University of Houston

Black Holes

As Information Scramblers

Spring-2024

Profesor: Anna Vershynina

Bhavay Tyagi

April 14, 2024

Contents

1 Introduction and Motivation

1.1 Dualities in Physics

The existence of common dynamics in different physical systems hints at the fact that an underlying symmetry is manifest in both the systems and such systems are called "Dual" to one another. Mathematically, it is the equivalence of the partition function describing the two systems:

$$Z_{sys1} = Z_{sys2}. \tag{1}$$

A simple, and well known, example is the **Wave-particle duality**. Where depending on what the question is, you can treat, for example electrons, as particles or waves. The duality that we're interested in is the **Quantum-Gravity** duality. The most striking fact about this is that we think "Quantum" relates to something small and light (particles) and "Gravity" relates to something big and heavy (Planets, Galaxies, Black Holes). We know that the quantum description of particles is probabilistic while Einstein's General Relativity governs the behavior of astrophysical objects by studying "geometrical curving" of spacetime due to these massive objects.
Q: If these two things were to be Dual to one another, do we think that the spacetime is fluctuating, probabilistic?

1.2 What's the information problem?

The arguments here are best explained with intuitive *gedanken* experiments. This is also the approach I will follow to make a schematic arguments throughout this review. Imagine a book written using the Rotokas[1] alphabet. Let's calculate the Entropy of the book. The possible configurations to arrange the 12 letters with an average word length of 5 letters is ${}^{12}C_5$. Let the book have $O(3000)$ words. So

$$\Omega = ({}^{12}C_5)^{\,3000} \tag{2}$$

possible configurations of letters in the book. Hence, the entropy of the book is given by

$$S = k_B ln\Omega \tag{3}$$

which is obviously a strictly a positive number. Now imagine dropping the book into a Black Hole Fig 1.

1.2.1 Black Holes Have No Hair

A profound but counter-intuitive fact about Black Holes: Any black-hole can be **completely** characterized by its Mass (M), Charge (Q) (Riessner-Nordstrom) and Angular Momentum (J) (Kerr)[2]. This is a powerful theorem since it tells us that black holes are like no other objects in the universe. Imagine two planets, they can have vastly complex and different geographical, biological properties (which is what we mean by hair) but if you collapse them into a black hole, the black hole completely loses information about the original planets (initial state). It is only characterized by the final state: (M, Q, J).

Now note that dropping the book into the black hole we can imagine that the black hole mass increased by a finite amount. But according to the theorem above the final state of the black hole is given by

$$\Omega = (M, Q, J)$$

Therefore,

$$S = k_B ln\Omega = k_B ln(1) = 0 \tag{4}$$

[1] Rotokas is considered by linguists to have the fewest letters of any alphabet in the world. It has only 12 letters and is spoken by a few thousand people in New Guinea.

[2] A powerful realization by John Wheeler.

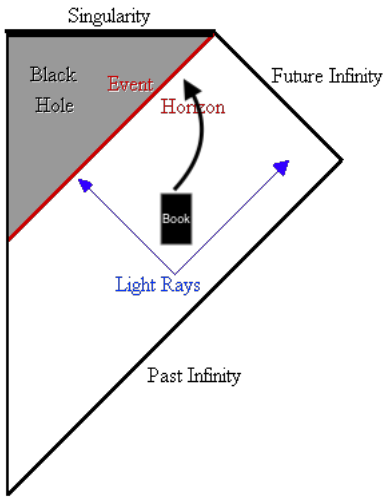

Figure 1: Spacetime diagram of a near black hole region illustrating the informatin paradox.

This violates the **second law of thermodynamics**

$$\Delta S \geq 0. \tag{5}$$

This immediately tells us that this astrophysical (macroscopic) view of characterizing black holes is missing some information about the microscopic degrees of freedom that would lead to some greater (or equal) number of configurations. Which would then preserve the second law.

1.3 Black Holes as a Testing Ground

1.3.1 Then why still choose black holes?

The most natural way of answering this question (with a naive-intuitive motivation) is to study Black Holes because these are astrophysical objects (heavy) who radiate quanta [3] whose de-broglie wavelength is comparable their own size. That's striking because every quantum (small) particle is considered "small" when it satisfies this property. So black holes can be treated as quantum objects[3] when viewed from the outside.

$$\lambda_{\text{H-ATOM}} \sim 10^{-10} m = \text{its size}. \tag{6}$$

$$\lambda_{\text{Hawking}} = \text{ size of black hole and radiates with a rate of } \sim 1 \text{ quanta/light-crossing time}$$

For example for a "small" Black Hole of Mass $M \sim M_\odot$ (one solar mass), we have the radiation of 10^5 photons per second whose $\lambda_{\text{Hawking}} \sim 1$ km. Such an astrophysical black hole would would take 10^{65} years to evaporate. A quantum computation on the the "collected" radiation will be exponential in the black hole entropy which means about $10^{10^{80}}$ more years to perform this calculation. We can avoid this problem by creating our own black holes which are significantly smaller. This is possible if we push some given constituents within their mutual Schwarzschild radius. If the constituents are of $O(1)$ then that requires energies $m_p \sim 10^{-8}$kg (Planck Mass). This exceeds the energy of the Large Hadron Collider by a factor of 10^{15}.

[3]Note: They aren't really quantum objects, but they can be treated like one. This is an important difference, but one that enforces our definition of Dual systems. This is also a consequence of the AdS/CFT correspondence given by Juan Maldacena. This is the most profound realization of Dualities in physics. I suggest the reader to read about this to get a deeper understanding.

What are we even trying to do then?
Black Holes exist, and our world is fundamentally quantum. Hence, nature must find a way to accomodate both.[4]

2 The Harlow-Hayden Proposal

2.1 AMPS Firewall Paradox

To understand the arguments carefully we need to first understand an oberserver dependent thought experiement. In 2012 Almheiri, Marlot, Polchinski and Sully (AMPS) proposed a thought experiment which described what an observer would experience while entering a black hole. Recall from Quantum Field Theory the fact that the QFT vacuum has large short-ranged entanglement. What this means is that when an observer approaches the event horizon and you see a Hawking photon emerge from the horizon, there will be an entangled photon just inside the event horizon. Think of this as a bunch of Bell Pairs around the Horizon. Now if the observer doesn't see these Bell pairs when crossing the horizon they wouldn't see a smooth spacetime but instead a wall of Planck-energy photons which would instantaneously disintegrate them [9]. This is what's called the firewall.

2.2 Black Holes as Unitary Quantum Systems

2.2.1 A Quick Restatement of the Problem

Stephen Hawking and Jacob Bekenstein did their calculation [7] and proved that Black Holes are thermal objects and had some temperature. As a result it emits thermal radiation and will evaporate in some exponential amount of time. This radiation when collected outside could be measured[5]. It is assumed that this radiation carries information about the infalling matter but when it is carefully collected and measured outside it was observed that the density matrix describing it was mixed. Now we know that Black Holes evolutionary dynamics should be unitary. Which means that if we start from a pure state $|\psi\rangle$ and then apply multiple Us that is

$$UU...U\,|\psi\rangle \tag{7}$$

we should still be able to invert all of that and get back to the pure state. However that doesn't happen. **A pure state evolves into a mixed state**, which is crazy.

2.2.2 A Pure Information Theoretic Story of An Outside Observer

Let us now think of Black Holes as quantum systems when viewed from the outside and treat them as the fastest scramblers[6] in the universe. Let the Black Hole be "described" by n qubits[7] in the simplest state

$$|0...0\rangle$$

and its evolution be described by some complicated "random" quantum circuit C. Let the output state (Hawking Radiation) of the circuit be a pure random state $|\psi\rangle_{Random}$. Now imagine we have access to only first k qubits. The reduced density matrix for this would be

$$\rho = \sum_{i}^{2^{n-k}} pi\,|\psi_i\rangle\,\langle\psi_i|$$

[4] A situation where our reasoning is motivated by anthropic arguments.
[5] At least in principle.
[6] Scrambling: the spread of any perturbation throughout all degrees of freedom of the system and the time required for this to happen is called scrambling time.
[7] Just a warning to the reader that this is a very simplified analogy, it is almost impossible to treat black holes as a simple set of qubits. However it is not problematic here for the purposes of our analysis.

here we trace over the remaining qubits. Notice that there are two regions of interest

- $k < n/2$: Then one can check that $rank(\rho) = 2^k$ and ρ will be close to being maximally mixed.
- $k > n/2$: Then $rank(\rho) = 2^{n-k} < 2^k$. ρ is no longer maximally mixed in this case.

What this indicates is that when exactly half of the qubits emerge out of the black hole, the outside observer let's say Alice, can access the correlations between the Hawking photons and the infalling matter. This is conjectured to happen after "Page Time"[8]. See fig 2

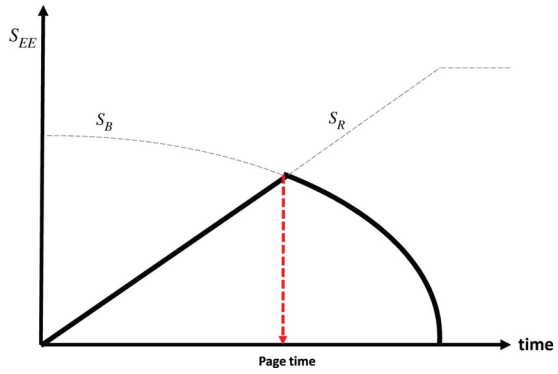

Figure 2: This is called the Page Curve. Which tels us that the entropy of the radiation coming out of the black can not be ever increasing. It has to start goiing down after page time to respect unitary dynamics.

To prove the above point a similar infromation tracking calculation[9] is shown for such a scenario see fig 4, with the black hole being replaced by an Alice-Bob communication protocol. But they don't have a classical channel between them. In this the authors track Entropy propagation through mutual information.

$$I(B:R) = S(B) + S(R) - S(BR) \tag{8}$$

Where $S(R) = -tr(\rho_R \log_2 \rho_R)$ and I is bounded between $0 \leq I(B:R) \leq 2min(S(B), S(R))$[10]. If Alice prepares some initial Bell-pair state and allow the state to evolve under some unitary dynamics then when finally it is Bob's turn to measure things and he has access to only the first k qubits. He will see that Entanglement leaks and spreads in a complex way throughout all degrees of the system. However if Bob waits long enough which means $k > n/2$ then he will see the mutual information reaching the upper bound which is 2.

2.2.3 The Paradox

Imagine Alice sets up this experiment of n qubits in a known initial state. Alice also knows how this will evolve unitarily to form a black hole and then evaporate. Alice also puts a Dyson sphere surrounding the black hole which captures all the Hawking photons and puts them into a quantum computer for processing. Alice waits for at least the Page Time (10^{67}) years, let $2n/3$ photons come out of the black hole giving us three subsystems

- R (think of this as Radiation): $k = 2n/3$
- B (think of this as Reference): The very next qubit coming out.
- H: Remaining qubits.

[8] A time scale named after physicist After Don Page.
[9] The reader should look at [5]
[10] This is due to properties of entroy. See [5]

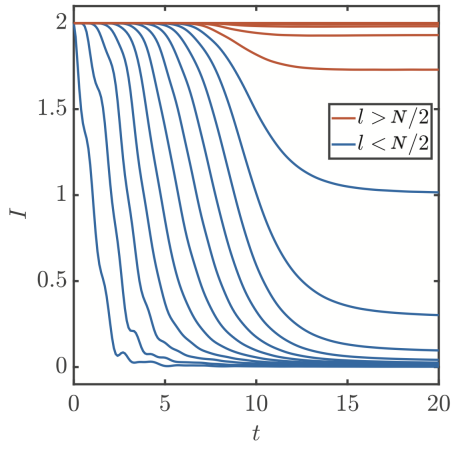

Figure 3: Ballistic information propagation in a qubit system for N=22 spins [5].

We expect that B is entangled with R. The state ρ describing the joint state of $k+1$ qubits is not maximally mixed. Alice now puts the leftmost qubit of R in a maximally entangled state (Bell pair) with B such that $I_{BR} = S_B + S_R - S_{B+R} = 2$ and then jumps into the black hole. Recall that the qubit B coming out of the black must also be maximally entangled with a qubit in H inside the horizon and Alice should be able to observe this entanglement as well. This violates the *Principle of Monogamy of Entanglement*[11]. So either the entanglement between B and R can be observed or between B and H can be. See Fig 4.

3 The HH Decoding Task

The firewall paradox or at least a part of it can be translated into a computational problem [6].
Task at Hand:
Consider a circuit C that maps n-qubits $|0\rangle^{\otimes n}$ to $|\psi\rangle_{RBH}$ (a tri-partite state, where B is a single qubit). The existence of a unitary U is guaranteed that acts on the the R part of the state which puts the leftmost qubit of R and B into $1/\sqrt{2}\,(|00\rangle + |11\rangle)$. Challenge is to apply this U to R.
The above task is doable since the argument guarantees the existence of such a U but the question is: Is this problem even computationally tractable?

Recall now that subsystem R has $k > n/2$ qubits and therefore ρ_{RB} is not maximally mixed. If the state $|\psi\rangle_{RBH}$ is an output of a random circuit, we expect entanglement between R and B. If we try to do this using an actual quantum circuit as in Fig 2 then the circuit required to distill the entanglement between R and B would have an exponential size[12]. The caveat here is that we're restricted by physical arguments that the action of the unitary U will on the R part of the system. Which is essentially what we have access to. Hence, the triviality of inverting C is out of question. The connection is further made from the following theorem, which seeming relates the solution of this problem to an unrelated problem.

Theorem: If the HH Decoding task can be done in polynomial time for arbitrary circuit C, then SZK $\subseteq$ BQP.

Let's break this down.

[11]The same qubit can't be maximally entangled with two other qubits.
[12]In terms of number of gates and time. So the size in this context means both space and time

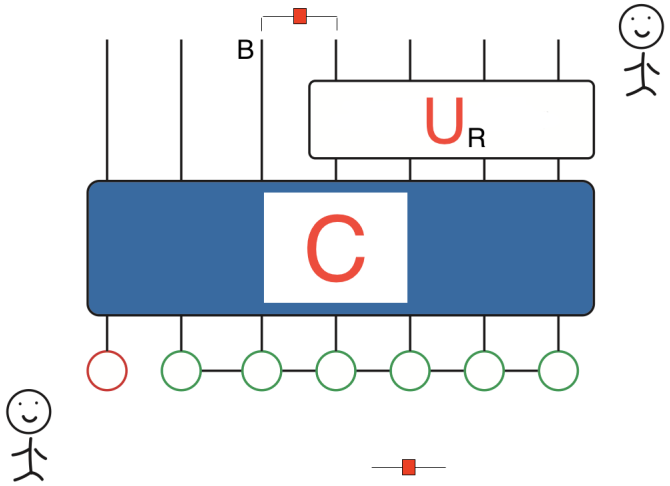

Figure 4: The red square with a line denotes a Bell Pair $= \frac{|00\rangle+|11\rangle}{\sqrt{2}}$

3.1 Lightening Review of Quantum Complexity Theory

This is the Quantum version of the Classical computational complexity. Broadly speaking the way complexity is measured is by estimating the amount of resources (space and time) would be required by an algorithm as a function of the size of the input. Classic examples include
P: Problems in this class are solvable in time $t \sim O(N^k)$.
NP: Given a solution, problems in this class can be verified in polynomial time. However finding the solution might not be possible in polynomial time. Now where does "Quantum" enter this picture?

- **BQP**: Class of all languages $L \subseteq \{0,1\}^*$ for which there exists a P-uniform family of polynomial-size quantum circuits $\{C_n\}_{n\geq 1}$ acting on $p(n)$ qubits (for some polynomial p) over some finite universal gate set $\mathcal{G}$ such that for all n and for all $x \in \{0,1\}^n$

$$x \in A \implies P\left[C_n \text{ accepts } |x\rangle \otimes |0\rangle^{\otimes p(n)-n}\right] \geq 2/3$$

$$x \notin A \implies P\left[C_n \text{ accepts } |x\rangle \otimes |0\rangle^{\otimes p(n)-n}\right] \leq 1/3$$

  It contains all decision problems that can be solved in polynomial time when using a quantum computer [1]. Now with the presence of the *Toffoli* gate we can simulate all classical digital computation which means P $\subseteq$ BQP. Telling us that all digital calculations can be done on a quantum computer.

- **SZK**: Class of all languages $L \subseteq \{0,1\}^*$ for which there exists a probabilistic protocol between Alice (a polynomial-time verifier) and Bob(all powerful but untrustworthy prover with unbounded computational resources). In other words these are the class of decision problems for which a "yes" answer can be verified by a statistical zero-knowledge proof protocol. By exchanging messages with the prover, the verifier must become convinced (with high probability) that the answer is "yes," without learning anything else about the problem (statistically).
  Classic example is *Graph (Non)-Isomorphism* See Appendix A.

The reductionist argument is that if the HH Task can be done in polynomial time then a problem called "Set Equality" can also be solved in quantum polynomial time.

Set Equality: Given a black box access to two injective functions (maps which are not permutation symmetric) $f, g : \{0.1\}^n \to \{0,1\}^{p(n)}$, where we're promised that either

1. Range(f) = Range(g), or
2. Range$(f) \cap$ Range$(g) = \emptyset$

The problem is to decide which.

Theorem: Any Quantum Algorithm for Set Equality must make $\Omega(N^{1/3})$ queries.
This relates to the HH decoding as follows:
Let the polynomial-size $p(n)$ Circuit prepare

$$|\psi\rangle_{RBH} = \frac{1}{\sqrt{2^{n-1}}} \sum_{x\in\{0,1\}^n} (|x,0\rangle_R |0\rangle_B |f(x)\rangle_H + |x,1\rangle_R |1\rangle_B |g(x)\rangle_H) \tag{9}$$

This circuit can prepare the above state given that it can compute f and g. How does this encode Set Equality?
Consider

- Case 1: Range$(f) \cap$ Range$(g) = \emptyset$ In this case, since the ranges are disjoint, the H register decoheres any entanglement between R and B, exactly as if H had measured B. This implies that ρ_{RB} is not entangled. Thus, the HH task is void since the original setup is violated.
- Case 2: Range(f) = Range(g) In this case Alice uses their quantum computer to act on R and does the following mapping:

$$Id : |x,0\rangle \to |x,0\rangle$$
$$|x,1\rangle \to \left|f^{-1}(g(x)),1\right\rangle$$

This yields

$$|\psi\rangle_{RBH} = \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} (|x,0\rangle_R |0\rangle_B + |x,1\rangle_R |1\rangle_B) |f(x)\rangle_H \tag{10}$$

and we can see that B and the left-most qubit of R are indeed in a Bell state $\frac{1}{\sqrt{2}}(00 + 11)$, as we desired.

Therefore, as a recap if the HH task was easy, given f and g for which we wanted to solve set-equality, we can start by preparing the $|\psi\rangle_{RBH}$ state, apply the unitary ($\equiv$ doing HH), then finally projecting onto the Bell state to check if we succeeded. For Case 2, as we can see we would succeed with probability 1. For Case 1, we would succeed with probability at most 1/2. Thus, we can decide with bounded error probability, whether we want to choose Case 1 or Case 2. If set equality is hard for a quantum computer then so is the HH decoding task.

4 Final Remarks

1. The role of Black Holes in all the above arguments is to scramble our prepared quantum system and provide an inaccessible region of spacetime. This restricts our quantum computation to any region outside the black hole. Typically other chaotic physical systems do not have the property of violating the principle of monogamy of entanglement.
2. The HH task tells us that the current understanding of "effective" or approximate theories, namely Quantum Field Theory and Gravity, work well under certain circumstances fail as soon as we're able to solve a problem in polynomial time which is currently considered exponentially hard. This hints at a more complete quantum theory of gravity is currently missing from the framework. Previously it was known that these theories fail at very high energies (UV regimes) and large curvatures (Big Bang and Black Holes), however the HH argument gives us another regime of failiure which is the regime of exponential computational complexity.

4.1 Coming Full Circle AdS/CFT

I would like to conclude this review by this small qualitative example of the connection between our most prominent theories of quantum gravity and quantum circuit complexity. Recall I started this report by talking about the importance of Dualities in modern physics. The most prominent example is the AdS/CFT duality. The AdS/CFT correspondence is a holographic way of treating different systems, which says that under certain circumstances we have an equivalence between a $D + 1$ dimensional quantum theory of gravity living in the bulk of asymptotically AdS space and a "regular" quantum theory in D spacetime dimensions living on the boundary of this AdS space. If we consider warmholes in the bulk we see that the length of the warmhole keeps increasing. Since we also know that this is equivalent to a quantum theory on the boundary we need to have something corresponding to this ever increasing length even beyond equilibrium timescales. This turns out to be the circuit complexity of the quantum system [8].

5 References

References

[1] Scott Aaronson's Lecture notes for the 28th McGill Invitational Workshop on Computational Complexity arxiv:1607.05256

[2] Daniel Harlow, Black holes in quantum gravity arxiv:2304.10367

[3] Lectures on Holography by Nabil Iqbal

[4] S. W. Hawking, Particle Creation by Black Holes, Commun. Math. Phys. 43 (1975) 199–220. [Erratum: Commun.Math.Phys. 46, 206 (1976)].

[5] Scrambling Dynamics and Out-of-Time Ordered Correlators in Quantum Many-Body Systems: a Tutorial https://arxiv.org/abs/2202.07060

[6] Quantum Computation vs. Firewalls https://arxiv.org/abs/1301.4504

[7] Breakdown of predictability in gravitational collapse Phys. Rev. D 14, 2460 – Published 15 November 1976

[8] Computational pseudorandomness, the wormhole growth paradox, and constraints on the AdS/CFT duality https://arxiv.org/abs/1910.14646

[9] Black Holes: Complementarity or Firewalls? https://arxiv.org/abs/1207.3123

Appendix

A Graph Isomorphism

Consider two graphs $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$ are isomorphic. Which means if you permute the vertices of G_2 you can turn it into G_1. There is currently *no polynomial time classical or quantum algorithm known for this graph isomorphism problem.* Now imagine you meet a great complexity theorist and they claim to be able to solve it but they keep their abilities to solve it a secret. Would this scientist be able to convince you that they indeed have solved the problem without revealing anything about the structure of the graphs. As absurd as it may sound but the answer is yes. Imagine the theorist randomly permutes vertices of G_1 such that $G_1 \to G_3$ and sends it to you. You can then choose to flip a coin and depending on the outcome you can challenge the theorist to tell you if $G_3 \simeq G_1/G_2$. He will succeed with probability 1 is they were really isomorphic but will fail with probability at most $1/2$ if they aren't.