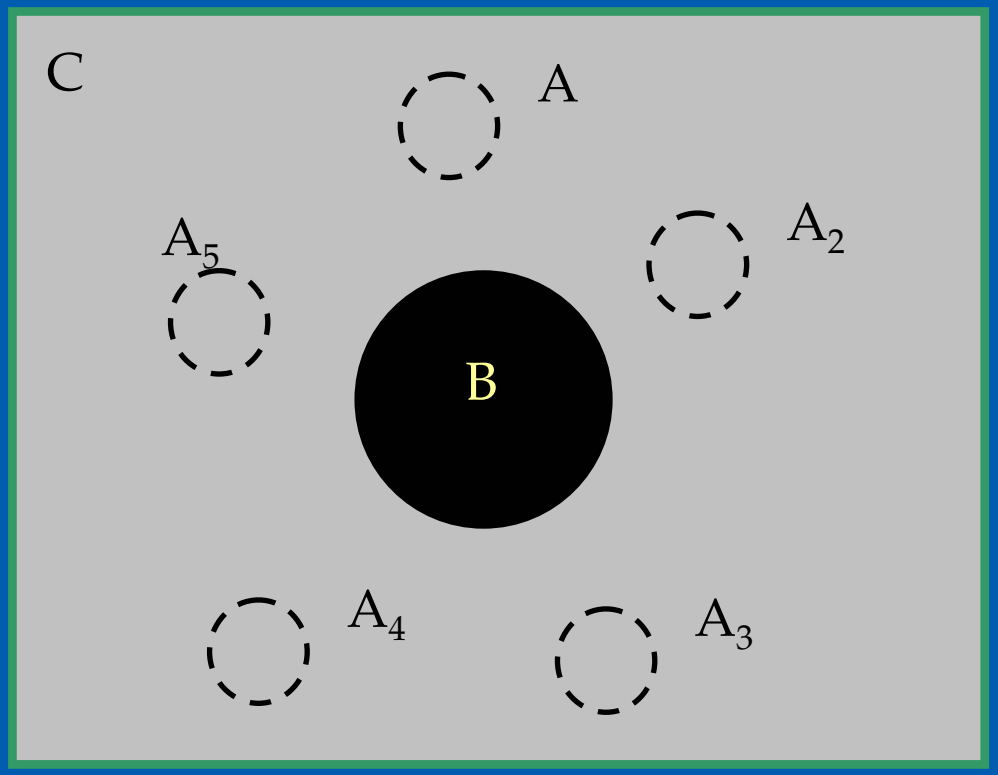
C = all radiated particles

How long must Alice wait until the "information about A" gets radiated?

Equivalently, how long until the orange blob has forgotten about A?

For sufficiently mixing dynamics,
information about A is released *almost immediately*.

Lessons for black hole information loss from cryptography?



t_0: Pure state:
B: Black hole
C: Rest of universe

t_1: Thermal Hawking radiation

t_2: Radiation but no black hole

Standard question: Is final state mixed or pure?

New question: Is final state of *some* radiation purified by rest of universe?

Summary

- Forgetting is the basic primitive of quantum information theory
- Detailed understanding of how to do it most efficiently
- These methods are generated by generic unitary transformations: could be useful for understanding real physics

http://arxiv.org/abs/quant-ph/0606225