Entropic Uncertainty Relation

Hasan Iqbal

CSE, UCONN

July 11, 2020

QUANTUM COPS

-The Uncertainty Principality-

Fact

Position and momentum of a particle can not be known simultaneously with arbitrary precision.

Problem

- How much we can't know?
- How about other observables?

History

Heisenberg: heuristics
Kennerd:

$$\sigma(Q) * \sigma(P) \geq \frac{\hbar}{2}$$

Robertson(1929):

$$\sigma(X) * \sigma(Y) \geq \frac{1}{2}|\langle\psi|\,[X, Y]\,|\psi\rangle|$$

Everett(1957):

Formulate it using Entropy?

(A lot happend)

Maasen-Uffink(1988):

$$H(X) + H(Z) \geq \log \frac{1}{c}$$

Problem with SD

SD

Let r.v. X = {-1, 0, 1} with equal probability. Then S. D. $\sigma(X) = \sqrt{\frac{2}{3}}$. Now, if X $\neq$ 0, counterintuitively $\sigma(X) = 1$.

Entropic uncertainty

$$H(X) = -\sum_i p_i * log(p_i) = 1.58 \tag{1}$$

Then in the changed scenario, $H(X) = 1$. Noticably, the uncertainty about X has decreased, as we would expect it to.

Maassen-Uffink Relation

Stronger statement (Coles. et. al)

$$H(A) + H(B) \geq log\frac{1}{c} + H(\rho) \tag{2}$$

Where, c is the maximum overlap of eigenvectors of A and B.

Density Matrix

Informal definition

Just another way to express a state. Pure or mixed

Examples

$$
\begin{aligned}
|\psi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle \\
p(|0\rangle) &= \langle\psi|\,|0\rangle\langle 0|\,|\psi\rangle = \langle 0|\,|\psi\rangle\langle\psi|\,|0\rangle = |\alpha|^2 \\
\\
|\phi\rangle &= \alpha\,|+\rangle + \beta\,|-\rangle \\
p(|+\rangle) &= \langle\phi|\,|+\rangle\langle +|\,|\phi\rangle = \langle +|\,|\phi\rangle\langle\phi|\,|+\rangle = |\alpha|^2
\end{aligned}
\tag{3}
$$

Density Matrix (cont.)

Examples

$$
\begin{aligned}
|\psi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle \\
|\psi\rangle\langle\psi| &= (\alpha\,|0\rangle + \beta\,|1\rangle) * (\alpha\,\langle 0| + \beta\,\langle 1|) \\
|\psi\rangle\langle\psi| &= \begin{bmatrix} \alpha^2 & \alpha\beta \\ \beta\alpha & \beta^2 \end{bmatrix} \textit{ and } |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \\
p(|0\rangle) &= \langle\psi|\,|0\rangle\langle 0|\,|\psi\rangle = tr(|0\rangle\langle 0| * |\psi\rangle\langle\psi|) = |\alpha|^2
\end{aligned}
\tag{4}
$$

Density Matrix (cont.)

Mixed state

$$\rho = \sum_i p_i \left|\psi_i\right\rangle\left\langle\psi_i\right| \tag{5}$$

Example

A system produces $|0\rangle$ 80% of the time but 20% of the time it produces a state $|\psi'\rangle$ where it's a superposition of $|0\rangle$ and $|1\rangle$.

$$\begin{aligned} |\psi\rangle &= |0\rangle \\ |\psi'\rangle &= \sqrt{\frac{7}{10}}\,|0\rangle + \sqrt{\frac{3}{10}}\,|1\rangle \end{aligned} \tag{6}$$

$$\rho = .8 * |\psi\rangle\langle\psi| + .2 * |\psi'\rangle\langle\psi'| = \begin{bmatrix} .9400 & .0917 \\ .0917 & .0600 \end{bmatrix}$$

Shannon and von Neumann

Shannon Entropy

Example

$$H(X) = -\sum_i p_i log(p_i)$$

R.v X = Coin Toss with p(head) = .7

$$H(X) = -.7 * log(.7) - .3 * log(.3) = .8813$$

Von Neumann Entropy

Example

$$S(\rho) = -tr(\rho log \rho) = -\sum_i \lambda_i log \lambda_i \tag{7}$$

$$|\psi\rangle = \sqrt{\frac{3}{9}}|+\rangle + \sqrt{\frac{6}{9}}|-\rangle, \rho = |\psi\rangle\langle\psi| = \begin{bmatrix} .7738 & -.0556 \\ -.0556 & .0040 \end{bmatrix} \tag{8}$$

$$S(\rho) = -.7778 * log(.7778) - 0 * log(0) = .2821$$

Relative Entropy

Informal Definition

Measure distance of two density matrices.

$$S(\rho||\sigma) = tr(\rho log \rho) - tr(\rho log \sigma) \tag{9}$$

Example

$$\rho = \begin{bmatrix} .8600 & .0917 \\ .0917 & .1400 \end{bmatrix}, \sigma = \begin{bmatrix} .9900 & .0436 \\ .0436 & .0100 \end{bmatrix}$$

$$\begin{aligned} S(\rho||\sigma) &= trace(\rho * log(\sum_i \lambda_i |v_i\rangle\langle v_i|)) - trace(\rho * log(\sum_j \lambda_j |v_j\rangle\langle v_j|) \\ &= .3837 \end{aligned} \tag{10}$$

Finally...

The proof!

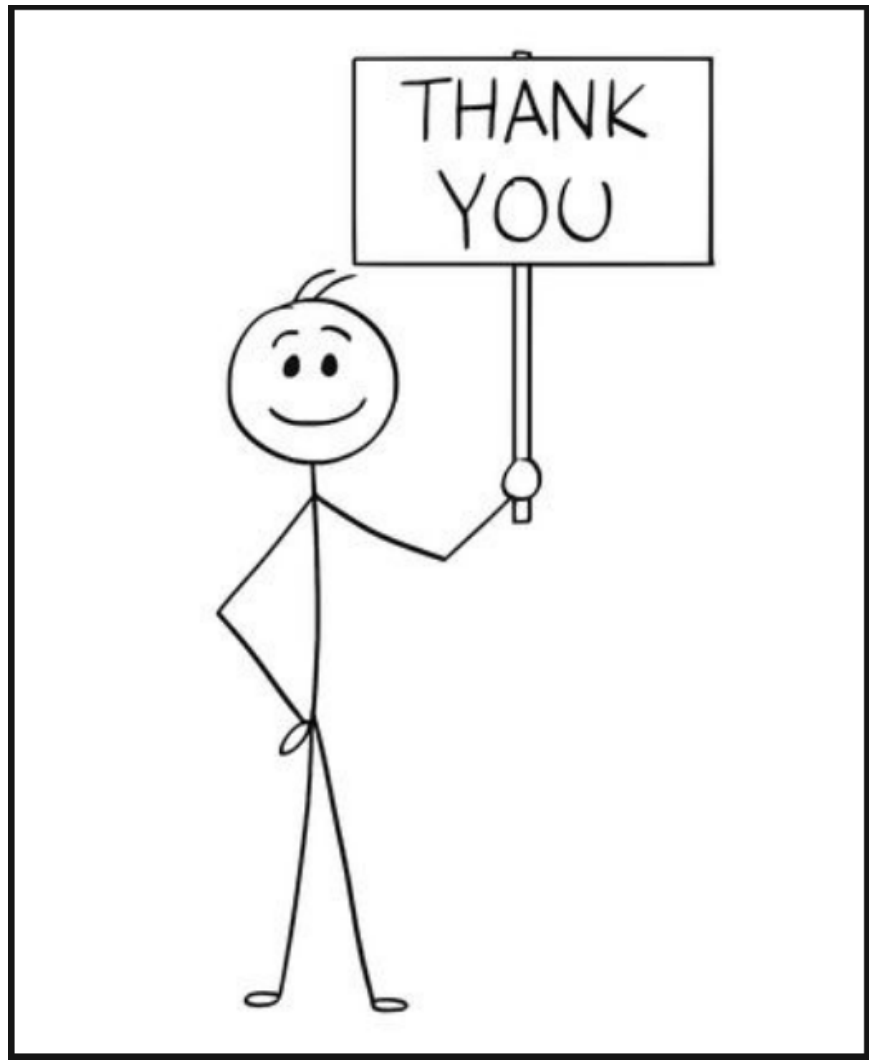
Application in Cryptography

Proving unconditional security

1. Describe the situation using density matrix
2. Calculate difference of entropy between Eve and Bob
3. Show that for any permissible attack, secret could still be shared

Key-rate Equation

$$\text{key rate} = inf\left(H(A|E) - H(A|B)\right)$$


THANK
YOU