Oblivious Transfer, Non-Local Boxes, and Quantum Channels

Nicolas Gisin[*] Sandu Popescu[†‡] Valerio Scarani[§] Stefan Wolf [¶] Jürg Wullschleger[||]
[*]Group of Applied Physics, University of Geneva, 10, rue de l'École-de-Médecine, CH-1211 Genève 4, Switzerland.
E-mail: Nicolas.Gisin@physics.unige.ch
[†]H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, U.K.
[‡]Hewlett-Packard Laboratories, Stoke Gifford, Bristol BS12 6QZ, U.K.
E-mail: S.Popescu@bristol.ac.uk
[§]Centre for Quantum Technologies, National University of Singapore, S13, 2 Science Drive 3, Singapore 117542
E-mail: valerio@quantumlah.org
[¶]Computer Science Department, ETH Zürich, ETH Zentrum, CH-8092 Zürich, Switzerland.
E-mail: wolf@inf.ethz.ch
[||]Department of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, U.K.
E-mail: j.wullschleger@bristol.ac.uk

***Abstract*— *Oblivious transfer* (or *OT* for short) is of paramount importance in cryptography or, more precisely, two- and multi-party computation. In *one-out-of-two chosen OT*, a sender inputs two bits, one of which the receiver can choose to read; the sender does not learn which, and the receiver gets no additional information. It has been shown that oblivious transfer is cryptographically equivalent to a *non-local box (NLB)*. (This fact led to the insight that OT is essentially a *symmetric* primitive.) In this note, we study OT as a *communication* primitive, and show that it is the idealized classical analog to a *quantum-bit channel (QC)* in very much the same sense as an NLB is of an EPR pair: With OT, the channel's "classical" behavior can be obtained perfectly, whereas a QC allows for approximating OT with probability roughly 85%, while 75% is the classical limit.**

I. Introduction

A. Quantum Entanglement and Non-Locality

One of the most interesting and surprising consequences of the laws of quantum physics is the phenomenon of *entanglement*. In 1935, Einstein, Podolsky, and Rosen [10] initiated a discussion on its non-local behavior. Let us consider, for instance, the following, *maximally entangled* state, called *singlet* or, alternatively, *EPR* or *Bell state*:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \ . \tag{1}$$

The state $|\psi^-\rangle$ has the property that when the two qubits are measured in the same basis, the measurements lead to perfectly anti-correlated results. When the bases enclose an angle of φ, the probability of opposite results is $\cos^2\varphi$. This behavior is observed even if the two measurement events are spatially separated.

The message of [10] was that quantum physics was incomplete in the sense that it should be augmented by certain *hidden parameters* pre-determining the results of measurements. However, it was shown later by Bell [2] that such hidden-parameter models fail to explain quantum-physical behavior in general: The measurement results are random, and the randomness is generated at the time of the measurement and not beforehand. Other, related results had been obtained by von Neumann [19], Gleason [11], Specker [16], Jauch and Piron [12], and Kochen and Specker [13].

The behavior of a bipartite quantum state under measurements can be described by a conditional probability distribution $P_{AB|XY}$—also called two-party information-theoretic primitive—where X and Y denote the chosen bases (settings) and A and B the corresponding outcomes (see Figure 1).

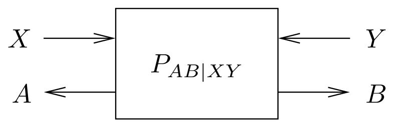

Fig. 1. A two-party information-theoretic primitive.

Clauser, Horne, Shimony, and Holt [7] were the first to recognize that there exist pairs of measurement bases such that the resulting behavior of $|\psi^-\rangle$ is not local, i.e., cannot be explained by shared classical information (see Figure 2). They showed that a certain inequality — now called *CHSH Bell inequality* — cannot be violated by any local system, but *is* violated when an EPR pair is measured.

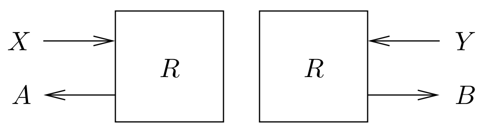

Fig. 2. A local system.

The behavior of $|\psi^-\rangle$ is, hence, *non-local*. It is important to note that non-local behavior, although explainable classically only by communication, does *not* allow for signaling. In order to understand non-locality and its consequences better, Popescu and Rohrlich [14] have introduced a "non-locality machine," called *non-local box* or NLB for short.

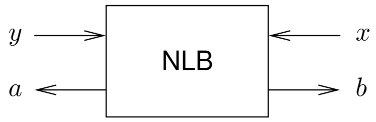

Fig. 3. The non-local box.

The behavior of NLB is inspired by the one of $|\psi^-\rangle$, but it is "more non-local" than the one of any quantum state. The (binary) inputs and outputs of NLB are (X, Y) and (A, B), respectively, and A and B are random bits satisfying

$$\begin{aligned} \text{Prob}[A = B \mid (X,Y) \neq (1,1)] &= 1 \ , \\ \text{Prob}[A = B \mid (X,Y) = (1,1)] &= 0 \ . \end{aligned}$$

In other words, A and B satisfy $A \oplus B = X \cdot Y$. Furthermore, from each parties point of view, A and B must be completely random: For all $a, b, x, y \in \{0, 1\}$, we require that

$$\begin{aligned} \text{Prob}[A = a \mid X = x] &= 1/2 \ , \\ \text{Prob}[B = b \mid Y = y] &= 1/2 \ . \end{aligned}$$

Therefore, NLB is *no-signaling*, as it does not allow for the transmission of any information.

We can now understand Bell's theorem in an intuitive way: The *CHSH Bell inequality* is simply an upper bound on the success probability of simulating NLB.

Let the inputs to NLB be chosen at random. Let us first look at the classical simulation of NLB. It is easy to see that a randomization of the strategies does not improve the probability of a correct output. Therefore, both A and B just have two values—one for input 0 and one for input 1—that they will output. Since there is always a pair of inputs such that the output of the two players is wrong, they can achieve an accuracy of at most 0.75. If the players have access to an EPR state $|\psi^-\rangle$, they can carry out measurements in bases that are rotated with respect to each other by the angle of $\pi/8$, and get an accuracy of

$$\cos^2\left(\frac{\pi}{8}\right) \approx 0.85 \ . \tag{2}$$

Furthermore, it has been shown that one call to NLB allows for *perfectly* simulating the joint behavior of a singlet state under arbitrary von Neumann measurements [6]. It is, therefore, fair to say that NLB is an idealized classical analog of a Bell state.

B. Oblivious Transfer

Oblivious transfer, introduced by Wiesner [20] under the name of "multiplexing" and by Rabin [15], is a primitive of paramount importance in cryptography, in particular two- and multi-party computation. In *chosen 1-out-of-2 oblivious transfer* or OT for short, one party, called the *sender*, has two binary inputs b_0 and b_1, whereas the other party, the *receiver*,

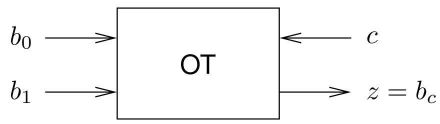

Fig. 4. Chosen 1-out-of-2 oblivious transfer.

inputs a *choice bit* c. The latter then learns b_c but no additional information, while the sender remains ignorant about c.

OT has been shown universal for multi-party computation, i.e., *any* secure computation can be carried out if OT is available. An example is *secure function evaluation*, which is an important special case of multi-party computation; here, a number of players want to secretly and correctly evaluate a function to which each player holds an input. "Secretly" means that no (unnecessary) information about the players' inputs is revealed.

In this note, we are interested in OT from the viewpoint of communication complexity rather than cryptography. In particular, the described reductions are not cryptographic: a party can obtain *more* information than specified.

C. Classical Teleportation

Quantum teleportation [3] is the simulation of sending a qubit over a quantum channel, using a shared EPR pair and two bits of classical communication. *Classical teleportation* [5] is the term used for the following reduction. Given a box simulating the classical behavior of an EPR pair, e.g., a singlet $|\psi^-\rangle$, and one bit of classical communication, one can simulate sending a qubit over a quantum channel and carrying out a von Neumann measurement on the received qubit. The idea is as follows [5]: Alice chooses, for her part of the EPR pair, a measurement basis consisting of the state she wants to send and its orthogonal complement, and communicates the outcome to Bob, who inverts his measurement result if and only if Alice has measured the state orthogonal to the one to be sent. Together with the result that NLB allows for simulating the behavior of an EPR pair under von Neumann measurements, this leads to a realization of classical teleportation with *one use of NLB and one bit of classical communication*. When another result, by Bacon and Toner [17], is used stating that the EPR behavior under projective measurements can be simulated using one bit of communication, then one obtains the possibility of classical teleportation using two bits of classical communication.

D. Resources Inequalities

Similar as in [8], [9], we will use *resources inequalities* to express the relations between different communication resources. For two resources R and R', we write

$$R \succeq R'$$

if there exists a protocol that simulates R' using R and shared randomness. If this simulation is not always successful, but only with probability p, then we write

$$R \overset{p}{\succeq} R' \ .$$

This notation allows us to rephrase the results mentioned earlier: Let $[c \to c]$ be a perfect communication channel that transmits one (classical) bit and let $[q \to q]$ be a perfect channel that transmits one qubit. Furthermore, let $[qq]$ be two maximally entangled qubits, and let $[q_c q_c]$ be equal to $[qq]$, with the restriction that the two players can only access their qubit by applying a von Neumann measurement. We can rephrase the reductions mentioned earlier as

$$\mathsf{NLB} \succeq [q_c q_c] \overset{0.85}{\succeq} \mathsf{NLB} .$$

Let $[q_c \to q_c]$ be a channel that receives a description of a qubit, and send it to the receiver, who can access the qubit by applying a von Neumann measurement. Classical teleportation [5] can now be written as

$$[q_c q_c] + [c \to c] \succeq [q_c \to q_c] .$$

It follows that we also have

$$\mathsf{NLB} + [c \to c] \succeq [q_c \to q_c] ,$$

i.e., $[q_c \to q_c]$ can be simulated using NLB and $[c \to c]$.

II. Relations among Classical Communication Resources

Using very simple reductions, we can now also find resources inequalities for $[c \to c]$, NLB, and OT. First of all, it is easy to see that

$$\mathsf{OT} \succeq [c \to c] ,$$

as the receiver may always chose to read the first bit. Then, we also have

$$[c \to c] \succeq \mathsf{NLB}$$

because we can simulate NLB in the following way. Let x and y be the input to NLB, and a and b the outputs, and let r be the a shared random bit. The first player outputs $a := r$ and sends x over $[c \to c]$ to the second player, who outputs $b := c + y \cdot x$. Finally, we also have

$$\mathsf{NLB} + [c \to c] \succeq \mathsf{OT}$$

by the following simulation of OT: Let x and y be the input to the NLB, and a and b are the outputs. Let b_0 and b_1 be the inputs of the sender to OT, and let c be the input and z be the output of OT. To simulate OT, the sender chooses $x := b_0 \oplus b_1$ and the receiver $y := c$ as inputs to NLB. The sender then sends $m := x_0 \oplus a$ over $[c \to c]$, and the receiver outputs $z := m \oplus b$. We have

$$z = m \oplus b = x_0 \oplus a \oplus b = b_0 \oplus (b_0 \oplus b_1)c = b_c .$$

We get the following hierarchy:

$$\mathsf{NLB} + [c \to c] \succeq \mathsf{OT} \succeq [c \to c] \succeq \mathsf{NLB} .$$

Therefore, OT is the strongest, and NLB the weakest of these primitives. However, the ”distance” between them is at most $[c \to c]$ as OT can be simulated using $\mathsf{NLB} + [c \to c]$.

Note that this last protocol is even a reduction in a cryptographic sense, which means that besides their outputs, the players do not get any additional information, even if they behave dishonestly. An interesting and somewhat surprising consequence is that OT, just as NLB, is from a cryptographical point of view *symmetric*: OT from A to B can be perfectly securely reduced to a single instance of OT from B to A [22], [21].

III. Oblivious Transfer and the Quantum Channel

We will now show that instead of one NLB and one $[c \to c]$, one OT is in fact sufficient to simulate $[q_c \to q_c]$. Furthermore, using one $[q_c \to q_c]$, we may simulate OT with a probability of 0.85, while if only a $[c \to c]$ is available, this can be achieved with a maximal probability of 0.75. Therefore, we get, in the very same way as for NLB and $[q_c q_c]$, that

$$\mathsf{OT} \succeq [q_c \to q_c] \overset{0.85}{\succeq} \mathsf{OT} .$$

We can, therefore, conclude that OT is the classical analogue to a $[q \to q]$ in the same way as NLB is to $[qq]$!

A. Simulating $[q_c \to q_c]$ using OT

The reduction of classical teleportation to OT works as follows. Let l_1 and l_2 be two random vectors on the Poincaré sphere, and let $l_\pm := l_1 \pm l_2$. (These vectors are the randomness shared by the two parties.) Let v_A and v_B be the vectors determining the state Alice wants to send and the measurement Bob wants to perform, respectively. Then the inputs to OT are as shown in Figure 5. (Here, sg denotes the signum function.)

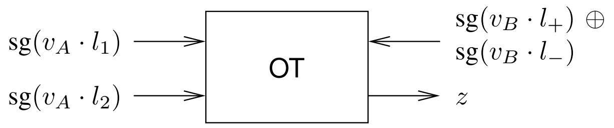

Fig. 5. Reducing classical teleportation to oblivious transfer.

Bob's output is the bit

$$z \oplus \mathrm{sg}(v_B \cdot l_+) \oplus 1 .$$

We have

$$z = \mathrm{sg}(v_A \cdot l_1) \oplus [\mathrm{sg}(v_A \cdot l_1) \oplus \mathrm{sg}(v_A \cdot l_2)] \cdot [\mathrm{sg}(v_B \cdot l_+) \oplus \mathrm{sg}(v_B \cdot l_-)] .$$

Hence, we obtain the same expression as in [5] (see also [17]).

B. Simulating OT using $[q_c \to q_c]$

Let now Alice and Bob be connected by a quantum channel over which they are allowed to send exactly one qubit. They want to simulate OT (with an error as small as possible) with Alice as sender and Bob as receiver. Alice has inputs b_0 and b_1 and Bob c, i.e., Bob wants to know b_c. Alice takes a qubit $|\phi\rangle = |0\rangle$ and rotates it by an angle of

$$\phi(b_0, b_1) = \begin{cases} -\pi/8 & \text{if } (b_0, b_1) = (0,0) , \\ \pi/8 & \text{if } (b_0, b_1) = (0,1) , \\ -3\pi/8 & \text{if } (b_0, b_1) = (1,0) , \\ 3\pi/8 & \text{if } (b_0, b_1) = (1,1) . \end{cases} \quad (3)$$

She gets

$$|\phi\rangle = \cos(\phi(b_0, b_1))|0\rangle + \sin(\phi(b_0, b_1))|1\rangle \tag{4}$$

and sends $|\phi\rangle$ to Bob. If $c = 1$, Bob applies a Hadamard transform on $|\phi\rangle$, but leaves it unchanged otherwise. He then measures $|\phi\rangle$ in the computational basis and outputs the outcome of this measurement. It is easy to verify that his output is equal to b_c with a probability of $\cos^2(\pi/8) \approx 0.85$ (which is the same as for the simulation of NLB using an EPR pair).

If Alice and Bob are only allowed to communicate one classical bit, the best Alice can do is to choose one of the two input bits and send it to Bob. Therefore, Bob will only be able to output the correct value b_c with probability 0.75 if all inputs are random. (Again, this is the same success probability as for NLB without an EPR pair.)

IV. Concluding Remarks and Open Problems

We have shown that oblivious transfer can be seen as the classical analogue of sending a qubit over a quantum channel in the same sense as NLB is for measuring an EPR pair:

$$\frac{\text{Oblivious transfer}}{\text{Quantum-bit channel}} = \frac{\text{Non-local box}}{\text{EPR pair}} \ .$$

Note that our simulation of a quantum channel does not preserve *privacy*, i.e., the players get more information than they would, had they only black-box access to a quantum channel. It is an open problem whether there is an efficient simulation that is private, too.

Acknowledgment

This work was supported by the Swiss National Science Foundation (SNF).

Some of the results of this paper were presented at *Information Theory Workshop (ITW) 2005* in Punta del Este, Uruguay. Results related to ours were also obtained in [1].

References

[1] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, Dense Quantum Coding and a Lower Bound for 1-way Quantum Automata, quant-ph/9804043, 1998.

[2] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, *Physics*, Vol. 1, pp. 195–200, 1964.

[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, Teleporting an unknown quantum state via dual classical and EPR channels, *Phys. Rev. Lett.*, Vol. 70, pp. 1895-1899, 1993.

[4] C. H. Bennett and S. J. Wiesner, Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states, *Phys. Rev. Lett.*, 69:2881, 1992.

[5] N. Cerf, N. Gisin, and S. Massar, Classical teleportation of a quantum bit, *Phys. Rev. Lett.*, Vol. 84, No. 11, 2000.

[6] N. Cerf, N. Gisin, S. Massar, and S. Popescu, Simulating maximal quantum entanglement without communication, *Phys. Rev. Lett.*, Vol. 94, 2005. See also quant-ph/0410027.

[7] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys. Rev. Lett.*, Vol. 23, pp. 880, 1969.

[8] I. Devetak, A.W. Harrow, and A. Winter A family of quantum protocols, quant-ph/0308044, 2003.

[9] I. Devetak, A.W. Harrow, and A. Winter A resource framework for quantum Shannon theory, quant-ph/0512015, 2005.

[10] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, *Phys. Rev.*, Vol. 41, 1935.

[11] A. M. Gleason, Measures on the closed subspaces of a Hilbert space, *J. Math. Mech.*, Vol. 6, 885, 1957.

[12] J. M. Jauch and C. Piron, Can hidden variables be excluded in quantum mechanics?, *Helv. Phys. Acta*, Vol. 36, 827, 1963.

[13] S. Kochen and E. Specker, The problem of hidden variables in quantum mechanics, *Journal of Mathematics and Mechanics*, Vol. 17, No. 1, 1967.

[14] S. Popescu and D. Rohrlich, Nonlocality as an axiom, *Foundations of Physics*, Vol. 24, pp. 379, 1994.

[15] M. Rabin, How to exchange secrets by oblivious transfer, *Technical Report TR-81, Harvard Aiken Computation Laboratory*, 1981.

[16] E. Specker, Die Logik nicht gleichzeitig entscheidbarer Aussagen, *Dialectica*, Vol. 14, pp. 239–246, 1960.

[17] B. Toner and D. Bacon, Communication cost of simulating Bell correlations, *Phys. Rev. Lett.*, Vol. 91, No. 18, 2003.

[18] W. van Dam, *On quantum computation theory*, Ph.D. thesis, University of Oxford, 2000.

[19] J. von Neumann, *Mathematische Grundlagen der Quanten-Mechanik*, Verlag Julius-Springer, Berlin, 1932. *Mathematial Foundations of Quantum Mechanics*, Princeton University, Princeton, 1955.

[20] S. Wiesner, Conjugate coding, *Sigact News*, Vol. 15, No. 1, 1983.

[21] S. Wolf and J. Wullschleger, Oblivious transfer and quantum non-locality, quant-ph/0502030, 2005.

[22] S. Wolf and J. Wullschleger. Oblivious transfer is symmetric. In *Advances in Cryptology — EUROCRYPT '06*, volume 4004 of *Lecture Notes in Computer Science*, pages 222–232. Springer-Verlag, 2006.