Topics in Quantum Information	**U. Waterloo CO 781, Spring 2004**
Ashwin Nayak (Instructor)	**Annika Niehage (Scribe)**
Strong Coin Flipping. Entropy.	**June 1, 2004**

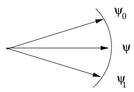
1 Strong Coin Flipping

Protocol (optimized version due to [Ambainis '01, Spekkens & Rudolph '02])

1. A: $a \in_R \{0, 1\}$, prepares $|\psi_a\rangle = \frac{1}{\sqrt{2}}(|aa\rangle + |22\rangle)$
   sends one qutrit to B
2. B: $b \in_R \{0, 1\}$ sends to A
3. A: sends a and the remaining qutrit to B. Her outcome is $c_A = a \oplus b$.
4. B: checks whether the 2 qutrits are in state $|\psi_a\rangle$. His outcome is $c_B = a \oplus b$, if the check succeeds. Otherwise, he aborts the protocol.

Cheating Strategies When the two players are honest, their outcomes are equal, and are unbiased. However, either of the two players can bias the other's outcome quite easily.

1. **Bob:** measures qutrit in the $0, 1, 2$ basis; he sees $'a'$ w. p. $\frac{1}{2}$, and sends $b = a$ to force outcome $= 0$; he sees '2' w. p. $\frac{1}{2}$, and sends a random bit $'b'$ in which case he succeeds in getting $c_A = 0$ with probability $\frac{1}{2}$.
   Overall $\Pr(c_A = 0) = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$.
2. **Alice:** A simple strategy to get outcome 0 would be to switch her value for a if required in step 3. However, there is an even better quantum strategy.
   She prepares $\psi = \frac{\psi_0+\psi_1}{||\psi_0+\psi_1||} = \frac{|00\rangle+|11\rangle+2|22\rangle}{\sqrt{6}}$:



   and in step (3), sends $b = a$ to get outcome 0 ($c_B = 0$).

$$
\begin{aligned}
\Pr(c_B = 0) &= \frac{|\langle\psi|\psi_0\rangle|^2 + |\langle\psi|\psi_1\rangle|^2}{2} \\
&= \left|\frac{1}{\sqrt{2 \cdot 6}}(1+2)\right|^2 \\
&= (\frac{\sqrt{3}}{2})^2 = \frac{3}{4}
\end{aligned}
$$

The above strategies are the best possible:

Theorem 1 *If at most one of A or B is honest, then* $\Pr(\text{outcome} = 0/1) \leq \frac{3}{4}$.

(In this game, all bets are off when both parties deviate from the protocol. Indeed, there is no clear way for an independent observer to verify which person deviated from the protocol.)

The protocol illustrates how quantum states allow us to get around classical impossibility results regarding coin flipping games. (And also those for ideal quantum protocols; compare the kind of commitment used in this protocol to the result on ideal bit commitment we saw earlier in this course.)

Fact 2 *In any classical coin flipping protocol, at least one of Alice and Bob can force the outcome to one value (0 or 1, depending on the protocol) with probability 1.*

(Convince yourselves of this fact!)

We will divide the proof in two cases. The following two lemmata prove the theorem.

Lemma 3 *If A is honest, then*

$$\Pr(c_A = 0) \quad \leq \quad \frac{3}{4}.$$

The same bound holds when Bob wants to force $c_A = 1$.

Proof : Bob has to send $b = a$ to get $c_A = 0$. This is equivalent to deducing 'a' optimally from the state of the qutrit sent in step (1).

Let $\rho_a = \mathrm{Tr}_A(|\psi_a\rangle\langle\psi_a|)$. Then we get the following density matrices for the qutrit sent in step (1):

$$\rho_0 = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\rho_1 = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Bob receives one of these two states at random. From last lecture, we know that the maximal probability of guessing which state he has is

$$\frac{1}{2} + \frac{\|\rho_0 - \rho_1\|_{\mathrm{tr}}}{4} \quad = \quad \frac{1}{2} + \frac{1}{4} \quad = \quad \frac{3}{4}.$$

□

Lemma 4 *If B is honest, then*

$$\Pr(c_B = 0) \leq \frac{3}{4}.$$

Similarly we can show that the same bound holds if Alice wants to force $c_B = 1$.

Proof : The analysis here is from [Kerenidis,Nayak '04].

Observation: Alice's probability of cheating only increases, if in step (3), she always sends $a = b$.

General cheating strategy: A prepares $|\psi\rangle \in \mathcal{H} \otimes \mathbb{C}^3 \otimes \mathbb{C}^3 = \mathcal{H} \otimes \mathcal{H}_r \otimes \mathcal{H}_c$, and sends the $\mathcal{H}_c$ part to B. In step (3) she sends $a = b$ and does a unitary U_a on the $\mathcal{H} \otimes \mathcal{H}_r$ part of ψ, and sends the $\mathcal{H}_r$ qutrit to B.

To bound her maximum cheating probability, we condition on the value of the bit picked by Bob. Condition on $b = 0$:

$$\Pr(c_B = 0) \quad = \quad \langle\psi_0|\ \mathrm{Tr}_{\mathcal{H}}(|\tilde{\psi}_0\rangle\langle\tilde{\psi}_0|)\ |\psi_0\rangle$$

where $|\tilde{\psi}_a\rangle = (U_a \otimes I)|\psi\rangle$. We get a similar expression when $b = 1$.

The overall probability of cheating is then.

$$\begin{aligned}
\Pr(c_B = 0) &= \frac{1}{2}(\langle\psi_0|\sigma_0|\psi_0\rangle + \langle\psi_1|\sigma_1|\psi_1\rangle) \\
&= \frac{1}{2}(\mathrm{F}(|\psi_0\rangle\langle\psi_0|, \sigma_0) + \mathrm{F}(|\psi_1\rangle\langle\psi_1|, \sigma_1))
\end{aligned}$$

where $\sigma_i = \mathrm{Tr}_{\mathcal{H}}(|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|)$.
Note:

1. The density matrix of the $\mathcal{H}_c$ qutrit remains unchanged after step (1). I.e., $\mathrm{Tr}_{\mathcal{H}_r}(\sigma_0) = \mathrm{Tr}_{\mathcal{H}_r}(\sigma_1) = \sigma$
2. Also, from the definition of fidelity, we see that if $\omega_0,\ \omega_1$ over $\mathcal{H} \otimes \mathcal{K}$, then

   $$\mathrm{F}(\omega_0, \omega_1) \quad \leq \quad \mathrm{F}(\tilde{\omega}_0, \tilde{\omega}_1)$$

   where $\tilde{\omega}_i = \mathrm{Tr}_H(\omega_i)$. (Every purification of ω_0 is also a purification of $\tilde{\omega_0}$, etc.)

$$\begin{aligned}
\Pr(c_B = 0) &\leq \frac{1}{2}(\mathrm{F}(\rho_0, \sigma) + \mathrm{F}(\rho_1, \sigma)) \\
&\leq \max_{\sigma} \frac{1}{2}(\mathrm{F}(\rho_0, \sigma) + \mathrm{F}(\rho_1, \sigma))
\end{aligned}$$

Exercise: Show that

$$\max_{\sigma}(\mathrm{F}(\rho_0, \sigma) + \mathrm{F}(\rho_1, \sigma)) \quad \leq \quad 1 + \sqrt{\mathrm{F}(\rho_0, \rho_1)}.$$

Remember:

$$\begin{aligned}
\rho_0 &= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\rho_1 &= \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

Therefore we get the following equation:

$$\begin{aligned}
\sqrt{\mathrm{F}(\rho_0, \rho_1)} &= \|\sqrt{\rho_0} \cdot \sqrt{\rho_1}\|_{\mathrm{tr}} \\
&= \left\| \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\|_{\mathrm{tr}} \\
&= \left\| \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\|_{\mathrm{tr}} \\
&= \frac{1}{2}
\end{aligned}$$

So

$$\Pr(c_B = 0) \quad \leq \quad \frac{1}{2}(1 + \frac{1}{2}) = \frac{3}{4}$$

$\square$

2 Mixed states and entropy

Let X be a random variable over the set $\{0,1\}^n$, with distribution $\{p_x, x\}$. The randomness in the distribution or equivalently in the random variable is quantified by its *entropy*. Intuitively, this quantity allows us to measure our ignorance about the state of the variable.

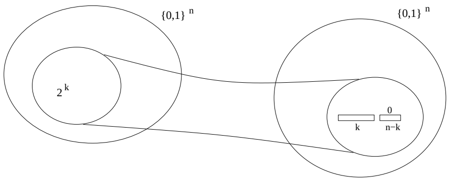
Definition 5 *The* **Shannon Entropy** *is defined as*

$$\mathrm{H(X)} \quad = \quad \sum_x p_x \log_2 \frac{1}{p_x}$$

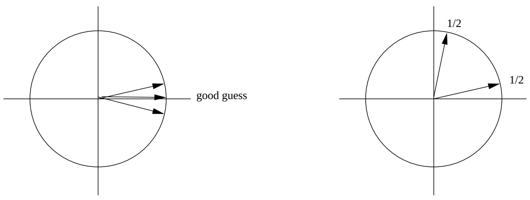
In many different contexts this tells us how many bits of information are "contained in" X.

For example, the distribution $\{(\frac{1}{2},0),(\frac{1}{2},1)\}$ has entropy 1.

If we consider a uniformly random element from a subset of size 2^k taken from $\{0,1\}^n$, we see that it has entropy k. This is intuitively what we would expect, since there is a one-to-one correspondence between the 2^k elements and the 2^k strings of which the last $n-k$ bits are all zero.



Consider a mixed state $\{(\frac{1}{2},|\Phi_0\rangle),(\frac{1}{2},|\Phi_1\rangle)\}$. It is tempting to assign this an entropy of 1. However, if the angle between the two states is very small then the vector in the middle is a good approximation to either of them. So there is little randomness in the state. On the other hand, if the states are almost orthogonal, then the mixed state resembles a uniformly random bit.



So the quantum case is very subtle. We would like to be able to take into account the distinguishability of the states in a mixture (equivalently, their orthogonality) in defining its entropy. Von Neumann entropy allows us to do exactly this.

Remember that the following properties hold for a density matrix ρ:

- it is positive semi definite (PSD),
- $\mathrm{Tr}(\rho) = 1$

It is thus possible to write $\rho = \sum_i \lambda_i |\Phi_i\rangle\langle\Phi_i|$ where the $|\Phi_i\rangle$ form an orthonormal basis and the λ_i are the corresponding eigenvalues. This gives us a distribution $\{\lambda_i, |\Phi_i\rangle\}$, much akin to a classical one, where all the states in the support of the distribution are perfectly distinguishable.

To transfer the idea of a measure for information to the quantum case, we now use the following definition:

Definition 6 *The* **von Neumann entropy** *of a mixed state X or equivalently its density matrix ρ_X is defined by*

$$\mathrm{S(X)} \quad := \quad \mathrm{H}(\mathrm{spectrum}(\rho_\mathrm{X})).$$

It has much the same properties as Shannon entropy, but also differs from it in unexpected ways:

1. $\mathrm{S(X)} \geq 0$, and if $|\Phi_x\rangle \in \mathbb{C}^d$, then $\mathrm{S(X)} \leq \log \mathrm{d}$.
2. It is invariant under unitary operations on the mixed state.
3. It is concave: $\mathrm{S(pX + (1-p)Y) \geq pS(X) + (1-p)S(Y)}$.
4. It is subadditive: $\mathrm{S(XY) \leq S(X) + S(Y)}$.
5. $\mathrm{H(XY) \geq H(X)}$, whereas $\mathrm{S(XY) \ngeq S(X)}$.

   An example where this monotonicity fails is $|\Phi+\rangle_{XY}$. The joint state is pure, therefore has entropy 0, but any single qubit in it is uniformly distributed.

   However, $\mathrm{S(XY) \geq |S(X) - S(Y)|}$. This is the Araki-Lieb inequality.