8.S372/18.S996 Quantum Information Science III **Fall 2020**

Lecture 20: November 10, 2020

Lecturer: Aram Harrow *Scribe: Yuan Lee, Shreya Vardhan*

In this lecture, we complete the discussion on merging and re-visit k-designs.

20.1 Black holes as mirrors

Black holes can be formed in general relativity from the gravitational collapse of a star in a pure state. Once the black hole is formed, it behaves in many respects like a thermal state: it emits radiation at a certain temperature, and can be associated with a thermodynamic entropy. However, the evolution from a pure state to a mixed state would violate the unitarity of quantum mechanics.

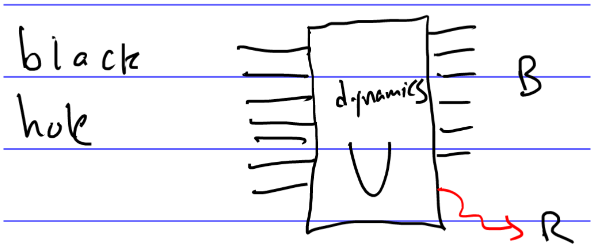
To see the same problem from another perspective, consider the following setup: Alice throws a diary into the black hole. Where does the information in the diary go? There are a few different options, but each of these presents some problems:

- The information is destroyed. This violates the unitarity of quantum mechanics.
- The information escapes gradually through the Hawking radiation. This violates the prediction from classical general relativity that nothing can escape from behind the horizon. Recently, a further problem with this option, known as the "firewall paradox", has also been discussed (see 1207.3123). This involves certain implications of monogamy of entanglement.
- The information escapes at the end. This violates the Bekenstein bound, which is a bound on the amount of entropy that can be contained within a given spatial region, as it implies that towards the end of the evaporation process, a very small region would have a very large entropy.
- There is a Planck-size black hole remnant left over at the end of the evaporation process. This violates the Bekenstein bound and destabilizes low-energy physics.
- A large black hole remnant is left over. This would imply that Hawking radiation stops being emitted at a relatively early time, which contradicts fairly reliable predictions of semiclassical gravity.

The difficulty of accepting any of these options lies at the heart of the conflict between general relativity and quantum mechanics.

It turns out (Hayden and Preskill, 0708.4025) that information discarded in an old black hole can be quickly recovered, given that we possess the Hawking radiation previously emitted from the black hole. This is a consequence of merging.

We can think of the black hole's time evolution as a unitary black box.



If the black hole starts off as a pure state, then the combined state $|\psi(t)\rangle_{BR}$ will be pure at all times t, if we assume the dynamics is unitary. Assuming that the time evolution operator $U(t)$ is Haar-random, the entropy of the black hole and the radiation are equal to $S(B)_{\psi(t)} = S(R)_{\psi(t)} = \min(|B|, |R|)$.

This gives rise to the Page curve (1301.4995): the entropy of the black hole increases until the Page time, after which its entropy decreases to zero.[2]

Now we consider the process of discarding information from Alice into an old black hole. To keep track of the information in Alice's qubits, we maintain a reference system that is (maximally) entangled to Alice's information.

Let the initial and final states be ρ and σ respectively. We now consider the state $\sigma_{NB'}$ that is shared by the black hole and the reference state. We expect this to be close to the maximally mixed state $\tau_N \otimes \tau_{B'}$. In fact, using the decoupling inequality from last lecture,

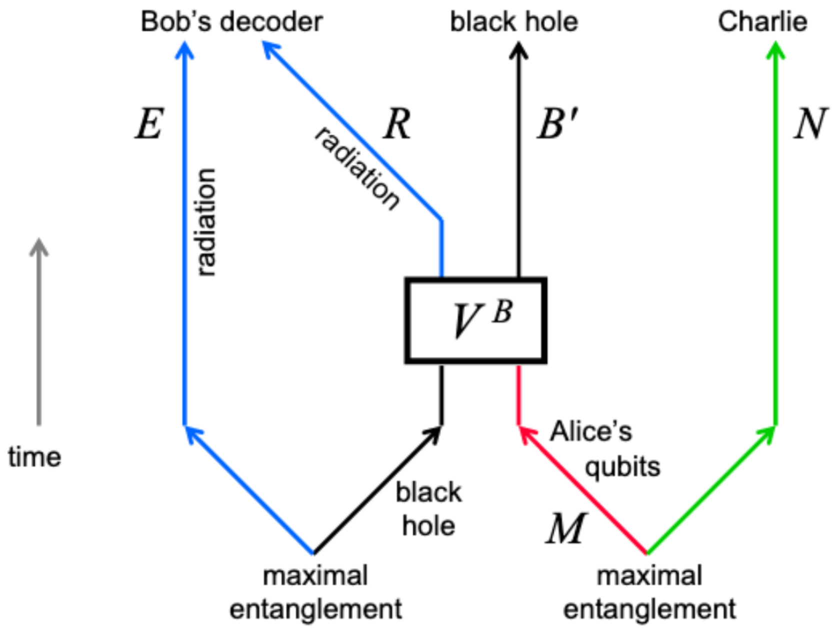
$$\mathbb{E}\|\sigma_{NB'} - \tau_N \otimes \tau_{B'}\|_1^2 \leq \frac{d_B d_B}{d_R^2} \mathrm{tr}\rho_{NB}^2 = \frac{d_N^2}{d_R^2}.$$

This distance is independent of the black hole dimension d_B.

In the above calculation, we use the fact that the black hole is old in the equation $\mathrm{tr}\rho_{NB}^2 = d_N/d_B$, because ρ_{NB} would then be maximally-mixed.

Applying Uhlmann's theorem allows us to perform merging: we can reconstruct Alice's entanglement with the reference system using the radiation in RE.

[2] Aside: an article about black hole entropies was recently published in *Quanta*.



σ

ρ

20.2 Quantum capacity theorem (by merging)

Merging also gives a direct argument for the quantum capacity theorem (quant-ph/0702005).

As before, given a channel $N : A' \to B$, let its Stinespring dilation be $V_N : A' \to BE$. The coherent information is then $I_c(\phi_{A'}, N) = S(B)_{V(\phi)} - S(E)_{V(\phi)}$.

Let $|\gamma\rangle_{ABE} = (I_A \otimes V_{A' \to BE}) |\phi\rangle_{AA'}$. With n copies of $|\gamma\rangle$, let $\Pi_{A^n \to S}$ be a projector onto a "typical subspace" S. In particular, we choose the projector Π such that the projection onto the subsystem S is maximally mixed. In other words, if $|\Psi\rangle_{SB^nE^n} = (\Pi_{A^n \to S} \otimes I_{B^nE^n}) |\gamma\rangle^{\otimes n}$ up to normalization, then $\Psi_S = I_S/d_S$. The state Ψ would be close to the actual typical projection $\tilde{\Psi}$ in the subsytem E.

Then rank$\tilde{\Psi}_{E^n} \leq 2^{n(S(E)_\phi + \delta)}$ and tr$\tilde{\Psi}^2_{B^n} \leq 2^{-n(S(B)_\phi - \delta)}$.

Note that we can also write $|\Psi\rangle_{SB^nE^n} = (I_S \otimes V^{\otimes n}) |\Phi\rangle_{SS'}$, where Φ is the maximally-entangled state.

Like in Shannon's noisy coding theorem, we choose a random codespace R using a fixed projector $P_{S \to R}$ and a Haar-random unitary $U_{S \to S}$, and conjugating $P_{S \to R}$ with $U_{S \to S}$. Then, the encoded state is

$$\begin{aligned} |\psi\rangle_{RB^nE^n} &= \sqrt{\frac{|S|}{|R|}} (PU \otimes I_{B^nE^n}) |\Psi\rangle_{SB^nE^n} \\ &= (I_R \otimes V^{\otimes n} U^\top) |\Phi\rangle_{RR'} . \end{aligned}$$

Here,

$$\mathbb{E}\|\tilde{\psi}_{RE^n} - \tilde{\psi}_R \otimes \tilde{\psi}_{E^n}\|_1^2 \leq d_R(\text{rank}\tilde{\psi}_{E^n})(\text{tr}\psi_{SE^n}^2) = d_R 2^{-n(S(B)_\phi - S(E)_\phi - 2\delta)}.$$

If $d_R \leq 2^{n(I_c(\phi,N)-3\delta)}$, the above distance is bounded above by $2^{-n\delta}$. Hence, for sufficiently small $\delta > 0$, the R and E^n subsystems are decoupled on average. We can strengthen this to worst-case decoupling by further restricting the codespace, allowing Bob to reconstruct Alice's state by merging.

20.3 Unitary k-designs

Let the matrix of all expected monomials $M(U) = U_{a_1b_1} \ldots U_{a_kb_k} U^*_{c_1d_1} \ldots U^*_{c_kd_k}$ under a distribution of unitaries μ be

$$\begin{aligned} G^k_\mu &= \mathbb{E}_{U\sim\mu}[(U \otimes U^*)^{\otimes k}] \\ &= \text{proj span } \{(I^{\otimes k} \otimes p_d(\pi))\,|\Phi_d\rangle^{\otimes k} : \pi \in S_k\}, \end{aligned}$$

where S_k is the set of permutations between k qudits, $p_d(\pi)$ is the qudit permutation operator and Φ_d is the maximally-entangled state.

We say that a distribution μ on $U(d)$ is a *k-design* if

$$G^k_\mu = G^k_{\text{Haar}}.$$

Equivalently, for all matrices ρ,

$$\mathbb{E}_{U\sim\mu}[U^{\otimes k}\rho(U^\dagger)^{\otimes k}] = \mathbb{E}_{U\sim\text{Haar}} U^{\otimes k}\rho(U^\dagger)^{\otimes k}.$$

1-designs satisfy $\mathbb{E}[U\rho U^\dagger] = I/d$. We saw previously that the uniform distribution over the d^2 Pauli matrices form a 1-design. Moreover, the uniform distribution over a set of $O(d/\epsilon^2)$ random unitaries is an ϵ-approximate 1-design. Drawing a random unitary or Pauli matrix is cheaper than drawing a random unitary from the ϵ-net for $U(d)$, which has $(1/\epsilon)^{d^2}$ elements.

However, 1-designs are not enough for merging. For example, applying a random Pauli does not generate entanglement in an intially unentangled state, whereas applying a Haar-random unitary does.

It turns out that 2-designs are sufficient for most applications, including merging. An example of a 2-design is the uniform distribution over the set of Clifford operations.

To show that the Cliffords form a 2-design, first note that we can decompose all matrices into sums of Pauli matrices. Therefore, it suffices to consider the action of the Cliffords on the Paulis.

Next, let C be a random Clifford on n qubits, and let $p \in \{0,1,2,3\}^n$. Defining $\sigma_q = \sigma_{q_1} \otimes \ldots \otimes \sigma_{q_n}$,

$$C\sigma_p C^\dagger = \begin{cases} I & \text{if } p = 0^n, \\ \sigma_q & \text{for random } q \neq 0^n \text{ if } p \neq 0^n. \end{cases}$$

Therefore,

$$\mathbb{E}[(C\sigma_p C^\dagger) \otimes (C\sigma_q C^\dagger)] = \begin{cases} I & \text{if } p = q = 0^n, \\ \frac{1}{4^n-1}\sum_{r\neq 0^n} \sigma_r \otimes \sigma_r & \text{if } p = q \neq 0^n, \\ 0 & \text{if } p \neq q. \end{cases}$$

Note that $\sum_r \sigma_r \otimes \sigma_r = 2^n\text{SWAP}$ (where the sum includes $r = 0$). Therefore,

$$\mathbb{E}[(C\sigma_p C^\dagger) \otimes (C\sigma_q C^\dagger)] \in \text{span}\,\{I, \text{SWAP}\}.$$

This implies that the uniform distribution over the Clifford group is a 2-design, since SWAP commutes with $U \otimes U$.

In fact, the uniform distribution over the Cliffords is also a 3-design, but not generally a 4-design.

It is more expensive to draw a uniform sample from the Clifford group than the Pauli group, as the Clifford group has size 2^{n^2}. However, it is still cheaper than drawing from an ϵ-net of $U(d)$.

It turns out that we can generate approximate k-designs for any k using a sufficiently large set of random unitaries. We find the number of unitaries needed using the matrix Chernoff bound, which states that

$$P\left(\|\frac{1}{n}\sum_{i=1}^{n} X_i\|_\infty \geq \delta\right) \leq 2de^{-n\delta^2},$$

where $X_1, \ldots, X_n$ are iid $d \times d$ matrices with mean zero and $\mathbb{E}\|X_i\|_\infty \leq 1$.

If μ is the uniform distribution over m random unitaries $\{U_1, \ldots U_m\}$, it is convenient to define

$$X_i = (U_i \otimes U_i^*)^{\otimes k} - G^k_{\text{Haar}}.$$

Then $G^k_\mu - G^k_{\text{Haar}} = (1/m)\sum_{i=1}^m X_i$. Therefore,

$$\|G^k_\mu - G^k_{\text{Haar}}\|_\infty \leq \delta \text{ if } m = O(k(\log d)/\delta^2)$$
$$\Rightarrow \|G^k_\mu - G^k_{\text{Haar}}\|_1 \leq \delta \text{ if } m = O(d^{2k}k(\log d)/\delta^2).$$

We can get a lower bound on the rank n of $\mathbb{E}[U^{\otimes k} \left|0\right\rangle \left\langle 0\right|^{\otimes k} (U^\dagger)^{\otimes k}] \approx \Pi_{\text{sym}}/\text{tr}\Pi_{\text{sym}}$ for any approximate k-design over U:

$$n \geq \text{tr}\Pi_{\text{sym}} = \binom{d+k-1}{k} = O(d^k).$$