Lecture 17

QUANTUM CRYPTOGRAPHY. PART 2 - Dense coding, quantum teleportation and key distribution

of the course "Fundamentals of Quantum Computing"
(by IAPS *and* QUANTERALL*)*

Stoyan Mishev

INSTITUTE *for* ADVANCED PHYSICAL STUDIES

NEW BULGARIAN UNIVERSITY

September 23, 2022

План

Dense Quantum Coding

Quantum teleportation

Dense Quantum Coding

PHYSICAL REVIEW LETTERS

VOLUME 69 | 16 NOVEMBER 1992 | NUMBER 20

Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States

Charles H. Bennett
IBM Research Division, T. J. Watson Research Center, Yorktown Heights, New York 10598

Stephen J. Wiesner
74 Parkman Street, Brookline, Massachusetts 02146

(Received 16 June 1992)

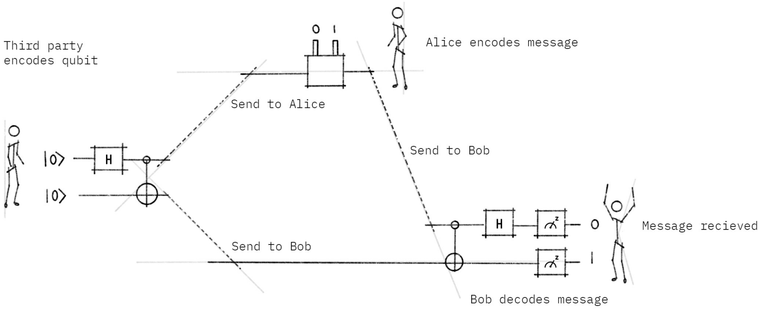
As is well known, operations on one particle of an Einstein-Podolsky-Rosen (EPR) pair cannot influence the marginal statistics of measurements on the other particle. We characterize the set of states accessible from an initial EPR state by one-particle operations and show that in a sense they allow two bits to be encoded reliably in one spin-$\frac{1}{2}$ particle: One party, "Alice," prepares an EPR pair and sends one of the particles to another party, "Bob," who applies one of four unitary operators to the particle, and then returns it to Alice. By measuring the two particles jointly, Alice can now reliably learn which operator Bob used.

C. Bennett, S. Wiesner, Phys. Rev. Lett. 69, 2881 (1992)
(Einstein–Podolsky–Rosen state == entangled state)

Dense Quantum Coding

Alice and Bob both hold one qubit of an entangled two-qubit state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



https://qiskit.org/textbook/ch-algorithms/superdense-coding.html

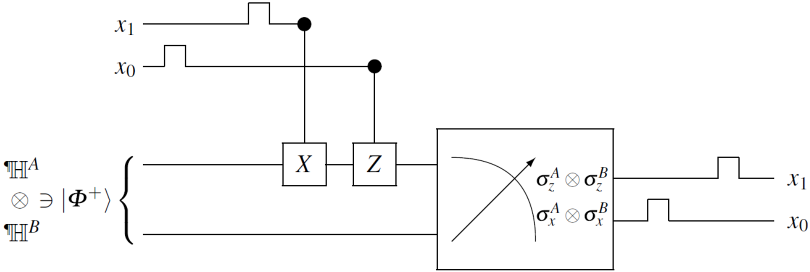
Alice wants to send Bob a sign - one the following digits $\{00, 01, 10, 11\}$. For that she chooses to act on the entagled state $|\Phi^+\rangle$ by a respective operator:

$$U^A(00) = \mathbf{1}^A$$
$$U^A(01) = \boldsymbol{\sigma}_z^A$$
$$U^A(10) = \boldsymbol{\sigma}_x^A$$
$$U^A(11) = \boldsymbol{\sigma}_z^A \boldsymbol{\sigma}_x^A$$

to obtain the states $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$.
On its side Bob measures the values of the observables $\sigma_z^A \otimes \sigma_z^B$ and $\sigma_x^A \otimes \sigma_x^B$. From their eigenvalues he understands the sign.

Dense Quantum Coding

Alice wants to send the classical bits x_1x_0	So she applies $U^A(x_1x_0)$	The state of the total system becomes $\left(U^A \otimes \mathbf{1}\right)\lvert\Phi^+\rangle$	on which Bob measures $\sigma_z^A \otimes \sigma_z^B$ and $\sigma_x^A \otimes \sigma_x^B$ and observes the values
00	$\mathbf{1}^A$	$\lvert\Phi^+\rangle$	$+1\ ,\ +1$
01	σ_z^A	$\lvert\Phi^-\rangle$	$+1\ ,\ -1$
10	σ_x^A	$\lvert\Psi^+\rangle$	$-1\ ,\ +1$
11	$\sigma_z^A\sigma_x^A$	$\lvert\Psi^-\rangle$	$-1\ ,\ -1$



Quantum teleportation

PHYSICAL REVIEW LETTERS

VOLUME 70 | 29 MARCH 1993 | NUMBER 13

Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels

Charles H. Bennett,[1] Gilles Brassard,[2] Claude Crépeau,[2],[3]
Richard Jozsa,[2] Asher Peres,[4] and William K. Wootters[5]

[1] *IBM Research Division, T.J. Watson Research Center, Yorktown Heights, New York 10598*
[2] *Département IRO, Université de Montréal, C.P. 6128, Succursale "A", Montréal, Québec, Canada H3C 3J7*
[3] *Laboratoire d'Informatique de l'École Normale Supérieure, 45 rue d'Ulm, 75230 Paris CEDEX 05, France*[a]
[4] *Department of Physics, Technion–Israel Institute of Technology, 32000 Haifa, Israel*
[5] *Department of Physics, Williams College, Williamstown, Massachusetts 01267*

(Received 2 December 1992)

An unknown quantum state $|\phi\rangle$ can be disassembled into, then later reconstructed from, purely classical information and purely nonclassical Einstein-Podolsky-Rosen (EPR) correlations. To do so the sender, "Alice," and the receiver, "Bob," must prearrange the sharing of an EPR-correlated pair of particles. Alice makes a joint measurement on her EPR particle and the unknown quantum system, and sends Bob the classical result of this measurement. Knowing this, Bob can convert the state of his EPR particle into an exact replica of the unknown state $|\phi\rangle$ which Alice destroyed.

C.H. Bennet, G. Brassard, C. Crepeau, R. Jozsa, A. Perez, W.K. Wootters, Phys. Rev. Lett. 70(13), 1895 (1993)

In dense coding A. wanted to transfer a number to B. while in "teleportation" A. wants to “send” B. a qubit.

[1] see Scherer, p.254

In dense coding A. wanted to transfer a number to B. while in "teleportation" A. wants to “send” B. a qubit. Again A. and B. both hold a qubit in a two-qubit entagled state

$$|\Phi^+\rangle^{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

[1] see Scherer, p.254

In dense coding A. wanted to transfer a number to B. while in "teleportation" A. wants to “send” B. a qubit. Again A. and B. both hold a qubit in a two-qubit entagled state

$$|\Phi^+\rangle^{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

The qubit A. wants to “send” is a different one:

$$|\Psi^+\rangle = a|0\rangle + b|1\rangle.$$

A. explores the product state $|\Psi^+\rangle|\Phi^+\rangle^{AB}$ which equals to [1]:

$$= \frac{1}{2}\Big[|\Phi^+\rangle^{SA} \otimes |\psi\rangle^B + |\Psi^+\rangle^{SA} \otimes \left(\sigma_x^B|\psi\rangle^B\right) + |\Phi^-\rangle^{SA} \otimes \left(\sigma_z^B|\psi\rangle^B\right) + |\Psi^-\rangle^{SA} \otimes \left(\sigma_x^B\sigma_z^B|\psi\rangle^B\right)\Big]$$

[1] see Scherer, p.254

$$
\begin{aligned}
|\psi\rangle^S \otimes |\Phi^+\rangle^{AB} &= \left(a|0\rangle^S + b|1\rangle^S\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle^A \otimes |0\rangle^B + |1\rangle^A \otimes |1\rangle^B\right) \\
&= \frac{1}{\sqrt{2}}\Bigg[a \underbrace{|0\rangle^S \otimes |0\rangle^A}_{=\frac{1}{\sqrt{2}}\left(|\Phi^+\rangle^{SA}+|\Phi^-\rangle^{SA}\right)} \otimes |0\rangle^B + a \underbrace{|0\rangle^S \otimes |1\rangle^A}_{=\frac{1}{\sqrt{2}}\left(|\Psi^+\rangle^{SA}+|\Psi^-\rangle^{SA}\right)} \otimes |1\rangle^B \\
&\qquad + b \underbrace{|1\rangle^S \otimes |0\rangle^A}_{=\frac{1}{\sqrt{2}}\left(|\Psi^+\rangle^{SA}-|\Psi^-\rangle^{SA}\right)} \otimes |0\rangle^B + b \underbrace{|1\rangle^S \otimes |1\rangle^A}_{=\frac{1}{\sqrt{2}}\left(|\Phi^+\rangle^{SA}-|\Phi^-\rangle^{SA}\right)} \otimes |1\rangle^B\Bigg] \\
&= \frac{1}{2}\Big[|\Phi^+\rangle^{SA} \otimes \left(a|0\rangle^B + b|1\rangle^B\right) + |\Psi^+\rangle^{SA} \otimes \left(a|1\rangle^B + b|0\rangle^B\right) \\
&\qquad + |\Phi^-\rangle^{SA} \otimes \left(a|0\rangle^B - b|1\rangle^B\right) + |\Psi^-\rangle^{SA} \otimes \left(a|1\rangle^B - b|0\rangle^B\right)\Big] \\
&= \frac{1}{2}\Big[|\Phi^+\rangle^{SA} \otimes |\psi\rangle^B + |\Psi^+\rangle^{SA} \otimes \left(\sigma_x^B|\psi\rangle^B\right) \\
&\qquad + |\Phi^-\rangle^{SA} \otimes \left(\sigma_z^B|\psi\rangle^B\right) + |\Psi^-\rangle^{SA} \otimes \left(\sigma_x^B\sigma_z^B|\psi\rangle^B\right)\Big] .
\end{aligned}
\tag{6.7}
$$

A. applies $\sigma_z^S \otimes \sigma_z^A$ and $\sigma_x^S \otimes \sigma_x^A$

Measured value of		State after measurement
$\sigma_z \otimes \sigma_z$	$\sigma_x \otimes \sigma_x$	
$+1$	$+1$	$\lvert\Phi^+\rangle$
$+1$	-1	$\lvert\Phi^-\rangle$
-1	$+1$	$\lvert\Psi^+\rangle$
-1	-1	$\lvert\Psi^-\rangle$

to obtain two digits which she sends to B.

A. applies $\sigma_z^S \otimes \sigma_z^A$ and $\sigma_x^S \otimes \sigma_x^A$

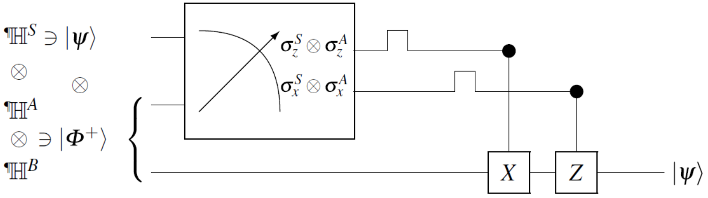
Measured value of		State after measurement
$\sigma_z \otimes \sigma_z$	$\sigma_x \otimes \sigma_x$	
$+1$	$+1$	$\|\Phi^+\rangle$
$+1$	-1	$\|\Phi^-\rangle$
-1	$+1$	$\|\Psi^+\rangle$
-1	-1	$\|\Psi^-\rangle$

to obtain two digits which she sends to B.
B. on its side using the same correspondance as A. was using in "dense coding"

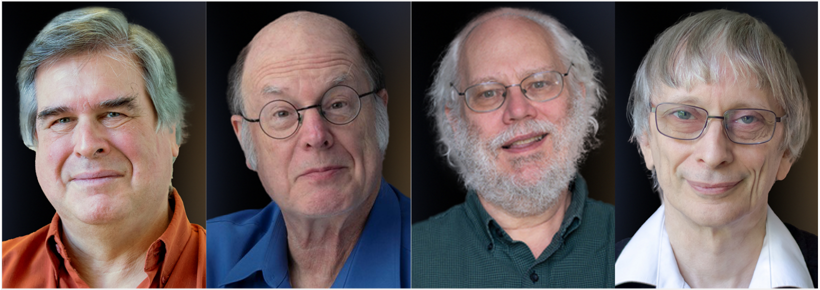
$$U^B(00) = \mathbf{1}^B$$
$$U^B(01) = \sigma_z^B$$
$$U^B(10) = \sigma_x^B$$
$$U^B(11) = \sigma_z^B \sigma_x^B$$

to transform his qubit from the entangled state and transform it to $|\psi\rangle$.

Alice measures $\sigma_z^S \otimes \sigma_z^A$ and $\sigma_x^S \otimes \sigma_x^A$ to observe	The three-qubit total state after measurement is then: $\lvert\Psi\rangle^{SA} \otimes$ Bob's qubit-state	From bits received Bob determines to apply U^B	The state of Bob's qubit then becomes
$+1\,,+1$	$\lvert\Phi^+\rangle \otimes \lvert\psi\rangle$	$\mathbf{1}^B$	$(\mathbf{1}^B)^2\lvert\psi\rangle = \lvert\psi\rangle$
$+1\,,-1$	$\lvert\Phi^-\rangle \otimes \sigma_z^B\lvert\psi\rangle$	σ_z^B	$(\sigma_z^B)^2\lvert\psi\rangle = \lvert\psi\rangle$
$-1\,,+1$	$\lvert\Psi^+\rangle \otimes \sigma_x^B\lvert\psi\rangle$	σ_x^B	$(\sigma_x^B)^2\lvert\psi\rangle = \lvert\psi\rangle$
$-1\,,-1$	$\lvert\Psi^-\rangle \otimes \sigma_x^B\sigma_z^B\lvert\psi\rangle$	$\sigma_z^B\sigma_x^B$	$\sigma_z^B\sigma_x^B\sigma_x^B\sigma_z^B\lvert\psi\rangle = \lvert\psi\rangle$



September 22, 2022


From left to right: Gilles Brassard, Charles H. Bennett, Peter Shor, and David Deutsch

https://perimeterinstitute.ca/news/quantum-computing-pioneers-earn-breakthrough-prize https://qiskit.org/textbook/ch-algorithms/superdense-coding.html

NEXT LECTURE

OCTOBER 7th, 2022

THANK YOU FOR YOUR ATTENTION!

БЛАГОДАРЯ ЗА ВНИМАНИЕТО!