International Journal of Quantum Information
Vol. 9, Nos. 7 & 8 (2011) 1737–1744

DOI: 10.1142/S0219749911008222

ENTANGLEMENT AND SUPERDENSE CODING WITH LINEAR OPTICS

MLADEN PAVIČIĆ

Chair of Physics, Faculty of Civil Engineering,
University of Zagreb, Croatia
pavicic@grad.hr

Received 16 May 2011

We discuss a scheme for a full superdense coding of entangled photon states employing only linear optics elements. By using the mixed basis consisting of four states that are unambiguously distinguishable by a standard and polarizing beam splitters we can deterministically transfer four messages by manipulating just one of the two entangled photons. The sender achieves the determinism of the transfer either by giving up the control over 50% of sent messages (although known to her) or by discarding 33% of incoming photons.

Keywords: Superdense coding; quantum communication; Bell states; mixed basis.

1. Introduction

Superdense coding (SC)[1] — sending up to two bits of information, i.e. four messages, by manipulating just one of two entangled qubits (two-state quantum systems) — is considered to be a protocol that launched the field of quantum communication.[2] Apart from showing how different quantum coding of information is from the classical one — which can encode only two messages in a two-state system — the protocol has also shown how important entanglement of qubits is for their manipulation.

Such an entanglement has proven to be a genuine quantum effect that cannot be achieved with the help of two classical bit carriers because we cannot entangle classical systems. To use this advantage of quantum information transfer, it is very important to keep the trade-off of the increased transfer capacity balanced with the technology of implementing the protocol. The simplest and most efficient implementation is the one that would use photons manipulated by linear optics elements such as beam splitters, polarizers, and wave plates and only one degree of freedom — polarization.

Since entangled qubits applied to the teleportation required Bell states, all subsequent attempts to implement SC — as another transportation protocol — concentrated on Bell states. The idea was to send four messages via four Bell states [see Eq. (1)] and herewith achieve a $\log_2 4 = 2$ bit transfer. To this aim, a recognition of all four Bell states was required.

The first linear optics implementation has reached only three quarters (three messages) of its theoretical two-bit (four messages) channel capacity, i.e. $\log_2 3 = 1.585$ bits. This was because a recognition of two Bell states $|\Psi^+\rangle$ and $|\Psi^-\rangle$ was achieved while the other two $|\Phi^\pm\rangle$ that could not be told apart were both used to send one and the same message.[3] This partial realization of the superdense protocol was named *dense coding*. In 2001, Calsamiglia and Lütkenhaus proved[4] that the dense coding was all we could achieve with Bell states and linear optics.

Therefore in Ref. 5 we dispensed with the Bell state basis and introduced the *mixed basis* which enabled us to go around the Calsamiglia−Lütkenhaus no-go proof and carry a superdense coding with linear optics.

The finding revealed that the notion of superdense coding was not operationally well defined, mostly because no particular application of this protocol in quantum computation and/or quantum communication has been found so far.

In this paper, we therefore consider three possible operational definitions and implementation of the superdense coding.

2. Mixed Basis and Entanglement

We define a mixed basis as a basis which consists of the following two Bell states

$$|\chi^{1,2}\rangle = |\Psi^\pm\rangle = (|H\rangle_1|V\rangle_2 \pm |V\rangle_1 H\rangle_2)/\sqrt{2} \tag{1}$$

and the following two computational basis states

$$|\chi^3\rangle = |H\rangle_1|H\rangle_2, \quad |\chi^4\rangle = |V\rangle_1|V\rangle_2, \tag{2}$$

where H (V) represents horizontal (vertical) photon polarization. We shall not use the other two Bell states $|\Phi^\pm\rangle = (|\chi^3\rangle \pm |\chi^4\rangle)/\sqrt{2}$. Both Bell and computational bases can be expressed by means of the mixed basis.

Let us first see why we cannot use only the computational basis, then why we cannot use only the Bell basis, and in the end why we *can* use the mixed basis. We consider photons being sent to a beam splitter after which we try to split them with the help of polarizing beam splitters (PBS) and then detect them by means of detectors with photon number resolution.

When we send two parallelly polarized photons to a beam splitter from its opposite sides they will always emerge from the same side, bunched together and showing the so-called Hong-Ou-Mandel interference dip [Sec. 3.2].[6] It has been calculated that both bunched photons keep the polarization direction they had before they entered the beam splitter.[7–9] So we can discriminate $|\chi^3\rangle$ and $|\chi^4\rangle$ from each other and from $|\chi^{1,2}\rangle$ with photon number resolution detectors or up to an arbitrary precision with single photon detectors. If we sent perpendicularly polarized photons — the other two states of the computational basis — to a beam splitter, they would either bunch together (50%) or emerge from the opposite sides of the beam slitter (50%).[7] The two photons that are split are correlated but unpolarized. Therefore, we cannot distinguish between $|HV\rangle$ and $|VH\rangle$ in 50% of the events and we again end up with the channel capacity $\log_2 3$ as for the Bell states.

On the other hand, in the Bell basis we can discriminate between $|\Psi^+\rangle$ and $|\Psi^-\rangle$ but not between $|\Phi^+\rangle$ and $|\Phi^-\rangle$ [Sec. 4.1].[6] At a polarization preserving (metallic) BS, $|\Psi^-\rangle$ photons split and $|\Psi^+\rangle$ photons bunch together but have different polarization so that we can split them at PBSs behind BS. $|\Phi^\pm\rangle$ photons also bunch together but being entangled (unpolarized but correlated in polarization) both photons from a pair project to either $|H\rangle$ or $|V\rangle$, i.e. either both go through or are both reflected from PBSs.

So, we can unambiguously discriminate two states from the computational basis, $|HH\rangle, |VV\rangle$, two from the Bell basis, $|\Psi^\pm\rangle$, as well as any one of them from each other by means of photon number resolution detectors. Thus we can discriminate all four $|\chi^i\rangle$, $i = 1, \ldots, 4$ and now there comes the question how to prepare them.

Alice gets $|\Psi^+\rangle$ photons by means of spontaneous parametric down conversion in a BBO crystal.[3] To send $|\chi^1\rangle = |\Psi^+\rangle$ she puts nothing in the path of her photon. To send $|\chi^2\rangle = |\Psi^-\rangle$ she puts in HWP(0°) (half-wave plate) in the path. It changes the sign of the vertical polarization. To send $|\chi^3\rangle$ she takes out HWP(0°) and puts in HWP(45°) and a polarizer (*pol*) oriented horizontally. Her *pol* is of a PBS type: $|H\rangle$ photon passes through and $|V\rangle$ is reflected from it. HWP(45°) turns $|\Psi^+\rangle$ into $|\Phi^-\rangle$ and *pol* projects both photons to state $|H\rangle$ in half of the occurrences. In the other half of the occurrences, Alice's photon is reflected from her *pol* and we have both photons in state $|V\rangle$, i.e. the pair in state $|\chi^4\rangle$. Alice might detect these "wrong" photons with the help of a detector d. Below we will specify what Alice can do next. To send $|\chi^4\rangle$, Alice is making use of a reflection from her PBS and then the "wrong" photons go through.

We stress here that the preparation of $|\chi^3\rangle$ and $|\chi^4\rangle$ includes physics of entangled systems because whenever Alice sends her qubit through a polarizer oriented horizontally or vertically, the other qubit from the entangled pair (originally in the state $|\Phi^+\rangle$) will be immediately set into $|H\rangle$ and $|V\rangle$ state for any subsequent measurement along H or V directions, respectively.

We noticed above that "in a way" Alice does not have a control over the choice of her photon while preparing $|\chi^3\rangle$ and $|\chi^4\rangle$ states. Her photon can go either way in her PBS. But she does know which way it took *after* it did so. And this opens a question of an operational definitions and implementation of the SC.

3. Operational Definitions of SC

In the absence of a well-defined application, there can be three possible operational definitions and implementations of SC.

We start with a formal definition.

Definition 1. SC is a technique used in quantum information theory to send two bits of classical information using only one qubit, with the aid of entanglement.

To make this definition more operational we restate it following Ref. 10.

Definition 2. In SC, a sender (Alice) can send a message consisting of two classical bits using one quantum bit (qubit) to the receiver (Bob). The input to the circuit is one of a pair of qubits entangled in the Bell basis state. The other qubit from the pair is sent unchanged to Bob. After processing the former qubit in one of four ways, it is sent to Bob, who measures the two qubits, yielding two classical bits. The result is that Bob receives two classical bits which match those that Alice sent by manipulating just her qubit.

Even this definition is not operational enough because several elements remained unspecified:

- (i) the owner of the pair can be Alice, Bob, or Anna;
- (ii) Alice might be required to send each photon she receives from the source to Bob or might not be required to do so;
- (iii) Alice might be required to have a control over sent messages or not.

We shall consider all the aforementioned options.

In the original version of their superdense coding, Bennett and Wiesner[1] assume that Bob is the proprietor of entangled pairs and that he sends Alice one qubit from each of his pairs. She manipulates her qubits and sends it back to Bob. Bob expects of Alice to return him each qubit he sent her. In our version she might do that [option (b)] or might not do so [options (a) and (c)].

In the first coding experiment,[3] Alice [Bob in the cited reference] owns the entangled pairs, manipulates one of the qubits, and then sends both qubits of Bob [Alice in the cited reference]. In our version Alice might [option (c)] or might not [options (a) and (b)] own the pairs.

Three possible scenarios that operationalize the options are:

- (a) Alice is assumed to send Bob a comprehensible message by means of four elementary messages $|\chi^i\rangle$, $i = 1, \dots, 4$. Bob is the owner of the source; he sends one photon to Alice and keeps one for himself. (A) She manipulates her qubits and sends to Bob only those ones over which she can have a control; she discards those over which she cannot have a control. Anna might also be the owner of the source. She sends one qubit to Bob and one to Alice and they proceed as from point (A) above;
- (b) Alice is assumed to send Bob an intelligible but not necessarily a comprehensible message by means of four elementary messages $|\chi^i\rangle$, $i = 1, \dots, 4$. Anna owns the BBO crystal and sends one qubit to Bob and one to Alice. (B) Alice sends either original or cloned qubits to Bob; she does not have a control over 50% of her messages (assuming they are evenly distributed) but she does have records of all the messages she sent. Alternatively, Bob can own the source and send one photon to Alice and keeps one for himself. Then they proceed as from point (B) above;

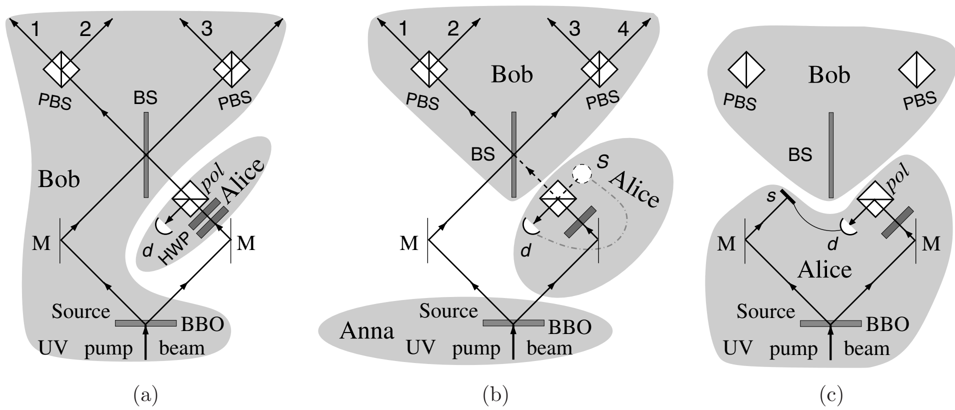

Fig. 1. Superdense coding. Operational definitions (a), (b), and (c) that we consider in the text.

(c) Alice owns the source. This scenario is essentially different from the previous ones because Alice can discard not only the qubit which she could not control but also the other qubit from the pair. Bob never finds out that the pair ever existed. Alice can transfer comprehensible messages deterministically.

These three operational scenarios are shown in Fig. 1. Interpretations of the scenarios essentially depend on applications. We elaborate on their applications in Sec. 4 and here we just discuss when the scenarios can be considered deterministic.

(a) Alice is being sent her qubits and Bob expects her to use as many of them as she can. Alice sends $|\chi^1\rangle$ and $|\chi^2\rangle$ with an efficiency ideally approaching 100%. When sending $|\chi^3\rangle$ or $|\chi^4\rangle$ she has only 50% probability of success, but she knows when she was successful and when not — her detector will not click when she was and will click when she was not. Bob will also know when Alice was not successful because he will then receive only one photon. So they can discard unsuccessful attempts. Now the question emerges whether we have an application for which it would be important to worry about the lost photon pairs. If not, we can speak of ideally deterministic SC. Application proposed in Sec. 4 supports it.

(b) Anna is demanding and wants Alice to use all the photons she sends her. However, she expects of Alice only to sends states $|\chi^i\rangle$, $i = 1, 2, 3, 4$ as she can. So, when sending say $|\chi^3\rangle$ Alice sends half of them through her PBS as "they choose" and clone the other half with the help of quantum dots (deterministic cloning of definite known polarization is possible). We give an application of this scenario in Sec. 4.

(c) Alice owns the source and both photons. She is allowed to manipulate just one photon but she can stop the other if her photon chooses a "wrong" exit from her PBS. Here the question emerges whether we can have any reason not to allow

Alice to stop the whole pair. Again everything depends on the application. But in the absence of a dominant SC application we can again speak of ideally deterministic SC. In Sec. 4 we give an application which makes use of such a coding.

4. Discussion

Efficient recognition of all four Bell basis states is undoubtedly essential for teleportation because they describe entanglement of photons which serve as "carriers" for teleportation. However, for SC it is essential that we transfer four messages by manipulating just one of the originally entangled qubits.

We showed that in the current absence of prevailing application of SC we can carry it out deterministically with the linear optics in three different ways. Here we present some possible applications of the coding in quantum cryptography. As opposed to "pure" SC, its cryptography application will include classical channels but we keep the basic SC scenarios from Sec. 3.

(a) Bob and Alice discard unsuccessful messages (33%). Alice repeats every such message. Information transfer with successful messages can be considered deterministic in the absence of applications which would forbid discarding unsuccessful messages. Application can be the *ping-pong* quantum cryptography protocol.[11,12] Since in this protocol we do not have to have a classical channel through which Alice would inform Bob which messages to keep and which to discard as in BB84 protocol, Alice and Bob make a direct deterministic transfer of comprehensible messages with their 67% of messages. The transfer is done with four messages per Alice's qubit and with linear optical elements. The discarded 33% of messages do not impair the quality of the transfer in any way. Moreover, in the ping-pong protocol they need not be discarded but can be used as a control channel;

(b) Alice takes care only to send all her photons as she can. So, she can send four different messages (four different photon states $|\chi^i\rangle$, $i = 1, 2, 3, 4$) by manipulating just one photon but does not have a control over half of the states she sends, although she deterministically knows which messages she sent. Application might again be a ping-pong protocol. Alice can inform Bob on the cloned photons (with a delay) over a public (classical) channel so that Bob can change the received "wrong" message into the one Alice intended to send. The message is still unreadable to Eve provided Alice randomly changes the orientation of her qubit and informs Bob on it with a delay;

(c) Alice sends messages cleanly and deterministically to Bob by stopping both photons whenever her photons come from the "wrong" exit. Alice repeats every such message. Bob does not know anything about the existence of the "wrong" pairs. In the ping-pong protocol Alice can use a public channel to tell Bob (with a delay) to erase his qubit from the pair containing Alice's "wrong qubit."

In the end we would like to discuss the following possible objection to our approach: "A SC applies to message generation and not to a message recognition; therefore, we cannot discard 25% of "wrong" messages in our options (a) and (c); hence, (a) and (c) are only an alternative scheme to achieve dense coding." The answer to this objection is simple.

First, we do not discard 25% but 33% of messages assuming that they are equally distributed. This is because for an equal distribution of messages we have to compensate for the messages ($|\chi^{3,4}\rangle$) that cannot be sent in half of Alice's attempts by increasing the number of her attempts to do so. Let n be the number of each of the four messages. Each unsuccessful attempt to send $|\chi^{3,4}\rangle$ Alice has to repeat until the messages go through. That gives $4n + n + n = 100\%$ and the percentage of each of the sent messages is 16.7%. The percentage of each kind of "wasted" (repeated) messages is also 16.7% and this reduces the efficiency of the four encoded messages by 33%: $4 \times 0.67 = 2.7$. Hence, our protocol only transfers four messages — while the dense coding transfers only three — and has the channel capacity per photon pairs generated at the source $\log_2 2.7 = 1.433$ — while the dense coding has $\log_2 3 = 1.585$.

Second, we deterministically generate four different messages *after* first discarding 33% of unusable detections. Hence, our protocol is not an alternative scheme of dense coding. In particular,

(1) pair generation of photon pairs in the photon source and message generation are two independent things; there is no physical reason why Alice and Bob should not be allowed to shrink the number of photons they obtain from the crystal, for Alice's generation of messages;
(2) both, our protocol and the dense coding protocol are about message generation but with our protocol we are able to transfer four messages, while with the dense coding we can transfer only three; in dense coding Bob cannot discriminate between two of four messages while in our protocol he can deterministically discriminate all four ($|\chi^i\rangle$, $i = 1, 2, 3, 4$) messages.
(3) if any of the two protocol can be considered nondeterministic it is the dense coding one because there Bob cannot discriminate between $|\Phi^-\rangle$ and $|\Phi^+\rangle$.

As for point (1) above we stress that similar discarding of unwanted events is a standard technique of the quantum information engineering. Consider, e.g. generation of entangled photons on demand from three spontaneous parametric down-conversion sources.[13–15] We discard photon detections after photon detections until we finally get a right set of four detections that tell us that the remaining two photons are entangled and ready for usage. Actually we discard so many of them that within a required time window we have a success probability of the order of 10^{-6}. In this procedure a detection of four photons determines the entangled photons on demand and in our procedure Alice's manipulation of her qubits determines the number of superdense coded pairs; discarded pairs are irrelevant for the coding and play no role in it; relevant are only those that carry Alice's messages to Bob.

Acknowledgment

Supported by the Ministry of Science, Education, and Sport of Croatia through project No. 082-0982562-3160.

References

1. C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69** (1992) 2881.
2. J. T. Barreiro, T.-C. Wei and P. G. Kwiat. *Nature Phys.* **4** (2008) 282.
3. K. Mattle, H. Weinfurter, P. G. Kwiat and A. Zeilinger, *Phys. Rev. Lett.* **76** (1996) 4656.
4. J. Calsamiglia and N. Lütkenhaus, *App. Phys. B* **72** (2001) 67.
5. M. Pavičić, Superdense coding with linear optics, preprint (2011), arXiv:1104.1802.
6. Z.-Y. J. Ou, *Multi-Photon Quantum Interference* (Springer, Berlin, 2007).
7. M. Pavičić, *Phys. Rev. A* **50** (1994) 3486.
8. M. Pavičić, *Quantum Computation and Quantum Communication: Theory and Experiments* (Springer, Berlin, 2005).
9. M. Pavičić and J. Summhammer, *Phys. Rev. Lett.* **73** (1994) 311.
10. B. Rubin, Superdense coding (2011), demonstrations.wolfram.com/SuperdenseCoding.
11. K. Boström and T. Felbinger, *Phys. Rev. Lett.* **89** (2002) 187902-1.
12. K. Boström and T. Felbinger, *Phys. Lett. A* **372** (2008) 3953.
13. S. Barz, G. Cronenberg, A. Zeilinger and P. Walther, *Nature Phot.* **4** (2010) 553.
14. P. Kok, *Nature Phot.* **4** (2010) 504.
15. C. Wagenknecht, C.-M. Li, A. Reingruber, X.-H. Bao, A. Goebel, Y.-A. Chen, Q. Zhang, K. Chen and J.-W. Pan, *Nature Phot.* **4** (2010) 549.