

Oblivious Transfer and Quantum Channels

Nicolas Gisin* Sandu Popescu^{†‡} Valerio Scarani* Stefan Wolf[§] Jürg Wullschlegel[§]

*Group of Applied Physics, University of Geneva, 10, rue de l'École-de-Médecine, CH-1211 Genève 4, Switzerland.

E-mail: {Nicolas.Gisin,Valerio.Scarani}@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

[§]Computer Science Department, ETH Zürich, ETH Zentrum, CH-8092 Zürich, Switzerland.

E-mail: {wolf,wjuerg}@inf.ethz.ch

Abstract—We show that oblivious transfer can be seen as the classical analogue to a quantum channel in the same sense as non-local boxes are for maximally entangled qubits.

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 [6] initiated a discussion on non-local behavior. Let us consider, for instance, the following, *maximally entangled* state, called *singlet* or, alternatively, *EPR* or *Bell state*:

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

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—even when the two measurement events are spatially separated. The conclusion of [6] was that quantum physics was incomplete in the sense that it should be augmented by certain *hidden parameters* determining the results of measurements. However, it was shown later by von Neumann [15], Gleason [7], Specker [12], Jauch and Piron [8], Bell [2], and Kochen and Specker [9] that such hidden-parameter models fail to explain quantum-physical behavior in general.

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

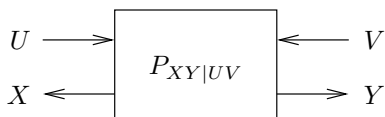


Fig. 1. A two-party information-theoretic primitive.

Bell [2] was the first to recognize that there exist pairs of measurement bases such that the resulting behavior is not local, i.e., cannot be explained by shared classical information

(see Figure 2). He showed that there exist certain inequalities (now called *Bell inequalities*) that cannot be violated by any local system, but which *are* 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 [10] have introduced a “non-locality machine,” called *non-local box* or *NL box* for short. The behavior of the NL box 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 the NL box are (U, V) and (X, Y) , respectively, and X and Y are random bits satisfying

$$\begin{aligned} \text{Prob}[X = Y | (U, V) \neq (1, 1)] &= 1, \\ \text{Prob}[X = Y | (U, V) = (1, 1)] &= 0. \end{aligned}$$

In other words, X and Y satisfy $X \oplus Y = U \cdot V$.

Using such NL boxes, we can understand Bell’s theorem in very intuitive way, since the *CHSH Bell inequality* corresponds to an upper bound on the success probability of simulating an NL box.

Let the inputs to the NL box be chosen at random. Let us first look at the classical simulation of an NL box. 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

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

Furthermore, it has been shown that one call to an NL box allows for *perfectly* simulating the joint behavior of a singlet state under arbitrary von Neumann measurements [5]. It is, therefore, fair to say that the NL box is the classical analogue of a Bell state.

B. Oblivious Transfer

Oblivious transfer, introduced by Wiesner [16] under the name of “multiplexing” and by Rabin [11], is a primitive of paramount importance in cryptography, in particular two- and multi-party computation. In *chosen 1-out-of-2 oblivious transfer* or $\binom{2}{1}$ -OT for short, one party, called the *sender*, has two binary inputs b_0 and b_1 , whereas the other party, the *receiver*, inputs a *choice bit* c . The latter then learns b_c but no additional information, while the sender remains ignorant about c .

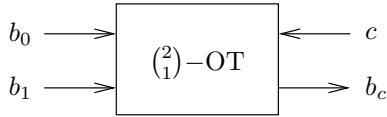


Fig. 3. Chosen 1-out-of-2 oblivious transfer.

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, and where a number of players want to secretly and correctly evaluate a function to which each player holds an input; here, “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.

In [17], it has been shown that $\binom{2}{1}$ -OT and the NL box are roughly the same primitive in a cryptographic sense, i.e., one can be reduced to the other. An interesting and somewhat surprising consequence thereof is that $\binom{2}{1}$ -OT, just as the NL box, is *symmetric*: $\binom{2}{1}$ -OT from A to B can be perfectly reduced to a single instance of $\binom{2}{1}$ -OT from B to A [18].

In terms of communication complexity, we have the following reductions. $\binom{2}{1}$ -OT can be reduced to one realization of an NL box plus one bit of (classical) communication as follows. Let (b_0, b_1) and c be the parties’ inputs for $\binom{2}{1}$ -OT. Then they input $b_0 \oplus b_1$ and c to the NL box, respectively, and receive the outputs X and Y with $X \oplus Y = (b_0 \oplus b_1)c$. The first party then sends $X \oplus b_0$ to the other, who computes

$$(X \oplus b_0) \oplus Y = b_0 \oplus (b_0 \oplus b_1)c = b_c,$$

as desired.

Conversely, $\binom{2}{1}$ -OT can be used to realize an NL box. If the inputs to the latter are u and v , then the parties input $(r, r \oplus u)$ (where r is a random bit) and v to the $\binom{2}{1}$ -OT. The sender’s output is then r , and the receiver’s output is his output from $\binom{2}{1}$ -OT, i.e., $r \oplus uv$. We, hence, have for the outputs that

$$r \oplus (r \oplus uv) = uv,$$

as requested.

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* [4] 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 [4]: 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 an NL box 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 an NL box and one bit of classical communication*. When another—*weaker*—result, by Bacon and Toner [13], 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.

II. CONNECTION BETWEEN OBLIVIOUS TRANSFER AND QUANTUM CHANNELS

In this section we show that—instead of one NL box and one classical bit of communication—one oblivious transfer (and shared randomness) is enough to perfectly simulate a quantum channel with a von Neumann measurement. Note that our discussion in the previous section shows that this is a strictly weaker primitive.

Furthermore, in the case of an NL box and EPR pairs, the inverse is true as well, with identical success probabilities: Using a quantum channel, one can simulate oblivious transfer with a probability of about 0.85, whereas with a classical channel one cannot be better than 0.75.

We can, therefore, conclude that oblivious transfer is the classical analogue to a quantum channel, in the same way as an NL box is for the EPR pair.

A. Simulating a Quantum Channel using Oblivious Transfer

The reduction of classical teleportation to $\binom{2}{1}$ -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 $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ -OT are as shown in Figure 4. (Here, sg denotes the signum function.)

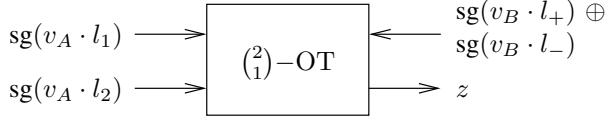


Fig. 4. Reducing classical teleportation to oblivious transfer.

Bob's output is the bit

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

We have

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

Hence, we obtain the same expression as in [4] (see also [13]).

B. Simulating Oblivious Transfer using a Quantum Channel

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

$$\phi(b_0, b_1) := \frac{\pi}{8}(2b_0 + 4b_1 - 3) . \quad (3)$$

She gets

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

and send $|\phi\rangle$ to Bob. If $c = 1$, Bob applies a Hadamard transform on $|\phi\rangle$ and 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

$$\cos^2\left(\frac{\pi}{8}\right) \approx 0.85 , \quad (5)$$

which is the same as for the simulation of an NL box 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, we get the same success probability as for the NL box without an EPR pair. Results related to ours were obtained in [1].

III. CONCLUDING REMARKS AND OPEN PROBLEMS

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

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

ACKNOWLEDGMENT

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

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] N. Cerf, N. Gisin, and S. Massar, Classical teleportation of a quantum bit, *Phys. Rev. Lett.*, Vol. 84, No. 11, 2000.
- [5] 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.
- [6] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, *Phys. Rev.*, Vol. 41, 1935.
- [7] A. M. Gleason, Measures on the closed subspaces of a Hilbert space, *J. Math. Mech.*, Vol. 6, 885, 1957.
- [8] J. M. Jauch and C. Piron, Can hidden variables be excluded in quantum mechanics?, *Helv. Phys. Acta*, Vol. 36, 827, 1963.
- [9] S. Kochen and E. Specker, The problem of hidden variables in quantum mechanics, *Journal of Mathematics and Mechanics*, Vol. 17, No. 1, 1967.
- [10] S. Popescu and D. Rohrlich, Causality and nonlocality as axioms for quantum mechanics, quant-ph/9709026, 1997.
- [11] M. Rabin, How to exchange secrets by oblivious transfer, *Technical Report TR-81, Harvard Aiken Computation Laboratory*, 1981.
- [12] E. Specker, Die Logik nicht gleichzeitig entscheidbarer Aussagen, *Dialectica*, Vol. 14, pp. 239–246, 1960.
- [13] B. Toner and D. Bacon, Communication cost of simulating Bell correlations, *Phys. Rev. Lett.*, Vol. 91, No. 18, 2003.
- [14] W. van Dam, *On quantum computation theory*, Ph.D. thesis, University of Oxford, 2000.
- [15] J. von Neumann, *Mathematische Grundlagen der Quanten-Mechanik*, Verlag Julius-Springer, Berlin, 1932. *Mathematical Foundations of Quantum Mechanics*, Princeton University, Princeton, 1955.
- [16] S. Wiesner, Conjugate coding, *Sigact News*, Vol. 15, No. 1, 1983.
- [17] S. Wolf and J. Wullschleger, Oblivious transfer and quantum non-locality, quant-ph/0502030, 2005.
- [18] S. Wolf and J. Wullschleger, Oblivious transfer is symmetric, <http://ePrint.iacr.org/2004/336>, 2004.