Quantum Information Theory

(from a user, for the user)

Ashwin Nayak
University of Waterloo

Outline

Some illustrative applications

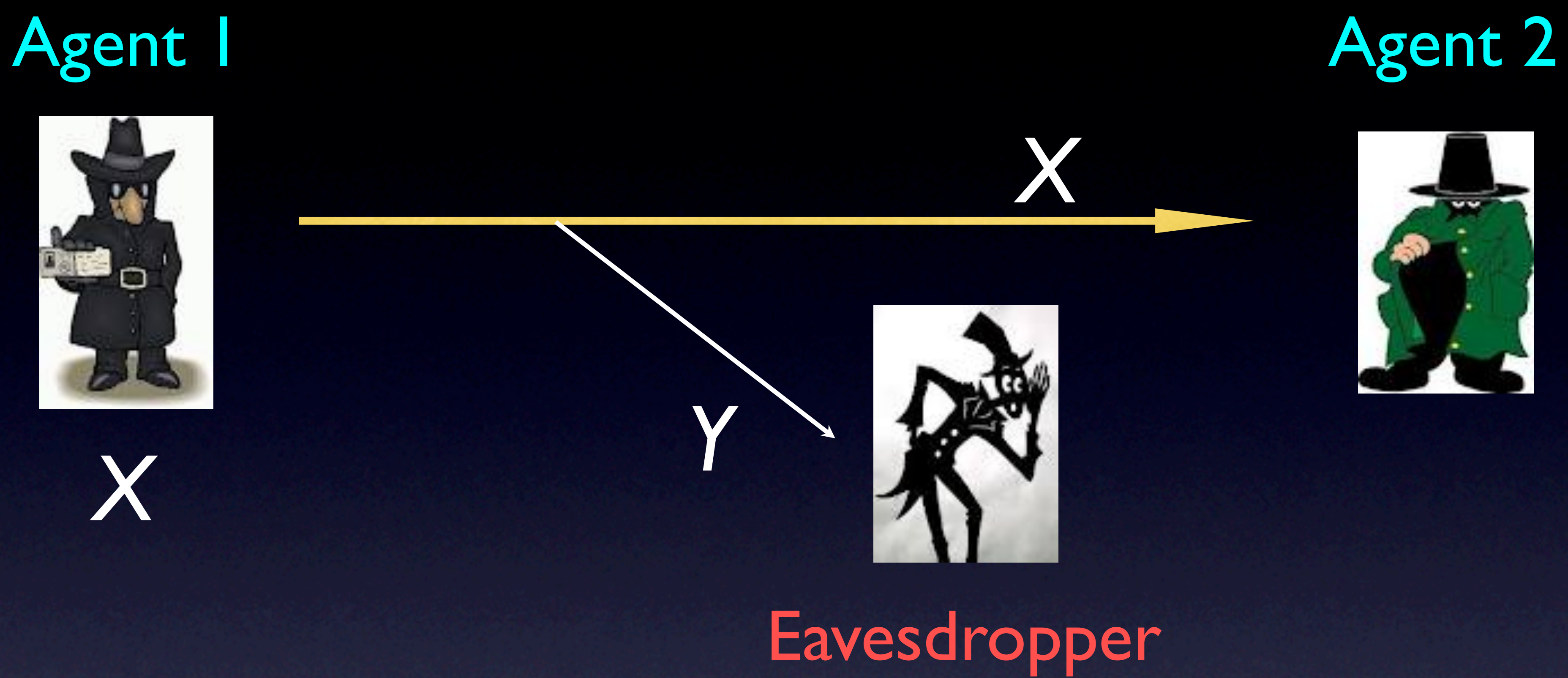
Basics of quantum information

Entropic quantities

Outlook

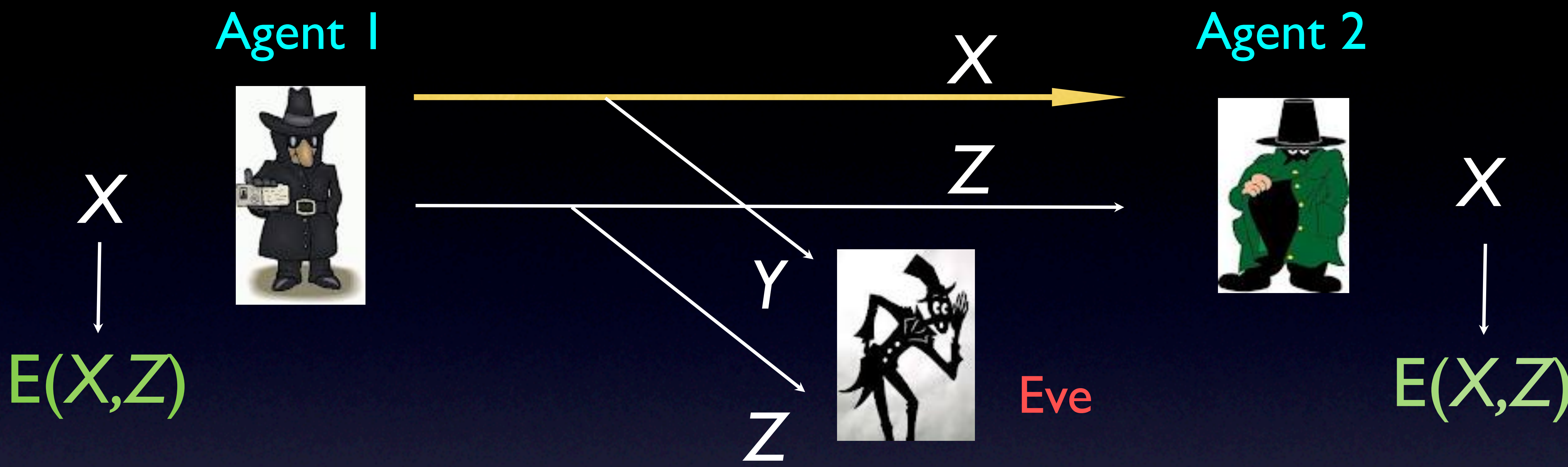
Application I

Privacy amplification



- A1 shares n uniformly random bits X with A2
- Eve obtains some information in the form of a quantum state Y
- Can they distill a more secure key ?

Randomness extraction



- A1 generates uniformly random bits *Z*, sends to A2
- Both compute *K* = E(*X*,*Z*) where E is a suitable *randomness extractor*
- Eve sees the seed *Z*, may measure *Y* depending on *Z*
- Would like *K* to be nearly uniform, even given *Y*,*Z*

Ta-Shma construction

- Based on Trevisan extractor, assuming Y has b qubits
- Reconstruction paradigm => *Random access code*

If Eve can distinguish K from uniform, there is a "short" string A, such that given any index i and q independent copies of Y, outputs bit X_i with probability $\geq p$.

- Code length is linear in n
- Superadditivity of information =>

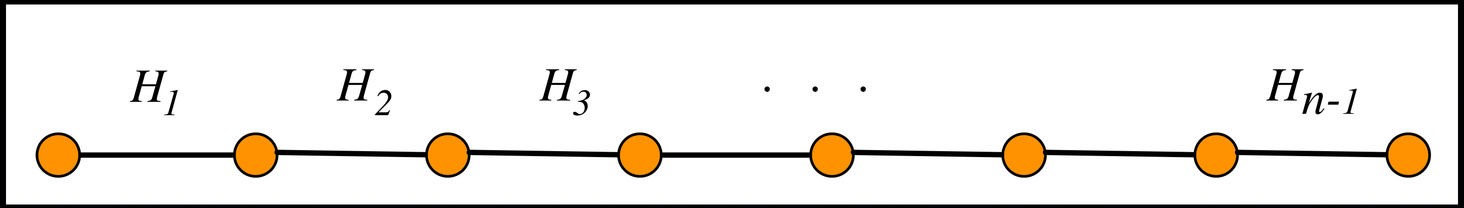
$$(1 - H(p))\, n \leq \Sigma_i\ I(X_i : Q) \leq S(Q) \leq |A| + qb$$

[Ambainis, N., Ta-Shma, Vazirani; N.]

- If b is "small", no such distinguisher exists. So E is *quantum-proof.*

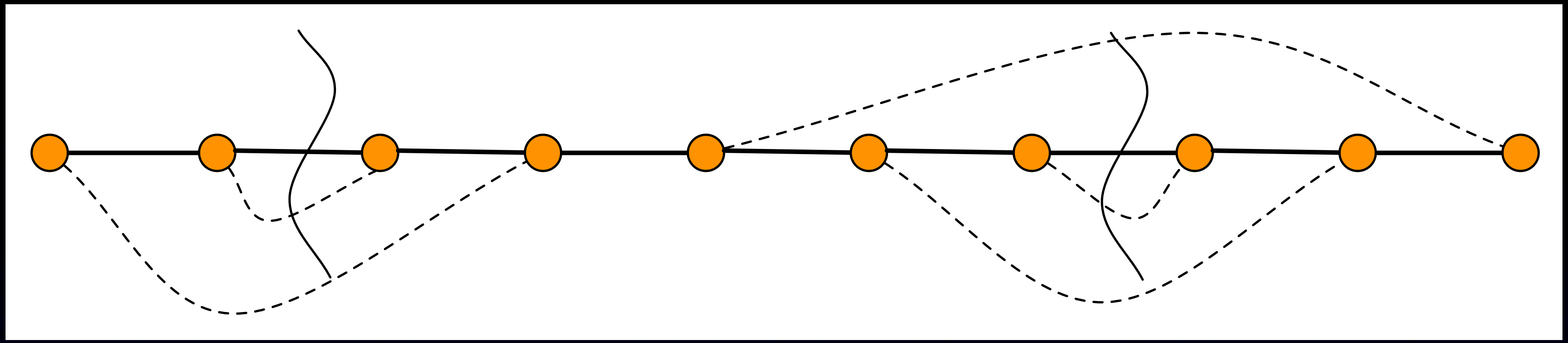
Application II

Local Hamiltonian problem in 1-D



- n particles on a line, each d-level
- nearest neighbour interaction H_i between i and $i+1$, Hermitian, $\| H_i \| \leq 1$
- Would like to understand properties of the *ground state* of the Hamiltonian $H = \sum_i H_i$
- QMA-hard to estimate ground energy to within additive error 1/poly [Aharonov, Gottesman, Irani, Kempe]
- If H has spectral gap $\Omega(1)$, such approximation is tractable [Landau, Vazirani, Vidick]

Area law

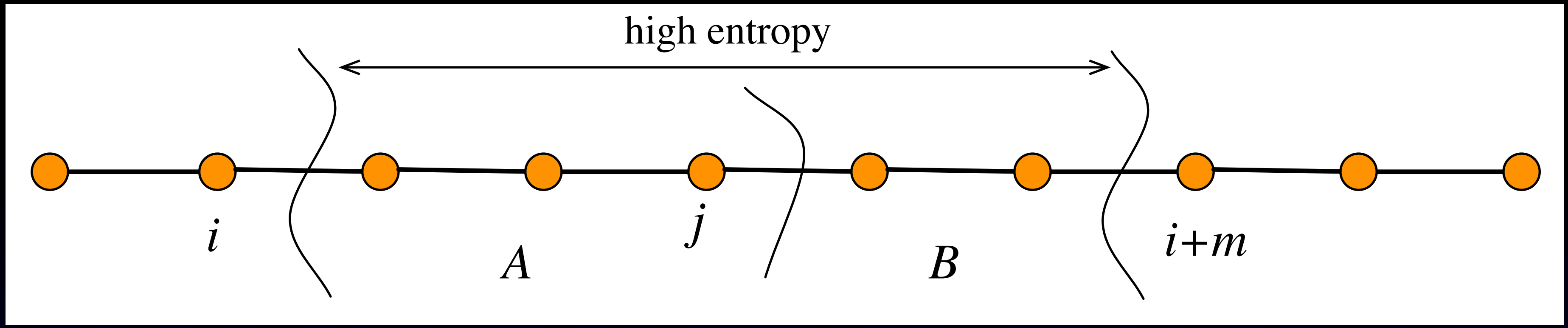


- A general state may be highly *entangled* across an interval
- Example: particles paired above may each be in the maximally entangled state $(1/\sqrt{d})\ \Sigma_j\ e_j \times e_j$

  So, the *entropy* of the *reduced state* of an interval of length L may be $L \log d$ (maximal)

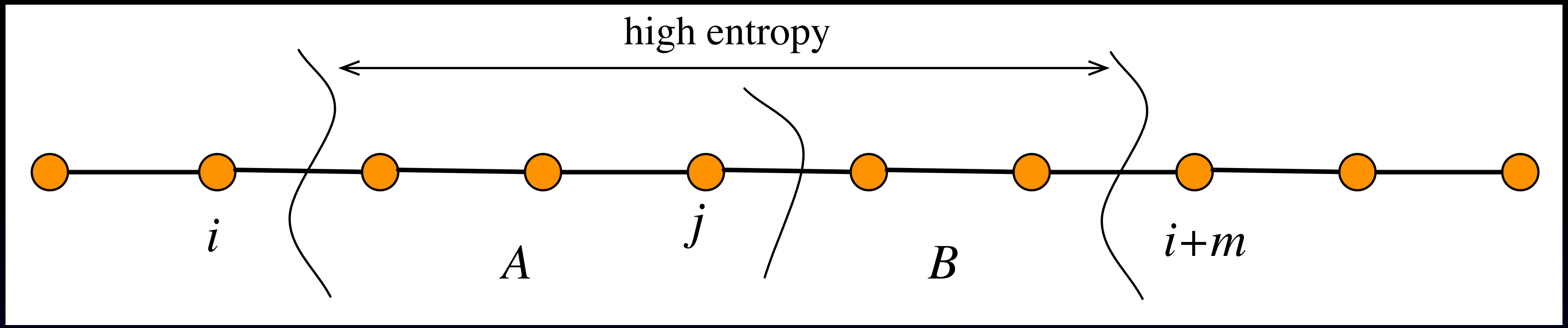
- If H has spectral gap $\Omega(1)$, the entropy is constant, independent of L [Hastings; Aharonov, Arad, Kitaev, Landau, Vazirani]
- Basis for efficient algorithm

Key step in Hastings' proof



- If the entropy at cut i is "high", entropy for all cuts up to $i + m$ is high
- Let A, B be contiguous intervals of length L within this
- Let $S(\rho_{AB}), S(\rho_A), S(\rho_B)$ be the entropies of the corresponding reduced states
- In general, $S(\rho_{AB})$ may be as high as $S(\rho_A) + S(\rho_B)$
- Lieb-Robinson bound => entanglement mostly within
- There is a measurement that distinguishes ρ_{AB} from $\rho_A \times \rho_B$ with $\exp(-c\,L)$ probability of error

Hastings' proof continued…



- By monotonicity of *relative entropy* (data processing inequality),

$$c' L \leq S(\rho_A) + S(\rho_B) - S(\rho_{AB})$$

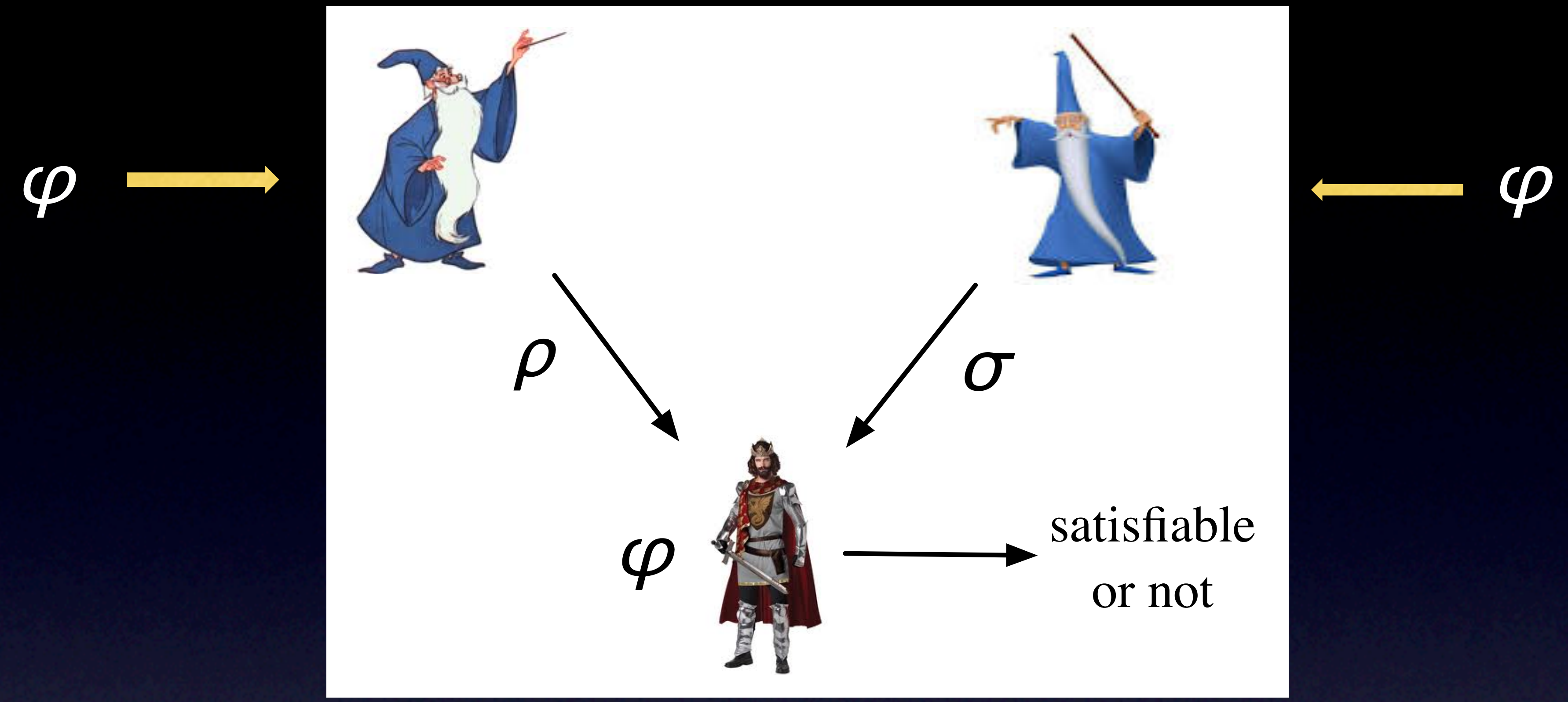
$$\Rightarrow \quad S_{2L} \leq 2 S_L - c' L$$

$$\Longrightarrow \quad S_L \approx L \log d - c'' L \log L$$

- Contradiction, if L is large. So entropy is small across every cut.

Application III

Short quantum proofs for 3Sat



- NP witness for 3Sat has length n
  (shorter proofs would imply a subexponential algorithm)

- Surprisingly, two *unentangled* quantum provers can convince an efficient quantum verifier of satisfiability with constant soundness and with proofs of length $O(\sqrt{n}\ \mathrm{polylog}(n))$
  [Aaronson, Beigi, Drucker, Fefferman, Shor; Chen and Drucker; Harrow and Montanaro]
- How short can the quantum proofs be?

Optimality of the proof system

- Unentangled quantum proofs of length shorter than $n^{1/2-\varepsilon}$ would imply subexponential time algorithm for 3Sat
  [Brandao and Harrow]
- Goal of the algorithm is to optimize verifier's acceptance over product states (a quadratic objective function)
- Instead, optimize over states which are approximately so
- Observation: Product states are infinitely extendible
- A bipartite state $\rho \times \sigma$ over AB may be extended to $\rho \times \sigma \times \sigma \times \sigma \times \sigma \ldots$ $AB_1B_2B_3B_4 \ldots$
- Every reduced state on AB_i is identical to that on AB

Monogamy of entanglement

- A k-extendible state τ_{AB} is "close" to the convex hull $S_{A:B}$ of the set of product states

$$\| \tau_{AB} - S_{A:B} \|_{locc-1} \leq c \, (\log \dim(A) / k)^{1/2}$$

[Brandao, Christandl, Yard; Brandao and Harrow]

- Consequence of the chain rule for mutual information and the Pinsker inequality

- Intuition: system A cannot be simultaneously strongly entangled with all k subsystems B_i

- k-extendibility can be expressed using semi-definite programming constraints

- Optimization over k-extendible states for $k \approx \log \dim(A)$ within error ε doable in time $\exp((\log \dim(A))^2 / \varepsilon^2)$

See notes for:

Basics of quantum information

Entropic quantities

Outlook

Quantum information theory is being *reinvented* as we speak

Information measures tailored to the task at hand, are replacing traditional notions

- *Conditional min-entropy* for privacy amplification, *tensor rank* for approximation of one-D ground states

Much sought: measure for the information gained by receiving an additional part of a state

- Conditional mutual information?