Classical simulation of entanglement swapping with bounded communication

Branciard, C.; Brunner, N.; Buhrman, H.; Cleve, R.; Gisin, N.; Portmann, S.; Rosset, D.; Szegedy, M.

Published in:
Physical Review Letters

DOI:
10.1103/PhysRevLett.109.100401

Citation for published version (APA):
Entanglement appears under two different forms in quantum theory, namely, as a property of states of joint systems and as a property of measurement eigenstates in joint measurements. By combining these two aspects of entanglement, it is possible to generate nonlocality between particles that never interacted, using the protocol of entanglement swapping. We show that even in the more constraining bilocal scenario where distant sources of particles are assumed to be independent, i.e., to share no prior randomness, entanglement swapping can be simulated classically with bounded communication, using only 9 bits in total. Our result thus provides an upper bound on the nonlocality of the entanglement swapping process.
It is therefore a natural question to ask whether or not the classical simulation of protocols involving both entangled states and entangled measurements is possible with bounded communication, and how much communication is required. Here, we investigate this question for the scenario of entanglement swapping [27], where quantum particles that never interacted become nonlocally correlated after their twins underwent a joint measurement. We work in the scenario of bilocality [28,29], in which the shared randomness we will use in the simulation protocol is assumed to originate from two independent sources (see Fig. 1). Since entanglement swapping can be achieved with fully uncorrelated quantum sources, even experimentally [30,31], it is indeed natural to impose an equivalent constraint on the simulation model.

Importantly the constraint of bilocality makes the simulation of entanglement swapping a challenging problem. The goal is basically to generate singlet nonlocal correlations between two parties which are initially fully uncorrelated. At first sight this may even appear to be impossible with finite communication, in the light of a result by Massar et al. [32], showing that simulating singlet correlations requires either infinite shared randomness (between the two parties simulating the state) or infinite communication. Here however, we will show that the process of entanglement swapping can be simulated with 9 bits, by presenting an explicit protocol. Since the communication cost of the cheapest protocol can be considered as a measure of its nonlocality, our result provides an upper bound on the nonlocality of entanglement swapping.

The entanglement swapping process.—We consider three distant parties, Alice (A), Bob (B) and a Referee (R). R shares two maximally entangled qubit pairs in the state \( |\Psi^+\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) \) with A and B, respectively. The first pair is produced by a source located between A and R, the second one is produced by an independent source located between B and R; see Fig. 1 (i). Accordingly, Alice and Bob are initially uncorrelated. By performing a Bell state measurement, i.e., a two-qubit joint measurement which features four maximally entangled Bell states as eigenstates, R projects A and B’s particles onto one of the Bell states. R can thus “swap” entanglement to A and B. This protocol is essentially identical to the celebrated quantum teleportation protocol [33]; entanglement swapping is basically a teleportation of entanglement.

To complete the protocol, the Referee needs to communicate the result of his measurement \( r \)—by sending 2 bits of classical communication—to (say) Bob, who can then apply a suitable unitary local transformation to his qubit to finally share a definite Bell state with Alice, say \( |\Psi^+\rangle \). Upon receiving measurement settings \( x \) and \( y \) (represented by unit vectors on the Bloch sphere) and performing the corresponding projective measurements on their respective qubit, Alice and Bob obtain binary measurement outcomes \( a = \pm 1 \) and \( b = \pm 1 \), respectively. These outcomes exhibit nonlocal correlations of the form

\[
E(x, y) = P(a = b|x, y) - P(a \neq b|x, y) = -x \cdot y,
\]

with random marginals.

A classical simulation of this protocol in the bilocal scenario would then amount to the following [see Fig. 1 (ii)]: Alice and Bob receive as inputs the measurement directions \( x \) and \( y \), independently of the random variables \( \lambda_{AR} \) and \( \lambda_{RB} \) they may each share (independently) with R. After a finite amount of information exchange between the three parties, Alice and Bob produce their outputs which, after averaging over the shared random variables, must be correlated as in (1) [34]. At this point, it is instructive to recall the result of Massar et al. [32], which implies that correlations of the form (1) are impossible to simulate with finite communication when A and B only have finite shared randomness (in the sense that their shared randomness could be established with bounded communication)—even if they may each have an additional source of infinite randomness, independent for A and B. The present scenario may at first glance appear similar: initially, A and B each only have access to independent sources of infinite randomness, \( \lambda_{AR} \) and \( \lambda_{RB} \), respectively, shared with the Referee. After any finite exchange of communication between the parties (including R), Alice and Bob could only share some finite amount of randomness. Intuition suggests that the result of [32] implies that, from such randomness, correlations of the form (1) cannot be simulated with finite communication, and entanglement swapping is impossible to simulate in a bilocal manner [35]. However, the present scenario differs from that of [32] in that the third party, R, can share an infinite

![FIG. 1 (color online). (i) The scenario of entanglement swapping with two fully independent sources of \( |\Psi^+\rangle \) states. The Referee sends to Bob the result \( r \) of his Bell state measurement. Upon receiving these 2 bits of communication, Bob can apply the adequate unitary operation to his qubit such that Alice and Bob finally share a singlet state. (ii) The classical simulation of entanglement swapping in the bilocal scenario, i.e., with two uncorrelated sources of shared random variables \( \lambda_{AR} \) and \( \lambda_{RB} \). The three parties exchange messages symbolized by the thick dashed arrows. Here we present a simulation protocol using 9 bits of communication in total.](image-url)
amount of randomness with $A$ and $B$ independently—by having access to both $\lambda_{AR}$ and $\lambda_{RB}$—and can exchange some (finite number of) bits with $A$ and $B$. This seemingly subtle difference dramatically changes the situation: despite the above heuristic reasoning, entanglement swapping can be simulated with finite communication in a bilocal manner, as we now show.

**Simulation protocol.**—We start by deriving a protocol for the simulation of equatorial measurements $\mathbf{x} = (\cos \phi_A, \sin \phi_A, 0)$ and $\mathbf{y} = (\cos \phi_B, \sin \phi_B, 0)$. In this case, the correlation (1) is equivalent to

$$P(a = b | \phi_A, \phi_B) = \frac{1 - \cos(\phi_A - \phi_B)}{2} = \sin\left(\frac{\phi_A - \phi_B}{2}\right)^2.$$  

(2)

Note, in particular, that if $\phi_A = \phi_B$, then $P(a = b | \phi_A = \phi_B) = 0$, as expected from the anticorrelations of the singlet state.

Let us divide the equator of the Bloch sphere into $2m$ sectors of the same size, and assume that Alice and the Referee (the Referee and Bob) share a random variable $\lambda_{AR}$ ($\lambda_{RB}$), with $\lambda_{AR}$ and $\lambda_{RB}$ uniformly distributed in $[0, \frac{\pi}{m}]$. Let Alice tell Bob in which sector her setting (modulo $\pi$) lies, and send him the additional bit $c_A = \left[ \phi_A \text{mod} \frac{\pi}{m} \right]$ (we use the Iverson bracket, with $[E] = 1$ if the expression $E$ is true, $[E] = 0$ otherwise); let the Referee send to Bob the bit $c_R = [\lambda_{AR} < \lambda_{RB}]$; and let Bob calculate the bit $c_B = [\lambda_{RB} < (\phi_B \text{mod} \frac{\pi}{m})]$.

To warm up and gain some intuition, assume that Alice and Bob's settings both lie in $[0, \frac{\pi}{2}]$, and let Alice simply output $a = +1$. If $c_A = c_R = c_B$, then Bob knows that (with probability 1) $\phi_A \neq \phi_B$; let him then also (for now) output $b = a = +1$. On the other hand, if $c_A \neq c_R$ or $c_A\neq c_B$, it could be the case that $\phi_A = \phi_B$; to ensure that $P(a = b | \phi_A = \phi_B) = 0$, Bob must output $b = -a = -1$. The probability that Alice and Bob give the same output is then (assuming $\phi_A < \phi_B$; the case $\phi_A \geq \phi_B$ being similar)

$$P(a = b | \phi_A < \phi_B) = P(c_A = c_B = c_R | \phi_A < \phi_B)$$

$$= P(\phi_A < \lambda_{AR} < \lambda_{RB} < \phi_B | \phi_A < \phi_B)$$

$$= \int_{\lambda_{AR}}^{\phi_A} \frac{\lambda_{AR}}{\pi} d\lambda_{AR} \int_{\lambda_{AR}}^{\phi_B} \frac{\lambda_{RB}}{\pi} d\lambda_{RB}$$

$$= \frac{m^2}{2\pi^2} (\phi_A - \phi_B)^2.$$  

(3)

If $m \geq \frac{1}{\sqrt{2}}$, this probability is too large (for any $\phi_A, \phi_B \in [0, \frac{\pi}{m}]$), compared to the desired value of $\sin(\phi_A - \phi_B)^2$ (2). Now, one can actually make use of some freedom in the case $c_A = c_R = c_B$, and ask Bob to output $b = a = +1$ only with some probability $\rho$ (and to output $b = -a = -1$ with probability $1 - \rho$). By letting $\rho$ depend on $\phi_B$ and $\lambda_{RB}$, and take the particular form $\rho(\phi_B - \lambda_{RB}) = \frac{m^2}{\pi^2} \cos(\phi_B - \lambda_{RB})$, we obtain, as desired,

$$P(a = b | \phi_A, \phi_B) = \frac{m^2}{\pi^2} \int_{c_A}^{\phi_B} \frac{d\lambda_{RB}}{\pi} \int_{\lambda_{AR}}^{\phi_B} \frac{d\lambda_{RB}}{\pi} \rho(\phi_B - \lambda_{RB})$$

$$= \sin\left(\frac{\phi_A - \phi_B}{2}\right)^2.$$  

(4)

In order now to extend this protocol to all possible equatorial measurements $\phi_A, \phi_B \in [0, 2\pi]$, one needs to find adequate strategies for Bob (i.e., adequate functions $\rho(\phi_B - \lambda_{RB}) \in [0, 1]$) for all possible sectors where Alice and Bob's settings may lie, and for all possible values of the bits $c_A, c_R$ and $c_B$. We were able to find such strategies for the case $m = 4$; see Table I. This leads us to define the following protocol:

**Protocol 1.**—Let Alice and the Referee (the Referee and Bob) share a random variable $\lambda_{AR}$ ($\lambda_{RB}$), with $\lambda_{AR}$ and $\lambda_{RB}$ uniformly distributed in $[0, \frac{\pi}{4}]$. After reception of Alice and Bob's measurement settings $\phi_A, \phi_B$, the three parties proceed as follows:

(i) Alice calculates $a = \text{sign}(\sin \phi_A) = \pm 1$, $j_A = \left\lfloor \frac{\phi_A}{\pi} (\phi_B \text{mod} \pi) \right\rfloor \in [0, 1, 2, 3]$, $j_A' = (\phi_A - j_A \frac{\pi}{4} \text{mod} \pi) \in [0, \frac{\pi}{4}]$ (and $c_A = [\phi_A < \lambda_{AR}] \in [0, 1]$). She sends $j_A$ (2 bits) and $c_A$ (1 bit) to Bob, and outputs $a$.

<table>
<thead>
<tr>
<th>$j_A$</th>
<th>$c_B$</th>
<th>$c_R$</th>
<th>$\gamma$</th>
<th>$\phi_A$</th>
<th>$\phi_B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 0</td>
<td>0 0 0</td>
<td>0 0 0</td>
<td>$\frac{\pi}{18}$ cos $\gamma$</td>
<td>$\frac{\pi}{18}$ cos $\gamma$</td>
<td>0</td>
</tr>
<tr>
<td>0 0 1</td>
<td>0 0 1</td>
<td>0 0 1</td>
<td>$\frac{\pi}{18}$ cos $\gamma$</td>
<td>$\frac{\pi}{18}$ cos $\gamma$</td>
<td>0</td>
</tr>
<tr>
<td>0 1 1</td>
<td>0 1 1</td>
<td>0 1 1</td>
<td>$\frac{\pi}{18}$ cos $\gamma$</td>
<td>$\frac{\pi}{18}$ cos $\gamma$</td>
<td>0</td>
</tr>
<tr>
<td>1 0 0</td>
<td>1 0 0</td>
<td>1 0 0</td>
<td>$\frac{\pi}{18}$ cos $\gamma$</td>
<td>$\frac{\pi}{18}$ cos $\gamma$</td>
<td>0</td>
</tr>
<tr>
<td>1 1 0</td>
<td>1 1 0</td>
<td>1 1 0</td>
<td>$\frac{\pi}{18}$ cos $\gamma$</td>
<td>$\frac{\pi}{18}$ cos $\gamma$</td>
<td>0</td>
</tr>
</tbody>
</table>
(ii) The Referee calculates \( c_R = [\lambda_{AR} < \lambda_{RB}] \in \{0,1\} \) and sends it to Bob (1 bit).

(iii) After reception of \( j_A \), Bob calculates \( \beta = \text{sign}[\sin(\phi_B - j_A \frac{\pi}{2})] \) and \( \phi'_B = (\phi_B - j_A \frac{\pi}{2} \mod \pi) \in [0, \pi[. \) He determines the index \( j_B = \lfloor \frac{j_A}{2} \rfloor \in \{0,1,2,3\} \) of the sector where his angle \( \phi'_B \) lies, and the bit \( c_B = [\lambda_{RB} < \phi'_B - j_B \frac{\pi}{2}] \in \{0,1\} \). Depending on \( j_B, \ c_A, \ c_R, \ \phi'_B \) and \( \lambda_{RB} \), he outputs \( b = \beta \) with probability

\[
\varphi_{c_A,c_R}^{j_B}(\phi'_B - \lambda_{RB}), \quad \text{and} \quad b = -\beta \text{ with probability}
\]

\[
1 - \varphi_{c_A,c_R}^{j_B}(\phi'_B - \lambda_{RB}),
\]

for the functions \( \varphi_{c_A,c_R}^{j_B} \) defined in Table I.

As explicitly shown in the Supplemental Material [36], the above protocol gives the desired probability

\[
P(a = b | \phi_A, \phi_B) = \sin^2 \left( \frac{\alpha + \beta}{2} \right)
\]

for all possible equatorial measurements, using 4 bits of communication. It can then be extended in the following way to all measurement directions on the Bloch sphere, using a similar technique as in [10]:

**Protocol 2.**—For measurement directions \( x = (\sin \theta_A \cos \phi_A, \sin \theta_A \sin \phi_A, \cos \theta_A) \) and \( y = (\sin \theta_B \cos \phi_B, \sin \theta_B \sin \phi_B, \cos \theta_B) \), the three parties

(i) run Protocol 1 with input angles \( \phi_A \) and \( \phi_B \); Alice and Bob obtain intermediate outputs \( a_0 \) and \( b_0 \).

(ii) run Protocol 1 a second time (using a new set of in independent variables \( \lambda_{AR}, \lambda_{RB} \)), with the outputs \( a_1 \) and \( b_1 \) of this run and

This second protocol now simulates the desired correlation \( E(x, y) = -x \cdot y \) for all possible projective measurements by Alice and Bob, with 8 bits of communication; for more details on the calculations, see Supplemental Material. Note that Protocols 1 and 2 do not simulate the correct marginals. In order to randomize the marginals, Alice can—at the very end of the protocol—generate a random bit and send it to Bob; depending on the value of this bit, they will both flip their outcomes or not. All in all, the entanglement swapping correlations can thus be simulated with 9 bits of communication.

**Discussion.**—We thus have proved that remarkably, the entanglement swapping process can be simulated with bounded communication, even in a bilocal scenario where Alice and Bob are (as in the quantum case) completely uncorrelated before the protocol is run, and therefore do not have any prior shared randomness. Our protocol provides an upper bound on the nonlocality of entanglement swapping in terms of its communication cost. It is an open question whether fewer bits of communication are actually sufficient; it might indeed be possible to simulate equatorial measurements more efficiently than with Protocol 1, or to find a more direct protocol that does not treat separately the azimuth and zenith angles of the measurement settings, more in the spirit of the Toner-Bacon simulation protocol for singlet correlations [13].

Next, it is natural to consider the simulation of multistage entanglement swapping, which is essential for long distance quantum communication. Now, \( N \) referees (\( R_1, R_2, \ldots, R_N \)) are placed on a line between Alice and Bob. Two neighboring referees share a singlet state, while \( R_1 \) and \( R_N \) share singlet states with \( A \) and \( B \), respectively; each referee performs a joint measurement, leaving at the end the particles of Alice and Bob entangled. Whereas the quantum protocol has a straightforward and nice iterative character, we were not able to find a simulation protocol with a finite amount of communication in a \( (N + 1) \)-locality scenario [29]. Consider for instance the case with one additional referee \( R_2 \). Analogously to our Protocol 1, assume that Alice and \( R_1 \) share the random variable \( \lambda_{AR_1, R_1} \), \( R_1 \) and \( R_2 \) share \( \lambda_{R_1, R_2} \), and \( R_2 \) and Bob share \( \lambda_{R_2, B} \), all uniformly and independently distributed on some interval \([0, \frac{\pi}{m}]\). After some finite communication, Bob could for instance [as in our first attempt, before Eq. (3)] output \( b = a = 1 \) if and only if \( [\phi_A < \lambda_{AR_1}] = [\lambda_{AR_1} < \lambda_{R_1, R_2}] = [\lambda_{R_1, R_2} < \lambda_{R_2, B}] = [\lambda_{R_2, B} < \phi_B] \). This would result in the probability \( P(a = b | \phi_A, \phi_B) \in \left[0, \frac{\pi}{m} \right] = \frac{m^2}{2 \pi} |\phi_A - \phi_B|^2 \), which scales cubically with \( |\phi_A - \phi_B| \), and is therefore too small when \( \phi_A \) is close to \( \phi_B \). It is unclear how to change the cubic scaling with finite communication. The following questions remain open: can multistage entanglement swapping be simulated with finite communication? Or can one prove, that above a certain value of \( N \), an infinite amount of communication is necessary?

We thank Jean-Daniel Bancal, Yeong-Cherng Liang, Stefano Pironio, Tim Ráez, and Ronald de Wolf for discussions. This work was supported by a UQ Postdoctoral Research Fellowship, the NSF grant CCF-0832787, the UK EPSRC, the EU DIQIP, the EU FP7 grant project 255961 QCS, Canada’s NSERC and CIFAR, the Swiss NCCR-QSIT, the US ARO, and the European ERC-AG QORE.

---

[34] Note that we do not explicitly consider the simulation of the Referee’s Bell state measurement (BSM). One could easily include this in the simulation protocol, by letting for instance the Referee and Bob share a random result for the BSM, and by letting Bob apply an appropriate transformation to his measurement setting directly.