The Uncertainty Principle in the Presence of Quantum Memory

TECHNISCHE UNIVERSITÄT DARMSTADT

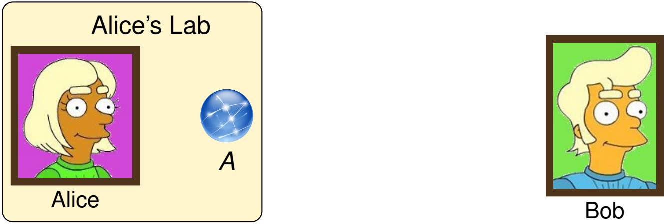
How entanglement changes the game.

Joseph M. Renes — TECHNISCHE UNIVERSITÄT DARMSTADT

Mario Berta
Matthias Christandl — LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Roger Colbeck
Renato Renner — ETH Zürich

The Uncertainty Principle Game



1. Alice is going to measure one of the observables X or Z on A
2. She first tells Bob which and asks him to predict the outcome
3. How well can he do?

Not Terribly Well

Known Results

TECHNISCHE UNIVERSITÄT DARMSTADT

- Heisenberg, of course [Z. Phys. 43, 172 (1927)]:

$$\Delta X \Delta Z \geq \frac{1}{2} \left| \langle [X, Z] \rangle \right|$$

- Entropic version by Maassen & Uffink [PRL 60, 1103 (1988)]:

$$H(X) + H(Z) \geq -2 \log c$$

for $c = \max_{|\psi_x\rangle, |\varphi_z\rangle} \left| \langle \psi_x | \varphi_z \rangle \right|$ (eigenvectors of X, Z), and Shannon entropy H.

- Classical Side Information Doesn't Help [M. Hall, PRL 74, 3307 (1995)]:

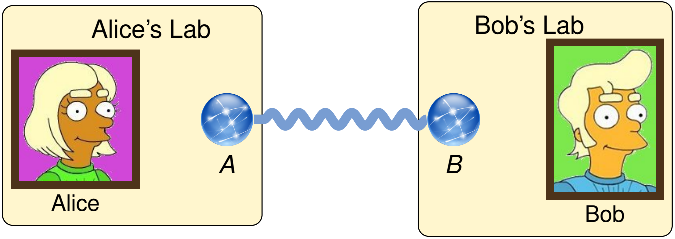
  Suppose Bob is given a classical random variable Y, correlated with Alice's system.

  Since Alice's state obeys the Uncertainty Principle for every Y, Y doesn't help Bob.

Does *Quantum* Side Information Help?

TECHNISCHE UNIVERSITÄT DARMSTADT

- Now Bob has an additional *quantum* system. Can he use it to aid his prediction, perhaps by measuring it in some way?
  (especially when his measurement depends on what Alice wants to measure)



- If this system is entangled with Alice's system, then Bob can always win!
  1. Imagine the Alice-Bob system is a spin singlet.
  2. Identical measurements on each end produce opposite outcomes, so
  3. Bob can measure his system and predict Alice's measurement outcome.
- Uncertainty principle **does not hold** in the presence of quantum memory

Fixing the Uncertainty Principle

TECHNISCHE UNIVERSITÄT DARMSTADT

- Fortunately, the uncertainty principle can be fixed!
- With quantum side information B (and measurements on system A),

$$H(X^A|B) + H(Z^A|B) \geq -2\log c + H(A|B)$$

  Note that $H(A|B) < 0$ only if state is entangled
- Proof:
  - uses conditional min/max entropies, and
  - strong subadditivity, plus
  - *lots* of smoothed entropy relations!

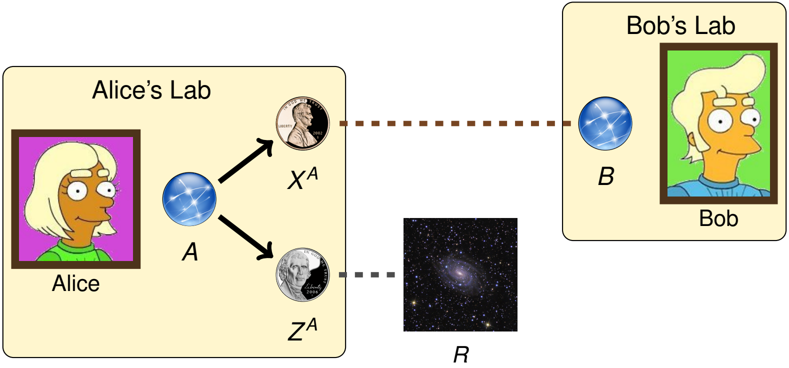
- Details can be found in arXiv:0909.0950

Alternate Form

Let R be the purification of AB. Then,

$$H(X^A|B) + H(Z^A|R) \geq -2\log c.$$

Info about complementary *observables* trades off between complementary *observers*.



Applications

TECHNISCHE UNIVERSITÄT DARMSTADT

Decoupling!

$$H(X^A|B), H(Z^A|B) \leq \epsilon \;\Rightarrow\; ||\psi^{AR} - \psi^A \otimes \psi^R||_1 \leq 2\sqrt{2\epsilon}$$

Very useful in quantum Shannon theory & quantum cryptography