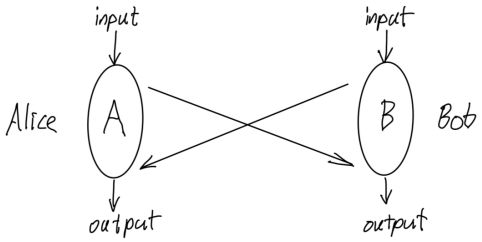
Nonlocal CNOT and f-CNOT problem

Richard Cleve

March 11, 2024

This project concerns a variant of the communication complexity framework, where two parties, Alice and Bob, each receive input data and they are each required to produce output data. The communication framework is the following. Alice is allowed to send a message to Bob, and Bob is allowed to send a message to Alice. *However*, this communication is with *crossed messages*, which means that Alice must send her message before receiving Bob's message and likewise Bob must send his message before receiving Alice's message. This is weaker than the



standard two-message communication complexity framework, where (say) Alice sends a message to Bob and then, after Bob has received the message from Alice, he sends a message to Alice.

This crossed-message communication structure can be enforced by timing the inputs and outputs so that the light cones permit a signal to travel from one party to the other, but do not permit a round of back-and-forth communication.

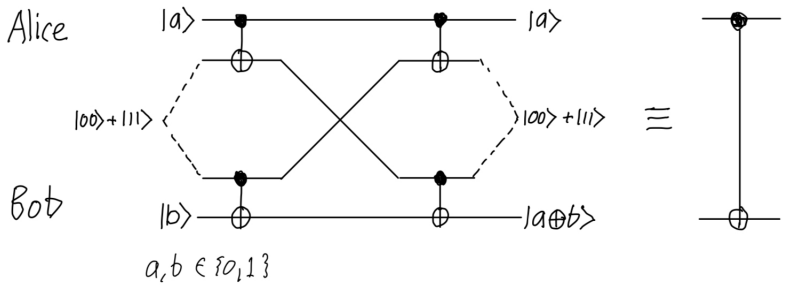
It turns out that, if the parties share a sufficient amount of entanglement then there are many tasks that can be performed in this model. One major question is: how much entanglement is necessary and sufficient?

What is the motivation for studying questions of this sort? In short, there are at least two communities who care. If there are lower bounds implying that a large amount of entanglement is required then it's a win for the "position-verification cryptography" community of researchers (because it implies that certain cryptographic protocols would require a lot of entanglement to break). On the other hand, if there are upper bounds showing that not too much entanglement is required then it's a win for some people in the "AdS/CFT" community (because it would mean that processes on the boundary can simulate processes in the bulk in a reasonable way, without an extravagant amount of entanglement).

1 An introductory example: nonlocal CNOT

Suppose that Alice and Bob receive input qubits Q and R (respectively) and they are required to apply a CNOT gate across their qubits, and then Alice and Bob output Q and R (respectively). Of course, this is trivial to solve if the communication can be back-and-forth: Alice can send qubit Q to Bob, who can apply the CNOT gate to (Q,R) and then send Q back to Alice. However, such back-and-forth communication is not allowed in the crossed-message model.

It is remarkable that, if Alice and Bob share a Bell state then can implement this CNOT gate in the crossed-message model. A method (loosely based on "gate teleportation") is illustrated in the following circuit diagram.

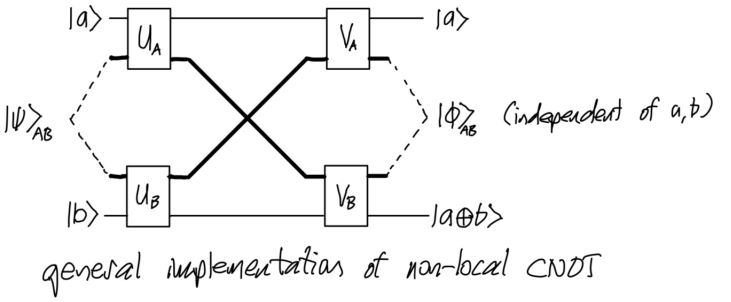


Although the diagram illustrates the case where Q and R are in a computational basis state $|ab\rangle$, the fact that the final state of the two middle qubits is independent of ab inplies that this is a correct implementation of the CNOT gate for arbitrary 2-qubit input states.

Rigidity conjecture

It is an easy exercise to check that the above protocol does not work correctly if the Bell state is replaced by an unentangled state, such as $|00\rangle$. I conjecture that a Bell state is *necessary* to implement a nonlocal CNOT and, moreover, that there is a *rigidity theorem*, to the effect that *any* implementation must essentially be of the above form.

To state my conjecture more technically, consider any implementation of the local CNOT in the crossed messages model. The form of any such a protocol is like this:



where the resource state $|\psi\rangle_{AB}$ is some bipartite state, and the final state of the resource registers $|\phi\rangle_{AB}$ does not depended on ab (which is a necessary condition to implement a CNOT gate). Then the conjecture can be stated as follows.

Conjecture 1. *There exist local isometries to Alice and Bob's systems that put the resource state into the form*

$$|\psi\rangle_{AB} = \big(|00\rangle_{AB} + |11\rangle_{AB}\big) \otimes |\psi'\rangle_{AB} \tag{1}$$

and the local operations into the form

$$U_A = \mathsf{CNOT} \otimes U'_A \tag{2}$$
$$U_B = \mathsf{CNOT} \otimes U'_B \tag{3}$$
$$V_A = \mathsf{CNOT} \otimes V'_A \tag{4}$$
$$V_B = \mathsf{CNOT} \otimes V'_B. \tag{5}$$

In other words, the conjecture says that, lurking within any protocol for the nonlocal CNOT, is the simple protocol at the beginning of this section (possibly obscured by additional qubits and unitary operations on them that are irrelevant to the protocol).

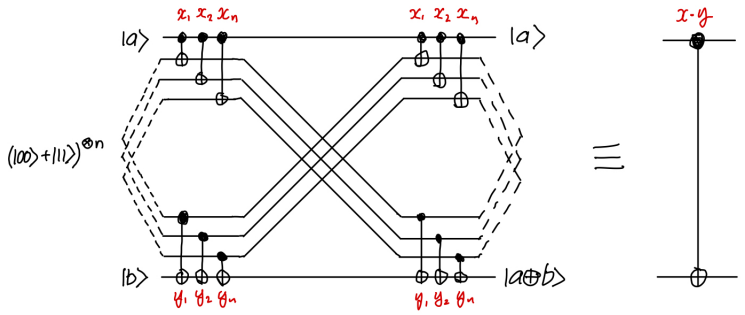
I am pursuing an approach to prove this and am cautiously optimistic that it will succeed. But, without a proof, I don't know for sure. If, instead of a proof, I find a counterexample then that might provide me with insight that helps me make a course-correction in the investigation.

2 The more general f-CNOT problem

The nonlocal CNOT problem is an inroad into a larger problem, the f-CNOT problem, which is defined for any $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ as follows. Alice and Bob receive as input: classical inputs $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ (respectively), as well as qubits Q and R (respectively), and their goal is to simulate the following (nonlocal) operation on their respective qubits:

$$\begin{cases} \mathsf{CNOT} \text{ gate} & \text{if } f(x,y) = 1 \\ \text{identity op} & \text{if } f(x,y) = 0. \end{cases} \tag{6}$$

Here's how to implement f-CNOT for the inner product function $f(x,y) = \sum_{k=1}^{n} x_k y_k \bmod 2$ using n Bell states of entanglement (where a gate labelled by a classical bit means that the gate in applied if and only if the classical bit is 1):



My conjecture is that this is optimal in entanglement usage (i.e., n Bell states are necessary to accomplish this) and that there is a rigidity result of a similar flavor similar to that of Conjecture 1, to the effect that *any* method for f-CNOT is effectively of the above form. I'm less confident about whether this is true (and proving it involves challenges beyond the methodology that I envisage for Conjecture 1), but it is a goal that I am striving for.

Further questions

Robust rigidity

So far, I've only mentioned the *exact* case, where the CNOT must be implemented with fidelity 1. However, I'm also interested in a *robust* version of these rigidity results, which informally would go something like this: Let $\epsilon > 0$ and $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be the inner product function. Then (the conjecture is) any implementation of f-CNOT *within fidelity* $1 - \epsilon$ is, up to local isometries, *approximately* of the form of that of figure on page 3 with respect to some distance measure $\delta > 0$, where δ is a function of ϵ that approaches 0 as ϵ approaches 0.

I view the investigation of rigidity for the exact case as a stepping stone towards a robust rigidity result.

Other functions than inner product

What about f-CNOT for other functions than inner product?

Using standard techniques in position-verification involving teleportation and generalizations of the the so-called "garden hose" methodology, it is straightforward to show that, for any $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ computable in non-deterministic log-space, it is possible to solve f-CNOT with entanglement polynomial in n. But, for arbitrary polynomial-time computable functions, the best known entanglement upper bound is exponential in n.

It would be good to get a better understanding of whether there are new tricks that enable f-CNOT for all poly-time computable functions with polynomial entanglement; or to provide evidence to the contrary.

Connections to other problems in the crossed-message model

f-CNOT can be regarded as a variant of more commonly considered problems like f-routing and f-BB84. There are some similarities among the known implementations among these problems that enable one implementation to be adapted to work for another. These similarities fall short of formal *reductions* between these problems (though it might be possible to prove that such reductions exist).

Why f-CNOT?

Why do I want focus my attention on f-CNOT instead of f-routing and f-BB84? The answer is that I see structural properties in f-CNOT that appear to make it more amenable to analysis than the other problems. In particular, for Conjecture 1, I can show that the structure of the messages in the bottom figure on page 2 is that of a certain kind of secret-sharing scheme, which I think can only be implemented in one way.