A Letters Journal Exploring the Frontiers of Physics

October 2013

EPL, **104** (2013) 20006
doi: 10.1209/0295-5075/104/20006

www.epljournal.org

Universality of computation in real quantum theory

A. Belenchia[1], G. M. D'Ariano[2,3] and P. Perinotti[2,3]

[1] *SISSA - via Bonomea 265, 34136 Trieste, Italy*
[2] *QUIT Group, Dipartimento di Fisica, Università di Pavia - via Bassi 6, 27100 Pavia, Italy*
[3] *Istituto Nazionale di Fisica Nucleare, Gruppo IV - via Bassi 6, 27100 Pavia, Italy*

received 9 August 2013; accepted in final form 28 October 2013
published online 25 November 2013

PACS 03.67.-a – Quantum information
PACS 03.65.Ta – Foundations of quantum mechanics; measurement theory
PACS 03.67.Ac – Quantum algorithms, protocols, and simulations

Abstract – Recently de la Torre *et al.* (*Phys. Rev. Lett.*, **109** (2012) 090403) reconstructed Quantum Theory from its local structure on the basis of local discriminability and the existence of a one-parameter group of bipartite transformations containing an entangling gate. This result relies on universality of any entangling gate for quantum computation. Here we prove universality of C-NOT with local gates for Real Quantum Theory (RQT), showing that the universality requirement would not be sufficient for the result, whereas local discriminability and the local qubit structure play a crucial role. For reversible computation, generally an extra rebit is needed for RQT. As a by-product we also provide a short proof of universality of C-NOT for CQT.

Introduction. – In recent years quantum information has spawned an unprecedented revival of interest in quantum foundations, providing original lines of research based on the surprising power of quantum theory as a model for information processing. This has led many authors to believe that "information" is the key to the solution of the mystery of quantum mechanics [1,2]. Along these lines the seminal work of Hardy [3] has opened the way to the new axiomatization program [4–7], including the derivation of the theory from information-theoretical principles [8,9].

Some of the attempts at an informational axiomatization explored the possibility of deriving the bipartite correlations of the theory from the local qubit structure [10], however this approach in the absence of further restrictions lead to the inclusion of spurious correlations for more than two systems. Reference [11] has then reconstructed quantum theory in this way, with the addition of local discriminability and the existence of a one-parameter group of bipartite transformations containing an entangling gate. For the derivation of this result the universality of entangling gates for quantum computation [12,13] plays a crucial role.

The existence of a universal gate set with a single bipartite gate is characteristic of quantum computation, as opposed to the classical one [14–16]. Since universality of a bipartite gate plays a crucial role in the result of ref. [11], one may wonder if it is specific only of quantum theory, or it holds instead also for other probabilistic theories, in the absence of the requirements of local discriminability and the local qubit structure, as is the case, *e.g.*, of RQT. Local discriminability, in particular, plays an important role in the classification of probabilistic theories (for a thorough exploration of local tomography, which is an equivalent formulation of local discriminability, see ref. [17]).

In the present letter we will prove that universality of C-NOT with local gates holds indeed also for RQT. Differently from Complex Quantum Theory (CQT), for RQT generally an extra rebit is needed for reversible computation. We formulate universal computation with a single bipartite gate as an informational axiom in the context of general probabilistic theories, then focusing on CQT and RQT only, and providing simple proofs of universality for both theories. The simplified proof is useful also in the complex case, since it provides a much shorter derivation than the original ones [13–16]. In the real case, an interesting feature pops up, which is the requirement of a single overhead rebit for the circuit implementation of arbitrary orthogonal (*i.e.* real unitary) transformations. The extra qubit is needed in order to make the determinant positive for all the orthogonal matrices representing circuits on the input register.

The presence of an extra qubit is relevant also in the comparison of quantum computation with complex and real qubits, as in ref. [18], where the equivalence of the two models is established. Interestingly, the extra real qubit in this context is needed in order to account for the real and imaginary part of the state of the simulated complex input registers, which is unrelated to the positive determinant issue of the present letter. Moreover, in ref. [18] a notion of universality is introduced, in terms of the possibility of simulating CQT through RQT circuits. However, this notion is different from the universality property used here, which is based on the decomposition of circuits of RQT.

Universal gate sets. – We say that a general probabilistic theory admits computation with a *strongly universal* bipartite gate if every reversible transformation of N elementary systems (*i.e.* bits, qubits, rebits, etc.) can be perfectly simulated by a circuit of N elementary systems made only of local reversible transformations and sufficiently many uses of the bipartite gate. We say that the theory admits a *weakly universal* bipartite gate if every reversible transformation of N elementary systems can be perfectly simulated by a circuit of $N + p(N)$ elementary systems made only of local reversible transformations and sufficiently many uses of a single bipartite gate, discarding the auxiliary $p(N)$ systems, where $p(x)$ is a polynomial in x.

Strong universality in complex quantum theory. We provide now a simplified proof that the C-NOT is strongly universal for computation in CQT.

The elementary system in quantum computation is the qubit. The Hilbert space for a register of N qubits is $\mathbb{C}^{2^N}$, and its reversible transformations form the Lie group $\mathbf{SU}(2^N)$.

Every element of $\mathbf{SU}(2^N)$ is the exponential of an anti-Hermitian operator. For a single qubit the group $\mathbf{SU}(2)$ has the following generators:

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{1}$$

We also introduce the bipartite C-NOT gate $V = V^\dagger$ in $\mathbf{SU}(4)$,

$$V|i\rangle|j\rangle := |i\rangle|i \oplus j\rangle, \tag{2}$$

where $|i\rangle$ is an element of the computational basis $\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2$, while $\oplus$ denotes the sum modulo 2. The qubit on the left is named *control* and the qubit on the right is named *target*. Speaking about universality, one may think that the gate $\bar{V}$ with the target and the control exchanged, is different from the gate V; however, in this spirit, one can also notice that $\bar{V}$ is obtained from V using local gates as follows:

$$\bar{V} := (H \otimes H)V(H \otimes H), \tag{3}$$

where H is the Hadamard gate,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{4}$$

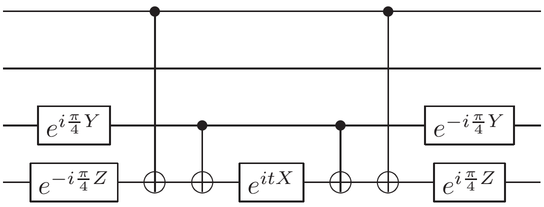

Fig. 1: Relization of the multipartite unitary transformation $U = \exp(itX \otimes I \otimes Z \otimes Y)$ using only C-NOTs and local gates corresponding to rotations of $\pm\pi/2$ around the Y and Z axes.

The bipartite swap gate $P|\phi\rangle|\psi\rangle = |\psi\rangle|\phi\rangle$ can be obtained from the C-NOT gate V as $P = V\bar{V}V$.

When multiple qubits are involved in the computation, we will denote by V_{ij} the C-NOT where the i-th qubit is the control and the j-th qubit is the target.

In the following we will denote by $\mathcal{L}$ the basis for the Lie algebra $\mathbf{su}(2^N)$ of the group $\mathbf{SU}(2^N)$:

$$\mathcal{L}_N := \{L_1 \otimes L_2 \otimes \cdots \otimes L_N\} \backslash \{I^{\otimes N}\}, \ L_j \in \{I, X, Y, Z\}. \tag{5}$$

The special case in which only one L_j for fixed j is different from the identity corresponds to the basis for the Lie algebra of the local gates of the j-th qubit.

We now prove some preliminary lemmas which are needed for the main theorem.

Lemma 1. *Starting from the element $X_N := I^{\otimes(N-1)} \otimes X$ one can generate the whole basis $\mathcal{L}_N$ only conjugating with C-NOTs and local gates.*

Proof. Using the following trivial identity

$$V(I \otimes X)V^\dagger = X \otimes X, \quad P(I \otimes X)P^\dagger = X \otimes I, \tag{6}$$

we can generate all strings in $\mathcal{L}_N$ with $L_j \in \{I, X\}$ by conjugating X_N with a string of C-NOTs V_{jN}. Conjugating with local gates we can then generate the whole $\mathcal{L}_N$. ■

As an example of realization of gate according to Lemma 1 is given in fig. 1.

We thus proved that with local gates and the two-bit entangling gate C-NOT we can obtain all gates of the form $\exp(it\Lambda)$, with $\Lambda \in \mathcal{L}_N$. By repeated applications of such gates for varying t and Λ we generate the subgroup $\mathbf{H} \subseteq \mathbf{SU}(2^N)$.

We now have the following lemma.

Lemma 2. *The subgroup $\mathbf{H} \subseteq \mathbf{SU}(2^N)$ is dense in $\mathbf{SU}(2^N)$.*

Proof. The statement is an immediate consequence of the Lie-Trotter formula,

$$e^{a\Lambda_1 + b\Lambda_2} = \lim_{n\to\infty} \left(e^{\frac{a\Lambda_1}{n}} e^{\frac{b\Lambda_2}{n}} \right)^n, \tag{7}$$

where convergence is to be considered in the strong topology [19]. ■

The last lemma that we need is the following.

Lemma 3 (**Brylinski** [13]). *Let* $\boldsymbol{G}$ *be a compact Lie group. If* $H_1, \dots, H_k$ *are closed connected subgroups and they generate a dense subgroup of* $\boldsymbol{G}$*, then they generate* $\boldsymbol{G}$*.*

We now have all elements for proving our first main theorem.

Theorem 1 (**strong universality of C-NOT**). *The C-NOT gate is strongly universal for quantum computation.*

Proof. We observe that for each $\Lambda \in \mathcal{L}$ the one-parameter subgroup of $\mathbf{SU}(2^N)$ $\left\{e^{i\Lambda t},\ t \in [0, 2\pi)\right\}$ is closed and connected. Then we apply Lemma 3 where the groups H_k are the one-parameter Lie groups obtained by exponentiating each element of $\mathcal{L}_N$. ■

Weak universality in real quantum theory. We now prove universality for RQT. This theory shares a lot of features with CQT, and in some sense it is "contained" in it. Nevertheless, it has also some important differences from CQT, the main one consisting in the failure of local discriminability, which must be replaced in the case of RQT by bilocal discriminability [17,20].

The group of reversible transformations on $\mathbb{R}^{2^N}$, *i.e.* transformations that preserve the norm of vectors, is the ortogonal group $\mathbf{O}(2^N)$ that is a compact not connected Lie group. Now we want to prove that the C-NOT (which is an ortogonal operator) and local gates are sufficient to generate all the gates in $\mathbf{SO}(2^N)$.

Notice that the $\bar{V}$ gate can still be obtained from the C-NOT with local $\mathbf{SO}(2)$ gates as follows:

$$\bar{V} = (\tilde{Y}\tilde{H} \otimes \tilde{H})V(\tilde{H}\tilde{Y} \otimes \tilde{H}), \tag{8}$$

where

$$\tilde{Y} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \tilde{H} := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \in \mathbf{SO}(2). \tag{9}$$

Hence we also get the SWAP gate $P = V\bar{V}V$. We now prove universality along lines analogous to the proof for CQT. We will need to consider the transformations of $\mathbf{O}(2^N)$ with determinant equal to -1 separately, because these cannot be obtained via the exponential map as before.

Let us start with the first task, *i.e.* obtaining all $\mathbf{SO}(2^N)$ from C-NOT and local gates. Since every orthogonal matrix is the exponential of an antisymmetric matrix, a basis $\mathcal{L}'_N$ of $\mathbf{so}(2^N)$ can be taken as the set of strings of $\tilde{Y}, X, Z, I$, with the constraint that they are antisymmetric. It is easy to verify that this amounts to require that a string $L_1 \otimes L_2 \otimes \dots \otimes L_N \in \mathcal{L}'_N$ must contain an odd number of $L_i = \tilde{Y}$. We can now prove the following lemma.

Lemma 4. *Starting from local gates, one can generate the whole basis* $\mathcal{L}'_N$ *only conjugating with C-NOTs and local gates.*

Proof. The proof proceeds by induction. For the case of two rebits, the generators of local gates are then $I \otimes \tilde{Y}$ and $\tilde{Y} \otimes I$. If we conjugate these generators with C-NOT and SWAP we obtain

$$Z \otimes \tilde{Y}, \qquad \tilde{Y} \otimes X, \qquad X \otimes \tilde{Y}, \qquad \tilde{Y} \otimes Z, \tag{10}$$

namely we have the full set $\mathcal{L}'_2$ of six generators of the $\mathbf{so}(4)$ algebra. The induction hypothesis is now that starting from $I^{\otimes(N-1)} \otimes \tilde{Y}$ we can obtain an arbitrary string in $\mathcal{L}'_{N-1}$ conjugating with C-NOT and local gates, and we have to prove that we can obtain an arbitrary string in $\mathcal{L}'_N$ only conjugating wiht C-NOT and local gates. By hypotesis we then have the following generators:

$$I \otimes \tilde{Y} \otimes B, \qquad I \otimes X \otimes A, \qquad I \otimes Z \otimes A,$$

where A is an arbitary string of length $N-2$ with an odd number of $\tilde{Y}$ and B is an arbitary string of length $N-2$ with an even number of $\tilde{Y}$. Acting on these operators with C-NOT and SWAP we obtain

$$Z \otimes \tilde{Y} \otimes B, \qquad X \otimes X \otimes A.$$

Now we can replace Z with X and viceversa by acting with the local gate $\tilde{H}$ modulo a sign on Z (the sign is not relevant, since we are considering Lie-algebra elements). Finally, acting with C-NOT on $X \otimes Z \otimes A$ we obtain $\tilde{Y} \otimes \tilde{Y} \otimes A$. This concludes the induction proof. ■

We can now easily prove the following theorem.

Theorem 2 (**strong universality in** $\mathbf{SO}(2^N)$). *The C-NOT gate is strongly universal for the group* $\mathbf{SO}(2^N)$ *in real quantum theory.*

Proof. The whole group $\mathbf{SO}(2^N)$ is generated by using Lemma 3 in the same way as for theorem 1. ■

Notice, however, that we can only generate the Lie group $\mathbf{SO}(2^N)$, namely the connected component of the orthogonal group containing the identity, but it is impossible to obtain in this way a gate that has determinant equal to -1. Indeed, if we start from a local gate with determinant -1 or even the C-NOT gate, and take the tensor product with the identity or another unit determinant gate, we always obtain a gate with determinant $+1$. This follows directly from the following property of the Kronecker product: *i.e.* if $A \in \mathbf{O}(2^N)$ and $B \in \mathbf{O}(2^M)$ then

$$\mathrm{Det}(A \otimes B) = \mathrm{Det}(A)^{2^M}\,\mathrm{Det}(B)^{2^N}. \tag{11}$$

The solution to this problem is given in the proof of the following theorem.

Theorem 3 (**weak universality of C-NOT in RQT**). *The C-NOT gate is weakly universal for real quantum computation.*

Proof. We already proved universality for gates in $\mathbf{SO}(2^N)$ in theorem 2. Suppose now that one wants to construct an N-rebits gate S with determinant -1. In this case, he can instead use an ancillary rebit and consider the $(N+1)$-rebits gate $I \otimes S$. Since by eq. (11) the determinant of $I \otimes S$ is 1, by theorem 2 this gate can be obtained from a local one using C-NOT and local gates. We have thus proved the weak universality of local gates and C-NOT for RQT. ■

Conclusion. – In this letter we have seen that in RQT local gates and C-NOT, are universal for reversible computation, as in CQT, but an additional ancillary rebit is needed for universality of RQT. Using a similar line of proof we have also provided a very simple and short proof of universality for CQT. We conjecture that RQT has a weak-universality property due to the fact that it does not satisfy local discriminability. An interesting question for future developments is whether the universality property is a good axiom for CQT in the presence of causality and local discriminability.

REFERENCES

[1] Brassard G., *Nat. Phys.*, **1** (2005) 2.

[2] Fuchs C. A., arXiv:quant-ph/0205039 (2002).

[3] Hardy L., arXiv:quant-ph/0101012 (2001).

[4] Dakic B. and Brukner Č., in *Deep Beauty: Understanding the Quantum World through Mathematical Innovation*, edited by Halvorson H. (Cambridge University Press, Cambridge) 2011, p. 365.

[5] D'Ariano G. M., in *Philosophy of Quantum Information and Entanglement*, edited by Bokulich A. and Jaeger G. (Cambridge University Press, Cambridge, UK) 2010, p. 85.

[6] Masanes L. and Müller M. P., *New J. Phys.*, **13** (2011) 063001.

[7] Hardy L., arXiv:1104.2066 (2011).

[8] Chiribella G., D'Ariano G. M. and Perinotti P., *Phys. Rev. A*, **84** (2011) 012311.

[9] Brukner Č., *Physics*, **4** (2011) 55.

[10] Barnum H., Beigi S., Boixo S., Elliott M. B. and Wehner S., *Phys. Rev. Lett.*, **104** (2010) 140401.

[11] de la Torre G., Masanes L., Short A. J. and Müller M. P., *Phys. Rev. Lett.*, **109** (2012) 090403.

[12] Harrow A. W., *Quantum Inf. Comput.*, **8** (2008) 715.

[13] Brylinski J.-L. and Brylinski R., in *Mathematics of Quantum Computation*, edited by Brylinski R. and Chen G. (Chapman and Hall, Boca Raton) 2002, p. 101.

[14] Barenco A., Bennett C. H., Cleve R., DiVincenzo D. P., Margolus N., Shor P., Sleator T., Smolin J. A. and Weinfurter H., *Phys. Rev. A*, **52** (1995) 3457.

[15] DiVincenzo D. P., *Phys. Rev. A*, **51** (1995) 1015.

[16] Deutsch Y., *Proc. R. Soc. London, Ser. A*, **425** (1989) 73.

[17] Hardy L. and Wootters W. K., *Found. Phys.*, **42** (2012) 454.

[18] Rudolph T. and Grover L., arXiv:quant-ph/0210187 (2002).

[19] Ichinose T. and Tamura H., *Lett. Math. Phys.*, **70** (2004) 65.

[20] Chiribella G., D'Ariano G. M. and Perinotti P., *Phys. Rev. A*, **81** (2010) 062348.