Constraining the doability of relativistic quantum tasks

Kfir Dolev

1Stanford Institute for Theoretical Physics, Stanford University, Palo Alto, California 94305, USA

We show within the framework of relativistic quantum tasks that the doability of any task is fully determined by a small subset of its parameters that we call its “coarse causal structure”, as well as the distributed computation it aims to accomplish. We do this by making rigorous the notion of a protocol using a structure known as a spacetime circuit, which describes how a computation is preformed across a region of spacetime. Using spacetime circuits we show that any protocol that can accomplish a given task can, without changing its doability, undergo significant geometric modifications such as changing the background spacetime and moving the location of input and output points, so long as the coarse causal structure of the task is maintained. Besides giving a powerful tool for determining the doability of a task, our results strengthen the no-go theorem for position based quantum cryptography to include arbitrary sending and receiving of signals by verifier agents outside the authentication region. They also serve as a consistency check for the holographic principle by showing that discrepancies between bulk and boundary causal structure can not cause a task to be doable in one but not the other.

I. INTRODUCTION

The framework of relativistic quantum tasks has recently produced results which are of interest to cryptography and holography. On the cryptographic side it was shown that unconditionally secure bit commitment protocols exist [6], and that a large class of secure position based cryptography protocols do not [3]. On the holographic side, by considering that tasks doable in the bulk must also be doable in the boundary, new bulk geometric relations were discovered [9].

In this paper we prove that, together with the distributed computation it aims to accomplish, the coarse causal structure of a task, i.e. whether or not there is a causal curve between any given input point and any given output point, fully determines the task’s doability, i.e. whether or not it is possible to accomplish. To do so we define precisely a notion of doability in terms of a structure known as a spacetime circuit. Heuristically, a spacetime circuit is a normal quantum circuit, but with wires taken literally as causal curves in spacetime, and wire ends taken as points in spacetime at which quantum systems are given as inputs or returned as outputs. A task will be called doable if there exists a spacetime circuit which accomplishes it. We show that any spacetime circuit accomplishing a task can be modified to only make use of the task’s coarse causal structure. This modified circuit can easily be adapted to any task differing from the original by placement of input and output points so long as the coarse causal structure is maintained. We stress that the existence of regions which can be signaled by multiple input points and can signal multiple output points, which we call the task’s fine causal structure, is irrelevant.

The paper is organized in the following way: section 2 reviews spacetime circuits. Section 3 reviews relativistic quantum tasks, provides a formal definition of their doability, and speculates on possible shortcomings of this definition. Section 4 introduces the main claim of this paper, that task doability is determined solely by a tasks coarse causal structure and aimed computation, and section 5 provides a proof of this claim. Section 6 discusses applications of our results to position based quantum cryptography and holography, and section 7 discusses the results and future work.

FIG. 1. A spacetime circuit. Blue, green, and red points represent input, gate, and output points respectively. The directed edges connecting the points represent the trajectory of physical systems. Dashed grey lines represent the relevant light cones of the points.
II. SPACETIME CIRCUITS

In this section we provide a definition of a spacetime circuit, a form of which has been introduced in [11], for later use in defining and analyzing the doability of a task. A spacetime circuit will consist of three types of points: “input”, “output”, and “gate” points, as well as links connecting either two causally connected points of different type or two causally connected gate points.

The input, output, and gate points represent points in space in which quantum channels act on quantum systems. Input points are given systems collectively in a variable state, while output points return other systems. The channels may additionally act on auxiliary systems. Each link represents a causal curve a system takes starting at the point at which it was output by some channel and ending at the point at which it is input to another.

We now give a formal definition of a spacetime circuit, followed by a detailed anthropomorphic description of its meaning.

Definition: For $p,q \in \mathcal{M}$, $p < q$ denotes that there exists a causal curve in $\mathcal{M}$ from $p$ to $q$. $\mathcal{I}^+(p)$ denotes all points in the causal future of $p$, and $\mathcal{I}^-(p)$ all points in its causal past.

Definition: A spacetime circuit $C$ is an 11-tuple $C = (\mathcal{M}, c, r, g, \mathcal{S}, \mathcal{O}, \mathcal{E}, \mathcal{R}, \rho_{\mathcal{R}}, \gamma, \{\Lambda_p\})$, where

- $\mathcal{M}$ is the spacetime on which the task is defined.
- $c = (c_1, \ldots, c_n)$ is a tuple of $n$ spacetime points, called “input” points.
- $r = (r_1, \ldots, r_m)$ is a tuple of $m$ spacetime points, called “output” points.
- $g = (g_1, \ldots, g_l)$ is a tuple of $l$ spacetime points, called “gate” points.
- $\gamma \subseteq \{\{p,q\}|(p,q) \in (c \times r) \cup (c \times g) \cup (g \times g) \cup (g \times r)\}$ and $p \neq q$ and $p < q$ and furthermore we require that for all $g_i$ there exist $c_j$ and $r_k$ such that the graph $G = (c \cup g \cup r, \gamma)$ contains a directed path from $c_j$ to $r_k$ containing $g_i$. The elements of $\gamma$ are referred to as “edges”.
- $\mathcal{I} = \{\Lambda_p|p \in c\}$ is a collection of $n$ quantum systems called “input” systems.
- $\mathcal{O} = \{\Lambda_p|p \in r\}$ is a collection of $m$ quantum systems called “output” systems.
- $\mathcal{E} = \{\Lambda_p|p \in \mathcal{E}\}$ is a collection of $|\gamma|$ quantum systems called “transit” systems.
- $\mathcal{R} = \{\Lambda_p|p \in c \cup g \cup r\}$ is a collection of $n + m + l$ quantum systems, one associated with each input, output, and gate point, called “ancilla” systems.

- $\rho_{\mathcal{R}}$ is a state on $\mathcal{R}$.
- $\{\Lambda_p\} = \{\Lambda_p|p \in c \cup g \cup r\}$ a collection of CPTP maps with $\Lambda_p$ taking states in $S_{in}(p)$ to states in $S_{out}(p)$, where we define

$$S_{in}(p) = \{E_{(q,p)}|(q,p) \in \gamma\} \cup \{I_i|p = c_i\} \cup \{R_p\}$$

$$S_{out}(p) = \{E_{(p,q)}|(p,q) \in \gamma\} \cup \{O_i|p = r_i\}$$

Intuitively, a spacetime circuit can be viewed as a blueprint of a set of actions committed by three groups of individuals, one serving Alice, one serving Bob, and one serving Ronak. The groups are collectively referred to as “agencies” and their members “agents”. Generally, Bob’s agency distributes and collects input and output systems, while Alice’s agency picks up the input systems, moves and interacts systems around spacetime, and returns the output systems to Bob. Ronak’s agency is in charge of holding on to systems which purify the state of the input system. We will now describe in detail the actions of the three agencies.

The actions of Bob’s and Ronak’s agencies are few. At sometime in the far past, Bob prepares the systems $\mathcal{S}R$ in some state, and gives $R$ to Ronak. He then sends, to each input point $c_i$, an agent carrying $I_{c_i}$, to be transferred over to an agent of Alice’s. Bob also sends an agent to each output point $r_j$, to wait for an agent of Alice’s to return the output system $O_{r_j}$. Bob’s and Ronak’s agents then congregate in the very far future where they can manipulate the single system $\mathcal{S}R$.

Alice’s agency does the bulk of the work. To each point $p$ in $c \cup r \cup g$, Alice sends an agent holding $R_p$ (the letter “R” stands for “resource”, as all auxiliary entanglement Alice wishes her agents to share must be prepared ahead of time via the state of $\mathcal{S}R$). Upon arrival, the agents act according to the type of point Alice sent them to. An agent sent to an input point $c_i$ picks up $I_{c_i}$ from an agent of Bob’s, applies the channel $\Lambda_{c_i}$ to $I_{c_i}R_{c_i}$, and for each output system $E_{(c_i,p)} \in S_{out}(c_i)$ of that channel, sends $E_{(c_i,p)}$ to $p$. An agent sent to a gate point $g_i$ collects all incoming quantum systems $S_{in}(g_i)$, applies the channel $\Lambda_{g_i}$ to $S_{in}(g_i)R_{g_i}$, and sends all $E_{(g_i,p)} \in S_{out}(g_i)$ to $p$. Finally, an agent sent to an output point $r_i$ collects all incoming quantum systems $S_{in}(r_i)$, applies the channel $\Lambda_{r_i}$ to $S_{in}(r_i)R_{r_i}$, and transfers the resulting system $O_{r_i}$ over to an agent of Bob’s.

From this process, a channel naturally emerges:

Definition: The effective channel $\mathcal{N}_C$ of a spacetime circuit $C$ is a CPTP map taking states of $\mathcal{S}R$ to states of $\mathcal{S}R$, with an input $|\psi\rangle_{\mathcal{S}R}$ mapped to whatever state $\mathcal{S}R$ is in after the above actions are taken by the three agencies.

---

1 The $R$ system is called the reference system, not to be confused with the resource systems. It is distinguished from the resource systems by neither being in script nor having a subscript.
agencies when Bob sets the initial state of $\mathcal{I}R$ to $|\psi\rangle_{\mathcal{I}R}$.

With these structures in place we can now define the doability of a relativistic quantum task.

III. RELATIVISTIC QUANTUM TASKS AND THEIR DOABILITY

In this section we give a definition of a relativistic quantum task and proceed to define its doability in terms of spacetime circuits.

A task differs from a spacetime circuit in that rather than blueprinting Alice’s actions, it specifies the state in which Alice is required to return the output systems, as a function of the state in which Bob set the input systems. Bob and Alice may agree ahead of time that Bob is required to select an input state from an agreed upon subset of all possible input states. Asking if a task is doable is asking if there exists a set of actions Alice can preform in order to achieve the required output when she is given a legitimate input.

Formally, we can define a relativistic quantum task as a list of input and output points, input and output systems, and a set of channels, usually defined as all possible channels which implement a specified map on a subset of allowed input states. A task is defined to be doable if there exists a spacetime circuit with the same input/output points and systems whose effective channel is one of those listed in the task.

Definition: A relativistic quantum task $T$ is a 6-tuple $T = (\mathcal{M}, c, r, \mathcal{J}, \mathcal{O}, \{N_{\mathcal{I}R \rightarrow \mathcal{O}R}\})$, where

- $\mathcal{M}$ is the spacetime on which the task is defined.
- $c = (c_1, \ldots, c_n)$ is a tuple of $n$ spacetime points, called “input” points.
- $r = (r_1, \ldots, r_m)$ is a tuple of $m$ spacetime points called “output” points.
- $\mathcal{J} = \{I_p | p \in c\}$ is a collection of $n$ quantum systems called “input” systems.
- $\mathcal{O} = \{O_p | p \in r\}$ is a collection of $m$ quantum systems called “output” systems.
- $\{N_{\mathcal{I}R \rightarrow \mathcal{O}R}\}$ is a set of quantum channels, each from states on $\mathcal{I}R$ to states on $\mathcal{O}R$, with $R$ some reference system.

Definition: Let $T = (\mathcal{M}, c, r, \mathcal{J}, \mathcal{O}, \{N_{\mathcal{I}R \rightarrow \mathcal{O}R}\})$ be a relativistic quantum task. We define $T$ to be doable if there exists a spacetime circuit $C = (\mathcal{M}, c, r, g, \mathcal{J}, \mathcal{O}, \mathcal{R}, \rho, \gamma, \{\Lambda_p\})$ such that $N_C \in \{N_{\mathcal{I}R \rightarrow \mathcal{O}R}\}$. For such a circuit $C$ we say that $C$ accomplishes $T$.

As an example, consider the summoning task depicted in figure 2 and a spacetime circuit accomplishing it depicted in figure 3.

Note that this definition of doability is only accurate within the unrealistic regime where systems are infinitely localized, internally quantum but spatially classical.

---

2 There are extensions to this definition usually dealing with additional requirements or limitations on Alice. Generalization of our work to such scenarios appears straightforward.
FIG. 3. A spacetime circuit accomplishing the example sum-
moning task. The gate points simply divert the information
in the right direction. Notice this circuit makes use of the fact
that the shaded region, i.e. $J^+(c_0) \cap J^+(c_1) \cap J^-(r_1) \cap J^-(r_2)$, is non-empty.

FIG. 4. A seemingly difficult summoning task. The dashed
grey lines indicate the trajectory of light rays, while the solid
red lines indicate causal connections. The naive circuit in
3 cannot be used here because $J^+(c_0) \cap J^+(c_1) \cap J^-(r_1) \cap J^-(r_2) = \emptyset$. However, since this task has the same coarse
causal structure as the one in figure 2 it must be doable, and
indeed this is shown in 4.

IV. A NEW TASK DOABILITY INVARIANCE

In this section we formally present the main claim of this paper: that the doability of a task depends only on its
coarse causal structure and the distributed computations
it aims to accomplish. We then use summoning as an
example where a seemingly difficult task can be shown
to be doable by finding a simpler task with the same
coarse causal structure. In the next section we provide

a proof of this claim.

Definition: Let $T = (M, c, r, \mathcal{I}, \mathcal{O}, \{\mathcal{N}_{\mathcal{I}}\})$ and $U = (M', c', r', \mathcal{I}, \mathcal{O}, \{\mathcal{N}_{\mathcal{I}}\})$ be quantum tasks
with $|c| = |c'| = n$ and $|r| = |r'| = m$ and with $M, M'$ not containing closed time like curves. Then if for all
$i \in \{1, \ldots, n\}$ and for all $j \in \{1, \ldots, m\}$ we have $c_i < r_j$ if
and only if $c'_i < r'_j$, then we say $T$ and $U$ have the same
coarse causal structure.

Main Theorem: Let $T$ and $U$ be tasks with the same
coarse causal structure. Then $T$ is doable if and only if
$U$ is doable.

As an example application of this theorem, consider the
seemingly difficult summoning task depicted in figure 4.

To what information is doability blind? As the above
example shows, tasks with the same coarse causal structure may still differ by existence of regions which are signalled by multiple input points and or can signal multiple output points. The existence of such regions is the only additional geometric information that could possibly have affected task doability, and it is this additional information we call the fine causal structure. Thus we can meaningfully say that doability is insensitive to coarse causal structure preserving changes to the fine causal structure.

V. PROOF OF INVARIANCE

In this section we prove the main claim of this paper, that doability of a task depends only on its coarse causal structure and its aimed distributed computation. We do so by showing that given a doable task and a spacetime circuit accomplishing it, a second spacetime circuit can be constructed which accomplishes all tasks with the same coarse causal structure. This construction will make heavy use of normal and port-based teleportation, and borrows many ideas originally used to solve fundamental questions in position based quantum cryptography [1, 3, 5].

First we review the function of normal teleportation and port-based teleportation, and then give an example of how they can be used to modify a task. We then develop a notation which simplifies protocol modification when we sometimes refer to the bits a, b as a “normal key”.

A. Normal teleportation

For brevity and clarity, we review here only the function, not the implementation, of normal teleportation. For details on implementation see [10]. Normal teleportation consists of three parties (not agencies), Alice, Bob, and Ronak. Alice and Ronak each hold a qubit, labeled A and R respectively, together in the state $|\psi\rangle_{AR}$. Meanwhile Alice and Bob share a Bell pair. Alice would like to transfer the quantum information in A over to a system B held by Bob so that the state of B and R is $|\psi\rangle_{BR}$. Alice and Bob can perform local operations without any communication which “consume” the Bell pair they share, after which Bob and Ronak hold the quantum state $X_B^a Z_B^b \otimes I_R |\psi\rangle_{BR}$ with a and b two random classical bits held by Alice. Notice that this can be done even if Alice and Bob are at spacelike separated points. The reason information does not travel outside the light cone is that the system B will look maximally mixed to Bob until he is given the bits a and b and undoes the X and Z operations.

If Bob would like to teleport the information over to a quantum system C held by another party, Charlie, he need not wait until he receives the classical bits a, b from Alice. He and Charlie can immediately preform local operations so that the final state on C and R is $X_C^a Z_C^b X_C^a Z_C^b \otimes I_R |\psi\rangle_{CR}$, where $a'$ and $b'$ are two classical bits held by Bob. This time Charlie requires classical information from both Bob and Alice in order to recover the state.

We can phrase the function of normal teleportation as follows: a quantum system at a spacetime point p is encrypted and then moved to a point q spacelike separated from p, with the encryption “key” available at p. Thus we sometimes refer to the bits a, b as a “normal key”.

B. Port-based teleportation

Once again we review here only the function, not the implementation, of port-based teleportation. For details on implementation see [5].

The aim of port-based teleportation is the same as that of normal teleportation, to transfer the contents of A over to B held by Bob in such a way that if AR starts out in a pure state, BR will be in that same state after the protocol. However, instead of Alice and Bob sharing a Bell pair, they each hold N systems, $A^x$ and $B^x$ with $x \in \{1, ..., N\}$, collectively in some fixed state. The following becomes exactly possible in the $N \to \infty$ limit. Alice can preform local operations acting on A and all $A^x$ together, after which she learns the value of some random integer $x^* \in \{1, ..., N\}$, and $B^{x^*} R$ is left in the state $|\psi\rangle_{BR}$. The reason information does not travel outside the light cone is that Bob does not know the value of $x^*$.

Once again, if Bob wants to send the information to a third party Charlie, he need not wait until he receives the value of $x^*$. There are two ways Bob may proceed: either individually port teleporting each $B^x$, or port teleporting them all together. We will be primarily interested in the latter. This results in Charlie holding $N^2$ systems, $C^{1,1}, C^{1,N}, C^{2,1}, ..., C^{x^*,1}, ..., C^{x^*,N}, ..., C^{N,N}$, and Bob holding an integer $y^* \in \{1, ..., N\}$, such that $C^{x^*,y^*}$ holds the information originally in A. This time, in order for Charlie to retrieve A, he needs to know both $x^*$ and $y^*$. Notice that if he posses either one of these he can throw away all but N systems.

We can once again phrase this procedure in cryptographic language. Again, we can view port-based teleportation as a quantum system at a spacetime point p being encrypted and then moved to a point q spacelike separated from
FIG. 5. Normal teleportation

$\psi_{AB}$

$|00\rangle + |11\rangle_{A'B'}$

FIG. 6. Port-based teleportation.

$\psi_{AB}$

$X_B^a \otimes I_R |\psi\rangle_{BR}$

$a, b \in \{0, 1\}$

$p$, with the encryption “key” available at $p$. We will sometimes refer to this as the “port key”. However, this time the key is an identity of a quantum system hiding among many others, rather than the identity of a recovery operation needed on a single system.

C. Example: using teleportation to modify a protocol

Consider the task depicted in figure 7. Naively, one might assume that completion of this task requires the region...

$P \equiv J^+(c_2) \cap J^+(c_2) \cap J^-(r_1) \cap J^-(r_2)$ to be non-empty, so that a gate point can be placed which takes in $I_1 I_2$ and spits out $O_1 O_2$, as depicted in figure 8. If this were true it would be possible to verify that a computation was preformed in the region $P$. Indeed, this was the original idea behind position based quantum cryptography. However, it turns out that when $P = \emptyset$, the task is still doable provided $c_1$ and $c_2$ share enough entanglement ahead of time, as we will now show by modifying...
FIG. 7. Position based quantum cryptography (PBQC) task. Alice is given quantum systems $I_1$ and $I_2$ at two separate points. She is required to apply the channel $N_{I_1I_2} \rightarrow O_1O_2$ to $I_1I_2$ and output each of the resulting systems, $O_1$ and $O_2$ at their designated output points.

Rather than immediately physically moving $I_1$ and $I_2$, Alice can instruct her agents (ahead of time) to do the following: first, the agent at $c_1$ normal teleports the information in $I_1$ to $c_2$. If the initial state on $I_1I_2$ was $\rho_{I_1I_2}$, the agent at $c_2$ now holds $\tilde{I}_1\tilde{I}_2$ in the state $X^aZ^b\rho_{I_1I_2}Z^bX^a$. Now the agent at $c_2$ port teleports $\tilde{I}_1\tilde{I}_2$ back to $c_1$, leaving the agent at $c_1$ holding $N$ bipartite systems, $I_1^1I_2^1,...,I_1^NI_2^N$ with $I_1^xI_2^x$ containing $X^aZ^b\rho_{I_1I_2}Z^bX^a$, and with only the agent at $c_2$ knowing the value of $x^*$. The agent at $c_1$ can now apply the teleportation decryption, as well as the channel $N$ to each of the $N$ systems, leaving the agent with $N$ bipartite systems $O_1^1O_2^1,...,O_1^NO_2^N$ with $O_1^xO_2^x$ in the state $N(\rho_{I_1I_2})$. He then sends, for all $x$, $O_1^x$ to $r_1$ and $O_2^x$ to $r_2$, while the agent at $c_2$ sends the value of $x^*$ to both $r_1$ and $r_2$. The agents at $r_1$ and $r_2$ can therefore correctly identify $O_1^{x^*}$ and $O_2^{x^*}$ respectively as the systems they should output and they do so, completing the protocol.

Note that the above protocol never made use of $P$ being non-empty. Instead, the need for $P \neq \emptyset$ is replaced by clever teleportation between the input points. Our work generalizes this result to all such intermediary channel applications, showing that for a task to be accomplished, computations need only ever be done in input and output points, provided enough entanglement is available.

D. Chaining multiple teleportations

As we have seen from the previous example, to modify a protocol it is useful to combine both normal and port-based teleportation. To be able to describe more sophisticated modifications, we need to develop language for when arbitrarily many of both of these teleportation types are done. We will also need to introduce a technique which will be essential when using them multiple times, which we call re-indexing teleportation.

To begin developing this language we note that we would like to avoid constantly introducing new names for quantum systems each time a teleportation step is needed. We will refer to the original quantum systems specified by a spacetime circuit with capital roman letters, i.e. $A, B, C, ...$, and we decorate these with additional notation to denote teleportation manipulations of these systems which occur when agent actions deviate from those that were meant to be performed in the
A key holds "reverse distributive". This means that if an agent remove any unwanted phases). The advantage of port-based teleportation is that operations on this information until the recipient gains knowledge of the keys to assemble it and all of the keys in order to remove the Pauli corrections. Thus $A[p_1]$ denotes a system which carries the information that should have been in $A$, encrypted by a key which is available at position $p_1$. If the agent at $p_2$ then teleports $A[p_1]$ to $p_3$ which in turn teleports it to $p_4$ and so on until $p_n$, then we say that the agent at $p_n$ holds $A[p_1, p_2, ..., p_{n-1}]$ and that any other agent $p_i$ holds $key(A)$. To unlock the information in $A[p_1, p_2, ..., p_{n-1}]$ locally, it will be necessary to assemble it and all of the keys in order to remove the Pauli encryptions in the opposite order they occurred (or in a different order, and then use knowledge of the keys to remove any unwanted phases).

The advantage of normal teleportation is that it is "reverse distributive". This means that if an agent holds $(A[q]) (B[q])$ then we could equally say he holds $(AB)[q]$. As we will see, this is not so for port based teleportation. The disadvantage of normal teleportation is that, since it places a Pauli encryption on the underlying information, it is not possible to preform arbitrary computations on this information until the recipient gains knowledge of the key.

### 2. Port based teleportation

If instead the teleportation from $p_1$ to $p_2$ was port-based, we say the agent at point $p_2$ holds systems $A[x_1]$ with $x_1$ running from 1 to $N$, and that the agent at point $p_1$ holds $x_1^*$, the value of the index which holds the true information sent. If the agent at $p_2$ then teleports all $N$ systems $A[x_1]$ to $p_3$, which then port teleports all $N^2$ systems to $p_4$, and so on until $p_n$, then we say that the agent at $p_n$ holds the $N^{n-1}$ systems $A[x_1,...,x_{n-1}]$ while any other agent at point $p_i$ holds $x_i^*$. To unlock the information in $A[x_1,...,x_{n-1}]$ locally it will be necessary to assemble it and all $x_i^*$ in order to know which of the many systems hold the true information. Notice that these encryptions can be removed in any order.

The advantage of port-based teleportation is that operations may be preformed on the data underneath its encryption. If an agent holds $A^x$, this means they holds $N$ systems one of which contains the information $A$ would have in the original circuit. If they preform a channel $N$ on all systems, they thus end up with $(N(A))^x$.

The disadvantage of port teleportation is that, unlike normal teleportation, it is not "reverse distributive", that is, if an agent holds $A^x B^y$ it is not possible to write this as $(AB)^z$ for some index $z$. This is because $(AB)^z$ implies that the $N$ copies of the $A$ systems and the $N$ copies of the $B$ systems come paired up, with the agent knowing that one of these pairs contains the information $AB$ would have in the original circuit. If the agent holds $A^x B^y$ no such pairing is possible without additional information.

### 3. Mixing teleportations

Let us consider a few examples in which different types of teleportation are done in succession. Consider the case of three agents situated at points $p_1, p_2$, and $p_3$, with $p_1$ initially holding $A$. Suppose $p_1$ normal teleports $A$ to $p_2$, which then port teleports it to $p_3$. We can describe this process visually via the following table.

| step | $p_1$ | $p_2$ | $p_3$ | action          |
|------|-------|-------|-------|----------------|
| 1    | $A$   | $p_1$ | $p_2$ | $A : p_1 \xrightarrow{NT} p_2$ |
| 2    | $key(A)$ | $A[p_1]$ | $p_2$ | $A : p_2 \xrightarrow{PT} p_3$ |
| 3    | $key(A)$ | $x^*$ | $A^x[p_1]$ |               |

TABLE I. A table describing a process of various teleportations chained together. The $p_i$ column denotes what information $p_i$ holds during that step of the process. We use the shorthand $A : p_1 \xrightarrow{NT}$ to denote that the agent at $p_1$ normal teleports $A$ to $p_2$. Similarly $A : p_1 \xrightarrow{PT}$ denotes the same but for port based teleportation.

In this case, in order to retrieve the original system $A$, assuming all the agents have come together, it is necessary to use $key(A)$ to remove the Pauli encryption from $A^x[p_1]$, and to identity the $x^{th}$ system as the correct one. This can either be done either by first having knowledge of $x^*$ thereby discarding all other $A^x$, and then applying $key(A)$ to the single system, or by first applying the key to all $A^x$ and then throwing away the other systems. In this sense the "port decryption" (using knowledge of $x^*$ to throw away extra systems) and the "normal decryption" (using knowledge of $key(A)$ to preform the Pauli corrections) can be applied independently and in either order in this case. For this reason, if, after step 3, $p_3$ port teleports $A^x[p_1]$ to $p_1$, the agent there can remove the normal encryption even though they do not know $x^*$. Things are slightly complicated when the two types of teleportation are done in the other order: In this case, even though the system at $p_3$, $A^x[p_2]$, is again encryption by both a normal and port teleportation, the port and normal decryptions can no longer be done independently in the following sense: suppose $A^x[p_2]$ is handed over to agent $p_1$, which uses their knowledge of $x^*$
to throw away all systems but $A^{x^*}[p_2]$, and then hands it over to the agent at $p_2$, but does not hand over $x^*$. The agent at $p_2$ can not retrieve $A$, because they do not know which of the $N$ keys they hold is the correct one. This subtlety is the reason we must introduce the technique we call “re-indexing” teleportation.

4. Re-indexing teleportation

In the proofs that follow the subtlety discussed above will manifest in variants of the following situation:

| step | $p_1$ | $p_2$ | action |
|------|-------|-------|--------|
| 1    | $x^*$ | $A^{x^*}[p_2]B$ key($A^{x^*}$) |        |

Suppose $p_1$ wants to teleport $A^{x^*}[p_2]B$ to $p_2$ so that $p_2$ may remove the normal encryption. Neither port based nor normal teleportation will do the job since $p_2$ will not know which of the keys to use.

To circumvent this issue we introduce the following “re-indexing” technique. $p_1$ and $p_2$ prepare ahead of time $N$ pairs of maximally entangled states between them, with each state having dimension large enough to port teleport $A^{x^*}$ and $B$ together. $p_1$ then port teleports $A^{x^*}[p_2]B$ across the $x^{i^{th}}$ pair. Then $p_2$ can apply key($A^{x^*}$) to each part of their end of the $x^{i^{th}}$ pair, and the decryption is done correctly. We notate this process as

| step | $p_1$ | $p_2$ | action |
|------|-------|-------|--------|
| 1    | $x^*$ | $A^{x^*}[p_2]B$ key($A^{x^*}$) |        |

We call this “re-indexing” because $A$ “regains” the $x$ index. Notice that this technique introduces a second index, as well as appends all indices being re-indexed to the other systems included in the teleportation. $p_2$ can now remove the normal encryption and preform arbitrary computations involving both $A$ and $B$.

See [5, E] for a realistic example in which the need for re-indexing appears.

E. Removing gate points from a circuit

We now prove a theorem which shows that given a circuit, a second circuit can be constructed which has the same effective channel as the first but which uses zero gate points. We later show that such a circuit accomplishes any task with the same coarse causal structure as the original.

To prove the theorem, we first define the “roots” of a gate point, which intuitively are all input points which may affect the contents of the systems entering the gate point. We then prove a lemma which shows that any gate point can be absorbed into its roots, and finally use this lemma to show that all gate points can be removed from a circuit.

![Diagram](image)

**FIG. 9.** Roots example. The roots of the gate point marked by a yellow circle are the five input points also marked by yellow circles. They are all the input points from which there is a directed path to the marked gate point. The edges participating in such directed paths are highlighted in yellow.

**Definition:** Let $C$ be a spacetime circuit. Let $G(C) = (\cup g \cup r, \gamma)$ be a graph and $p \in \cup g \cup r$. Let $Path?(q, p)$ denote the proposition “there exists a directed path from vertex $q$ to vertex $p$ in the graph $G(C)$”. Then we define the roots of $p$ as

$$\text{roots}(p) = \{ q \in c | Path?(q, p) \}$$

Figure 9 depicts an example of the roots of a gate point.

**Lemma:** (single gate removal lemma)

Let $C$ be a spacetime circuit. Consider a gate point
Suppose that every quantum system \( A \in S_{in}(g_i) \) is localized at the same point \( c_{z_0} \in \text{roots}(g_i) \), and is port encrypted as \( A^{x_1 \cdots \cdots x_k} \) with each port key \( x_i^* \) localized at some point \( c_{x_i} \in \text{roots}(g_i) \). Then given a sufficient amount of prearranged entanglement dispersed across \( \text{roots}(g_i) \), it is possible to preform local operations without any communication at the points \( \text{roots}(g_i) \) such that every system \( B \in S_{out}(g_i) \) is localized at the same point \( c_{y_0} \in \text{roots}(g_i) \) and encrypted as \( B^{y_1 \cdots \cdots y_k} \), i.e. \( (S_{out}(g_i))^{y_1 \cdots \cdots y_k} \) is localized to \( c_{y_0} \). Furthermore, each port key \( y_i^* \) is localized at some point in \( \text{roots}(g_i) \).

**Proof:** For each \( A^{x_1 \cdots \cdots x_k} \) with \( A \in S_{in}(g_i) \), normal teleport it point by point from \( c_{x_0} \) to \( c_{x_1} \) and so on until \( c_{x_k} \). At each point \( c_{x_i} \) use knowledge of the port key \( x_i^* \) to throw away all \( A^{x_1 \cdots \cdots x_i} \) with \( x_i \neq x_i^* \). Then normal teleport the system to a common point \( c_{y_0} \in \text{roots}(g_i) \) independent of \( A \). The result is \( A^{x_1 \cdots \cdots x_k} \) at \( c_{y_0} \), and key \( (A_s^{x_1 \cdots \cdots x_k})^{x_1 \cdots \cdots x_k} \) at \( c_{y_1} \) for \( l \geq 0 \). Once this has been done for all systems, pick a specific set of all nodes with edges pointing to \( g_k \) always pick a random gate point, move to another gate point by point to which only input points point is reached. By the single gate removal lemma, operations can be preformed at points in \( \text{roots}(g_i) \) such that the combined system \( (S_{out}(g_i))^{y_1 \cdots \cdots y_k} \) can be sent to \( c_{y_0} \) along with the port keys \( y_1^* \), \( \cdots \), \( y_k^* \) localized to \( c_{y_0} \). Then given a sufficient amount of prearranged entanglement dispersed across \( \text{roots}(g_i) \), it is possible to preform local operations without any communication at the points \( \text{roots}(g_i) \) such that every system \( B \in S_{out}(g_i) \) is localized at the same point \( c_{y_0} \in \text{roots}(g_i) \) and encrypted as \( B^{y_1 \cdots \cdots y_k} \), i.e. \( (S_{out}(g_i))^{y_1 \cdots \cdots y_k} \) is localized to \( c_{y_0} \). Furthermore, each port key \( y_i^* \) is localized at some point in \( \text{roots}(g_i) \).

Theorem: (total gate removal theorem)

Let \( C = (\mathcal{M}, c, r, g, S, \Theta, \Sigma, \mathcal{R}, \rho_{\mathcal{R}}, \gamma, \{\Lambda_p\}) \) be a spacetime circuit with \( \mathcal{M} \) not containing closed time like curves. Then there exists another spacetime circuit \( C' = (\mathcal{M}, c, r, \Theta, \mathcal{R}, \rho_{\mathcal{R}}, \gamma', \{\Lambda'_{p}\}) \) such that \( N_{\mathcal{C}} = N_{\mathcal{C'}} \).

**Proof:** Since \( \mathcal{M} \) contains no closed timelike curves, \( G(C) \) must be acyclic. Therefore if \( g \neq \mathcal{M} \), there exists a gate \( g_i \in g \) such that \( in(g_i) = \text{roots}(g_i) \), where \( in(g_i) \) is the set of all nodes with edges pointing to \( g_i \), as one can always pick a random gate point, move to another gate point pointing to it, and repeat the process until a gate point to which only input points point is reached. By the single gate removal lemma, operations can be preformed at points in \( \text{roots}(g_i) \) such that the combined system \( (S_{out}(g_i))^{y_1 \cdots \cdots y_k} \) can be sent to \( c_{y_0} \) along with the port keys \( y_1^* \), \( \cdots \), \( y_k^* \) localized to \( c_{y_0} \). Then given a sufficient amount of prearranged entanglement dispersed across \( \text{roots}(g_i) \), it is possible to preform local operations without any communication at the points \( \text{roots}(g_i) \) such that every system \( B \in S_{out}(g_i) \) is localized at the same point \( c_{y_0} \in \text{roots}(g_i) \) and encrypted as \( B^{y_1 \cdots \cdots y_k} \), i.e. \( (S_{out}(g_i))^{y_1 \cdots \cdots y_k} \) is localized to \( c_{y_0} \). Furthermore, each port key \( y_i^* \) is localized at some point in \( \text{roots}(g_i) \).

**Example:**

Given that the proof of the total gate removal theorem is somewhat technical, we provide, for the reader who wishes for greater clarity, a step by step example of the removal of multiple gates from a spacetime circuit. The circuit is shown in figure [10] and the gate removal protocol in table [II].

FIG. 10. Spacetime circuit used as an example in demonstration of the total gate removal theorem.
proof of main theorem

We are now prepared to prove the main result of this paper.

Main Theorem: Let $T$ and $U$ be tasks with the same coarse causal structure. Then $T$ is doable if and only if $U$ is doable.

Proof:

It is sufficient to show that if $T$ is doable and $T$ and $U$ have the same coarse causal structure, then $T$ is also doable. Let $T = (\mathcal{M}, c, r, \mathcal{I}, \mathcal{O}, \mathcal{F}, \mathcal{O}', \mathcal{R}, \rho_\mathcal{R}, \gamma, \{\Lambda_p\})$ be the circuit created by applying the total gate removal theorem to $\mathcal{C}$. Construct a third circuit $\mathcal{C}' = (\mathcal{M}', c', r', \mathcal{I}, \mathcal{O}, \mathcal{F}, \mathcal{O}', \mathcal{R}', \rho_\mathcal{R}', \gamma', \{\Lambda_p\})$. Since $T$ and $U$ have the same coarse causal structure, execution of this circuit is possible. But $\mathcal{C}' \in \{\mathcal{C}' | \mathcal{C}' \to R \} \subset \{\mathcal{C} \to \mathcal{R} \}$. Since $U$ is doable, $\mathcal{C}'$ is doable, as was to be shown.

VI. APPLICATIONS

A. Position Based Quantum Cryptography

The central question of position based quantum cryptography is, can an untrusted agency $P$ prove to another...
agency $V$ that one of $P$’s agents was in some spacetime region $\mathcal{R}$, without $V$ sending any agents into $\mathcal{R}$. Previous works have considered the case when $\mathcal{R}$ is one spatial sub-region of Minkowski space for some finite duration of time, i.e. $\mathcal{R} = R \times T \subset M^{d+1}$. In particular in [3] it was shown that position based quantum cryptography is not possible if it was shown that position based quantum cryptography is not possible if $V$ only places $n$ stationary agents $V_0, ..., V_n$ at a collection of spatial points $x_0, ..., x_n$ whose convex hull contains $\mathcal{R}$, the idea being that if the $V_i$’s send light signals which reach some point $y \in R$ together at time $t_0 \in T$, only an agent at $y$ at time $t_0$ could preform a computation involving information from all signals, while for all $i$ returning its output to $V_i$ at time $t_0 + |x_i - y|/c$. We now show that our results strengthen this no-go theorem to exclude any strategy involving $V$’s agents sending and receiving signals outside an authentication region which can be any sub-region of any spacetime containing no closed time-like curves. Suppose $V$ instructs his agents to publicly broadcast signals at some spacetime points $c_1, ..., c_n \notin \mathcal{R}$ and to pick up signals at some spacetime points $r_1, ..., r_m \notin \mathcal{R}$. $V$ hopes that he can choose these points, along with some channel $\mathcal{N}$, such that $\mathcal{N}$ could have only been applied to the outgoing signals if they were manipulated inside the region $\mathcal{R}$. In the language of this work, we can say that $V$ is attempting to give $P$ a relativistic quantum task with input and output points outside of $\mathcal{R}$ which can only be accomplished by a spacetime circuit with a gate point inside $\mathcal{R}$. However, by the total gate removal theorem, no such relativistic quantum task exists, and the efforts of $V$ are in vain.

B. Holography

The holographic principle, and in particular AdS/CFT, asserts that a physical theory on some bulk spacetime $M$ can be described entirely by another physical theory on its boundary, $\partial M$. For a task defined on $M$ with input and output points all in $\partial M$, we can define a “dual” task which differs only in that it is defined on $\partial M$ rather than $M$. Such bulk tasks are known as “asymptotic tasks”. It was recently noted in [9] that while if the conjectured duality of AdS/CFT is to stand then the doability of asymptotic tasks and their duals must be the same, the fine causal structure of an asymptotic task and its dual is not always the same. In particular it was shown that there exist configurations of the PBQC task shown in figure 7 with input and output points on the boundary of AdS for which the bulk has a non-empty $\mathcal{P}$ region, but the boundary does not. Thus on holographic grounds one may deduce that the existence of a non empty $\mathcal{P}$, and in fact any fine causal structure discrepancy between the bulk and boundary can not affect task doability. That we have explicitly shown this can be seen as a sanity check for holography.

VII. CONCLUSION

It has long been observed that entanglement can resolve otherwise insurmountable coordination issues [2]. Studying how the doability of tasks depends on the availability of entanglement is useful in developing a better understanding of its logistical power. Qualitatively, our results show that in a spacetime context, the effect of entanglement is to make irrelevant all of the “fine” causal details of the spacetime on which the task is defined. On a practical level, knowing the irrelevance of fine causal structure often greatly simplifies the determination of doability, as one may assume any fine causal structure consistent with the coarse causal structure of the task is present when attempting to construct a circuit, as exemplified by the seemingly difficult summoning task in figure 1 and the PBQC task with an empty $\mathcal{P}$ region. However, this is not always possible, and it remains to find an algorithmic way of determining the doability of an arbitrary task.

Though doability does not depend on the fine causal structure in the presence of unlimited entanglement, the amount of entanglement needed to remove all gate points from a circuit can easily become intractable when the construction we have provided is applied. Categorizing tasks by the precise entanglement cost of gate removal is a subject of future work. It is possible we may learn to construct efficient gate removal methods by studying the fine causal structure discrepancies between the bulk and boundary in AdS/CFT, and conversely we may learn about entanglement structure in AdS/CFT by knowing when entanglement must be present to deal with these discrepancies.

Finally, it is likely effects from quantum gravity such as limits on computational speed and complexity will have a non trivial impact on the doability of relativistic quantum tasks. We leave such an analysis to future work.

VIII. ACKNOWLEDGEMENTS

I thank Florian Speelman for pointing out an error in the original total gate removal theorem, which led to the introduction of re-indexing teleportation. I thank Alex May, Kianan Wan, Patrick Hayden, and Ayfer Ozgur for helpful conversations. I particularly thank Alex May for assisting in editing this paper, and Ayfer Ozgur for support and guidance. This work is supported by the Center for Science of Information (CSoI), an NSF Science and Technology Center, under grant agreement CCF-0939370. Lastly I thank the It From Qubit 2019 summer school, during which many ideas leading to this paper were first realized.

REFERENCES
[1] Salman Beigi and Robert Konig. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, sep 2011.

[2] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, Nov 2005.

[3] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, 2014.

[4] Patrick Hayden and Alex May. Summoning information in spacetime, or where and when can a qubit be? *Journal of Physics A: Mathematical and Theoretical*, 49(17):175304, 2016.

[5] Satoshi Ishizaka and Tohya Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Phys. Rev. Lett.*, 101:240501, Dec 2008.

[6] Adrian Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13(11):113015, 2011.

[7] Adrian Kent. Quantum tasks in minkowski space. *Classical and Quantum Gravity*, 29(22):224013, 2012.

[8] Adrian Kent, William J Munro, and Timothy P Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A*, 84(1):012326, 2011.

[9] Alex May. Quantum tasks in holography. *arXiv preprint arXiv:1902.06845*, 2019.

[10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[11] Dominique Unruh. Quantum position verification in the random oracle model. *IACR Cryptol. ePrint Arch.*, 2014:118, 2014.