US-India Advanced Institute on Thermalization

Tutorial on Quantum Information, large N, and AdS spacetimes

20 June 2013

1. *Ubiquitous relative entropy.* Recall from the lectures that the relative entropy is defined as $D(\rho\|\sigma) = \mathrm{Tr}[\rho\log\rho - \rho\log\sigma]$. D is an entropic measure of the distance between ρ and σ. Although it is not a metric, it is equal to zero if and only if $\rho = \sigma$.

   a) Suppose that $\sigma = \exp(-\beta H)/Z$ where $\beta = 1/T$ and $Z = \mathrm{Tr}\exp(-\beta H)$. Show that

   $$D(\rho\|\sigma) = \beta[F(\rho) - F(\sigma)] \tag{1}$$

   where F is the Helmholtz free energy function.

   b) Now suppose that ρ_{AB} is a density operator on $A\otimes B$, with $\rho_A = \mathrm{Tr}_B\,\rho_{AB}$ and $\rho_B = \mathrm{Tr}_A\,\rho_{AB}$. Show that

   $$D(\rho_{AB}\|\rho_A\otimes\rho_B) = I(A;B)_\rho. \tag{2}$$

   c) Let O_A and O_B be two observables such that $\|O_A\|_\infty, \|O_B\|_\infty \leq 1$. Show, for any state ρ_{AB} on $A\otimes B$, that

   $$\frac{1}{2}\left(\langle O_A O_B\rangle - \langle O_A\rangle\langle O_B\rangle\right)^2 \leq I(A;B)_\rho. \tag{3}$$

   Thus, the mutual information provides a general upper bound on the correlations that can be detected by any bounded operators.

2. *Entanglement of a random state.* Recall from class that we approximated a random unit vector in $\mathcal{H}_{BH} \otimes \mathcal{H}_{rad}$ as

$$|\varphi\rangle = \sum_j^b \sum_k^r g_{jk} |j\rangle_{BH} |k\rangle_{rad} \tag{4}$$

where the g_{jk} are independent complex Gaussians of mean zero and variance $1/d$, where $\dim \mathcal{H}_{BH} = b$, $\dim \mathcal{H}_{rad} = r$ and $d = br$. Show that the expected purity of φ_{rad} is

$$\frac{1}{r} + \frac{1}{b}. \tag{5}$$

(The exact value when normalization is taken into account is

$$\frac{b+r}{br+1}, \tag{6}$$

which is even smaller than our estimate. Feel free to try and work it out. If you don't know how, you will by the end of the third lecture.)

3. *Bit commitment.* Alice and Bob don't trust each other but would like to jointly execute a computation. One of the basic primitives from which they can build up the ability to perform complicated two-party computations is *bit commitment*. The idea is to mimic the functionality of a safe: Alice locks a bit in the safe and then transfers the safe to Bob. At some time in the future, Alice tells Bob the combination so that he can look inside the safe and determine the value of Alice's bit.

We will restrict our attention to protocols of the following form:

- **Commitment phase:** Alice selects a bit $b \in \{0, 1\}$. She then prepares a state $|\psi^{(b)}\rangle_{AB_1B_2}$ and sends the B_1 system to Bob.
- **Reveal phase:** Alice send the B_2 system to Bob. He measures a specified $0/1$-valued observable O and reports the outcome as the value of the bit.

An ideal bit commitment protocol has the following properties:

- **Hiding**: When Alice follows the protocol, the density operator $\psi_{B_1}^{(b)} = \mathrm{Tr}_{AB_2} |\psi^{(b)}\rangle\langle\psi^{(b)}|_{AB_1B_2}$ is independent of b. Bob therefore can't learn anything about b before the reveal phase.
- **Binding:** A dishonest Alice cannot change her mind after the commitment phase. In other words, it is impossible for Alice to change $|\psi^{(b)}\rangle$ into $|\psi^{(\neg b)}\rangle$ after the completion of the commitment phase.

Show that ideal bit commitment is impossible.

(Slightly Comical) References:

- Gilles Brassard, Claude Crépeau, Richard Jozsa and Denis Langlois. A quantum bit commitment scheme provably unbreakable by both parties. *Proceedings of the 34th Annual Symposium on Foundations of Computer Science.*, IEEE, 1993.
- Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*. 78(17):3414-3417, 1997.

4. *Trace distance and state distinguishability.* You will demonstrate that the trace distance $\|\rho - \sigma\|_1$ precisely captures the operational distinguishability between two quantum states ρ and σ. Step by step...

a) Given density operators ρ and σ, argue that there exist positive semidefinite operators P, Q such that $\rho - \sigma = P - Q$ and $\operatorname{Tr} PQ = 0$. Conclude that $\|\rho - \sigma\|_1 = 2 \operatorname{Tr} P$.

b) Given any hermitian operator $0 \le \Lambda \le I$, use this decomposition to show that

$$2 \operatorname{Tr}[\Lambda(\rho - \sigma)] \le \|\rho - \sigma\|_1. \tag{7}$$

c) Find a Λ saturating the inequality to conclude that

$$\|\rho - \sigma\|_1 = \max_{0 \le \Lambda \le I} 2 \operatorname{Tr}[\Lambda(\rho - \sigma)]. \tag{8}$$

d) A measurement to distinguish ρ and σ can be described by a pair of Hermitian projectors Π_ρ and Π_σ such that $\Pi_\rho + \Pi_\sigma = I$. Suppose that a system is generated in either state ρ or σ, each with equal probability, and you would like to determine which it is. Your probability of making a mistake is

$$p_{err}(\Pi_\rho, \Pi_\sigma) = \frac{1}{2} \operatorname{Tr} \rho \Pi_\sigma + \frac{1}{2} \operatorname{Tr} \sigma \Pi_\rho. \tag{9}$$

Show that

$$p_{err}(\Pi_\rho, \Pi_\sigma) = \frac{1}{2} \left\{1 - \operatorname{Tr}\left[\Pi_\rho(\rho - \sigma)\right]\right\} \tag{10}$$

and thereby conclude that the minimum over measurement choices of p_{err} is

$$\frac{1}{4} \left(2 - \|\rho - \sigma\|_1\right). \tag{11}$$

5. *Coupling constants and loop counting parameters*. Consider a scalar $\lambda\phi^3$ theory in six dimensions, coupled to a source (the number of dimensions won't matter, and we understand that this is a nonperturbatively unstable. We choose six dimensions because the coupling is dimensionless; we could make the same point with gauge theory in four dimensions, it's just slightly more complicated):

$$S = \int d^6x \left(\frac{1}{2}(\partial\phi)^2 - \frac{1}{2}m^2\phi^2 - \frac{1}{3}\lambda\phi^3 + J\phi \right) \tag{12}$$

Note that this appears in the Feynman path integral as

$$Z[J] = \int D\phi e^{\frac{i}{\hbar}S} \tag{13}$$

a) Consider a Feynman diagram for (say) corrections to the propagator. How do the tree level propagator and vertices scale with $\hbar$? How do they scale with g?

b) Show that a given Feynman diagram for correlation functions in momentum space scales as $\hbar^{L+N_e-1}$ where L is the number of loops and N_e the number of external legs. The number of loops corresponds to the number of unconstrained momenta in the diagram. Each internal propagator will carry momenta that will be integrated over; each external line will have fixed momenta; and each vertex will constrain the momenta consistent with momentum conservation. You may do this for ”bubble” diagrams (having no external lines – these compute the vacuum energy) if you wish.

c) By rescaling ϕ, show that you can write $S[\phi]/\hbar$ as $\tilde{S}/(g^2\hbar)$, where $\tilde{S}$ is *independent* of g. Argue that $g^2 \to 0$ is a good classical limit for the theory. Note that by this argument, diagrams scale as $(g^2\hbar)^{L+N_e-1}$, so even in the $\hbar = 1$ convention, g^2 (the *square* of the coupling) is a loop-counting parameter.

d) You may wish (at home) to see for yourself that the loop counting parameter in a nonabelian gauge theory is the square of the Yang-Mills coupling.

Ramond's book *Field Theory: A Modern Primer* has a good discussion of this; it should be in other good modern QFT textbooks.

6. *Coherent states are classical*. The point here is to show what the ”classical limit” looks like from the point of view of quantum mechanics. Consider a simple harmonic oscillator with the usual creation and annihilation operators $a^\dagger, a$. ”Coherent states” take the form

$$e^{\lambda a^\dagger}|0\rangle \equiv |\lambda) \tag{14}$$

a) Find the scaling of λ with $\hbar$ for $\langle x\rangle$ and $\langle p\rangle$ to be finite as $\hbar \to 0$.

b) Argue that $< xp >=< x >< p > +\mathcal{O}(\hbar)$ for these coherent states.

c) Find the scaling with $\hbar$ of the average particle number

d) Show that under time evolution, $|\lambda)$ evolves as $|\lambda(t))$.

One may similarly write down ”coherent states” for a large N theory. For this, see the beautiful review by L. Yaffe, *Rev. Mod. Phys.* **54** (1982), p. 407. The essential point with all such theories is that one needs a ”small parameter” and a class of operators and coherent states such that correlation functions of operators in these coherent states factorizes.

7. *The boundary of AdS*. Consider the metric for d-dimensional AdS in global coordinates:

$$ds^2 = -\left(1 + \left(\frac{\rho}{R}\right)^2\right) dt^2 + \frac{d\rho^2}{\left(1 + \left(\frac{\rho}{R}\right)^2\right)} + \rho^2 d\Omega_{d-1}^2 \tag{15}$$

where $d\Omega$ is the metric on the unit $(d-1)$-sphere. Show that a light ray emitted from $\rho = 0$ reaches $\rho = \infty$ in finite t.