Title: Towards quantum information processing in gravitating spacetimes"

Speakers: Alex May

Series: Perimeter Institute Quantum Discussions

Date: January 31, 2022 - 3:00 PM

URL: https://pirsa.org/22010076

Abstract: Aside from quantum mechanics, other areas in physics constrain information processing. From relativity, we know information cannot move faster than the speed of light. In quantum gravity, we expect but don't fully understand additional constraints, for instance on how densely information can be stored. Can we develop an understanding of information processing in the context of quantum gravity? Towards doing so, we consider quantum information within ``holographic" spacetimes, which have an alternative, non-gravitational, description. In that context questions about information processing in the presence of gravity can be translated to different questions about quantum information without gravity. As a specific example, we study constraints on computation within a gravitating region, and use the holographic description to argue that gravity constrains the complexity of operations that can happen inside the region. Along the way, we are led to new connections relating quantum gravity, position-based cryptography, quantum secret sharing and complexity theory.

Towards quantum information processing in gravitating spacetimes

Alex May
Stanford University

"Quantum tasks in holography"

Based on: 1902.06845, 1912.05649, 2105.08094,
AM; AM, J. Sorce, G. Penington; AM

2101.08855, 2101.08855, 2102.01810
AM; AM; AM, D. Wakeham

2202.xxxxx
AM, Sam Cree

Quantum information processing in spacetime

- Quantum information asks: Given the rules of quantum mechanics, how can information be processed?

- There are additional rules:

Relativity → no-signalling

Quantum Gravity → covariant entropy bound, others?

$\boxed{\text{What can we say about information processing when considering the physics of quantum gravity?}}$

↳ what is the right framework to address this?

Outline

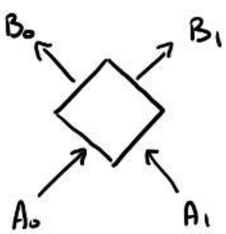
- Big picture idea:

For spacetimes described "holographically", we can translate questions about QI with gravity to questions about QI without gravity

Present new results on NLQC today

In particular:

Does gravity constrain computation? → How much entanglement is required in non-local quantum computation?



complexity

cryptography

secret sharing

Outline

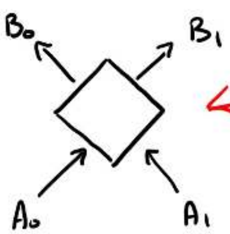
- Big picture idea:

For spacetimes described "holographically", we can translate questions about QI with gravity to questions about QI without gravity

In particular:

Present new results on NLQC today

Does gravity constrain computation? → How much entanglement is required in non-local quantum computation?



complexity

cryptography

secret sharing

Outline

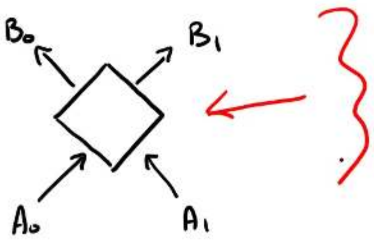
- Big picture idea:

For spacetimes described "holographically", we can translate questions about QI with gravity to questions about QI without gravity

Present new results on NLQC today

In particular:

Does gravity constrain computation? → How much entanglement is required in non-local quantum computation?



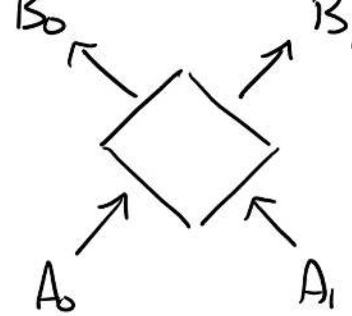
complexity

cryptography

secret sharing

Quantum information in a dynamical spacetime background

Complexity + gravity?



- One suggestion from Lloyd (2000) is that gravity constrains complexity

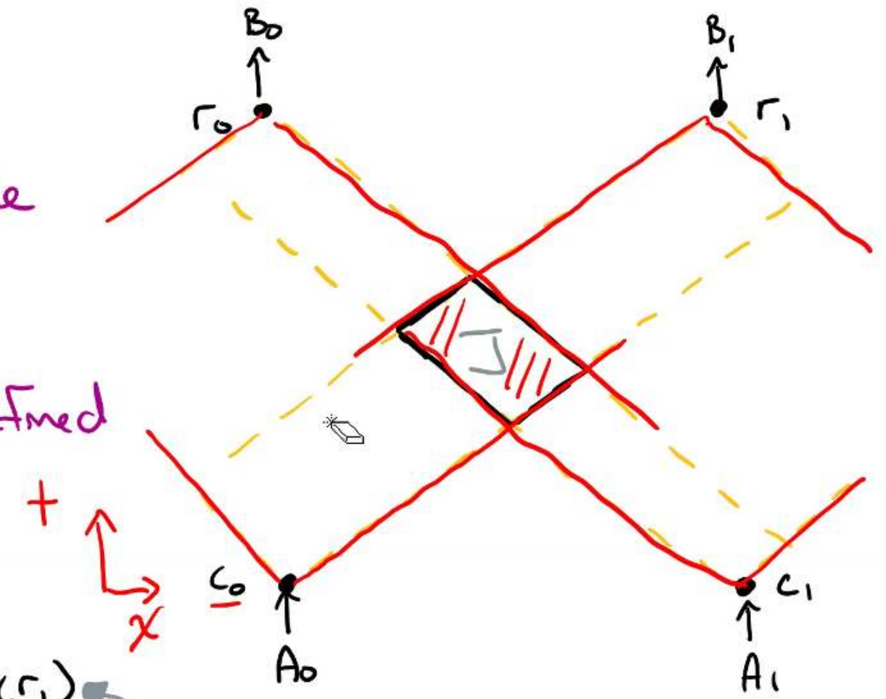
- Lloyd argued $\boxed{\text{Energy} \le M_{BH}}$ plus ordinary quantum mechanics would upper bound complexity
  - ↳ But, Jordan (2017) gave a counterexample!

- Jordan's construction ignores no-signalling, etc. In full quantum gravity, does gravity constrain complexity?

Defining the region

- Given a spacetime region $\mathcal{J}$ what computations can happen inside the region?

- To specify region $\mathcal{J}$ in a well defined way, pick c_0, c_1, r_0, r_1 s.t.



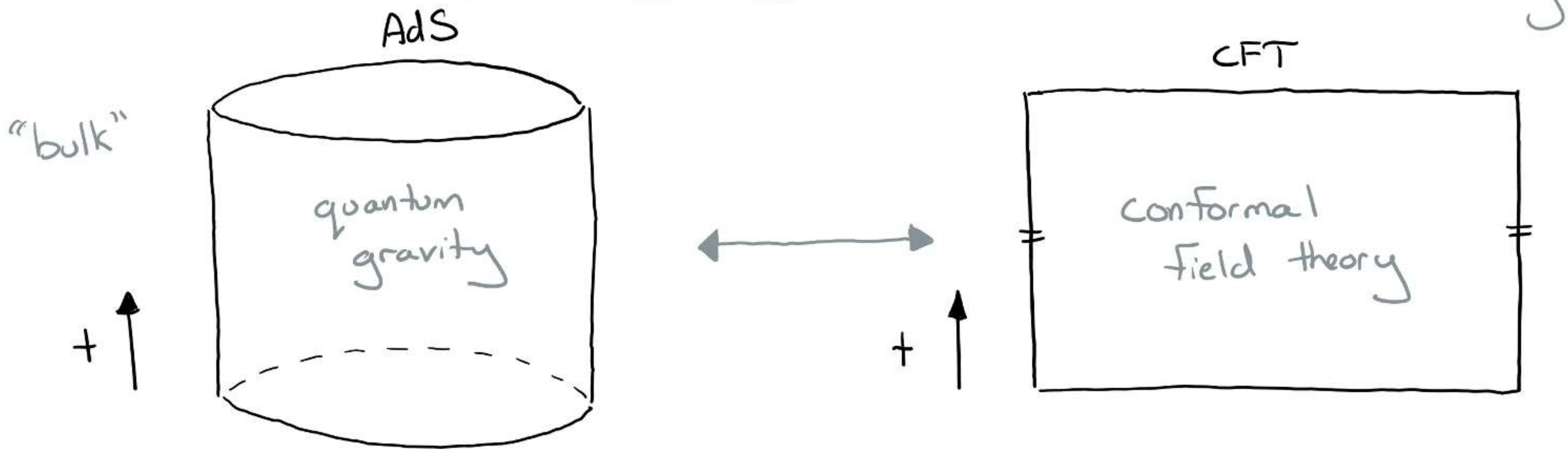
$$\mathcal{J} \equiv \mathcal{J}^+(c_0) \cap \mathcal{J}^+(c_1) \cap \mathcal{J}^-(r_0) \cap \mathcal{J}^-(r_1)$$

"scattering region"

- Give input systems A_0, A_1 at c_0, c_1, output systems B_0, B_1 at r_0, r_1.

AdS/CFT

- To understand QI with gravity, go to a setting where we understand quantum gravity better.

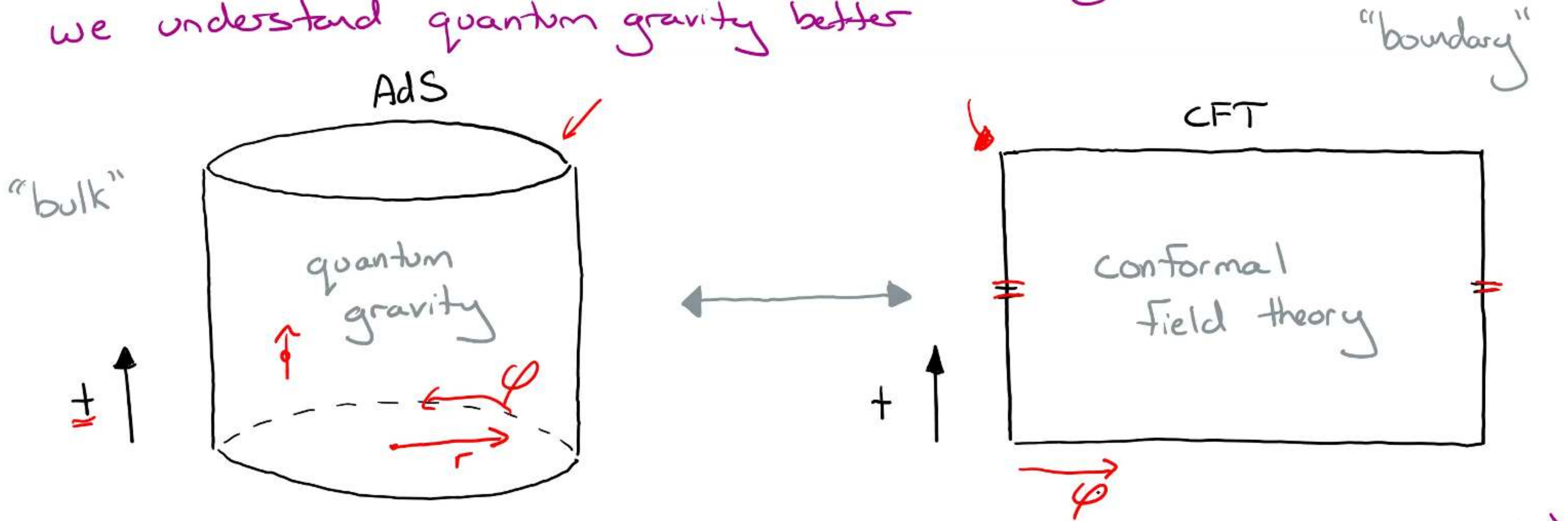


- Dynamical geometry (includes gravity)
- Includes quantum fields
- d + 1 dimensional

- Fixed geometry (no gravity)
- Includes quantum fields
- d dimensional

AdS/CFT

- To understand QI with gravity, go to a setting where we understand quantum gravity better

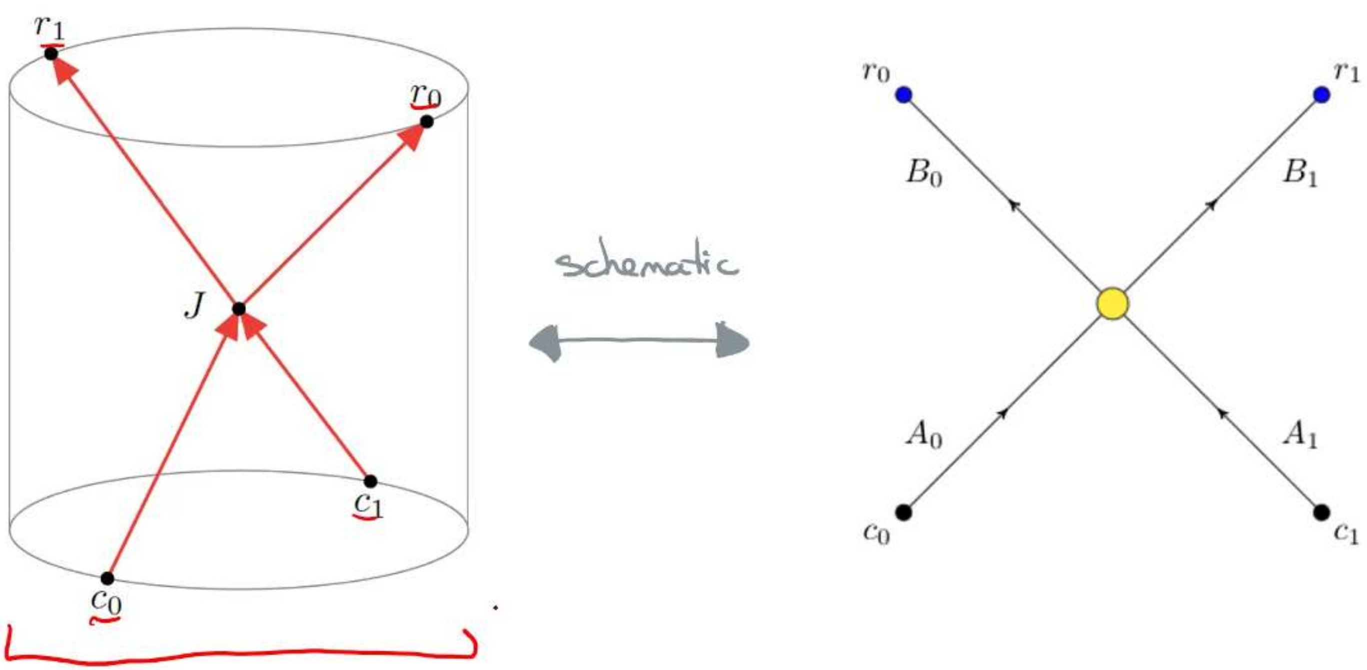


- Dynamical geometry (includes gravity)
- Includes quantum fields
- d + 1 dimensional

- Fixed geometry (no gravity)
- Includes quantum fields
- d dimensional

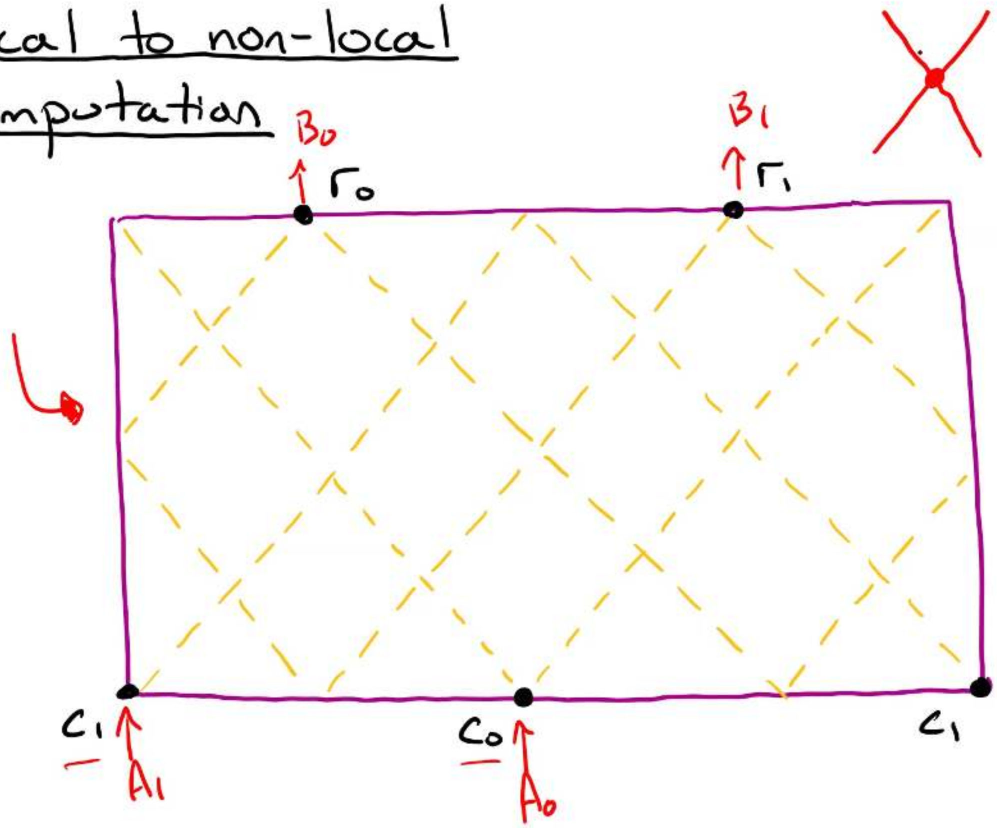
Local to non-local computation

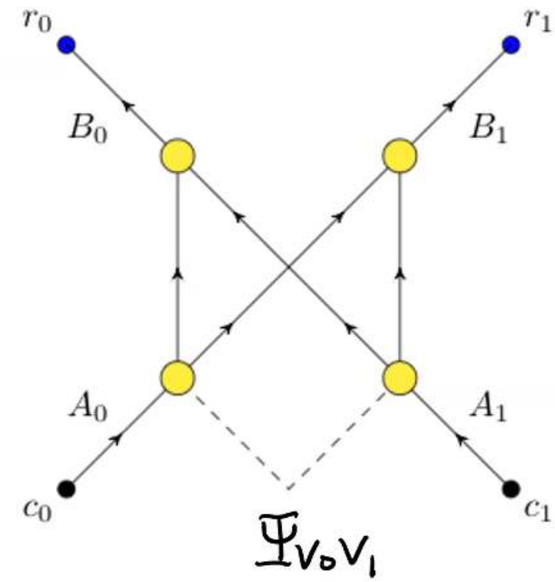
- Consider defining a scattering region in an AdS spacetime:



We'll ask: which computations can be performed inside J ?

Local to non-local computation



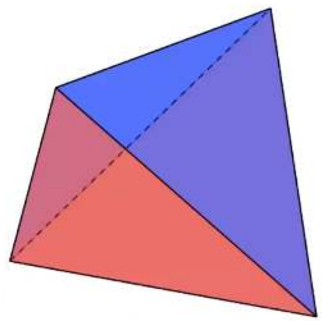


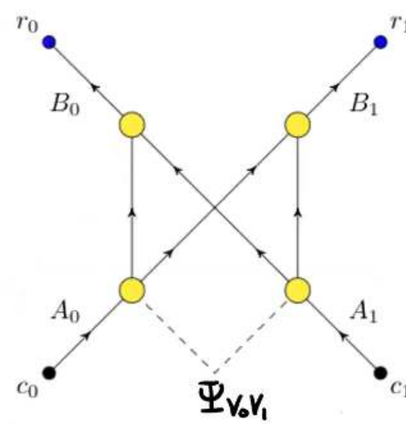
- Any computation which happens locally in the bulk is reproduced non-locally in the boundary

Entanglement in the boundary

- computable inside scattering region $\subseteq$ computable non-locally

scattering region

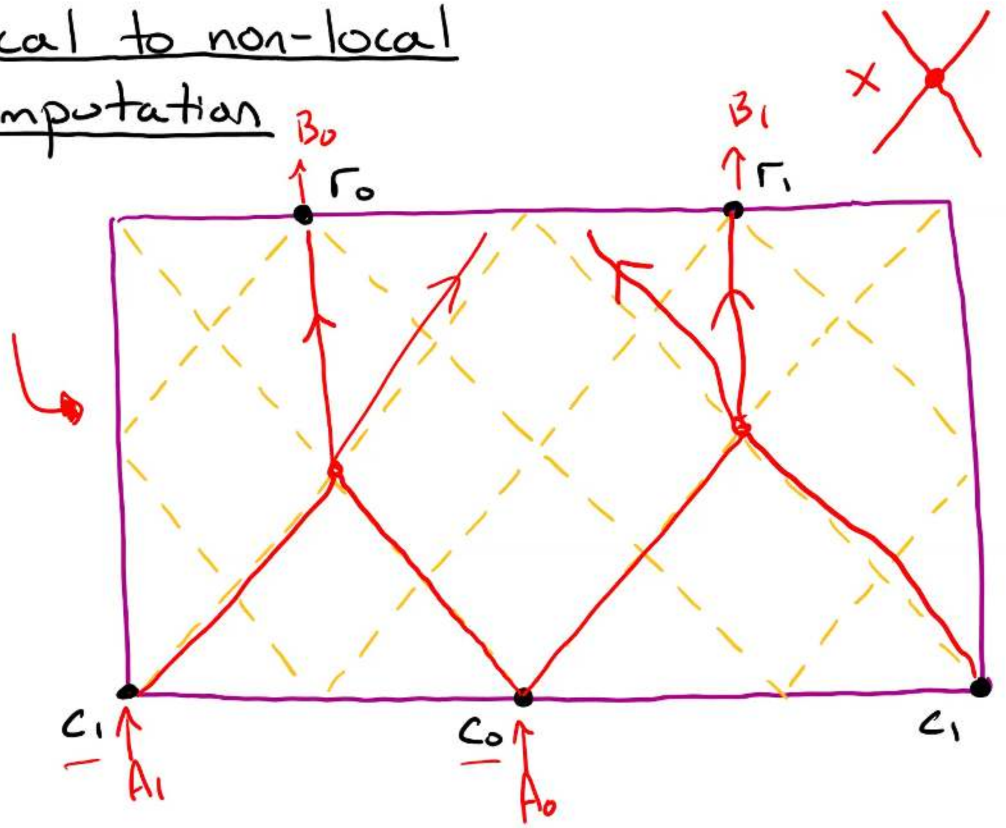


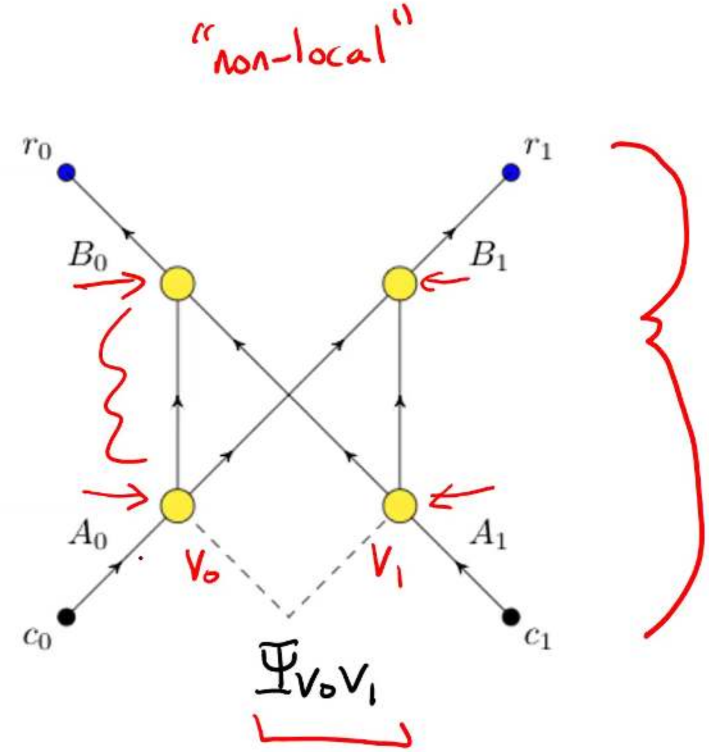


- More quantitatively,

computable inside a scattering region of area A_R	$\subseteq$	computable non-locally using resource state $\Psi_{V_0V_1}$ $I(V_0:V_1)_\Psi = \Theta(A_R)$

Local to non-local computation



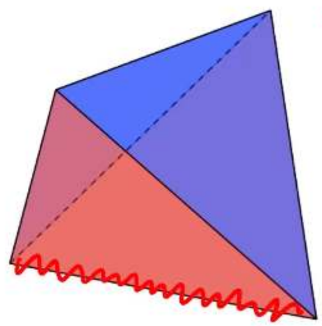


- Any computation which happens locally in the bulk is reproduced non-locally in the boundary

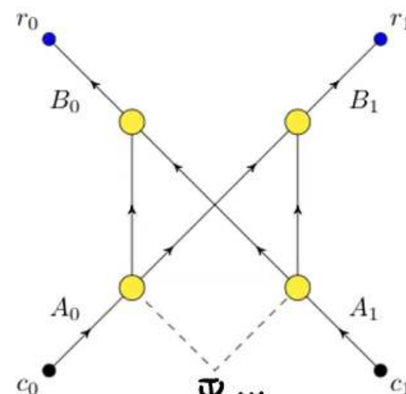
Entanglement in the boundary

- computable inside scattering region $\subseteq$ computable non-locally

scattering region



$\longleftrightarrow$



$\Psi_{V_0V_1}$

$J^+(c_0)$ . .

- More quantitatively,

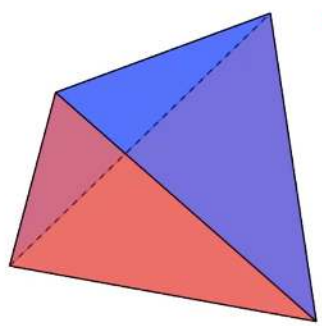
computable inside a scattering region of area A_R	$\subseteq$	computable non-locally using resource stat $\Psi_{V_0V_1}$ $I(V_0:V_1)_\Psi = \Theta(A_R)$

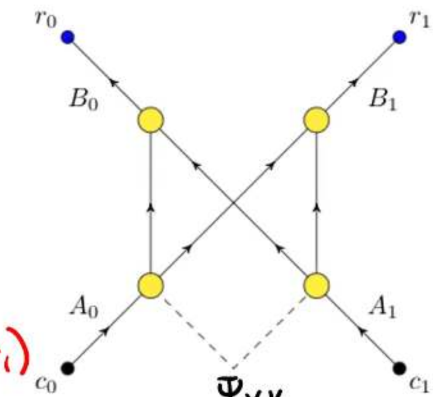
Entanglement in the boundary

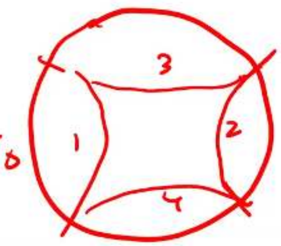
- computable inside scattering region $\subseteq$ computable non-locally

$A(1)+A(2)$
$-A(3)-A(4)$

scattering region







$R = \partial J^+(c_0) \cap \partial J^+(c_1) \cap J^-(r_0) \cap J^-(r_1)$

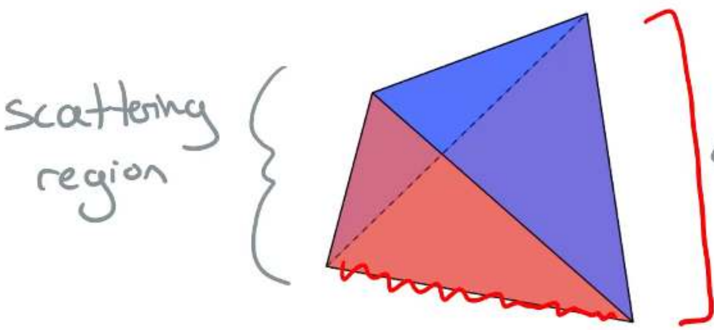
$\Psi_{V_0V_1}$

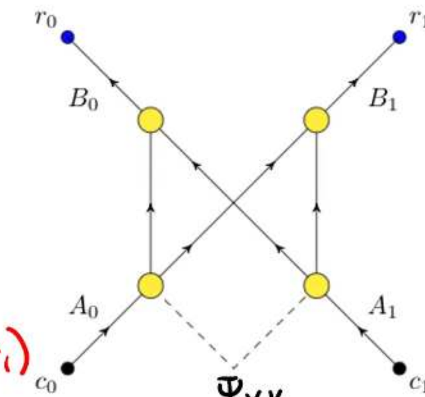
- More quantitatively,

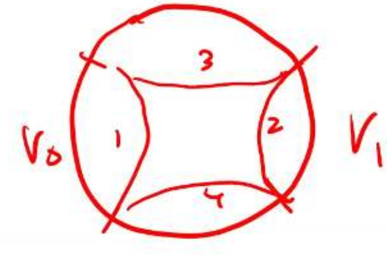
computable inside a scattering region of area A_R	$\subseteq$	computable non-locally using resource stat $\Psi_{V_0V_1}$ $I(V_0:V_1)_\Psi = \Theta(A_R)$

Entanglement in the boundary

- computable inside scattering region $\subseteq$ computable non-locally $\quad A_R \sim [A(1)+A(2)-A(3)-A(4)]$







$R = \partial J^+(c_0) \cap \partial J^+(c_1) \cap J^-(r_0) \cap J^-(r_1)$

$\Psi_{V_0V_1}$

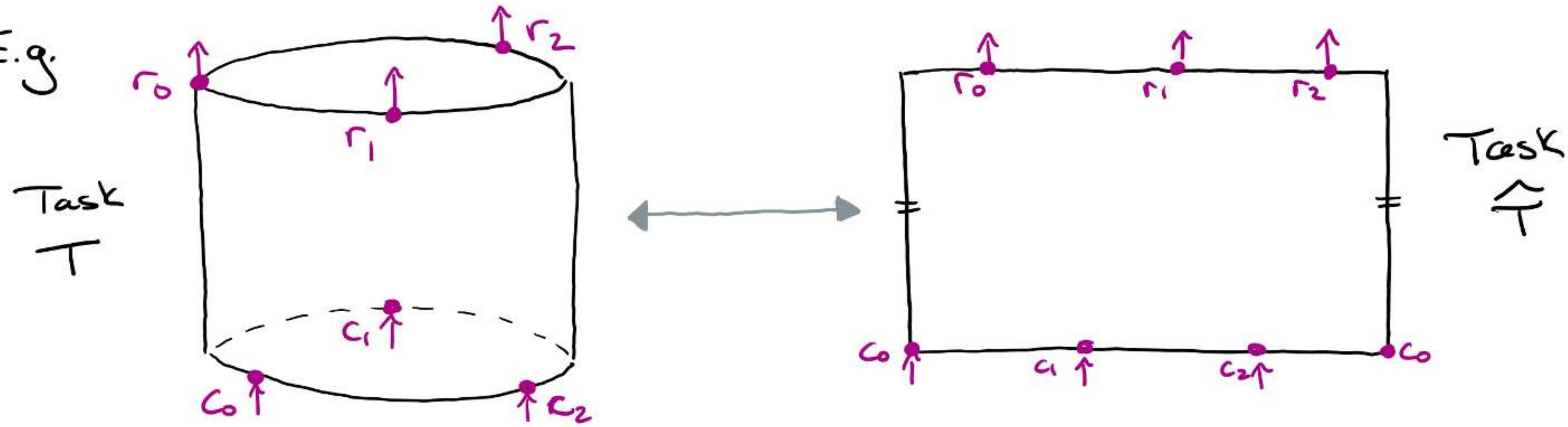
- More quantitatively,

computable inside a scattering region of area A_R	$\subseteq$	computable non-locally using resource stat $\Psi_{V_0V_1}$ $I(V_0:V_1)_\Psi = \Theta(A_R)$

Stepping back: bulk + boundary tasks

- More generally, we can relate bulk information processing tasks to boundary ones:

E.g.



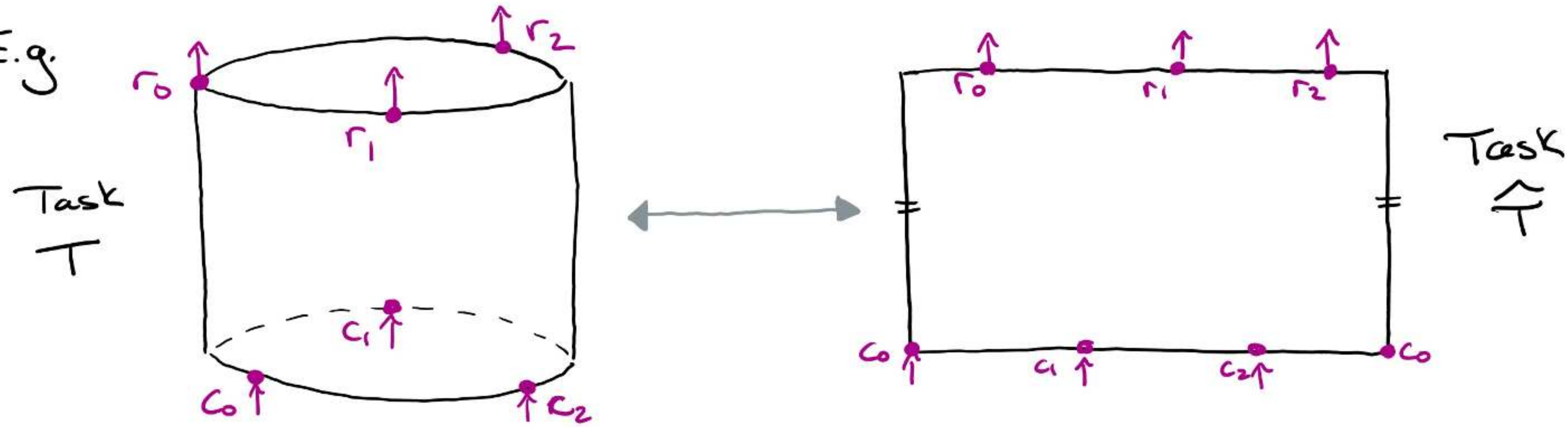
- Many other questions we can ask! (Focus on one for today)
- Can also use this perspective to study:

  gravity in AdS space, entanglement ~ geometry in AdS/CFT

Stepping back: bulk + boundary tasks

- More generally, we can relate bulk information processing tasks to boundary ones:

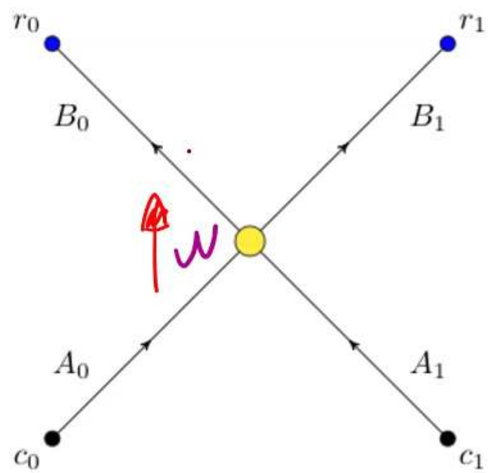
E.g.

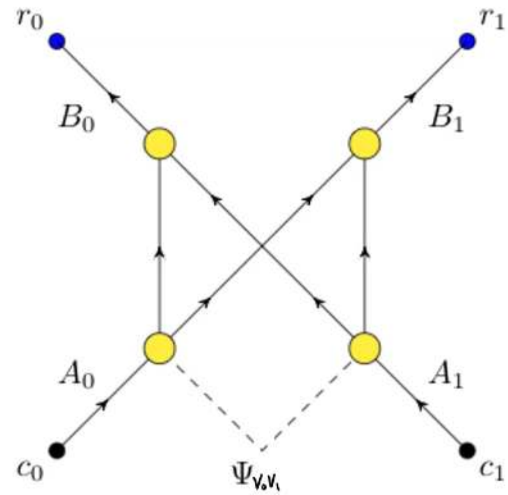


- Many other questions we can ask! (Focus on one for today)
- Can also use this perspective to study:
  gravity in AdS space, entanglement ~ geometry in AdS/CFT

Non-local quantum computation

Local





Non-local

Basic question:

$\boxed{\text{What property of } \mathcal{N} \text{ controls the entanglement needed to implement it non-locally?}}$

Complexity? - suggested by upper bounds
- would imply Lloyds idea

Does complexity control entanglement?

- One simple example: For Clifford unitaries on n qudits

Entanglement cost:

$\frac{1}{2} I(V_0 : V_1) \leq \underline{n} \, \underline{\log_2 K}$

Complexity:

$\underbrace{\mathrm{Mod}_K L}$.

measuring one qudit of output, note that

$L \subseteq \mathrm{Mod}_K L \subseteq P$

Idea: If complexity ~ entanglement, then <u>any</u> computation of complexity $\mathrm{Mod}_K L$ can be done non-locally with poly(n) entanglement

f-routing

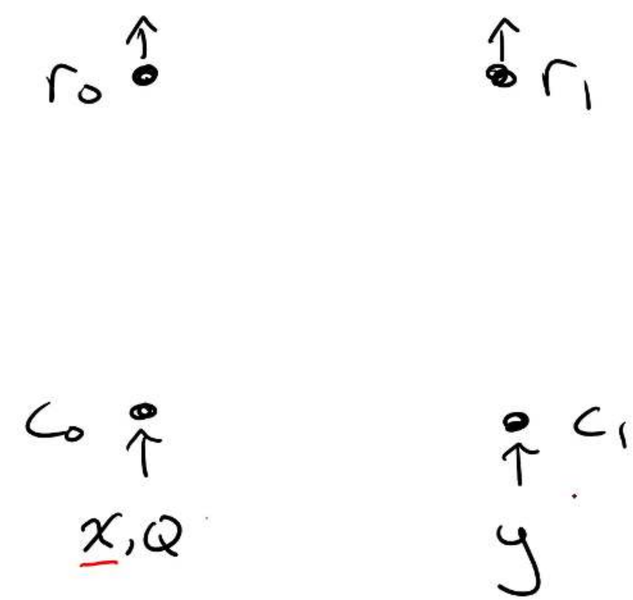
Test this idea using "f-routing":

- For a fixed $f : \{0,1\}^{2n} \to \{0,1\}$,

  Inputs: $x, y \in \{0,1\}^n$

  $Q \in \mathcal{H}_d$

  Output: bring Q to $r_{f(x,y)}$



- This is well studied because especially favourable for use in "position-based cryptography"

  ↳ Non-local computations = cheating strategies

Garden-hose + complexity (Buhrman et. al 2013)

- Most efficient known strategy is "garden-hose" protocol:

$$\#\,\text{EPR pairs used by garden-hose} \simeq 2^{\text{Memory}(f)}$$

$\leftarrow$ memory needed to compute f on a Turing machine

$$\boxed{\text{Entanglement cost is controlled by (space) complexity (in this protocol)}}$$

- Restricting to polynomial entanglement, can do $f \in L$

$\uparrow$ $O(\log n)$ space

Improvements to garden-hose?

- Can we do better than L? $L \not\subseteq Mod_k L$

  Based on complexity ~ entanglement, would expect yes.

- As well, from gravity perspective, if L is optimal, restricted to $\log(A_R)$ memory in scattering region of area A_R

- How might we do better?

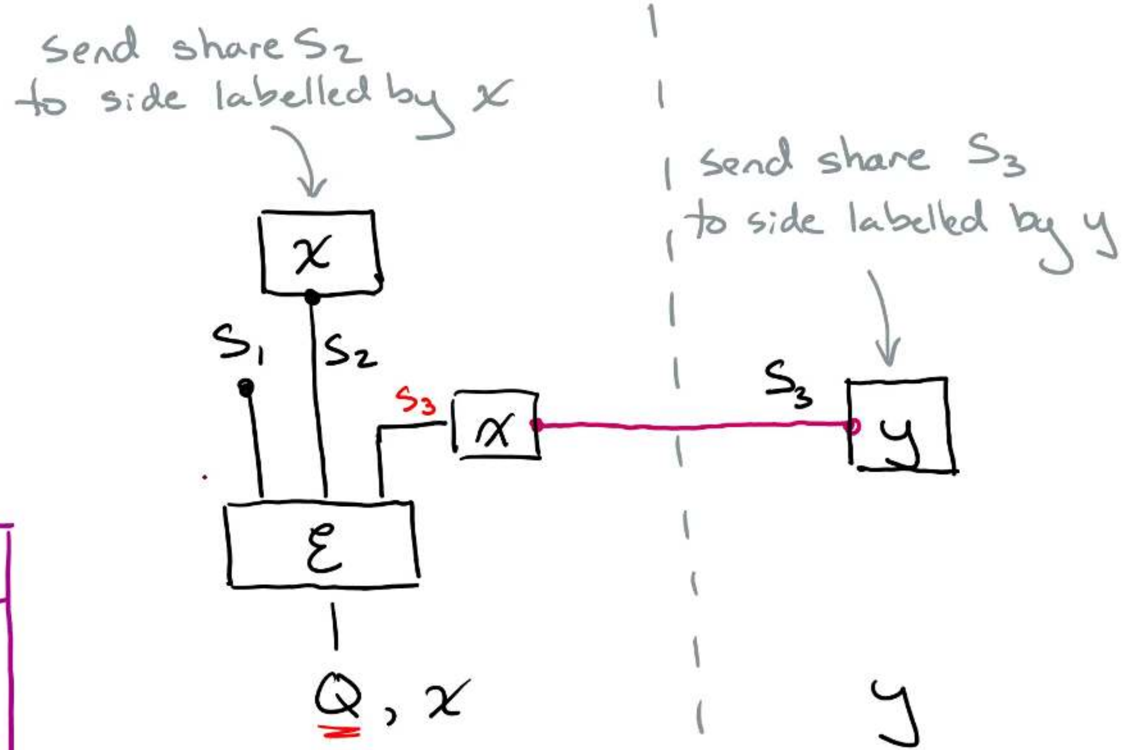
  ↳ AdS/CFT does NLQC and quantum error-correction plays important role there, lets try QECC?

Code-routing: by example

- Lets complete the routing task for

$$\boxed{f(x,y) = x \wedge y}$$

x	y	Left	Right
0	0	S_1, S_2, S_3	
0	1	S_1, S_2	S_3
1	0	$S_1, \quad , S_3$	S_2
1	1	$S_1,$	S_2, S_3



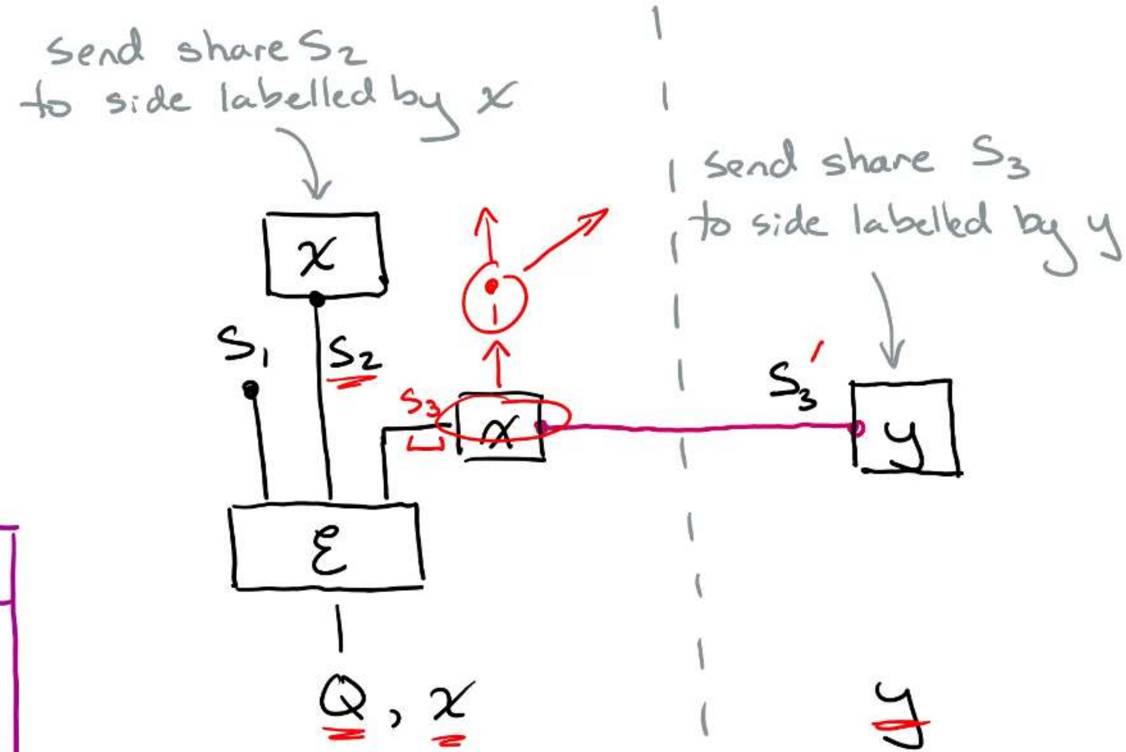
Any two shares recover Q, so this brings Q to side $x \wedge y$

Code-routing: by example

- Lets complete the routing task for

$$\boxed{f(x,y) = x \wedge y}$$

x	y	Left	Right
0	0	S_1, S_2, S_3	
0	1	S_1, S_2	S_3
1	0	$S_1, \ , S_3$	S_2
1	1	$S_1,$	S_2, S_3



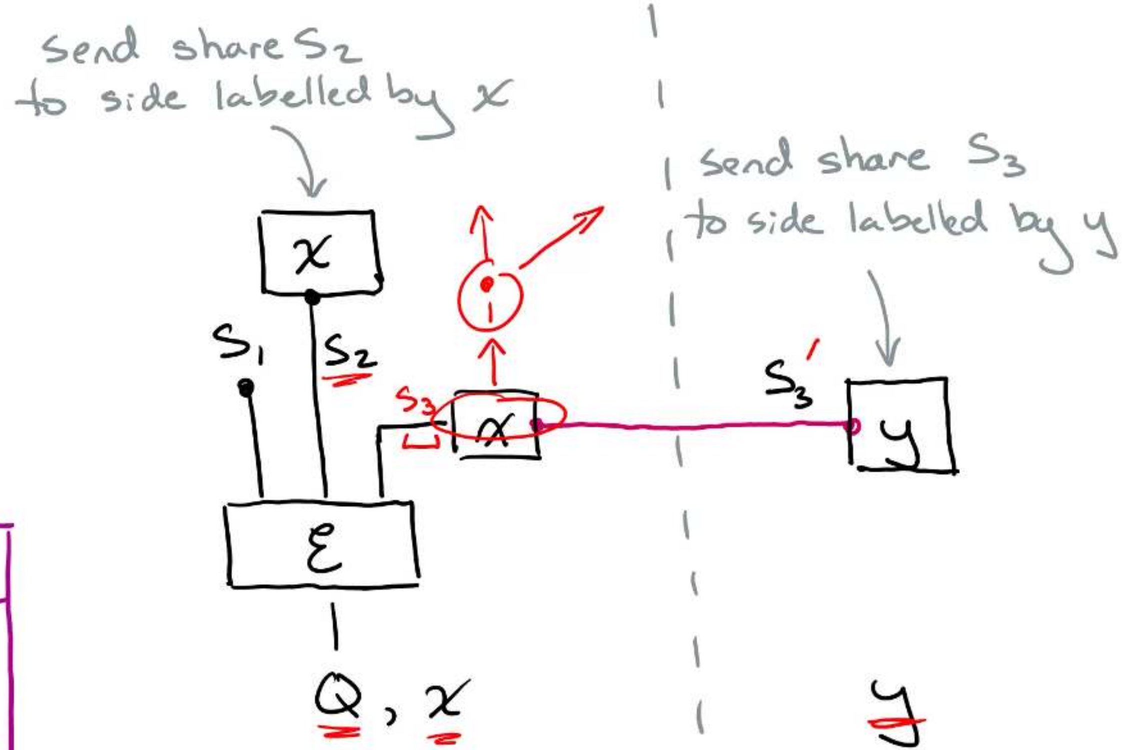
Any two shares recover Q,
so this brings Q to side $x \wedge y$

Code-routing: by example

- Lets complete the routing task for

$$\boxed{f(x,y) = x \wedge y}$$

x	y	Left	Right
0	0	S_1, S_2, S_3	
0	1	S_1, S_2	S_3
1	0	$S_1, \quad , S_3$	S_2
1	1	$S_1,$	S_2, S_3



Any two shares recover Q, so this brings Q to side $x \wedge y$

Quantum secret sharing

- Consider a quantum secret sharing scheme:

$$Q \xrightarrow[\mathcal{E}]{} \mathcal{S} = \{ S_1, S_2, S_3, \ldots S_n \}$$

- Label subsets $K(z) = \{ S_i : z_i = 1 \}$, define:

"Indicator function"

$$f_I(z) \equiv \begin{cases} 0 & \text{if learn nothing about } Q \text{ from } K(z) \\ 1 & \text{if can recover } Q \text{ from } K(z) \end{cases}$$

- Replace code with an arbitrary QSS:

$$\boxed{\text{entanglement to route on } f = f_I(z) \;\leq\; \text{"size" of QSS with indicator } f_I(z)}$$

Quantum secret sharing

- Consider a quantum secret sharing scheme:

$$Q \xrightarrow[\mathcal{E}]{} \mathcal{S} = \{ \underline{S_1, S_2, S_3, \dots S_n} \}$$

- Label subsets $\underline{K(z)} = \{ \underline{S_i} : \underline{z_i = 1} \}$, define:

$K(101) = \{S_1, S_3\}$

"Indicator function"

$$f_I(z) \equiv \begin{cases} \underline{0} & \text{if learn nothing about } Q \text{ from } \underline{K(z)} \\ 1 & \text{if can recover } Q \text{ from } K(z) \end{cases}$$

- Replace code with an arbitrary QSS:

$$\boxed{\begin{array}{ccc} \text{entanglement to} & \leq & \text{"size" of QSS} \\ \text{route on } f = f_I(z) & & \text{with indicator } f_I(z) \end{array}}$$

Complexity and QSS

- The best known QSS construction Smith (2000).

  ↳ Given indicator f_I, constructs QSS with size $O(SP(f_I))$

  size of a "span program" computing f

- Using this, and building on QSS based protocol:

$$E\text{-cost of } f \leq O(SP(f))$$

arbitrary function

- $\boxed{\text{Functions with poly sized span programs} = \text{Mod}_k L}$

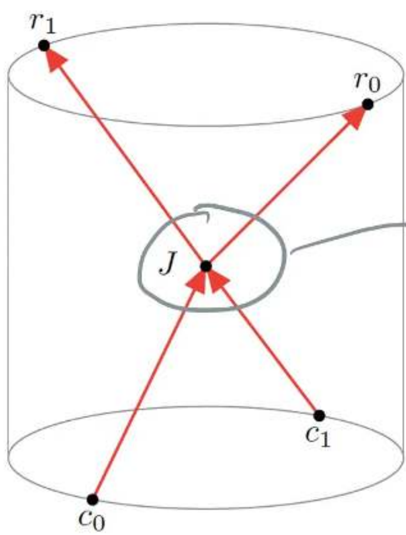
  → Aligns with expectation from complexity ~ entanglement

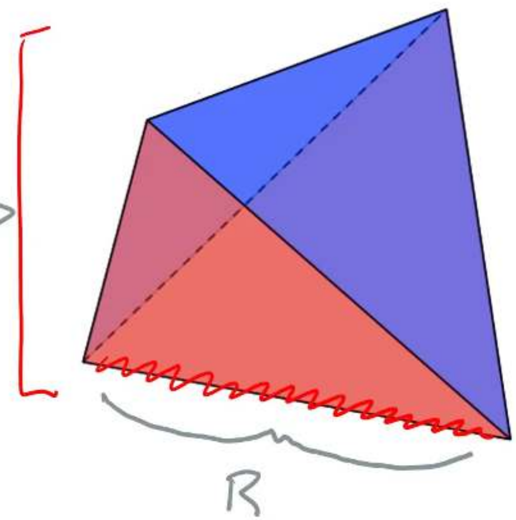
  → Does strictly better than garden-hose ($L \subseteq \text{Mod}_k L$)

Consequences of entanglement
lower bounds

Covariant entropy bound and scattering regions

- CEB gives an upper bound on how much entropy can pass into a region





CEB:

$$\boxed{\Delta S \leq \frac{\text{area}(R)}{4G_N}}$$

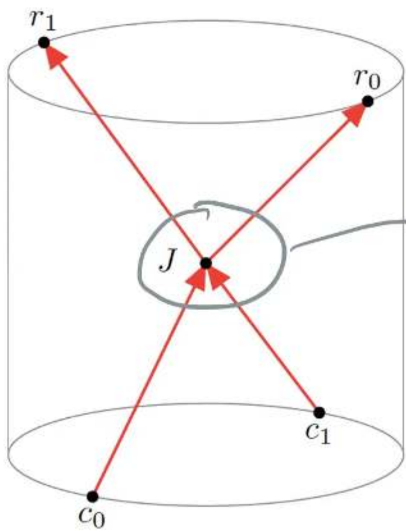
constraint on computation in scattering region

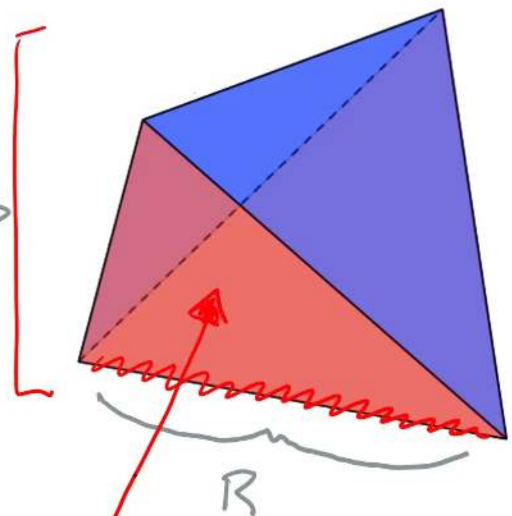
$$\boxed{\Delta S \leq \frac{1}{2} I(V_0 : V_1)}$$

- Using CEB + results from 1912.05649, 2101.08855

Covariant entropy bound and scattering regions

- CEB gives an upper bound on how much entropy can pass into a region





CEB:

$$\boxed{\Delta S \leq \frac{\text{area}(R)}{4G_N}}$$

constraint on computation in scattering region

- Using CEB + results from 1912.05649, 2101.08855

$$\boxed{\Delta S \leq \frac{1}{2} I(V_0 : V_1)}$$

Entanglement lower bounds

Can we recover this constraint from the boundary?

- Best known bound:

$$\frac{1}{2}\Delta S \leq \frac{1}{2} I(V_0 : V_1)$$

- Comes from a "monogamy-of-entanglement" game.

Comment: If there exists a "monogamy" game (or similar) where the optimal strategy is no better than guessing then recover $\Delta S \leq \frac{1}{2} I(V_0 : V_1)$

Entanglement lower bounds

$\boxed{\text{Any bound stronger than } \overset{=n}{\Delta S} \leq \frac{1}{2} I(V_1 : V_2) \text{ would be a novel constraint on QI in presence of gravity!}}$

- Exciting, but, keep in mind:

$$\left.\begin{array}{ll} ① & h(n) \leq E(f) \leq O(\text{size of span program}) \\ ② & E(f_I) \leq \text{size of QSS} \end{array}\right\} \text{consequences of code-routing}$$

Has only been limited success in proving explicit lower bounds on span programs / QSS, etc.

- Maybe a better idea:

$$\text{"complexity}(f)\text{"} \leq E(f)$$

Entanglement lower bounds

Any bound stronger than $\Delta S \leq \frac{1}{2} I(V_1 : V_2)$ would be a novel constraint on QI in presence of gravity!

- Exciting, but, keep in mind:

$$\left.\begin{array}{l} ① \; h(n) \leq E(f) \leq O(\text{size of span program}) \\ ② \qquad\quad E(f_I) \leq \text{size of QSS} \end{array}\right\} \text{consequences of code-routing}$$

Has only been limited success in proving explicit lower bounds on span programs / QSS, etc.

- Maybe a better idea:

$$\text{"complexity}(f)\text{"} \leq E(f)$$

Directions

NLQC

- Better lower bounds on entanglement?
  - Can we recover the CEB? (monogamy games)
  - Can we find new constraints on computation in the presence of gravity? (relationship to complexity theory)
- Improved protocols? Can we reach higher complexity with polynomial entanglement?

QI in QG

- What else can we ask about QI in presence of gravity?
  - what QI/complexity/crypto questions do they raise in the boundary?

Summary Thanks!

AdS/CFT

- QI in (holographic), gravitating spacetimes ⟷ QI without gravity } framework

↳ Computations in gravitating region ⟷ non-local quantum computation } application

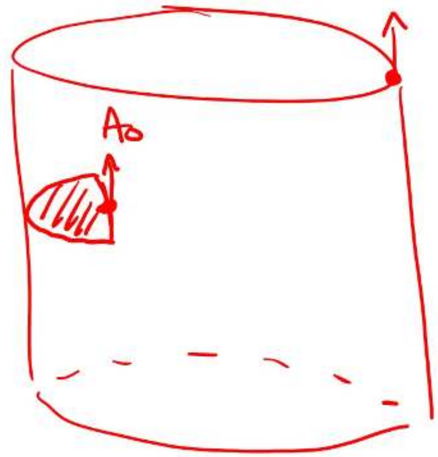
- Does complexity control entanglement?

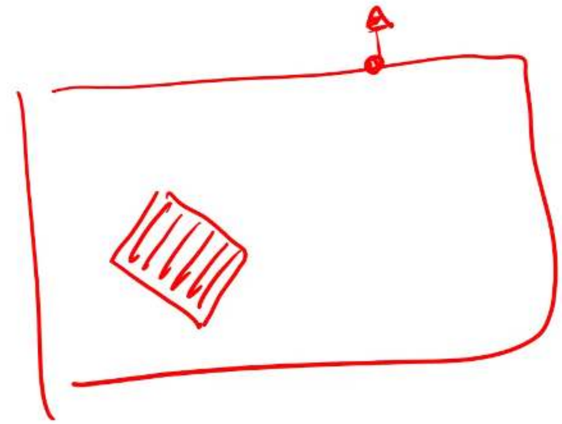
  ① Cliffords have linear entanglement ~ ModkL,

  ↳ Expect similar for other tasks

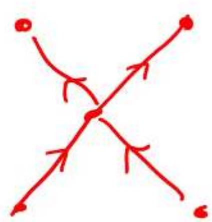
  ② For f-routing, get poly entanglement ~ ModkL by introducing code based protocol

1





blk



bnd