Quantum Entanglement Analysis based on Abstract Interpretation

Simon Perdrix

Oxford University Computing Laboratory
simon.perdrix@comlab.ox.ac.uk

Abstract. Entanglement is a non local property of quantum states which has no classical counterpart and plays a decisive role in quantum information theory. Several protocols, like the teleportation, are based on quantum entangled states. Moreover, any quantum algorithm which does not create entanglement can be efficiently simulated on a classical computer. The exact role of the entanglement is nevertheless not well understood. Since an exact analysis of entanglement evolution induces an exponential slowdown, we consider approximative analysis based on the framework of abstract interpretation. In this paper, a concrete quantum semantics based on superoperators is associated with a simple quantum programming language. The representation of entanglement, i.e. the design of the abstract domain is a key issue. A representation of entanglement as a partition of the memory is chosen. An abstract semantics is introduced, and the soundness of the approximation is proven.

1 Introduction

Quantum entanglement is a non local property of quantum mechanics. The entanglement reflects the ability of a quantum system composed of several subsystems, to be in a state which cannot be decomposed into the states of the subsystems. Entanglement is one of the properties of quantum mechanics which caused Einstein and others to dislike the theory. In 1935, Einstein, Podolsky, and Rosen formulated the EPR paradox [7].

On the other hand, quantum mechanics has been highly successful in producing correct experimental predictions, and the strong correlations associated with the phenomenon of quantum entanglement have been observed indeed [2].

Entanglement leads to correlations between subsystems that can be exploited in information theory (e.g., teleportation scheme [3]). The entanglement plays also a decisive, but not yet well-understood, role in quantum computation, since any quantum algorithm can be efficiently simulated on a classical computer when the quantum memory is not entangled during all the computation. As a consequence, interesting quantum algorithms, like Shor's algorithm for factorisation [19], exploit this phenomenon.

In order to know what is the amount of entanglement of a quantum state, several measures of entanglement have been introduced (see for instance [13]). Recent works consist in characterising, in the framework of the one-way quantum computation [20], the amount of entanglement necessary for a universal model of quantum computation. Notice that all these techniques consist in analysing the entanglement of a given state, starting with its mathematical description.

In this paper, the entanglement *evolution* during the computation is analysed. The description of quantum evolutions is done via a simple quantum programming language. The development of such quantum programming languages is recent, see [17,8] for a survey on this topic.

An exact analysis of entanglement evolution induces an exponential slowdown of the computation. Model checking techniques have been introduced [9] including entanglement. Exponential slowdown of such analysis is avoided by reducing the domain to stabiliser states (i.e. a subset of quantum states that can be efficiently simulated on a classical computer). As a consequence, any quantum program that cannot be efficiently simulated on a classical computer cannot be analysed.

Prost and Zerrari [16] have recently introduced a logical entanglement analysis for functional languages. This logical framework allows analysis of higher-order functions, but does not provide any static analysis for the quantum programs without annotation. Moreover, only pure quantum states are considered.

In this paper, we introduce a novel approach of entanglement analysis based on the framework of abstract interpretation [5]. A concrete quantum semantics based on superoperators is associated with a simple quantum programming language. The representation of entanglement, i.e. the design of the abstract domain is a key issue. A representation of entanglement as a partition of the memory is chosen. An abstract semantics is introduced, and the soundness of the approximation is proved.

2 Basic Notions and Entanglement

2.1 Quantum Computing

We briefly recall the basic definitions of quantum computing; please refer to Nielsen and Chuang [13] for a complete introduction to the subject.

The state of a quantum system can be described by a density matrix, i.e. a self adjoint[1] positive-semidefinite[2] complex matrix of trace[3] less than one. The set of density matrices of dimension n is $D_n \subseteq \mathbb{C}^{n\times n}$.

The basic unit of information in quantum computation is a quantum bit or *qubit*. The state of a single qubit is described by a 2×2 density matrix $\rho \in D_2$. The state of a register composed of n qubits is a $2^n \times 2^n$ density matrix. If two registers A and B are in states $\rho_A \in D_{2^n}$ and $\rho_B \in D_{2^m}$, the composed system A, B is in state $\rho_A \otimes \rho_B \in D_{2^{n+m}}$.

The basic operations on quantum states are unitary operations and measurements. A unitary operation maps an n-qubit state to an n-qubit state, and is

[1] M is self adjoint (or Hermitian) if and only if $M^\dagger = M$

[2] M is positive-semidefinite if all the eigenvalues of M are non-negative.

[3] The trace of M ($\mathrm{tr}(M)$) is the sum of the diagonal elements of M

given by a $2^n \times 2^n$-unitary matrix[4]. If a system in state ρ evolves according to a unitary transformation U, the resulting density matrix is $U\rho U^\dagger$. The parallel composition of two unitary transformations U_A, U_B is $U_A \otimes U_B$.

The following unitary transformations form an approximative universal family of unitary transformations, i.e. any unitary transformation can be approximated by composing the unitary transformations of the family [13].

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, CNot = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

A measurement is described by a family of projectors $\{\mathrm{P}_x, x \in X\}$ satisfying $\mathrm{P}_i^2 = \mathrm{P}_i$, $\mathrm{P}_i\mathrm{P}_j = 0$ if $i \neq j$, and $\sum_{x\in X} \mathrm{P}_x = \mathbb{I}$. A computational basis measurement is $\{\mathrm{P}_k, 0 \leq k < 2^n\}$, where P_k has 0 entries everywhere except one 1 at row k, column k. The parallel composition of two measurements $\{\mathrm{P}_x, x \in X\}$, $\{\mathrm{P}'_y, y \in Y\}$ is $\{\mathrm{P}_x \otimes \mathrm{P}'_y, (x, y) \in X \times Y\}$.

According to a probabilistic interpretation, a measurement according to $\{\mathrm{P}_x, x \in X\}$ of a state ρ produces the classical outcome $x \in X$ with probability $\mathrm{tr}(\mathrm{P}_x\rho\mathrm{P}_x)$ and transforms ρ into $\frac{1}{\mathrm{tr}(\mathrm{P}_x\rho\mathrm{P}_x)}\mathrm{P}_x\rho\mathrm{P}_x$.

Density matrices is a useful formalism for representing probability distributions of quantum states, since the state ρ of a system which is in state ρ_1 (resp. ρ_2) with probability p_1 (resp. p_2) is $\rho = p_1\rho_1 + p_2\rho_2$. As a consequence, a measurement according to $\{\mathrm{P}_x, x \in X\}$ transforms ρ into $\sum_{x\in X} \mathrm{P}_x\rho\mathrm{P}_x$.

Notice that the sequential compositions of two measurements (or of a measurement and a unitary transformation) is no more a measurement nor a unitary transformation, but a superoperator, i.e. a trace-decreasing[5] completely positive[6] linear map. Any quantum evolution can be described by a superoperator.

The ability to initialise any qubit in a given state ρ_0, to apply any unitary transformation from a universal family, and to perform a computational measurement are enough for simulating any superoperator.

2.2 Entanglement

Quantum entanglement is a non local property which has no classical counterpart. Intuitively, a quantum state of a system composed of several subsystems is

[4] U is unitary if and only if $U^\dagger U = UU^\dagger = \mathbb{I}$.

[5] F is trace decreasing iff $\mathrm{tr}(F(\rho)) \leq \mathrm{tr}(\rho)$ for any ρ in the domain of F. Notice that superoperators are sometimes defined as trace-perserving maps, however trace-decreasing is more suitable in a semantical context, see [18] for details.

[6] F is positive if $F(\rho)$ is positive-semidefinite for any positive ρ in the domain of F. F is completely positive if $\mathbb{I}_k \otimes F$ is positive for any k, where $\mathbb{I}_k : \mathbb{C}^{k\times k} \to \mathbb{C}^{k\times k}$ is the identity map.

entangled if it cannot be decomposed into the state of its subsystems. A quantum state which is not entangled is called *separable*.

More precisely, for a given finite set of qubits Q, let $n = |Q|$. For a given partition A, B of Q, and a given $\rho \in D_{2^n}$, ρ is biseparable according to A, B (or (A, B)-separable for short) if and only if there exist K, $p_k \geq 0$, ρ_k^A and ρ_k^B such that

$$\rho = \sum_{k \in K} p_k \rho_k^A \otimes \rho_k^B$$

ρ is entangled according to the partition A, B if and only if ρ is not (A, B)-separable.

Notice that biseparability provides a very partial information about the entanglement of a quantum state, for instance for a 3-qubit state ρ, which is $(\{1\}, \{2, 3\})$-separable, qubit 2 and qubit 3 may be entangled or not.

One way to generalise the biseparability is to consider that a quantum state is π-separable – where $\pi = \{Q_j, j \in J\}$ is a partition of Q – if and only if there exist K, $p_k \geq 0$, and $\rho_k^{Q_j}$ such that

$$\rho = \sum_{k \in K} p_k \left(\bigotimes_{j \in J} \rho_k^{Q_j} \right)$$

Notice that the structure of quantum entanglement presents some interesting and non trivial properties. For instance there exist some 3-qubit states ρ such that ρ is bi-separable for any bi-partition of the 3 qubits, but not fully separable i.e., separable according to the partition $\{\{1\}, \{2\}, \{3\}\}$. As a consequence, for a given quantum state, there is not necessary a *best representation* of its entanglement.

2.3 Standard and diagonal basis

For a given state $\rho \in \mathcal{D}^Q$ and a given qubit $q \in Q$, if ρ is $(\{q\}, Q \setminus \{q\})$-separable, then q is separated from the rest of the memory. Moreover, such a qubit may be a basis state in the standard basis ($\mathbf{s}$) or the diagonal basis ($\mathbf{d}$), meaning that the state of this qubit can be seen as a 'classical state' according to the corresponding basis.

More formally, a qubit q of ρ is in the standard basis if there exists $p_0, p_1 \geq 0$, and $\rho_0, \rho_1 \in \mathcal{D}^{Q \setminus \{q\}}$ such that $\rho = p_0 P_q^{\mathsf{true}} \otimes \rho_0 + p_1 P_q^{\mathsf{false}} \otimes \rho_1$. Equivalently, q is in the standard basis if and only if $P_q^{\mathsf{true}} \rho P_q^{\mathsf{false}} = P_q^{\mathsf{false}} \rho P_q^{\mathsf{true}} = 0$. A qubit q is in the diagonal basis in ρ if and only if q is in the standard basis in $H_q \rho H_q$.

Notice that some states, like the maximally mixed 1-qubit state $\frac{1}{2}(P^{\mathsf{true}} + P^{\mathsf{false}})$ are in both standard and diagonal basis, while others are neither in standard nor diagonal basis like the 1-qubit state $THP^{\mathsf{true}}HT$.

We introduce a function $\beta : \mathcal{D}^Q \to B^Q$, where $B^Q = Q \to \{\mathbf{s}, \mathbf{d}, \top, \bot\}$, such that $\beta(\rho)$ describes which qubits of ρ are in the standard or diagonal basis:

Definition 1. *For any finite Q, let $\beta : \mathcal{D}^Q \to B^Q$ such that for any $\rho \in \mathcal{D}^Q$, and any $q \in Q$,*

$$\beta(\rho)_q = \begin{cases} \bot & \textit{if } q \textit{ is in both standard and diagonal basis in } \rho \\ \mathbf{s} & \textit{if } q \textit{ is in the standard and not in the diagonal basis in } \rho \\ \mathbf{d} & \textit{if } q \textit{ is in the diagonal and not in the standard basis in } \rho \\ \top & \textit{otherwise} \end{cases}$$

3 A Quantum Programming Language

Several quantum programming languages have been introduced recently. For a complete overview see [8]. We use an imperative quantum programming language introduced in [15], the syntax is similar to the language introduced by Abramsky [1]. For the sake of simplicity and in order to focus on entanglement analysis, the memory is supposed to be fixed and finite. Moreover, the memory is supposed to be composed of qubits only, whereas hybrid memories composed of classical and quantum parts are often considered. However, contrary to the quantum circuit or quantum Turing machine frameworks, the absence of classical memory does not avoid the classical control of the quantum computation since classically-controlled conditional structures are allowed (see section 3.1.)

Definition 2 (Syntax). *For a given finite set of symbols $q \in Q$, a program is a pair $\langle C, Q\rangle$ where C is a command defined as follows:*

$$\begin{aligned} C ::= \ & \mathsf{skip} \\ & \mid C_1; C_2 \\ & \mid \mathsf{if}\ q\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2 \\ & \mid \mathsf{while}\ q\ \mathsf{do}\ C \\ & \mid \mathsf{H}(q) \\ & \mid \mathsf{T}(q) \\ & \mid \mathsf{CNot}(q, q) \end{aligned}$$

Example 1. Quantum entanglement between two qubits q_2 and q_3 can be created for instance by applying H and $CNot$ on an appropriate state. Such an entangled state can then be used to *teleporte* the state of a third qubit q_1. The protocol of teleportation [3] can be described as $\langle \mathsf{teleportation}, \{q_1, q_2, q_3\}\rangle$, where

$$\begin{aligned} \mathsf{teleportation} : \ & \mathsf{H}(q_2); \\ & \mathsf{CNot}(q_2, q_3); \\ & \mathsf{CNot}(q_1, q_2); \\ & \mathsf{H}(q_1); \\ & \mathsf{if}\ q_1\ \mathsf{then} \\ & \quad \mathsf{if}\ q_2\ \mathsf{then\ skip\ else}\ \sigma_x(q_3) \\ & \mathsf{else} \\ & \quad \mathsf{if}\ q_2\ \mathsf{then}\ \sigma_z(q_3)\ \mathsf{else}\ \sigma_y(q_3) \end{aligned}$$

The semantics of this program is given in example 2.

3.1 Concrete Semantics

Several domains for quantum computation have been introduced [12,1,14]. Among them, the domain of superoperators over density matrices, introduced by Selinger [18] turns out to be one of the most adapted to quantum semantics. Thus, we introduce a denotational semantics following the work of Selinger.

For a finite set of variables $Q = \{q_0, \dots, q_n\}$, let $\mathcal{D}^Q = D_{2^{|Q|}}$. Q is a set of qubits, the state of Q is a density operator in $\mathcal{D}^Q$.

Definition 3 (Löwner partial order). *For matrices M and N in $\mathbb{C}^{n\times n}$, $M \sqsubseteq N$ if $N - M$ is positive-semidefinite.*

In [18], Selinger proved that the poset $(\mathcal{D}^Q, \sqsubseteq)$ is a complete partial order with 0 as its least element. Moreover the poset of superoperators over $\mathcal{D}^Q$ is a complete partial order as well, with 0 as least element and where the partial order $\sqsubseteq'$ is defined as $F \sqsubseteq' G \iff \forall k \geq 0, \forall \rho \in \mathcal{D}_{k2^{|Q|}}, (\mathbb{I}_k \otimes F)(\rho) \sqsubseteq (\mathbb{I}_k \otimes G)(\rho)$, where $\mathbb{I}_k : \mathcal{D}_k \to \mathcal{D}_k$ is the identity map. Notice that these complete partial orders are not lattices (see [18].)

We are now ready to introduce the concrete denotational semantics which associates with any program $\langle C, Q\rangle$, a superoperator $[\![C]\!] : \mathcal{D}^Q \to \mathcal{D}^Q$.

Definition 4 (Denotational semantics).

$$[\![\mathsf{skip}]\!] = \mathbb{I}$$

$$[\![C_1; C_2]\!] = [\![C_2]\!] \circ [\![C_1]\!]$$

$$[\![\mathsf{U}(q)]\!] = \lambda\rho.U_q \rho U_q^\dagger$$

$$[\![\mathsf{CNot}(q_1, q_2)]\!] = \lambda\rho.CNot_{q_1,q_2}\rho CNot_{q_1,q_2}^\dagger$$

$$[\![\mathsf{if}\ q\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ ]\!] = \lambda\rho.\left([\![C_1]\!](\mathrm{P}_q^{\mathsf{true}}\rho\mathrm{P}_q^{\mathsf{true}}) + [\![C_2]\!](\mathrm{P}_q^{\mathsf{false}}\rho\mathrm{P}_q^{\mathsf{false}})\right)$$

$$\begin{aligned}[\![\mathsf{while}\ q\ \mathsf{do}\ C\ ]\!] &= \mathsf{lfp}\left(\lambda f.\lambda\rho.\left(f \circ [\![C]\!](\mathrm{P}_q^{\mathsf{true}}\rho\mathrm{P}_q^{\mathsf{true}}) + \mathrm{P}_q^{\mathsf{false}}\rho\mathrm{P}_q^{\mathsf{false}}\right)\right) \\ &= \textstyle\sum_{n\in\mathbb{N}} (F_{\mathrm{P}^{\mathsf{false}}} \circ ([\![C]\!] \circ F_{\mathrm{P}^{\mathsf{true}}})^n)\end{aligned}$$

where $\mathrm{P}^{\mathsf{true}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ *and* $\mathrm{P}^{\mathsf{false}} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $F_M = \lambda\rho.M\rho M^\dagger$, *and M_q means that M is applied on qubit q. We refer the reader to an extended version of this paper for the technical explanations on continuity and convergence.*

In the absence of classical memory, the classical control is encoded into the conditional structure $\mathsf{if}\ q\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2$ such that the qubit q is first measured according to the computational basis. If the first projector is applied, then the classical outcome is interpreted as *true* and the command C_1 is applied. Otherwise, the second projector is applied, and the command C_2 is performed. The classical control appears in the loop $\mathsf{while}\ q\ \mathsf{do}\ C$ as well.

As a consequence of the classical control, non unitary transformations can be implemented:

$$[\![\textsf{if } q \textsf{ then } q \textsf{ else } \sigma_x(q)\ ]\!] : \mathcal{D}^{\{q\}} \to \mathcal{D}^{\{q\}} = \lambda\rho.\mathrm{P}^{\textsf{true}}$$

$$[\![\textsf{while } q \textsf{ do } \mathsf{H}(q)\ ]\!] : \mathcal{D}^{\{q\}} \to \mathcal{D}^{\{q\}} = \lambda\rho.\mathrm{P}^{\textsf{false}}$$

Notice that the matrices $\mathrm{P}^{\textsf{true}}$ and $\mathrm{P}^{\textsf{false}}$, used in definition 4 for describing the computational measurement $\{\mathrm{P}^{\textsf{true}}, \mathrm{P}^{\textsf{false}}\}$ can also be used as density matrices for describing a quantum state as above.

Moreover, notice that all the ingredients for approximating any superoperators can be encoded into the language: the ability to initialise any qubit in a given state (for instance $\mathrm{P}^{\textsf{true}}$ or $\mathrm{P}^{\textsf{false}}$); an approximative universal family of unitary transformation $\{H, T, CNot, \sigma_x, \sigma_y, \sigma_z\}$; and the computational measurement of a qubit q with $\textsf{if } q \textsf{ then skip else skip}$.

Example 2. The program $\langle\textsf{teleportation}, \{q_1, q_2, q_3\}\rangle$ described in example 1 realises the teleportation from q_1 to q_3, when the qubits q_2 and q_3 are both initialised in state $\mathrm{P}^{\textsf{true}}$: for any $\rho \in \mathcal{D}_2$,

$$[\![\textsf{teleportation}]\!](\rho \otimes \mathrm{P}^{\textsf{true}} \otimes \mathrm{P}^{\textsf{true}}) = \left(\frac{1}{4} \sum_{k,l \in \{\textsf{true},\textsf{false}\}} \mathrm{P}^k \otimes \mathrm{P}^l\right) \otimes \rho$$

4 Entanglement Analysis

What is the role of the entanglement in quantum information theory? How does the entanglement evolve during a quantum computation? We consider the problem of analysing the entanglement evolution on a classical computer, since no large scale quantum computer is available at the moment. Entanglement analysis using a quantum computer is left to further investigations[7].

In the absence of quantum computer, an obvious solution consists in simulating the quantum computation on a classical computer. Unfortunately, the classical memory required for the simulation is exponentially large in the size of the quantum memory of the program simulated. Moreover, the problem **SEP** of deciding whether a given quantum state ρ is biseparable or not is NP Hard[8] [10]. Furthermore, the input of the problem **SEP** is a density matrix, which size is exponential in the number of qubits. As a consequence, the solution of a classical simulation is not suitable for an efficient entanglement analysis.

---

[7] Notice that this is not clear that the use of a quantum computer avoids the use of the classical computer since there is no way to measure the entanglement of a quantum state without transforming the state.

[8] For pure quantum states (i.e. $\mathrm{tr}(\rho^2) = \mathrm{tr}(\rho)$), a linear algorithm have been introduced [11] to solve the sub-problem of finding biseparability of the form $(\{q_0, \ldots, q_k\}, \{q_{k+1}, \ldots, q_n\})$ – thus sensitive to the ordering of the qubits in the register. Notice that this algorithm is linear in the size of the input which is a density matrix, thus the algorithm is exponential in the number of qubits.

To tackle this problem, a solution consists in reducing the size of the quantum state space by considering a subspace of possible states, such that there exist algorithms to decide whether a state of the subspace is entangled or not in a polynomial time in the number of qubits. This solution has been developed in [9], by considering stabiliser states only. However, this solution, which may be suitable for some quantum protocols, is questionable for analysing quantum algorithms since all the quantum programs on which such an entanglement analysis can be driven are also efficiently simulable on a classical computer.

In this paper, we introduce a novel approach which consists in approximating the entanglement evolution of the quantum memory. This solution is based on the framework of abstract interpretation introduced by Cousot and Cousot [5]. Since a classical domain for driving a sound and complete analysis of entanglement is exponentially large in the number n of qubits, we consider an abstract domain of size n and we introduce an abstract semantics which leads to a sound approximation of the entanglement evolution during the computation.

4.1 Abstract semantics

The entanglement of a quantum state can be represented as a partition of the qubits of the state (see section 2.2), thus a natural abstract domain is a domain composed of partitions. Moreover, for a given state ρ, one can add a flag for each qubit q, indicating whether the state of this qubit is in the standard basis $\mathbf{s}$ or in the diagonal basis $\mathbf{d}$ (see section 2.3).

Definition 5 (Abstract Domain). *For a finite set of variables Q, let $\mathcal{A}^Q = B^Q \times \Pi^Q$ be an abstract domain, where $B^Q = Q \to \{\mathbf{s}, \mathbf{d}, \top, \bot\}$ and Π^Q is the set of partitions of Q:*

$$\Pi^Q = \{\pi \subseteq \wp(Q) \setminus \{\emptyset\} \mid \bigcup_{X \in \pi} X = Q \textit{ and } (\forall X, Y \in \pi,\ X \cap Y = \emptyset \textit{ or } X = Y)\}$$

The abstract domain $\mathcal{A}$ is ordered as follows. First, let $(\{\mathbf{s}, \mathbf{d}, \top, \bot\}, \leq)$ be a poset, where $\leq$ is defined as: $\bot \leq \mathbf{s} \leq \top$ and $\bot \leq \mathbf{d} \leq \top$. $(B^Q, \leq)$ is a poset, where $\leq$ is defined pointwise. Moreover, for any $\pi_1, \pi_2 \in \Pi^Q$, let $\pi_1 \leq \pi_2$ if π_1 rafines π_2, i.e. for every block $X \in \pi_1$ there exists a block $Y \in \pi_2$ such that $X \subseteq Y$. Finally, for any $(b_1, \pi), (b_2, \pi_2) \in \mathcal{A}^Q$, $(b_1, \pi) \leq (b_2, \pi_2)$ if $b_1 \leq b_2$ and $\pi_1 \leq \pi_2$.

Proposition 1. *For any finite set Q, $(\mathcal{A}^Q, \leq)$ is a complete partial order, with $\bot = (\lambda q.\bot, \{\{q\}, q \in Q\})$ as least element.*

Proof. Every chain has a supremum since Q is finite. □

Basic operations of meet and join are defined on $\mathcal{A}^Q$. It turns out that contrary to $\mathcal{D}^Q$, $\langle \mathcal{A}^Q, \vee, \wedge, \bot, (\lambda q.\top, \{Q\}) \rangle$ is a lattice.

A removal operation on partitions is introduced as follows: for a given partition $\pi = \{Q_i, i \in I\}$, let $\pi \setminus q = \{Q_i \setminus \{q\}, i \in I\} \cup \{\{q\}\}$. Moreover, for any pair of qubits $q_1, q_2 \in Q$, let $[q_1, q_2] = \{\{q \mid q \in Q \setminus \{q_1, q_2\}\}, \{q_1, q_2\}\}$.

Finally, for any $b \in B^Q$, any $q_0, q \in Q$, any $k \in \{\mathbf{s}, \mathbf{d}, \top, \bot\}$, let

$$b_q^{q_0 \mapsto k} = \begin{cases} k & \text{if } q = q_0 \\ b_q & \text{otherwise} \end{cases}$$

We are now ready to define the abstract semantics of the language:

Definition 6 (Denotational abstract semantics). *For any program $\langle C, Q \rangle$, let $[\![C]\!]^\natural : \mathcal{A}^Q \to \mathcal{A}^Q$ be defined as follows: For any $(b, \pi) \in \mathcal{A}^Q$,*

$$[\![\mathsf{skip}]\!]^\natural(b,\pi) = (b,\pi)$$

$$[\![C_1; C_2]\!]^\natural(b,\pi) = [\![C_2]\!]^\natural \circ [\![C_1]\!]^\natural(b,\pi)$$

$$[\![\sigma(q)]\!]^\natural(b,\pi) = (b,\pi)$$

$$\begin{aligned} [\![\mathsf{H}(q)]\!]^\natural(b,\pi) &= (b^{q\mapsto\mathbf{d}}, \pi) \text{ if } b_q = \mathbf{s} \\ &= (b^{q\mapsto\mathbf{s}}, \pi) \text{ if } b_q = \mathbf{d} \\ &= (b,\pi) \text{ otherwise} \end{aligned}$$

$$\begin{aligned} [\![\mathsf{T}(q)]\!]^\natural(b,\pi) &= (b^{q\mapsto\top}, \pi) \text{ if } b_q = \mathbf{d} \\ &= (b^{q\mapsto\mathbf{s}}, \pi) \text{ if } b_q = \bot \\ &= (b,\pi) \text{ otherwise} \end{aligned}$$

$$\begin{aligned} [\![\mathsf{CNot}(q_1,q_2)]\!]^\natural(b,\pi) &= (b,\pi) \quad \text{if } b_{q_1} = \mathbf{s} \text{ or } b_{q_2} = \mathbf{d} \\ &= (b^{q_1\mapsto\mathbf{s}}, \pi) \quad \text{if } b_{q_1} = \bot \text{ and } b_{q_2} > \bot \\ &= (b^{q_2\mapsto\mathbf{d}}, \pi) \quad \text{if } b_{q_1} > \bot \text{ and } b_{q_2} = \bot \\ &= (b^{q_1\mapsto\mathbf{s}, q_2\mapsto\mathbf{d}}, \pi) \quad \text{if } b_{q_1} = \bot \text{ and } b_{q_2} = \bot \\ &= (b^{q_1,q_2\mapsto\top}, \pi \vee [q_1,q_2]) \quad \text{otherwise} \end{aligned}$$

$$[\![\mathsf{if}\ q\ \mathsf{then}\ C_1\ \mathsf{else}\ C_2\ ]\!]^\natural(b,\pi) = \left([\![C_1]\!]^\natural(b^{q\mapsto\mathbf{s}}, \pi\setminus q) \vee [\![C_2]\!]^\natural(b^{q\mapsto\mathbf{s}}, \pi\setminus q)\right)$$

$$\begin{aligned} [\![\mathsf{while}\ q\ \mathsf{do}\ C\ ]\!]^\natural(b,\pi) &= \mathsf{lfp}\left(\lambda f.\lambda\pi.\left(f \circ [\![C]\!]^\natural(b^{q\mapsto\mathbf{s}}, \pi\setminus q) \vee (b^{q\mapsto\mathbf{s}}, \pi\setminus q)\right)\right) \\ &= \bigvee_{n\in\mathbb{N}} \left(F_q^\natural \circ ([\![C]\!]^\natural \circ F_q^\natural)^n\right) \end{aligned}$$

where $F_q^\natural = \lambda(b,\pi).(b^{q\mapsto\mathbf{s}}, \pi\setminus q)$.

Intuitively, quantum operations act on entanglement as follows:

– A 1-qubit measurement makes the measured qubit separable from the rest of the memory. Moreover, the state of the measured qubit is in the standard basis.
– A 1-qubit unitary transformation does not modify entanglement. Any Pauli operator $\sigma \in \{\sigma_x, \sigma_y, \sigma_z\}$ preserves the standard and the diagonal basis of the qubits. Hadamard H transforms a state of the standard basis into a state of the diagonal basis and vice-versa. Finally the phase T preserves the standard basis but not the diagonal basis.

– The 2-qubit unitary transformation $CNot$, applied on q_1 and q_2 may create entanglement between the qubits or not. It turns out that if q_1 is in the standard basis, or q_2 is in the diagonal basis, then no entanglement is created and the basis of q_1 and q_2 are preserved. Otherwise, since a sound approximation is desired, $CNot$ is abstracted into an operation which creates entanglement.

Remark 1. Notice that the space needed to store a partition of n elements is $O(n)$. Moreover, meet, join and removal and can be done in either constant or linear time.

Example 3. The abstract semantics of the teleportation (see example 1) is $[\![\mathsf{teleportation}]\!]^\natural : \mathcal{A}^{\{q_1,q_2,q_3\}} \to \mathcal{A}^{\{q_1,q_2,q_3\}} = \lambda(b,\pi).(b^{q_1,q_2\mapsto\mathbf{s},q_3\mapsto\top},\bot)$. Thus, for any 3-qubit state, the state of the memory after the teleportation is fully separable.

Assume that a fourth qubit q_4 is entangled with q_1 before the teleportation, whereas q_2 and q_3 are in the state $\mathrm{P}^{\mathsf{true}}$. So that, the state of the memory before the teleportation is $[q_1,q_4]$-separable. The abstract semantics of $\langle \mathsf{teleportation}, \{q_1,q_2,q_3,q_4\}\rangle$ is such that

$$[\![\mathsf{teleportation}]\!]^\natural(b,[q_1,q_4]) = (b^{q_1,q_2\mapsto\mathbf{s},q_3\mapsto\top},[q_3,q_4])$$

Thus the abstract semantics predicts that q_3 is entangled with q_4 at the end of the teleportation, even if q_3 never interacts with q_4.

Example 4. Consider the program $\langle \mathsf{trap}, \{q_1,q_2\}\rangle$, where

$$\mathsf{trap} = \mathsf{CNot}(q_1,q_2);\mathsf{CNot}(q_1,q_2)$$

Since $CNot$ is self-inverse, $[\![\mathsf{trap}]\!] : \mathcal{D}^{\{q_1,q_2\}} \to \mathcal{D}^{\{q_1,q_2\}} = \lambda\rho.\rho$. For instance, $[\![\mathsf{trap}]\!](\frac{1}{2}(P^{\mathsf{true}}+P^{\mathsf{false}})\otimes P^{\mathsf{true}}) = \frac{1}{2}(P^{\mathsf{true}}+P^{\mathsf{false}})\otimes P^{\mathsf{true}}$.

However, if $b_{q_1} = \mathbf{d}$ and $b_{q_2} = \mathbf{s}$ then

$$[\![\mathsf{trap}]\!]^\natural(b,\{\{q_1\},\{q_2\}\}) = (b^{q_1\mapsto\top,q_1\mapsto\top},\{\{q_1,q_2\}\})$$

Thus, according to the abstract semantics, at the end of the computation, q_1 and q_2 are entangled.

4.2 Soundness

Example 4 points out that the abstract semantics is an approximation, so it may differ from the entanglement evolution of the concrete semantics. However, in this section, we prove the soundness of the abstract interpretation (theorem 1).

First, we define a function $\beta : \mathcal{D}^Q \to B^Q$ such that $\beta(\rho)$ describes which qubits of ρ are in the standard or diagonal basis:

Definition 7. *For any finite Q, let $\beta : \mathcal{D}^Q \to B^Q$ such that for any $\rho \in \mathcal{D}^Q$, and any $q \in Q$,*

$$\beta(\rho)_q = \begin{cases} \mathbf{s} & \textit{if } P_q^{\mathsf{true}}\rho P_q^{\mathsf{false}} = P_q^{\mathsf{false}}\rho P_q^{\mathsf{true}} = 0 \\ \mathbf{d} & \textit{if } (P_q^{\mathsf{true}}+P_q^{\mathsf{false}})\rho(P_q^{\mathsf{true}}-P_q^{\mathsf{false}}) = (P_q^{\mathsf{true}}-P_q^{\mathsf{false}})\rho(P_q^{\mathsf{true}}+P_q^{\mathsf{false}}) = 0 \\ \top & \textit{otherwise} \end{cases}$$

A natural soundness relation is then:

Definition 8 (Soundness relation). *For any finite set Q, let $\sigma \in \wp(\mathcal{D}^Q, \mathcal{A}^Q)$ be the soundness relation:*

$$\sigma = \{(\rho, (b, \pi)) \mid \rho \textit{ is } \pi\textit{-separable and } \beta(\rho) \leq b\}$$

The approximation relation is nothing but the partial order $\leq$: (b, π) is a more precise approximation than (b', π') if $(b, \pi) \leq (b', \pi')$. Notice that the abstract soundness assumption is satisfied: if ρ is π-separable and $\pi \leq \pi'$ then ρ is π'-separable. So, $(\rho, a) \in \sigma$ and $(\rho, a) \leq (\rho', a')$ imply $(\rho', a') \in \sigma$.

However, the best approximation is not ensured. Indeed, there exist some 3-qubit states [6,4] which are separable according to any of the 3 bipartitions of their qubits $\{a, b, c\}$ but which are not $\{\{a\}, \{b\}, \{c\}\}$-separable. Thus, the best approximation does not exist.

However, the soundness relation σ satisfies the following lemma:

Lemma 1. *For any finite set Q, any $\rho_1, \rho_2 \in \mathcal{D}^Q$, and any $a_1, a_2 \in \mathcal{A}^Q$,*

$$(\rho_1, a_1), (\rho_2, a_2) \in \sigma \implies (\rho_1 + \rho_2, \pi_1 \vee \pi_2) \in \sigma$$

Moreover, the abstract semantics is monotonic according to the approximation relation:

Lemma 2. *For any command C, $[\![C]\!]^\natural$ is $\leq$-monotonic: for any $\pi_1, \pi_2 \in \mathcal{A}^Q$,*

$$\pi_1 \leq \pi_2 \implies [\![C]\!]^\natural(\pi_1) \leq [\![C]\!]^\natural(\pi_2)$$

Proof. The proof is by induction on C.

Theorem 1 (Soundness). *For any program $\langle C, Q\rangle$, any $\rho \in \mathcal{D}^Q$, and any $a \in \mathcal{A}^Q$,*

$$(\rho, a) \in \sigma \implies ([\![C]\!](\rho), [\![C]\!]^\natural(a)) \in \sigma$$

Proof. The proof is by induction on C.

In other words, if ρ is π-separable and $\beta(\rho) \leq b$, then $[\![C]\!](\rho)$ is π'-separable and $\beta([\![C]\!](\rho)) \leq b'$, where $(b', \pi') = [\![C]\!]^\natural(b, \pi)$.

5 Conclusion and Perspectives

In this paper, we have introduced the first quantum entanglement analysis based on abstract interpretation. Since a classical domain for driving a sound and complete analysis of entanglement is exponentially large in the number of qubits, an abstract domain based on partitions has been introduced. Moreover, since the concrete domain of superoperators is not a lattice, no Galois connection can be established between concrete and abstract domains. However, despite the absence of best abstraction, the soundness of the entanglement analysis has been proved.

The abstract domain is not only composed of partitions of the memory, but also of descriptions of the qubits which are in a basis state according to the standard or diagonal basis. Thanks to this additional information, the entanglement analysis is more subtle than an analysis of interactions: the $CNot$ transformation is not an entangling operation if the first qubit is in the standard basis or if the second qubit is in the diagonal basis.

A perspective, in order to reach a more precise entanglement analysis, is to introduce a more concrete abstract domain, adding for instance a third basis, since it is known that there are three mutually unbiased basis for each qubit.

A simple quantum imperative language is considered in this paper. This language is expressive enough to encode any quantum evolution. However, a perspective is to develop such abstract interpretation in a more general setting allowing high-order functions, representation of classical variables, or unbounded quantum memory. The objective is also to provide a practical tool for analysing entanglement evolution of more sophisticated programs, like Shor's algorithm for factorisation [19].

Another perspective is to consider that a quantum computer is available for driving the entanglement analysis. Notice that such an analysis of entanglement evolution is not trivial, even if a quantum computer is available, since a tomography [21] is required to know the entanglement of the quantum memory state[9].

6 Acknowledgements

The author would like to thank Philippe Jorrand and Frédéric Prost for fruitful discussions. The author is supported by EC STREP FP6-033763 Foundational Structures for Quantum Information and Computation (QICS).

References

1. S. Abramsky. A Cook's tour of a simple quantum programming language. *3rd International Symposium on Domain Theory, Xi'an, China*, May 2004.
2. A. Aspect, P. Grangier, and G. Roger. Experimental tests of realistic local theories via Bell's theorem. *Phys. Rev. Lett.*, 47:460, 1981.
3. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.
4. C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal. Unextendible product bases and bound entanglement. *Phys. Rev. Lett.*, 82:5385, 1999.

[9] It mainly means that in order to obtain an approximation of the quantum memory entanglement, several copies of the memory state are consumed.

5. Patrick Cousot and Radhia Cousot. Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *POPL*, pages 238–252, 1977.
6. T. Eggeling and R. F. Werner. Separability properties of tripartite states with uuu -symmetry. *Phys. Rev. A*, 63(0421111), 2001.
7. A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of reality be considered complete? *Phys. Rev.*, 47(10):777–780, May 1935.
8. S. J. Gay. Quantum programming languages: Survey and bibliography. *Mathematical Structures in Computer Science*, 16(4), 2006.
9. S. J. Gay, A. K. Rajagopal, and N. Papanikolaou. Qmc: A model qmc: A model checker for quantum systems. arXiv:0704.3705, 2007.
10. L. Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the 35-th ACM Symposium on Theory of Computing*, page 10. ACM Press, New York, 2003.
11. Ph. Jorrand and M. Mhalla. Separability of pure n-qubit states : two characterizations. *IJFCS*, 14(5):797–814, 2003.
12. E. Kashefi. Quantum domain theory - definitions and applications. In *Proceedings of Computability and Complexity in Analysis (CCA03)*, 2003.
13. M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.
14. S. Perdrix. *Formal models of quantum computation: resources, abstract machines and measurement-based quantum computation (in french)*. PhD thesis, Institut National Polytechnique de Grenoble, 2006.
15. S. Perdrix. A hierarchy of quantum semantics. to appear in the Proceedings of the 3rd International Workshop on Development of Computational Models, 2007.
16. F. Prost and C. Zerrari. A logical analysis of entanglement and separability in quantum higher-order functions. arXiv.org:0801.0649, 2008.
17. P. Selinger. A brief survey of quantum programming languages. In *Proceedings of the 7th International Symposium on Functional and Logic Programming*, volume 2998 of *Lecture Notes in Computer Science*, pages 1–6. Springer, 2004.
18. P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.
19. P. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In IEEE Computer Society Press Shafi Goldwasser, editor, *Proceedings of the 35nd Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.
20. M. Van den Nest, A. Miyake, W. Dür, and H. J. Briegel. Universal resources for measurement–based quantum computation, 2006.
21. Andrew G. White, Alexei Gilchrist, Geoffrey J. Pryde, Jeremy L. O'Brien, Michael J. Bremner, and Nathan K. Langford. Measuring two-qubit gates. *J. Opt. Soc. Am. B*, 24(2):172–183, 2007.