

Quantum superposition of the order of parties as a communication resource

Adrien Feix, Mateus Araújo, and Časlav Brukner

Faculty of Physics, University of Vienna, Boltzmannngasse 5, 1090 Vienna, Austria

and Institute for Quantum Optics and Quantum Information (IQOQI), Boltzmannngasse 3, 1090 Vienna, Austria

(Received 31 August 2015; published 20 November 2015)

In a variant of communication complexity tasks, two or more separated parties cooperate to compute a function of their local data, using a limited amount of communication. It is known that communication of quantum systems and shared entanglement can increase the probability for the parties to arrive at the correct value of the function, compared to classical resources. Here we show that quantum superpositions of the direction of communication between parties can also serve as a resource to improve the probability of success. We present a tripartite task for which such a superposition provides an advantage compared to the case where the parties communicate in a fixed order. In a more general context, our result also provides semi-device-independent certification of the absence of a definite order of communication.

DOI: [10.1103/PhysRevA.92.052326](https://doi.org/10.1103/PhysRevA.92.052326)

PACS number(s): 03.67.Hk, 03.65.Ta, 03.67.Dd

I. INTRODUCTION

In its short history, the field of quantum information has been very successful in discovering and explaining differences between classical and quantum information processing—in particular a variety of advantages that the use of quantum resources confers over the use of classical resources [1].

Quantum resources provide an important benefit to *communication complexity tasks* [2–4] where two or more separated parties compute a function of their input strings, seeking to maximize the probability of success under the constraint of limited communication between them. Communicating quantum bits and sharing entanglement are two well-known resources that can be used to improve success probability in such scenarios [5].

A novel type of quantum resource—the *quantum switch*—allows for the order in which quantum gates are applied to be in a quantum superposition, using an auxiliary quantum system that coherently controls the order in which the gates are applied [6]. The quantum switch has been shown to reduce the required number of queries to “blackbox” unitaries required to solve certain computational tasks [6–10].

Here we find that the *quantum control of the direction of communication between parties* is a useful resource in communication complexity protocols. We demonstrate this by considering an explicit three-party communication task, in which Alice and Bob are each given input *trits* and Charlie has to determine whether or not they are equal. They are not allowed to share entanglement and the total communication is restricted to two qubits. We show that when the order of communication between parties is fixed (or classically mixed), the success probability is bounded below one. However, using the quantum switch to superpose the direction of communication between Alice and Bob, there exists a protocol that always succeeds.

II. PROCESS MATRIX FORMALISM

Superpositions of the direction of communication are readily described in the *process matrix formalism*, first introduced in Ref. [11]. We will briefly review some of its key aspects; for

an extensive introduction to the subject, we refer the reader to Ref. [12].

The most general quantum operation, a completely positive (CP) map, maps a density operator $\rho_{A_I} \in A_I$ to a density operator $\rho_{A_O} \in A_O$. Here, A_I (A_O) denotes the space of linear operators on the Hilbert space \mathcal{H}^{A_I} (\mathcal{H}^{A_O}); in general, the dimensions d_{A_I} and d_{A_O} of \mathcal{H}^{A_I} and \mathcal{H}^{A_O} do not have to be equal.

Using the Choi-Jamiołkowski [13,14] (CJ) isomorphism (where we follow the convention of Ref. [12]), one can represent a CP map $\mathcal{M}_A : A_I \rightarrow A_O$ as an operator,

$$\mathcal{M}_A := [(\mathcal{I} \otimes \mathcal{M}_A)(|I\rangle\langle I|)]^T \in A_I \otimes A_O, \quad (1)$$

where \mathcal{I} is the identity map and $|I\rangle := \sum_{j=1}^{d_{H_I}} |jj\rangle \in \mathcal{H}_I \otimes \mathcal{H}_I$ is a non-normalized, maximally entangled state and the superscript T denotes transposition. The inverse transformation is

$$\mathcal{M}_A(\rho) = \text{tr}_I[(\rho \otimes \mathbb{1})\mathcal{M}_A]^T. \quad (2)$$

Similarly, for two completely positive maps $\mathcal{M}_A : A_I \rightarrow A_O$ and $\mathcal{M}_B : B_I \rightarrow B_O$, the joint CJ matrix is the tensor product of the CJ matrix of the individual maps $\in A_I \otimes A_O \otimes B_I \otimes B_O$.

One can use this isomorphism to conveniently represent higher-order operations [11,15–18], which map quantum maps to quantum maps. These “superoperators” or “processes” can also be represented as *CJ matrices* themselves, by applying the CJ isomorphism repeatedly.

One can also meaningfully define operations acting *jointly on states and operations*. We will restrict our attention to the class of processes \mathcal{W} mapping *two CP maps and two states to two states*:

$$\begin{aligned} \mathcal{W}(\mathcal{M}_A, \mathcal{M}_B, \sigma_C, \rho_T) &= \text{tr}_{A,B}\{W \cdot \mathcal{M}_A \otimes \mathcal{M}_B \otimes \sigma_C \otimes \rho_T\} \\ &= \rho'_{CT}. \end{aligned} \quad (3)$$

III. PROCESSES WITH AND WITHOUT A DEFINITE ORDER OF COMMUNICATION

Quantum circuits form a well-known class of processes in which gates corresponding to the operations \mathcal{M}_A and \mathcal{M}_B

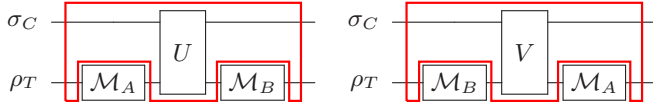


FIG. 1. (Color online) Examples of quantum circuits (in red) mapping two CPTP maps $\mathcal{M}_A, \mathcal{M}_B$ and two states σ_C, ρ_T to a state ρ'_{CT} . The order of applying gates is well defined— $A \leq B$ for the left circuit and $B \leq A$ for the right one.

appear in a fixed order (as depicted in Fig. 1). Either \mathcal{M}_A is applied before \mathcal{M}_B (corresponding to processes of the type $\mathcal{W}_{A \leq B}$) or \mathcal{M}_B is applied before \mathcal{M}_A (corresponding to processes $\mathcal{W}_{B \leq A}$) [17]. Identifying \mathcal{M}_A (\mathcal{M}_B) with Alice’s (Bob’s) operation, these “ordered processes” correspond to a definite order of signaling between Alice and Bob. More generally, we will also refer to classical mixtures thereof, which correspond to a classical random variable controlling the order of the process,

$$\mathcal{W}_{\text{ord.}} := p\mathcal{W}_{A \leq B} + (1-p)\mathcal{W}_{B \leq A}, \quad 0 \leq p \leq 1, \quad (4)$$

as “causally separable processes” [12,19].¹

Not all physically implementable processes are causally separable: The *quantum switch*, first introduced by Chiribella *et al.* [6], corresponds to the process \mathcal{W}_{sw} , which applies two CP maps to a target system ρ_T in an order that is controlled by the value of a quantum control system σ_C . The quantum switch for pure target and control states $|\psi\rangle_T, |\phi\rangle_C$ and unitary operations U_A (U_B) on Alice’s (Bob’s) side is given by

$$\mathcal{W}_{\text{sw}}(U_A, U_B, |\phi\rangle_C, |\psi\rangle_T) = \langle 0|\phi\rangle |0\rangle_C U_B U_A |\psi\rangle_T + \langle 1|\phi\rangle |1\rangle_C U_A U_B |\psi\rangle_T \quad (5)$$

and can be extended by linearity to mixed states and general CP maps on Alice’s and Bob’s side [8]. It is neither of the type $\mathcal{W}_{A \leq B}$ nor of the type $\mathcal{W}_{B \leq A}$. Since it is an extremal process, it also cannot be decomposed according to Eq. (4), which shows that there is no definite order of signaling for the quantum switch [12]. Rather, one should think of it as a *coherent superposition* of circuits or of directions of communication, controlled by a control qubit:

$$\frac{1}{\sqrt{2}} \left(|0\rangle_C \text{---} \boxed{U_A} \text{---} \boxed{U_B} \text{---} + |1\rangle_C \text{---} \boxed{U_B} \text{---} \boxed{U_A} \text{---} \right). \quad (6)$$

It has been shown that using such a quantum control of circuits provides an advantage in query complexity for certain computational tasks [6–9]. It has also been implemented experimentally, using an interferometric setup [10].

IV. THE TRIPARTITE HAMMING GAME

To demonstrate the relevance of the quantum switch in communication scenarios, we will introduce a communication game closely related to the distributed Deutsch-Josza promise

¹Note that the definition of causal separability in Ref. [19] slightly differs from ours.

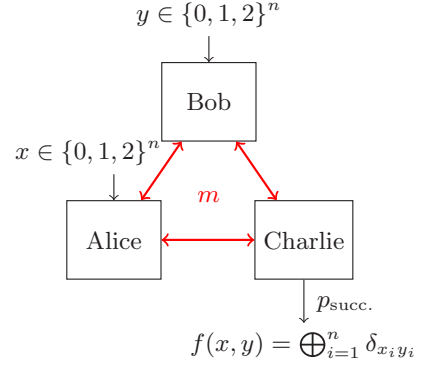


FIG. 2. (Color online) Tripartite $(n \log_2 3, m)$ -Hamming game where Alice and Bob receive input strings of the length $n \log_2 3$ bits, and Charlie has to compute $f(x, y)$. The total communication is m bits or qubits; no entanglement is preshared.

problem [5,20,21], the *simultaneous message passing* (SMP) model [2,22], and *random access codes* (RACs) [23–27].

In our tripartite game—as for the SMP—Alice and Bob receive input strings and Charlie computes a function of them. Communication between all of the parties and shared (classical) randomness are also allowed. Charlie has to compute the *parity of the Hamming distance of Alice’s and Bob’s input strings*, generalizing the function of the distributed Deutsch-Josza promise problem (here, however, *no promise* on the Hamming distance of the inputs is required).

More precisely, Alice and Bob both are given n trits ($x \in \{0, 1, 2\}^n$ and $y \in \{0, 1, 2\}^n$, respectively), and Charlie computes the Hamming parity $f(x, y)$ defined as

$$f(x, y) := \bigoplus_{i=1}^n \delta_{x_i y_i}. \quad (7)$$

In addition, the total length of the transcript communicated by Alice, Bob, and Charlie is restricted to be m bits (or qubits). This defines the $(n \log_2 3, m)$ -Hamming game depicted in Fig. 2; the average success probability associated to it will be referred to as p_{succ} .

Next we show that for the $(\log_2 3, 2)$ -Hamming game (which is equivalent to the equality game for trits), the success probability is bounded below one when Alice, Bob, and Charlie are restricted to using a causally separable process, i.e., when the direction of signaling is fixed or controlled by a classical random variable independent of the inputs. In contrast, using quantum control over the direction of signaling—the quantum switch—Charlie can always compute $f(x, y)$. This demonstrates that causally nonseparable processes are useful resources for communication tasks.

We will first consider the case where Alice, Bob, and Charlie can only implement *classical* operations and use a process with a definite order of communication (or a mixture thereof). The optimal strategy involves Alice encoding her input trit x into a bit $a(x)$ and sending it to Bob, who sends the function $b(a, y)$ to Charlie, who finally outputs a function $g(b)$.

The deterministic strategies are the vertices of a convex polytope in the nine-dimensional (all possible combinations of x and y) space of probabilities $p(c|x, y)$. Given that Alice,

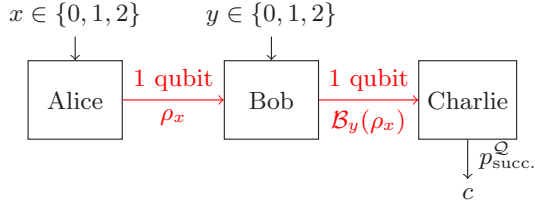


FIG. 3. (Color online) Optimal causally separable protocol for the equality game, where no entanglement is shared among the parties.

Bob, and Charlie share randomness, they can probabilistically combine deterministic strategies, reaching every point inside the convex polytope.

For equally distributed inputs, the probability of success for Charlie to output $f(x, y) = \delta_{x,y}$ is bounded by [28]

$$p_{\text{succ}}^c := \frac{1}{9} \sum_{x,y} p(c = \delta_{x,y} | x, y) \leq \frac{7}{9}. \quad (8)$$

One deterministic strategy saturating this bound consists of Alice encoding whether or not her input is 0 [$a(x) = \delta_{x,0}$] and Bob answering 1 only if he is sure that he and Alice both have input 0 [$b(a, y) = \delta_{y,0} \delta_{a,1}$]. Charlie simply returns Bob's answer. This strategy will fail only for input pairs $x = y = 1$ and $x = y = 2$.

We now turn to the case where Alice, Bob, and Charlie use a causally separable process (consisting of quantum channels) and have access to quantum operations, as shown in Fig. 3. The parties are allowed to share randomness but not entanglement. In the optimal protocol with two qubits of communication in total, Alice encodes her input trit into a qubit $x \mapsto \rho_x$ and Bob applies a completely positive trace-preserving (CPTP) map B_y for each value of his input trit y onto the incoming qubit; Charlie then performs a two-outcome positive operator-valued measure (POVM) $\{C_m\}$ on the resulting state.

For equally distributed inputs, the probability of success for causally separable strategies is bounded by

$$p_{\text{succ}}^Q \leq \frac{1}{9} \max_{\rho_x, \{B_y\}, \{C_m\}} \left(\sum_x \text{tr}\{C_1 B_x(\rho_x)\} + \sum_{x \neq y} \text{tr}\{C_0 B_y(\rho_x)\} \right), \quad (9)$$

which, in the Appendix, we prove to be

$$p_{\text{succ}}^Q \leq \frac{5}{6}. \quad (10)$$

Here, an optimal state preparation by Alice is

$$|a_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |a_1\rangle = \sin \frac{\pi}{8} |0\rangle + e^{i\pi/4} \cos \frac{\pi}{8} |1\rangle, \\ |a_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{-i\pi/4} |1\rangle), \quad (11)$$

where $\rho_x = |a_x\rangle\langle a_x|$. Bob projectively measures in the basis $|a_y\rangle, |a_y^\perp\rangle$, where $|a_y^\perp\rangle$ is orthogonal to $|a_y\rangle$, and prepares the state $|x+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ or $|x-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, depending on the outcome.

Charlie simply applies a projective measurement in $|x\pm\rangle$ basis, the outcome of which constitutes his guess c . The

TABLE I. Conditional probabilities of success with a causally separable process, for the optimal strategy (11), reaching $p_{\text{succ}}^Q = \frac{5}{6}$.

x, y	00	01	02	10	11	12	20	21	22
$p^Q(c = \delta_{x,y} xy)$	1	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$	1	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{3}{4}$	1

probability distribution arising from the optimal quantum strategy is shown in Table I.

We now show that when Alice, Bob, and Charlie can use the quantum switch to implement *quantum* control over the direction of communication between Alice and Bob, they can violate Eq. (10) maximally ($p_{\text{succ}}^{Q\text{-sw}} = 1$).

Alice and Bob apply unitaries U_A^x, U_B^y to a target system and the quantum switch coherently superposes the order in which they are applied. Charlie receives the resulting state and applies a two-outcome projective measurement Π^+, Π^- . Since Alice and Bob only have access to a qubit subspace, they each only send one qubit out of their laboratory, while Charlie sends no system out. The total communication between Alice, Bob, and Charlie is $m \leq \log_2(d_{A_0} d_{B_0} d_{C_0}) = 2$ qubits, in accordance with the assumptions of the $(\log_2 3, 2)$ -Hamming game.

Alice and Bob choose a Pauli gate corresponding to their input trit $U_A^i = U_B^i = \sigma_i$ and the control state is $|\phi\rangle_C = |x+\rangle_C$ (the state $|\psi\rangle_T$ is irrelevant); see Fig. 4. Inserting this into Eq. (5), Charlie receives the state

$$\mathcal{W}_{\text{sw}}(\sigma_x, \sigma_y, |x+\rangle_C, |\psi\rangle_T) \\ = \frac{1}{\sqrt{2}}(|0\rangle_C \sigma_y \sigma_x |\psi\rangle_T + |1\rangle_C \sigma_x \sigma_y |\psi\rangle_T) \\ = \frac{1}{2\sqrt{2}}(|x-\rangle_C [\sigma_y, \sigma_x] |\psi\rangle_T + |x+\rangle_C \{\sigma_y, \sigma_x\} |\psi\rangle_T), \quad (12)$$

where $[\cdot]$ is the commutator and $\{\cdot\}$ is the anticommutator.

If Charlie chooses a projective measurement on the resulting control system C , with $\Pi^+ = |x+\rangle\langle x+|_C$ and $\Pi^- = |x-\rangle\langle x-|_C$, he can determine whether $[\sigma_y, \sigma_x] = 0$ or $\{\sigma_y, \sigma_x\} = 0$ (because of the commutation relations of the Pauli matrices, one of them is always the case). If the former is true, Charlie deduces that $x = y$, otherwise that $x \neq y$. Hence,

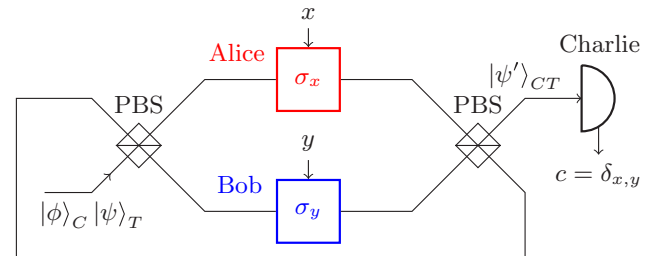


FIG. 4. (Color online) Linear optical implementation of the protocol using the quantum switch [9,29]. The control state $|\phi\rangle_C$ is encoded in polarization and the target state $|\psi\rangle_T$ in another photonic degree of freedom. Alice and Bob apply Pauli operators on the target system depending on their input x and y . Charlie performs a measurement in the $|x\pm\rangle$ basis on the outgoing control system C and consequently outputs $\delta_{x,y}$. Note that in the experiment of Ref. [10], the control state was instead encoded in path.

he can compute $f(x, y) = \delta_{x,y}$ with unit probability, violating the bound (10).

Note that the protocol can be extended to any $(m \log_2 3, 2m)$ Hamming game (Alice and Bob each are given m trits and have access to an m -qubit system). Alice and Bob apply $\bigotimes_i \sigma_{x_i}$ and $\bigotimes_i \sigma_{y_i}$ respectively; Charlie, by measuring the control qubit in the $|x \pm\rangle$ basis, can still determine whether $[\bigotimes_i \sigma_{x_i}, \bigotimes_i \sigma_{y_i}]$ or $\{\bigotimes_i \sigma_{x_i}, \bigotimes_i \sigma_{y_i}\}$ is zero. Since, for each different trit, a factor of -1 appears when permuting the corresponding Pauli matrices, an even number of differences in the trit strings of Alice and Bob will result in a vanishing commutator, and an odd number of differences will result in a vanishing anticommutator. Using the quantum switch, Charlie can therefore always find the Hamming parity (7).

V. CONCLUSIONS

We demonstrated that a quantum superposition of the direction of communication between parties is a useful resource in communication complexity problems. This was explicitly shown for the $(\log_2 3, 2)$ -Hamming game, where the probability of success for processes with a definite or classically mixed order of signaling is violated by using the quantum switch as a resource. The result points to the necessity for a general resource theory of communication to account for superpositions of the direction of communication. Note that having access to the quantum switch is *not* equivalent to sharing a maximally entangled state between Alice and Bob—for instance, the latter (through dense coding [30]) makes computing *any* binary function of two trits for Alice and Bob possible by exchanging just two qubits of communication, which is impossible with the quantum switch.

Our result also provides a *semi-device-independent* [31,32] way of certifying the causal nonseparability of a process, where Alice's and Bob's system is known to have (at most) a given dimension, but the operations themselves are not trusted. It lies between the stronger fully *device-independent* certification of causal nonseparability [11,19,33]—which was already shown to be impossible for the quantum switch [12,19]—and the weaker *device-dependent* certification through *causal witnesses* [12].

It would be interesting to improve the *scaling* (with the length of the inputs) of the reduction in communication achieved by using the quantum switch. To compute Hamming parity of two m -trit input strings, $2m$ qubits need to be exchanged using the quantum switch; making use of a process with a fixed order of communication, one can easily construct a protocol requiring only $m(1 + \log_2 3)$ qubits. Hence, both resources result in the same asymptotic scaling of communication for the Hamming game.

ACKNOWLEDGMENTS

We would like to thank Fabio Costa, Michael Cuffaro, Sam Fletcher, Jacques Pienaar, Michal Sedláč, Christopher Timpson, and Harald Weinfurter for useful discussions. We acknowledge support from the European Commission project RAQUEL (Project No. 323970); the Austrian Science Fund (FWF) through the Special Research Programme FoQuS,

the Doctoral Programme CoQuS and Individual Project (No. 2462), FQXi, and the John Templeton Foundation.

APPENDIX: PROOF OF THE CAUSALLY SEPARABLE QUANTUM BOUND ON THE EQUALITY GAME

Here we prove the validity of the quantum bound $p_{\text{succ}}^Q \leq \frac{5}{6}$. We start with Eq. (9):

$$p_{\text{succ}}^Q \leq \frac{1}{9} \max_{\rho_x, \{B_y\}, \{C_m\}} \left(\sum_x \text{tr}\{C_1 B_x(\rho_x)\} + \sum_{xy, x \neq y} \text{tr}\{C_0 B_y(\rho_x)\} \right). \quad (\text{A1})$$

We now use the fact that the POVM preceded by a CPTP map is still a POVM (the elements of which we will call B_x^0 and B_x^1), which can be thought of as being applied by Bob and Charlie together. This allows us to drop the optimization over $\{C_m\}$:

$$p_{\text{succ}}^Q \leq \frac{1}{9} \max_{\rho_x, \{B_y^{0,1}\}} \left(\sum_x \text{tr}\{B_x^1 \rho_x\} + \sum_{xy, x \neq y} \text{tr}\{B_y^0 \rho_x\} \right). \quad (\text{A2})$$

Since $\text{tr}\{B_x^0 \rho\} = 1 - \text{tr}\{B_x^1 \rho\}, \forall x$ (the probabilities sum to one), we can rewrite (A2) as

$$9p_{\text{succ}}^Q \leq 6 + \max_{\rho_x, \{B_y^1\}} \sum_y \text{tr} \left\{ B_y^1 \left(\rho_y - \sum_{x, x \neq y} \rho_x \right) \right\}. \quad (\text{A3})$$

We notice that each optimization over B_y^1 is independent; similarly to the one for optimal state distinguishability [1], we find that the optimal POVM elements B_y^1 are projectors on the positive eigenvalue subspace of $\rho_y - \sum_{x, x \neq y} \rho_x$. Using the Bloch vector decomposition $\rho_x = (\mathbb{1} + \boldsymbol{\sigma} \cdot \mathbf{a}_x)/2$, this leads to the result

$$p_{\text{succ}}^Q \leq \frac{1}{2} + \frac{1}{18} \max_{\|\mathbf{a}_x\|_2 \leq 1, \mathbf{a}_x \in \mathbb{R}^3} (\|\mathbf{a}_0 - \mathbf{a}_1 - \mathbf{a}_2\|_2 + \|\mathbf{a}_1 - \mathbf{a}_0 - \mathbf{a}_2\|_2 + \|\mathbf{a}_2 - \mathbf{a}_0 - \mathbf{a}_1\|_2). \quad (\text{A4})$$

Choosing $\mathbf{a}_0 = (1, 0, 0)^T$, parametrizing $\mathbf{a}_1, \mathbf{a}_2$ using spherical coordinates, and optimizing (A4), the analytical maximum turns out to be

$$p_{\text{succ}}^Q \leq \frac{5}{6},$$

with the optimal preparation and measurement strategies given in Eq. (11). Charlie measures in the $|x \pm\rangle$ basis; the channels of Bob are explicitly given by

$$\begin{aligned} B_0(\rho) &= \Pi_0^+ \rho \Pi_0^+ + \Pi_0^- \rho \Pi_0^-, \\ B_1(\rho) &= U_1 \Pi_1^+ \rho \Pi_1^+ U_1^\dagger + U_1 \Pi_1^- \rho \Pi_1^- U_1^\dagger, \\ B_2(\rho) &= U_2 \Pi_2^+ \rho \Pi_2^+ U_2^\dagger + U_2 \Pi_2^- \rho \Pi_2^- U_2^\dagger, \end{aligned} \quad (\text{A5})$$

where $\Pi_0^+ = |a_0\rangle\langle a_0|, \Pi_1^+ = |a_1\rangle\langle a_1|, \Pi_2^+ = |a_2\rangle\langle a_2|$ and the corresponding $\Pi_{0,1,2}^- = \mathbb{1} - \Pi_{0,1,2}^+$. The unitaries $U_{1,2}$ correspond to a basis transformation such that $U_{1,2} |a_{1,2}\rangle = |a_0\rangle$.

- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- [2] A. C.-C. Yao, *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing* (ACM, New York, 1979), pp. 209–213.
- [3] A. C.-C. Yao, *Proceedings of the 34th Annual Symposium on Foundations of Computer Science, Palo Alto, CA* (IEEE, Piscataway, New Jersey, 1993), pp. 352–361.
- [4] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, Cambridge, 2006).
- [5] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, *Rev. Mod. Phys.* **82**, 665 (2010).
- [6] G. Chiribella, G. M. D’Ariano, P. Perinotti, and B. Valiron, *Phys. Rev. A* **88**, 022318 (2013).
- [7] T. Colnaghi, G. M. D’Ariano, S. Facchini, and P. Perinotti, *Phys. Lett. A* **376**, 2940 (2012).
- [8] G. Chiribella, *Phys. Rev. A* **86**, 040301 (2012).
- [9] M. Araújo, F. Costa, and Č. Brukner, *Phys. Rev. Lett.* **113**, 250402 (2014).
- [10] L. M. Procopio, A. Moqanaki, M. Araújo, F. Costa, I. Alonso Calafell, E. G. Dowd, D. R. Hamel, L. A. Rozema, C. Brukner, and P. Walther, *Nat. Commun.* **6**, 7913 (2015).
- [11] O. Oreshkov, F. Costa, and Č. Brukner, *Nat. Commun.* **3**, 1092 (2012).
- [12] M. Araújo, C. Branciard, F. Costa, A. Feix, C. Giarmatzi, and Č. Brukner, *New J. Phys.* **17**, 102001 (2015).
- [13] M.-D. Choi, *Linear Alg. Appl.* **10**, 285 (1975).
- [14] A. Jamiołkowski, *Rep. Math. Phys.* **3**, 275 (1972).
- [15] G. Gutoski and J. Watrous, *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing* (ACM, New York, 2007), pp. 565–574.
- [16] G. Chiribella, G. M. D’Ariano, and P. Perinotti, *Europhys. Lett.* **83**, 30004 (2008).
- [17] G. Chiribella, G. M. D’Ariano, and P. Perinotti, *Phys. Rev. A* **80**, 022339 (2009).
- [18] M. S. Leifer and R. W. Spekkens, *Phys. Rev. A* **88**, 052130 (2013).
- [19] O. Oreshkov and C. Giarmatzi, [arXiv:1506.05449](https://arxiv.org/abs/1506.05449).
- [20] D. Deutsch and R. Jozsa, *Proc. R. Soc. London A* **439**, 553 (1992).
- [21] H. Buhrman, R. Cleve, and A. Wigderson, *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing* (ACM, New York, 1998), pp. 63–68.
- [22] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, *Phys. Rev. Lett.* **87**, 167902 (2001).
- [23] S. Wiesner, *SIGACT News* **15**, 78 (1983).
- [24] A. Nayak, *Proceedings of the 40th Annual Symposium on Foundations of Computer Science* (IEEE, Piscataway, New Jersey, 1999), pp. 369–376.
- [25] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, *J. ACM* **49**, 496 (2002).
- [26] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, *New J. Phys.* **8**, 129 (2006).
- [27] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, [arXiv:0810.2937](https://arxiv.org/abs/0810.2937).
- [28] Note that it is also a facet of the polytope since it is saturated by vertices spanning an eight-dimensional affine subspace.
- [29] G. Chiribella, R. Ioniciu, T. Jennewein, and D. Terno (private communication).
- [30] C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).
- [31] Y.-C. Liang, T. Vértesi, and N. Brunner, *Phys. Rev. A* **83**, 022108 (2011).
- [32] M. Pawłowski and N. Brunner, *Phys. Rev. A* **84**, 010302 (2011).
- [33] C. Branciard, M. Araújo, A. Feix, F. Costa, and Č. Brukner, [arXiv:1508.01704](https://arxiv.org/abs/1508.01704).