Information and Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

A branching distributed temporal logic for reasoning about entanglement-free quantum state transformations ☆

Luca Viganò [a,*], Marco Volpe [b], Margherita Zorzi [c]

[a] Department of Informatics, King's College London, UK
[b] Inria and LIX, École Polytechnique, Palaiseau, France
[c] Dipartimento di Informatica, Università di Verona, Italy

ARTICLE INFO

Article history:
Received 1 May 2015
Available online xxxx

Keywords:
Quantum computing
Quantum state transformations
Temporal logic
Distributed temporal logic
Natural deduction

ABSTRACT

The Distributed Temporal Logic DTL allows one to reason about temporal properties of a distributed system from the local point of view of the system's agents, which are assumed to execute independently and to interact by means of event sharing. In this paper, we introduce the Quantum Branching Distributed Temporal Logic QBDTL, a variant of DTL able to represent (entanglement-free) quantum state transformations in an abstract, qualitative way. In QBDTL, each agent represents a distinct quantum bit (the unit of quantum information theory), which evolves by means of quantum transformations and possibly interacts with other agents, and n-ary quantum operators act as communication/synchronization points between agents. We endow QBDTL with a DTL-style semantics, which fits the intrinsically distributed nature of quantum computing, we formalize a labeled deduction system for QBDTL, and we prove the soundness and completeness of this deduction system with respect to the given semantics. We give a number of examples and, finally, we discuss possible extensions of our logic in order to reason about entanglement phenomena.

1. Introduction

1.1. Background and motivation

The *Distributed Temporal Logic DTL* [17,5,6] allows one to reason about temporal properties of a distributed system from the local point of view of the system's agents: each asynchronous agent executes independently, evolves linearly along a time-line built upon some local events, and can interact with the other agents by means of event sharing. Distribution is implicit and properties of an entire system are formulated in terms of the local properties of the system's agents and their interaction. DTL's semantics was inspired by a conflict-free version of Winskel's *event structures* (see, e.g., [39]), enriched with information about sequential agents.

DTL has been initially proposed as a logic for specifying and reasoning about distributed information [17], but it has also been used in the context of security protocol analysis to reason about the interplay between protocol models and security

☆ The work presented in this paper was partially supported by the EU FP7 Marie Curie PIRSES-GA-2012-318986 project "GeTFun: Generalizing Truth-Functionality". Part of this work was carried out while Luca Viganò and Marco Volpe were at the Dipartimento di Informatica, Università di Verona, Italy.

* Corresponding author.
E-mail address: luca.vigano@kcl.ac.uk (L. Viganò).

http://dx.doi.org/10.1016/j.ic.2017.01.007
0890-5401/

properties [6]. In this paper, we show that, after a proper extension of the logic's syntax and semantics, DTL is also able to formally model (entanglement-free) quantum state transformations in an abstract, qualitative way.

Quantum computing is one of the most promising research fields of computer science as well as a concrete future technology (see [31] for a useful introduction to the basic notions of quantum computing as we here only very briefly summarize the notions that are relevant to our work in this paper). However, at least from the point of view of theoretical computer science, a number of foundational aspects are still underdeveloped: quantum complexity, quantum computability, quantum programming theory (and its logical account), quantum cryptography and security are all active but open research areas, which still require the development of ad hoc formal methods. These issues are complex to face since the physical model quantum computing is based on is sophisticated and all basic definitions and formal tools have to be reformulated in a non-standard way.

To illustrate this, and our contributions in this paper, in more detail, let us focus our attention on quantum data, in particular on the unit of quantum information, the *quantum bit* or *qubit*, for short. The qubit is the quantum counterpart of the classical bit and, mathematically, it is simply a normalized vector of the Hilbert space $\mathbb{C}^2$. Qubits can assume both classical values 0 and 1 (as the classical bit) and all their *superpositional values*, i.e., linear combinations such as $\alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ are called *amplitudes*, $|\alpha|^2 + |\beta|^2 = 1$ and $|c\rangle$, for $c \in \{0, 1\}$, is the so-called *Dirac Notation*, which is simply a denotation of basis states (which corresponds to the classical values a bit can assume).

Intuitively, whereas a classical bit can only be 0 or 1, a quantum bit can assume both the value 0 and the value 1 (with a certain associated probability) at the same time. It is possible to modify a quantum bit in two ways:

- by means of a suitable class of algebraic operators called *unitary transformations* (that are also called *quantum gates* and are a class of algebraic operators enjoying some good properties, which represent the pure quantum computational steps) or
- by *measuring* it, i.e., probabilistically reducing it to 0 or 1.

In this paper, we deal only with unitary transformations, leaving measurement for future work.

The definition of a qubit can, of course, be generalized: a *quantum register* or *quantum state* [41] is the representation of a system of n qubits (mathematically, it is a normalized vector of the Hilbert space $\mathbb{C}^{2^n}$). As for the single qubit, a quantum state can be modified by means of unitary algebraic operators.

Abstracting from any notion of control and considering only pure quantum transformations (i.e., unitary evolution of quantum states as computational steps), it seems to be interesting to provide a logical account of such a computation. The question then is: what is a logical approach suitable to represent quantum state evolution?

1.2. Contributions

The main contribution of this paper is the formalization of a logic and of an associated deduction system that allows one to formally represent and reason about unitary transformations of quantum states from a temporal multi-agent system perspective. More specifically, we view our contributions as two-fold.

First, we define the *Quantum Branching Distributed Temporal Logic* QBDTL, a significant variant of DTL that we introduce here to represent quantum state transformations in an abstract, *qualitative* way. In QBDTL, we abstract from the value of the qubits: we are not interested in encoding into our system syntactical and semantical information about amplitudes or basis values 0 and 1 (in this way, we avoid any *quantitative* information) and we focus instead on the way qubits evolve by means of unitary transformations. Following DTL's central notion, in QBDTL we do not only consider globally quantum states but also, and in particular, the single unit of information, i.e., we maintain the local perspective of the qubit in the quantum computation.

In other words, in QBDTL each agent represents a distinct qubit, which is the object/subject of computation and which evolves in time by means of quantum transformations and possibly interacts with other agents/qubits.

There is a crucial difference between our QBDTL and the original DTL formulation. DTL is based on linear time life-cycles for agents. In QBDTL (and this provides an additional contribution of our work), we go beyond linearity and consider branching time since we want to be as general as possible: at each step of the temporal evolution of an agent/qubit, the accessibility relation between worlds in the subtended Kripke-style model aims to capture each possible unitary transformation that can be applied to the qubit. A world (a state in the temporal life-cycle of an agent) represents (an abstraction of) a 1-qubit quantum state. n-ary quantum operators, which act simultaneously on more than one qubit (such as control operators, which play a crucial role in quantum computing), act as communication/synchronization points between agents/qubits.

Second, we give a deduction system $\mathcal{N}$(QBDTL) for QBDTL. In order to deal with all the semantical notions (temporal, quantum and synchronization information), we follow the style of *labeled deduction* [22,36,37], a framework for giving uniform presentations of different non-classical logics, where labels allow one to explicitly encode in the syntax additional information, of a semantic or proof-theoretical nature, that is otherwise implicit in the logic one wants to capture.

In addition to the works on DTL, and in particular the labeled tableaux system given in [5], our starting points for $\mathcal{N}$(QBDTL) are the labeled natural deduction system for the logic *UB* (i.e., the until-free fragment of *CTL*) given in [11] and the approach developed in [27,28], where a labeled modal deduction system with specific modalities able to describe

Please cite this article in press as: L. Viganò et al., A branching distributed temporal logic for reasoning about entanglement-free quantum state transformations, Inf. Comput. (2017), http://dx.doi.org/10.1016/j.ic.2017.01.007