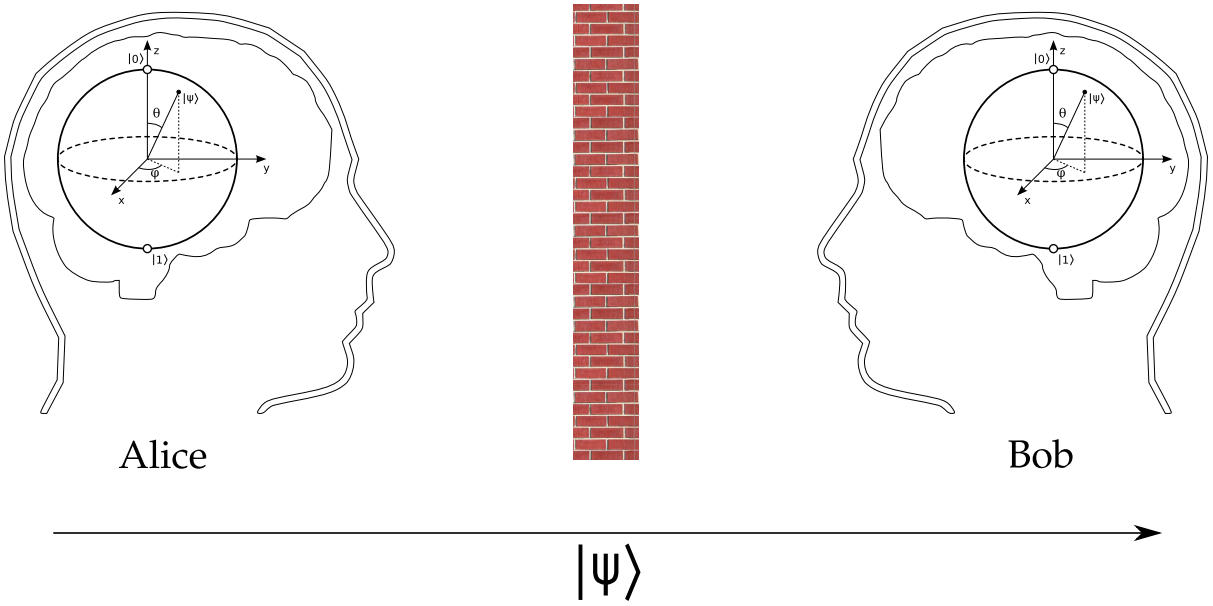
IMPERIAL COLLEGE LONDON

MSC. ADVANCED COMPUTING ISO 2

Epistemic Verification of Quantum Protocols



Author:
Graham MARKALL

Supervisor:
Dr. Alessio LOMUSCIO

Abstract

Recently, logics which can be used to reason about the knowledge state of agents in a distributed system in which quantum computation is performed have been developed. In this report, the three main approaches are surveyed and analysed. These logics are applied to perform verification of epistemic properties of the Quantum Teleportation protocol. The most well-developed approach is found to be one based on the Distributed Measurement-Based Computation semantics for quantum computation. We discuss how epistemic verification fits in to the wider context of quantum algorithm verification and how epistemic properties may be added to existing verification tools. Starting points for further research in this area are discussed.

Contents

Chapter 1

Introduction

The security of classical cryptography relies on the assumption that factoring large numbers is an intractable problem [43]. With the development of Peter Shor's polynomial-time quantum algorithm for integer factorisation [50], this assumption no longer holds. Although it seems that reliable physical implementations of quantum algorithms will not be developed for some time in the future, it is important to develop cryptographic algorithms which do not reply on this assumption.

Quantum algorithms for key distribution (QKD) which do not require this assumption to hold have been proposed. These include the BB84 protocol [9], and the Ben92 protocol [10]. The BB84 protocol has been theoretically proven to be "unconditionally secure"[41] - that it is secure against all conceivable attacks. However, a theoretical proof of security does not take practical implementation issues into consideration. As a result, practical implementations of Quantum Key Distribution may be open to attacks which are not possible against the theoretical model [30]. In order to ensure security of practical implementations of QKD protocols (and other quantum protocols), verification of models of practical implementations must be performed.

Several different techniques for protocol verification exist. This report focuses on an epistemic approach to verification, which considers the knowledge states of agents in a distributed multi-agent system (see Chapter 5 for a brief discussion of other techniques). The epistemic approach has been used in the verification of classical communication and security protocols since the first application was presented in [31].

1.1 Knowledge in Quantum Systems

There are fundamental differences between classical and quantum computation (see Section 2.2 for a brief overview of quantum computation). Existing epistemic logics are only equipped to deal with the classical case. As a result, it is difficult to apply these logics to perform verification of quantum protocols. It may be argued that there is a need to develop a new epistemic logic, a *quantum epistemic logic*. However, in developing a logic there are several questions which must be addressed, including:

- How should knowledge be defined?
- Should agents be regarded as knowing the state of arbitrary qubits in their possession?
- How can the set of quantum states be restricted to a finite set of states about which we may reason?

Three approaches to modelling knowledge in quantum systems have been presented in the literature in recent years. Each of these approaches will be described and analysed, in order to determine their strengths and weaknesses with regard to modelling the knowledge of agents in quantum systems. Each approach has also been applied to verify epistemic properties of the Quantum Teleportation protocol [11], in order to strengthen the analysis and demonstrate the characteristics of each approach.

1.2 Structure

A brief description of epistemic logic, quantum computation and quantum logic is given in Chapter 2 to familiarise the reader with these concepts. The three approaches are discussed in Chapter 3, and their application to verification of the Quantum Teleportation protocol is presented in Chapter 4. Related approaches to verification are discussed in Chapter 5. Conclusions and a brief summary of starting points for further work are given in Chapter 6.

Chapter 2

Background

2.1 Epistemic Logic

Epistemic logic [23] may be used for reasoning about the knowledge of agents in a distributed multi-agent system, and was originally proposed in [33]. The logic is based on a possible-worlds notion of knowledge - an agent considers that several possible *global states* may exist based on its *local state*. A global state consists of the local states of all the agents in the system. An agent *knows* that a statement is true if the statement is true in all of the worlds it considers possible.

Epistemic logics are a type of modal logic [14]. The frame over which the logics are evaluated consists of all of the possible global states of the system. An accessibility relation $\sim_i$ over the worlds is defined for each agent i in the system. Two worlds are related by $\sim_i$ if the local state of agent i is equal in both of the worlds. Therefore, global states which the agent i cannot distinguish are related by $\sim_i$. An interpretation (or valuation) defined over the frame gives the truth value of propositions at each global state. At a global state s of a frame $\mathcal{F}$, the formula ϕ is evaluated based on the interpretation function π:

$$\mathcal{F}, s \models \phi \text{ iff } \pi(s, \phi) = true$$

To formally describe the knowledge of agents, the modality K_i is introduced for each agent i. The statement $K_i\phi$ (Agent i knows ϕ) has the following semantics:

$$\mathcal{F}, s \models K_i\phi \text{ iff } \forall s' \simeq_i s : \mathcal{F}, s' \models \phi$$

Since the accessibility relation of the epistemic modality is an equivalence relation, the modality satisfies the axioms of the system S5. These axioms are:

$$K_i p \rightarrow p \qquad \text{(Truth)}$$
$$K_i p \rightarrow K_i K_i p \qquad \text{(Positive Introspection)}$$
$$\neg K_i p \rightarrow K_i \neg K_i p \qquad \text{(Negative Introspection)}$$

The consequence of the Truth axiom is that agents only know things which are true. The consequence of the Positive Introspection axiom is that if an agent knows a fact, it knows that it knows that fact. Finally, the consequence of Negative Introspection is that if an agent doesn't know a fact, it knows that it does not know that fact.

2.2 Quantum Computation

Quantum computation [46] is performed on the quantum analogue of bits, which are quantum bits, or *qubits*. A qubit is a state in a two dimensional Hilbert space. The basis for this space is regarded as a computational basis. Often the *standard basis* is used, which consists of the vectors

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \qquad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \tag{2.1}$$

An alternative basis which is sometimes used is the *Bell basis*:

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \qquad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \tag{2.2}$$

However, any basis may potentially be used as a computational basis. In general, qubits are of the form

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \text{where } |\alpha|^2 + |\beta|^2 = 1 \tag{2.3}$$

This means that the state of a qubit is a unit vector in two-dimensional Hilbert space. The state $|\psi\rangle$ referred to as a *superposition* of the basis vectors. It is in both the state $|0\rangle$ and $|1\rangle$ simultaneously, until it is measured. When a qubit in the state $\alpha|0\rangle + \beta|1\rangle$ is measured in the basis $\{|0\rangle, |1\rangle\}$, the outcome of the measurement will be either $|0\rangle$ with probability $|\alpha|^2$, or $|1\rangle$ with probability $|\beta|^2$. Also, the effect of the measurement is to "collapse" the state of the measured qubit to the state $|0\rangle$ or $|1\rangle$. In other words, when a qubit is measured, the system "decides" whether it is in the state $|0\rangle$ or $|1\rangle$ and collapses to that state.

2.2.1 Multiple Qubits

The state of a system of multiple qubits is the tensor product of the state vectors of the individual qubits which they consist of. For example, the state of a two qubit system made up of qubits q_1 and q_2 is given by $q_1 \otimes q_2$.

2.2.2 Quantum Gates

A *Quantum Gate* may be applied to a qubit (or qubits) which transforms its state in some defined way. All quantum gates may be represented by unitary matrices. The result of applying a quantum gate G to a qubit $|\psi\rangle$ is computed by multiplying the matrix representation of the gate by the state vector of the qubit. The four quantum gates which are used in the protocol considered in this report are as follows:

$$X = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} \qquad Z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix} \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \qquad CNOT = \begin{pmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{pmatrix}$$

The X, Z, and H (Hadamard) gates all operate on a single qubit. The $CNOT$ gate operates on two qubits. To calculate the result of applying the $CNOT$ gate to two qubits, the matrix representation of the gate is multiplied by the tensor product of the state vectors of the qubits.

2.2.3 Entanglement

Two qubits may be put in to an *entangled* state by application of the H gate to the first qubit and a subsequent application of the $CNOT$ gate to both qubits. The resulting state is a vector which cannot be written as the tensor product of two separate qubits. In this case, neither qubit is in a well-defined local state. The effect of entanglement is that operations on the first qubit have a deterministic effect on the second qubit, and vice-versa. This non-local effect occurs even if the entangled pair of qubits are spatially separated. Quantum protocols which exploit this non-local behaviour include the Quantum Teleportation and Quantum Key Distribution protocols.

There are four entangled states which may be generated from input qubits $|x\rangle$ and $|y\rangle$, and these states are written in shorthand as β_{xy}:

- When $x = y = 0$, the output of the entanglement operation is $(|0\rangle \otimes |0\rangle) + (|1\rangle \otimes |1\rangle)$, the state β_{00}.

- When $x = 0$ and $y = 1$, the output of the entanglement operation is $(|0\rangle \otimes |1\rangle) + (|1\rangle \otimes |0\rangle)$, the state β_{01}.
- When $x = 1$ and $y = 0$, the output of the entanglement operation is $(|0\rangle \otimes |0\rangle) - (|1\rangle \otimes |1\rangle)$, the state β_{10}.
- When $x = y = 1$, the output of the entanglement operation is $(|0\rangle \otimes |1\rangle) + (|1\rangle \otimes |0\rangle)$, the state β_{11}.

2.2.4 Quantum Circuits

A convenient notation for representing sequences of actions performed over multiple qubits is the quantum circuit notation. In a quantum circuit, the state vectors of the input qubits are shown to the left of the circuit. These qubits are then operated on by a sequence of operations moving from left to right across the circuit. The state vectors of the output qubits may be shown on the right.

An example of a quantum circuit which entangles two qubits is shown in Figure 2.1. The two input qubits in this case are both initially $|0\rangle$. The output qubits are $|\beta_{00}^1\rangle$ and $|\beta_{00}^2\rangle$, which are the first and second qubits respectively of an entangled pair in the state $|\beta_{00}\rangle$.

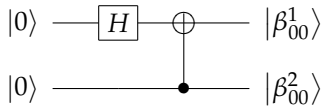


Figure 2.1: A quantum circuit for entangling two qubits.

2.2.5 Quantum Logic

Quantum logic is a logical system for reasoning about properties of quantum mechanical systems (see [13, 24] for more information). Essentially the logic has similarities to propositional logic, but the distributive law is excluded. The consequence of this is that the deduction theorem also fails for quantum logic.

It should be noted that the currently accepted view of quantum logic has little relation to quantum computing, although recently there have been attempts to bring together the two, including [42], and the Dynamic Epistemic Quantum Logic approach described in Section 3.4.

Chapter 3

Modelling Knowledge in Quantum Systems

3.1 Introduction

There are two approaches to modelling knowledge in multi-agent systems which perform quantum computation. A logical approach to proving correctness of quantum programs which enables reasoning about epistemic properties of quantum systems has recently been developed. In this chapter, we describe and analyse these three approaches. We conclude with a short comparison.

3.2 Qubit Message Passing Environments

The first attempt to define a semantics for representing the knowledge states of agents which perform quantum computation was put forward in [51]. The system of logic presented defines modalities for two types of knowledge: *classical knowledge*, which represents the knowledge available to an agent based upon their classical state only, and *quantum knowledge*, which represents the knowledge of an agent based upon the state vectors of qubits in their possession as well as their classical state. A description of the environments and the logic follows.

3.2.1 Environments

An environment is a system made up of a set of agents and a set of qubits. In the following definitions, it is assumed that the environment consists of N qubits and n agents. Each agent may be in possession of some of the qubits - however, each qubit is possessed by one agent at a time.

There is a classical communications channel between every pair of agents, and also from each agent to itself. This channel allows classical messages to be transmitted between any two agents reliably. Agents are also interconnected by quantum channels, which allow qubits to be transmitted from one agent to another. If a quantum system is implemented using photons as qubits, quantum channels may be physically realised by fibre optic cables [46].

3.2.2 The State of Environments

Four elements make up the classical state of an environment:

Variables. Each agent has a set of classical variables in which Boolean values are stored. $\mathtt{Var}_i$ is a set of variable names for each agent i. A function $\mathtt{var}$ is the assignment of a truth value to the variables of agent i, defined as $\mathtt{var}(i) : \mathtt{Var}_i \rightarrow \{0, 1\}$.

Qubit Locations. Each agent is aware of which qubits are in its possession. The injective function $\mathtt{loc} : [0, N] \rightarrow [0, n]$ is a mapping from qubits to agents. Intuitively this tells us which agent is in possession of a particular qubit. Conversely, $\mathtt{loc}^{-1}$ tells us which qubits an agent possesses.

Classical Messages. Agents can send messages to each other on reliable classical channels. A set of messages, $\texttt{Msg}$ is defined. This set also contains the value $\perp$, which represents an empty message. The mapping $\texttt{chan} : [1 \dots n]^2 \to \texttt{Msg}$ between classical channels and messages is defined. Intuitively, $\texttt{chan}(i, j) = \texttt{m}$ means that agent i has just sent the message $\texttt{m}$ to agent j.

Quantum Measurement Results. When an agent performs a measurement on one (or more) of its qubits, the outcome of the measurement is stored as parts of its classical state. The set $\texttt{res}(i) = (M^i, m_i)$ records a set of measurements, M, and their outcomes, m, which agent i has made. In the initial state, $\texttt{res}(i) = \emptyset$ for all agents since no measurements have been made. As measurements are made, each new measurement result is added to the set.

The classical state of an environment, s^c, is a tuple made up of these four elements:

$$s^c = \langle \texttt{var}, \texttt{loc}, \texttt{chan}, \texttt{res} \rangle$$

The quantum state of an environment, s^q is simply a unit vector in $\mathcal{Q}^N$. This vector is the tensor product of the state of all the qubits in the system. A global state s is a tuple made up of the classical and quantum state of the environment: $s = \langle s^q, s^c \rangle$.

An interpretation function is defined over the set S, which contains all possible states of a given Qubit Message Passing Environment. The set $\texttt{Prop}$ is a set of propositional atoms. The interpretation function is then defined by $\pi : S \times \texttt{Prop} \to \{0, 1\}$. Since quantum states which differ by a global phase factor $z \in \mathbb{C}$ where $|z| = 1$ are considered identical, the interpretation of Qubit Message Passing Environments whose state only differs by a global phase in the quantum states must be identical.

3.2.3 Actions

Agents are able to perform actions which affect the global state of the environment. These are:

Variable assignment. Agents may assign a Boolean value to one of their classical variables. The statement $v := b$ represents the assignment of the Boolean value b to the variable v where $v \in \texttt{Var}_i, b \in \{0, 1\}$.

Random Variable Assignment. Agents may also assign a random Boolean value to one of their classical variables. The action $\texttt{flip}(v)$ assigns a random value to the variable v where $v \in \texttt{Var}_i$.

Qubit transmission. An agent may use the quantum channel to transmit one of the qubits in its possession to another agent. This is represented by the statement $\texttt{transmit}(b, j)$ where $b \in \texttt{loc}^{-1}(i)$. The effect on the environment of this action is to change $\texttt{loc}(b)$ to equal j.

Classical Message Transmission. An agent may send a classical message using the classical channel to another agent, which is achieved by performing the action $\texttt{send}_{i,j}(\texttt{m})$. The effect of this is to set $\texttt{chan}(i, j) = \texttt{m}$ in the next state. Additionally, $\forall k : k \neq j, \texttt{chan}(i, k) = \perp$. Intuitively, this means that an agent may send a classical message to one agent at once.

Qubit Measurement. An agent may also perform a measurement on one or more of its qubits. The effect of the measurement is to collapse the states of the measured qubits to one of the vectors of the basis in which they are measured. The tuple (M, m) made up of the measurement, M, and its outcome m is added to the set $\texttt{res}(i)$.

3.2.4 Runs, Points, and Protocols

Runs. A *run*, $r : \mathbb{N} \to S$ maps the natural numbers on to the set of global states. This can be thought of as specifying the temporal evolution of an environment, as successive natural numbers map to successive states of the system.

Points. A *point* on a run, $r(m)$ is the global state of the system at a particular time m.

Protocols. A pattern of behaviour exhibited by an agent in the environment is characterised by its protocol, which describes what action an agent will take based upon its observations. An observation $\mathcal{O}_i$ represents the information which an agent has just acquired. A *protocol* for an agent i is formally defined as $P : \mathcal{O}_i^+ \rightarrow Act_i$. This means that an agent's choice of action may depend upon a sequence of observations. This also indicates that agents have perfect recall of their past observations.

Joint Protocols. A joint protocol is a tuple $\mathbf{P} = \langle P_1, \ldots, P_n \rangle$, where each $\mathbf{P}_i$ is a protocol for agent i. $\mathcal{R}(\mathcal{E}, \mathbf{P})$ is the set of all runs of the joint protocol $\mathbf{P}$ in the environment $\mathcal{E}$.

3.2.5 The Logic: Syntax and Semantics

Formulae ϕ are generated by following grammar, where p is a propositional atom:

$$\phi ::= p \mid \phi \mid \neg\phi \mid \phi \wedge \phi \mid K_i^c\phi \mid K_i^q\phi \mid \Box\phi \mid \texttt{init}(\phi)$$

Disjunction and implication may be defined in the familiar way. The modal operators and the `init` operator may be read as:

- $K_i^c\phi$: Agent i classically knows ϕ
- $K_i^q\phi$: Agent i quantumly knows ϕ
- $\Box\phi$: At all future times, ϕ
- $\texttt{init}(\phi)$: Initially, ϕ

Two equivalence relations over points are defined, $\sim_i^c$ and $\sim_i^q$, which are referred to as classical equivalence and quantum equivalence respectively. Points in which the local classical state of an agent i are equal are related by the relation $\sim_i^c$. Points in which both the local classical and quantum states of an agent i are equal are related by $\sim_i^q$. From these definitions, we can see that what is classically known by an agent is a subset of that which is quantumly known by an agent.

Formulae are evaluated with respect to an environment, $\mathcal{E}$, a joint protocol, $\mathbf{P}$, and a point on a run (r, m), where $r \in \mathcal{R}(\mathcal{E}, \mathbf{P})$. The full semantics are defined as follows:

1. $\mathcal{E}, \mathbf{P}, (r, m) \models p$ if $\pi(r(m), p) = 1$ when $p \in \texttt{Prop}$
2. $\mathcal{E}, \mathbf{P}, (r, m) \models K_i^c\phi$ if $\mathcal{E}, \mathbf{P}, (r', m') \models \phi$ for all points (r', m') of $\mathcal{R}(\mathcal{E}, \mathbf{P})$ such that $(r, m) \sim_i^c (r', m')$
3. $\mathcal{E}, \mathbf{P}, (r, m) \models K_i^q\phi$ if $\mathcal{E}, \mathbf{P}, (r', m') \models \phi$ for all points (r', m') of $\mathcal{R}(\mathcal{E}, \mathbf{P})$ such that $(r, m) \sim_i^q (r', m')$
4. $\mathcal{E}, \mathbf{P}, (r, m) \models \Box\phi$ if $\mathcal{E}, \mathbf{P}, (r, m') \models \phi$ for all $m' \geq m$
5. $\mathcal{E}, \mathbf{P}, (r, m) \models \texttt{init}(\phi)$ if $\mathcal{E}, \mathbf{P}, (r, 0) \models \phi$

3.2.6 Analysis

Having described the logic defined in this initial attempt, we note that there are several issues with the approach. These are:

Quantum gates. The set of actions which an agent may perform (Section 3.2.3) does not include application of a quantum gate to a qubit. As almost every quantum protocol includes the use of quantum gates, it is therefore only possible to verify a limited portion of any quantum protocol. Since an agent may use its current state to decide which quantum gates to apply to a qubit, or to parameterise quantum gates, it is not possible to fully model quantum protocols within this logical formalism.

Quantum Knowledge. It is not explicitly stated in the paper, but it appears that in order to make up for the lack of quantum gates, the concept of quantum knowledge may be used. As in the usual interpretation of epistemic logic, the quantum knowledge operator does not state that an agent is in a position to determine the truth of a given proposition, but that it has the information available to it including the state of its qubits to determine the truth, given unlimited resources to do so. There are several issues with quantum knowledge:

- Physically, an agent's possession of a qubit does not imply that it knows anything about the state of the qubit. It is only possible to obtain information about a qubit by measuring it, which irreversibly changes the states of the qubit. Consider a situation in which there are two agents A and B. Agent A may initialise a qubit to state $|+\rangle$ and then transmit this qubit to agent B. B will not know anything about the state of the qubit, and the only way to determine any information about the qubit is to measure it. So, suppose B decides to measure the qubit in the basis $\{|0\rangle, |1\rangle\}$ (or any other arbitrary basis). The outcome of the measurement will be either $|0\rangle$ or $|1\rangle$ (or a vector of the chosen basis), with equal probability. Not only has B not been able to correctly determine the state of the qubit, but has also destroyed the original state which the qubit was in when it was first received. Up until the state where B destroyed the state of the qubit by making a measurement, A was aware of the state of the qubit. However, the definition of quantum knowledge means that A no longer has quantum knowledge of the state of the qubit as soon as it has transmitted it to B. There is no general way for an agent to determine the state of a single unknown qubit in its possession. Therefore, the interpretation of quantum knowledge which equates possession of a qubit with knowledge of its state does not appear to be valid.
- It is argued by the authors that this difficulty may be overcome by considering that in practice, operations are not performed on single qubits, but in fact multiple qubits (ensembles) which are all initialised to the same state are used [15]. Measurements are performed by selecting a single qubit from the ensemble and measuring it alone. Many of the qubits of an ensemble may be measured, which gives a probability distribution of the state of qubits in the ensemble. Using this probability distribution, an agent may estimate the state of qubits in the ensemble.

  However, there are two problems with the ensemble interpretation:

  - It is pointed out by the authors themselves that the ensemble interpretation poses problems when considering the Quantum Teleportation protocol (see Section 4.2 for a description of the Quantum Teleportation protocol). One may assume that Alice's first qubit is actually an ensemble of qubits, and she selects a single one of these qubits to teleport to Bob. However, the ensemble interpretation no longer makes sense when considering Bob's qubit, as it is not an ensemble anymore, but a single qubit. An alternative interpretation of the protocol (which is not discussed in the paper) would be to suggest that Alice performs the teleportation protocol on all the qubits in the ensemble, so that Bob "receives" an ensemble of qubits. However, this presents a problem when Alice comes to measure her qubit and transmit the result classically to Bob, as her measurements will not all give the same result. If she were to transmit all of these measurement results to Bob, he would not know which measurement result pertains to which individual qubit in the ensemble. Therefore, he would not be able to apply the correct gates to change the state each individual qubit to equal the original state of Alice's first qubit.
  - Given additional knowledge of the expected state of a qubit (for example, it may be known that a qubit is in one of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$), it is be possible to determine with high probability the exact state of a qubit. However, in general there are an infinite number of possible states which a qubit may occupy. Therefore, an infinite number of measurements is required to determine the exact state of an unknown qubit. Therefore, it is not possible to determine the exact state of any qubit in general.

  Since both of these two problems appear insurmountable, it can be argued that the ensemble interpretation is not a valid one. As the interpretation of qubits as single qubits is also not valid, it appears that it is not possible to conceive a valid notion of quantum knowledge.

- Finally, the authors retreat a little further and argue that quantum knowledge does not model the knowledge which an agent may be in a position to compute given a realistic allocation of resources, but instead is an information-theoretic idealisation of knowledge representing the potential maximum knowledge which may be known at a given state. However, I would argue that there is no reason why this argument may not be extrapolated as far as suggesting that agents are omniscient: Since it is has been assumed that information which is physically un-knowable may be known (the state of an arbitrary qubit), there is no reason not to assume that other information which is also physically un-knowable may also be known. For example, the state of qubits possessed by other agents, the complete state of of other agents, or even the global state of the system may also be assumed to be known. Clearly, it is absurd for an agent to be completely aware of the global state. Similarly, also knowing any subset of the global state which is not part of the local state is also unrealistic.

Alongside the main problems with this approach, it is also difficult to employ this approach for automatic verification of epistemic properties of quantum protocols. Since the approach has been developed independently of any semantics of quantum computation, there is no way to specify a quantum protocol from which the runs may be generated. The only way to generate the runs of a given protocol is to do so by hand, in an ad-hoc manner.

Although it is not a barrier to verification of protocols, it is also noted that the probabilities which which a given measurement occurs are not modelled. Therefore, it is not possible to determine the probability with which a particular knowledge states arise.

Finally, no results which describe all of the steps of verification of any quantum protocols using Qubit Message Passing Environments have been presented. The published literature on this approach only states properties of various protocols without describing the process of verifying them. Essentially, this approach has not been shown to have been successfully used for verifying epistemic properties of any quantum protocols.

3.3 Distributed Measurement-Based Computation

An alternative approach to modelling knowledge in quantum systems has been developed which is built on top of a semantics for quantum computation. These semantics are known as the Measurement Calculus [18, 19], which is based on the one-way quantum computation model [49]. These semantics were extended to a distributed multi-agent setting to give *Distributed Measurement Based Computation* (DMC) [17]. Interestingly, the logic in this work does not contain any notion similar to the quantum knowledge of the previous approach.

First, a very brief explanation of the semantics of the Measurement Calculus will be given, and a short description of the extension to a multi-agent setting. Subsequently we describe the epistemic logic whose worlds are defined over the possible states of these multi-agent quantum systems. Finally, we compare this approach to the one previously described.

3.3.1 Measurement Patterns

Quantum programs which may be executed on a set of qubits are referred to as *Measurement Patterns*. Patterns operate over a computation space V, which is the set of qubits over which the pattern operates. The sets of input qubits I and output qubits O are subsets of V. The sequence of commands $\mathcal{A}$ represents the operations which the pattern performs on the qubits in the computation space. A pattern is completely specified by $\mathcal{P}(V, I, O, \mathcal{A})$.

The full semantics of measurement patterns is presented in [19]. For brevity these will not be repeated here. Instead, a short intuitive description of measurement patterns follows. The sequence of commands is made up of basic operations which are performed on the qubits in the computation space. Operations are executed sequentially, beginning with the rightmost operation. Each operation may be one of the following:

Entanglement. The entanglement operator E_{xy} entangles the qubits x and y, in a similar way to the entanglement circuit (Figure 2.1).

Measurement. The measurement operator M_i^α measures the qubit i in the basis $|+_\alpha\rangle, |-_\alpha\rangle$, given by:

$$|+_\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\alpha}|1\rangle)$$
$$|-_\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i\alpha}|1\rangle)$$

The result of measuring qubit i is denoted s_i, and it is assumed that the qubit is destroyed by the measurement (physically a qubit will not be destroyed by a measurement, but we can subsequently ignore its state). This means that the meaning of s_i is never ambiguous. We consider that $s_i = 0$ if the state of the qubit collapses to $|+_\alpha\rangle$ and $s_i = 1$ if its state has collapsed to $|-_\alpha\rangle$.

Measurements which are parameterised based on the results of earlier measurements are referred to as *dependent measurements*. A dependent measurement is given by ${}^t[M_i^\alpha]^s$, where s and t are the results of earlier measurements. The meaning of ${}^t[M_i^\alpha]^s$ is

$${}^t[M_i^\alpha]^s = M_i^{(-1)^s\alpha + t\pi}$$

From this definition it can be seen that M_i^α is equivalent to ${}^0[M_i^\alpha]^0$.

Corrections. The correction operators X_i and Z_i apply the X gate and Z gate respectively to the qubit i. These operators may also depend on previous measurement outcomes, and the notation for the dependent correction operators is X_i^s and Z_i^s where s is a previous measurement outcome. When $s = 0$, the correction operator is not applied, and when $s = 1$, the correction operator is applied.

It is clear that general unitary operators are not permitted in sequences of events. An additional restriction on the specification of measurement patterns is that all entanglement operations must be performed first. All measurement operations must be performed after the entanglement operations. Finally, correction operations may only be performed after measurement operations. This is not a drawback as this model of quantum computation is universal (for a proof see Section 4 of [18]). As an example, consider a pattern which applies the Hadamard gate to a qubit:

$$\mathfrak{H} = (\{1,2\}, \{1\}, \{2\}, X_2^{s_1} M_1^0 E_{12})$$

The computation space $V = \{1,2\}$, which states that the computation space consists of two qubits. The input set $I = \{1\}$ and the output set $O = \{2\}$. The input qubit is initially in an arbitrary state (call this state $|\psi\rangle$). The second qubit is initialised to $|+\rangle$ prior to the execution of this pattern. When the pattern executes, the two qubits are entangled and then the first qubit is measured. The correction operator X is applied to the second qubit depending on the result of the measurement outcome. If the first qubit collapsed to the state $|+\rangle$ then no correction is required, as the state of the output qubit is already equal to $H|\psi\rangle$. If the first qubit instead collapsed to the state $|-\rangle$, then the second qubit's state is equal to $XH|\psi\rangle$. Since X is its own inverse, applying the X correction transforms the state to $X^2H|\psi\rangle = H|\psi\rangle$, the desired outcome.

3.3.2 Quantum Networks

A *Quantum Network* is essentially a multi-agent system consisting of agents which perform classical and quantum computation. Agents may communicate over classical channels, and may transmit qubits over quantum channels. Quantum Networks are specified in a form which is similar to a process algebra [48]. The general form of a Quantum Network is:

$$\mathcal{N} = \mathbf{A}_1 : Q_1.\mathcal{E}_1 \mid \mathbf{A}_2 : Q_2.\mathcal{E}_2 \mid \ \ldots \ \mid \mathbf{A}_m : Q_m.\mathcal{E}_m \mid\mid \sigma$$

The $\mid$ symbol denotes a parallel composition of agents. σ is the quantum state of the network, consisting of the state of a set of qubits and their entanglement. The state of all qubits $|\psi\rangle$ is the tensor product of all the individual qubits in the system. The entanglement of qubits in the system is specified by the notation E_{xy}, which denotes that the qubits x and y are entangled.

$\mathbf{A}_n$ is the n-th agent in the network and is in possession of a set of qubits Q_n. The sequence E_n of *events* performed by agent A_n may be generated from the following set of actions:

Classical communication. Communication of classical information may take place over a classical channel. $\mathtt{c}!x$ denotes the transmission of the bound variable x over the classical channel, and $\mathtt{c}?y$ denotes the reception of a value, which is then bound to the free variable y.

Quantum Communication. Qubits may be transmitted over a quantum channel. $\mathtt{qc}!x$ denotes transmission of the qubit x and $\mathtt{qc}?y$ denotes reception of the qubit y.

Patterns. The agents may also execute patterns on the qubits in their possession. This essentially allows them to perform any quantum computation locally.

The grammar generating event sequences (where $\mathcal{P}$ is a pattern) is:

$$\mathcal{E} ::= \mathtt{c}!x \mid \mathtt{c}?x \mid \mathtt{qc}!q \mid \mathtt{qc}?q \mid \mathcal{P} \mid \mathcal{E}.\mathcal{E}$$

As with patterns, the event sequences are executed in right-to-left order. The state of the agents and the network at any given time is specified by a configuration. A configuration is of a similar form to that of a network, with the addition of a local state for each agent:

$$C = \sigma \mid\mid \Gamma_1, \mathbf{A}_1 : Q_1.\mathcal{E}_1 \mid \Gamma_2, \mathbf{A}_2 : Q_2.\mathcal{E}_2 \mid \Gamma_m, \mathbf{A}_m : Q_m.\mathcal{E}_m$$

The local state Γ_n of the agent $\mathbf{A}_n$ is used to record the outcomes of measurements. The event sequences, and state of the qubits are generally not equal to the initial state of the network. As events are executed, they are consumed, and qubits may be destroyed by measurement, or may be transmitted between agents.

3.3.3 An Interpretation Function over Configurations

The set of all possible future configurations of a quantum network may be determined by simulating its execution using the semantics of DMC. Once these states have been determined, an interpretation function may be defined over all of them. The function $I(C, \phi)$ defines the interpretation of fact ϕ in the configuration C. Facts are interpreted with respect to a network and a possible configuration of that network:

$$C, \mathcal{N} \models \phi \iff I(C, \phi) = true$$

Facts which may be defined are limited to the following specification:

$$C, \mathcal{N} \models (x = v) \iff \exists i.\Gamma_i(x) = v \tag{3.1}$$
$$C, \mathcal{N} \models (x = y) \iff \exists i.\Gamma_{i,j}(x) = \Gamma_j(y) \tag{3.2}$$
$$C, \mathcal{N} \models (\mathbf{A}_i \text{ has } q) \iff q \in Q_i \tag{3.3}$$
$$C, \mathcal{N} \models (q_1 \ldots q_n = \sigma) \iff q_1 \ldots q_n = \sigma \tag{3.4}$$
$$C, \mathcal{N} \models (q_i = q_j) \iff \exists \sigma.q_i = q_j = \sigma \tag{3.5}$$

Equations 3.1 and 3.2 refer to classical value and variable equality respectively. Equation 3.3 refers to the agent in possession of a particular qubit. The final two equations may only be applied to qubits whose state is known in some sense. Equation 3.4 describes equality of qubits where the state vector of the qubits are known. Equation 3.5 refers to the equality of qubits whose state vectors are unknown, but it is known that their state vectors are equal. Two additional functions, $init(x)$ and $fin(x)$ are defined which respectively give the initial state and final state of a classical variable or qubit. The standard propositional rules may also be applied to facts in the usual way, for example conjunction (e.g. $\phi_1 \wedge \phi_2$) and negation (e.g. $\neg\phi$).

Care must be taken when specifying a property using the $init(x)$ and $fin(x)$ functions, as they can lead to surprising properties. For example, the predicate $\phi = (init(x) = fin(y))$ will be true at all states in a protocol in which the final state of y is equal to the initial state of x - whilst this seems obvious,

combining this predicate with an epistemic modality ($K_i\phi$) effectively states that agent i "knows" ϕ at all times regardless of how the epistemic accessibility relation between states is defined. Whilst this is true, agent i may not know if the final state has been reached - therefore, they may not know if they are in a state in which the current value of y is equal to the initial state of x.

3.3.4 A Logic with Epistemic and Temporal Modalities

It is argued by the authors that it is not sensible to define a notion of quantum knowledge based on the possession of qubits for similar reasons to those given in Section 3.2.6. As such, only one epistemic accessibility relation, $\sim_i$, is defined for each agent i. The local state of each agent is made up of:

- Its classical state, Γ_i.
- Which qubits it possesses.
- The operations which it has applied to these qubits.
- The initial entanglement state of its qubits.

The epistemic modality K_i is defined in the usual way. In the configuration C, the agent i knows the fact ϕ when the fact ϕ is true in all of the other configurations which it considers possible based upon its local state:

$$C, \mathcal{N} \models K_i\phi \iff \forall C' \sim_i C : C' \models \theta \tag{3.6}$$

A temporal modality is also defined, since a temporal accessibility relation is defined over the enumerated future configurations of a network. Two configurations, C and C' are related by the temporal accessibility relation (written $C \implies C'$) if the configuration C' is obtained from the configuration C in one step of the execution semantics of DMC. The closure of this relation is $C \overset{\gamma}{\implies} C'$, which states that the configuration C' can be reached from the configuration C by a succession of steps of the execution semantics, given by the path γ. The temporal operators $\Box$ (always) and $\Diamond$ (eventually) are combined with path operators A (all paths) and E (there exists a path) to give the following semantics:

$$\begin{aligned}
C, \mathcal{N} &\models A\Box\phi \iff \forall\gamma, \forall C' \text{ with } C \overset{\gamma}{\implies} C' : C' \models \phi \\
C, \mathcal{N} &\models E\Box\phi \iff \exists\gamma, \forall C' \text{ with } C \overset{\gamma}{\implies} C' : C' \models \phi \\
C, \mathcal{N} &\models A\Diamond\phi \iff \forall\gamma, \exists C' \text{ with } C \overset{\gamma}{\implies} C' : C' \models \phi \\
C, \mathcal{N} &\models E\Diamond\phi \iff \exists\gamma, \exists C' \text{ with } C \overset{\gamma}{\implies} C' : C' \models \phi
\end{aligned}$$

Additionally, composite notions of knowledge may also be defined: Everybody knows (E_G), Common Knowledge (C_G) and Distributed Knowledge (D_G) are all defined in the usual way:

$$\begin{aligned}
C, \mathcal{N} &\models E_G\phi \iff \forall i \in G : C \models K_i\phi \\
C, \mathcal{N} &\models C_G\phi \iff \forall k > 0 : C \models E_G^k\phi \\
C, \mathcal{N} &\models D_G\phi \iff \forall C' \in \cap_i\{C'' \sim_i C\} : C \models \phi
\end{aligned}$$

3.3.5 Decision Procedure

A decision procedure for determining if a given epistemic property holds for a given network has been presented [21]. The decision procedure has been proven to be sound and terminating with respect to an epistemic specification and a DMC model of a quantum network. The steps of the decision procedure are as follows:

Generation of traces using DMC. A specification of a quantum network is supplied which specifies the network to be verified. All possible execution traces are generated from this network specification.

Specification of Security Properties. The security properties which are to be verified are specified as an Epistemic System, which states the security properties to be verified in terms of knowledge.

Generate Epistemic traces. Epistemic properties of agents are defined over the execution traces produced in the first step. These describe the knowledge of each agent at each state in the traces.

Verification of Properties. The properties given in the Epistemic System are compared against the epistemic properties of the agents in order to verify whether the specification is met by the network.

This decision procedure has been applied to the Quantum Secret Sharing protocol [40] to show that it is not secure. Additionally, the path of an attack which exploits the weakness of the protocol is discovered, and is presented in [21].

3.3.6 Analysis

This approach to modelling knowledge in quantum systems has several strengths over the previously discussed approach. The characteristics which distinguish it are:

A Semantics for Quantum Computation. Since the epistemic logic is evaluated over a model consisting of worlds which may be generated by execution of a formal specification, it is possible to automatically verify properties of a given network. Only the initial state of a quantum network, and the epistemic properties which are to be verified need to be supplied; generation of the possible worlds and model-checking of the epistemic formulae may be performed algorithmically. Because the necessary algorithms have already been developed, it is possible to produce an implementation of an epistemic model checker based on this work without further research.

Quantum Gates. Although arbitrary gates may not be defined, the measurement patterns which may be defined are universal, allowing any quantum computation to be represented in this formalism. Additionally, the measurement patterns which have been applied to local qubits are recalled by the agents in their classical state. This allows agents to distinguish between states in which they have performed operations on qubits for which the initial state was unknown.

Lack of Quantum Knowledge. As stated previously, the authors of this work argue that there is no such thing as quantum knowledge. Instead, knowledge in quantum systems is only about information which may be obtained classically. The lack of quantum knowledge avoids all of the issues associated with its existence.

Representative Semantics for Classical Knowledge. The definition of classical knowledge in this approach also appears more reasonable, as its equivalence relation takes into account the operations which have been performed locally upon qubits, and the initial entanglement state of its qubits. It is also useful that agents may only be aware of the initial entanglement state, since this allows attacks upon quantum protocols by adversaries to be modelled: For example, an attacker may provide a qubit to an agent which is entangled with another qubit which it retains. This scenario can be described using the DMC formalism.

Successful Application. Several results have been presented in the literature which describe and analyse the process of verifying several quantum protocols using this approach: Ekert's Quantum Key Distribution protocol [22] is verified in [16], the Quantum Secret Sharing protocol [40] is examined (and found to contain security issues) in [21], the Superdense Coding [12] and Quantum Teleportation [11] protocols were verified in [20]. The fact that a flaw was discovered in the Quantum Secret Sharing protocol is testament to the utility of this approach - had it been the case that no flaws were found in any of the protocols, it would have been difficult to accept that this work is truly useful for verifying epistemic (security) properties of quantum protocols.

Although the logic does not reason about probabilities, there are probabilities associated with measurements in the semantics of DMC. The probability of each transition between configurations in the model is equal to the probability of a transition given by the execution semantics of DMC. Using this property could allow an extension of the logic to be developed which may be used for reasoning about the probability of specific outcomes.

3.4 Dynamic Epistemic Quantum Logic

Dynamic Epistemic Quantum Logic is a recently-developed logical framework for reasoning about quantum mechanical behaviour and quantum programs. The logic may be thought of as being in three parts:

Propositional Logic. The propositional part of the logic deals with the truth or falsity of statements about a quantum system. For example, a proposition may mean "The state of qubit 3 is $|0\rangle$". All of the propositional axioms are admitted to the propositional part of the logic (including the distributive law).

Dynamic Logic. The dynamic part of the logic is used to represent actions performed upon a quantum system. These actions may be the application of a quantum gate to a qubit, or measuring a qubit. All of the axioms of Propositional Dynamic Logic (PDL) [14] are admitted to the dynamic part of the logic, with the exception of the test $\phi?$. A "quantum test" is a measurement, which changes the state of the system, and therefore a proposition which was false before the quantum test may be true after the quantum test. In PDL, propositions which are true after a successful test were also true before the test - therefore, the axioms for a PDL test are not appropriate for the quantum test.

Epistemic Logic. The epistemic part of the logic describes the information about the global system which is available in a subset of the system. Facts which are "known" to the subset under consideration are determined in the familiar way for an epistemic logic, by checking the truth of a proposition describing the fact in all of the possible worlds at a given state.

The motivation for the development of this logic was to create a system which may be used for reasoning about quantum behaviour without giving up any of the propositional axioms, as is commonly required in other quantum logics. The resulting logic are may be used to prove correctness of quantum protocols by deriving theorems which prove the correctness based on the axioms of the logic.

Throughout its development, the logic has been presented in various forms, which are all closely related. The logics are known as the Logic of Quantum Actions [4], the Logic of Quantum Programs [7, 3] and the Logic of Quantum Information Flow [5, 8, 6]. We will focus on the Logic of Quantum Information Flow, since it includes the epistemic part of the logic.

A brief description of the models over which the dynamic and epistemic logics are evaluated will first be given. Subsequently, the logical treatment of entanglement, and how this relates to the epistemic part of the logic is described. A description of the syntax and semantics of the logic will be given. Finally, we conclude by analysing the utility of the logic for epistemic verification and making comparisons to the previously-described approaches.

3.4.1 Quantum Transition Systems

The dynamic part of the logic is built up over a Quantum Transition system, which has a set of states Σ. These correspond to the states which a physical quantum system may occupy, which are characterised by one-dimensional subspaces ("rays") of a Hilbert space. The quantum system may contain an arbitrary number of qubits (Each qubit is denoted q_i), and therefore the Hilbert space may be of an arbitrary number of dimensions. The accessibility relation between two of the states of Σ is based upon the action of quantum gates (unitary transformations) and measurements of qubits. Two states s_1 and s_2 are related by the accessibility relation $s_1 \xrightarrow{R} s_2$ if the operation of the quantum gate or measurement R on s_1 leaves the system in the state s_2. It is clear from these definitions that there are an infinite number of worlds of all Quantum Transition Systems, since there are an infinite number of one-dimensional subspaces of any Hilbert space.

The authors state that a disadvantage of using rays as the definition of a state is that the phase of the system is lost. However, this is unlikely to be a problem for checking of most quantum security protocols, as phase-related effects are not present in these protocols.

3.4.2 Separation and Entanglement

Quantum systems made up of multiple qubits may be broken down into subsystems and considered separately. If we have a global system S (consisting of all the qubits in the system), the system may be broken down into a number of subsystems:

$$S = S_1 \otimes \cdots \otimes S_n \tag{3.7}$$

Each subsystem S_m may contain several qubits, and must contain at least one qubit. Two subsystems are separated if they do not share any entangled qubits. When two systems are separated, actions which are performed on one of the subsystems have no effect on the other subsystem. The actions which affect only the subsystem i are referred to as i-local actions.

An equivalence relation over possible global states from the point of view of the i^{th} system may be defined. Two states s and s' are i-equivalent ($s \simeq_i s'$) if and only there exists a j-local action U such that $s = U(j)$ when $i \neq j$. As a concrete example, consider a system of two qubits, q_1 and q_2. The compound system $S = q_1 \otimes q_2$. We (arbitrarily) define two subsystems S_1 and S_2 where $q_1 \in S_1$ and $q_2 \in S_2$. Assume that in the state s, $q_1 = |0\rangle$ and $q_2 = |0\rangle$. In this state, the qubits are clearly not entangled. Now, the action of applying the Hadamard gate H to the second qubit (call this action H_2) changes the state of the second qubit to $|+\rangle$. Call this new state s'. Since H_2 is a 2-local action such that $s' = H_2(s)$, the states s and s' are 1-equivalent, i.e. $s \simeq_1 s'$. From the point of view of subsystem S_1, both the states s and s' are equally possible.

A special constant c is also defined, which denotes that a system is *separated*, i.e. that it is not entangled. A subsystem s_1 is not entangled with another subsystem s_2 in the state s iff there exists a state s' such that $s \simeq_2 s' \simeq_1 c$.

3.4.3 Introducing a Knowledge Operator

Since there is an equivalence relation $\simeq_i$ for possible worlds based on the information available to the subsystem i, the authors argue that it is natural to define an epistemic modality, K_i whose accessibility relation is based on this equivalence relation. This knowledge operator is somewhat abstract, since it does not consider knowledge of an observer or agent in possession of the qubits, but rather only the information available about the global system based on the information available at subsystem i.

Since the accessibility relation is an equivalence relation, the epistemic modality satisfies the axioms of the system S5, much like the usual definition of an epistemic operator. Similarly, the truth of a statement involving this operator at a world w of a Quantum Transition System $\mathcal{QTS}$ may be defined as

$$\mathcal{QTS}, w \models K_i\phi \text{ if and only if } \forall w' : w \simeq_i w', \mathcal{QTS}, w' \models \phi \tag{3.8}$$

It should be noted that this epistemic modality is similar to the modality K_i^q of Qubit Message Passing Environments. Therefore, it is probably not very useful for actual verification of knowledge which an agent may be in possession of, since possession of the subsystem does not enable one to know the state of the qubits.

3.4.4 The Logic

The syntax of the logic is defined for propositions, ϕ, and for programs, π:

$$\begin{aligned} \phi &::= \mid \sigma_i \mid \neg\phi \mid \phi \wedge \phi \mid [\pi]\phi \mid K_i\phi \\ \pi &::= \mid \alpha_i \mid \phi? \mid \pi \cup \pi \mid \pi;\pi \mid \pi^* \end{aligned}$$

All of the axioms of Propositional Dynamic Logic are admitted, with the exception of the axiom regarding the test ($[p?]q \equiv p \rightarrow q$). The semantics of the logic without the epistemic operator are given in [7]. For simplicity, the full semantics will not be repeated here. Instead, a short description will be

given to provide the reader with an intuition of the semantics. The meaning of terms in the grammar generating ϕ are:

Propositions. σ is a propositional variable, or the special constant c. Propositional variables may be of the form b_i, which states that the qubit q_i is in the state $|b\rangle$. The truth of the propositional variable depends on whether the qubit is actually in that state. The proposition σ_i applies the proposition to a particular subsystem of the compound system. At a world w of a quantum transition system $\mathcal{QTS}$, $\mathcal{QTS}, w \models b_i$ iff the qubit q_i is in the state $|b\rangle$.

Negation. The proposition ϕ is a property, which may be testable (see the description of Quantum Tests below). The negation of a property $\neg\phi$ is the expression that a property ϕ does not hold - however, this negated property may not be testable itself. The set of all testable properties can be made up from all of the negation-free formulae of the logic.

Conjunction. The conjunction of two propositions ϕ_1 and ϕ_2 is given in the usual way by $\phi_1 \wedge \phi_2$, and this conjunction has the same meaning as in a Boolean algebra. $\mathcal{QTS}, w \models \phi_1 \wedge \phi_2$ iff $\mathcal{QTS}, w \models \phi_1$ and $\mathcal{QTS}, w \models \phi_2$.

Execution. The proposition $[\pi]\phi$ states that the property ϕ holds after execution of the program π. $\mathcal{QTS}, w \models [\pi]\phi$ if and only if for all w' such that $w \xrightarrow{\pi} w'$, $\mathcal{QTS}, w' \models \phi$.

Knowledge. The knowledge operator $K_i\phi$ is as described above (Equation 3.8).

The meaning of terms in the grammar generating π are:

Actions. α_i is the action of a quantum gate on the qubit or set of qubits i. If a formula is evaluated with respect to world w prior to the execution of the action, the remainder of the formula is evaluated at the world w' after the execution of the action if $w \xrightarrow{\alpha_i} w'$. Note that since actions are deterministic, there is always one α_i successor to any world w. $\mathcal{QTS}, w \models [\alpha_i]\phi$ iff for w' such that $w \xrightarrow{\alpha_i} w'$, $\mathcal{QTS}, w' \models \phi$.

Quantum Tests. The operator $\phi?$ is a successful test of a property ϕ. This corresponds to the measurement of qubits. Unlike the PDL test, the successful execution of a quantum test may also change the truth state of propositional variables . If the quantum test is successful, then the properties which were tested for will hold in the resulting world, even if they did not in the world in which they were tested. The quantum test will fail if the property of the qubits tested is orthogonal to the property tested. For example, if $q_1 = |0\rangle$ in a world w of a quantum transition system $\mathcal{QTS}$, $\mathcal{QTS}, w \models [1_1?]\bot$ since the outcome of measuring qubit q_1 will never be $|0\rangle$. For successful quantum tests, $\mathcal{QTS}, w \models [\phi_1?]\phi_2$ iff for all w' such that $w \xrightarrow{\phi_1?} w'$, $\mathcal{QTS}, w' \models \phi_2$.

Choice. A non-deterministic choice of programs π_1 and π_2 is given by $\pi_1 \cup \pi_2$. $\mathcal{QTS}, w \models [\pi_1 \cup \pi_2]\phi$ iff $\mathcal{QTS}, w \models [\pi_1]\phi$ or $\mathcal{QTS}, w \models [\pi_2]\phi$.

Composition. The execution of a program π_2 after the execution of a program π_1 is given by $\pi_1; \pi_2$. $\mathcal{QTS}, w \models [\pi_1; \pi_2]\phi$ iff $\mathcal{QTS}, w \models [\pi_1][\pi_2]\phi$.

Iteration. Iteration of a program π zero or more times is given by π^*. $\mathcal{QTS}, w \models [\pi^*]\phi$ iff $\mathcal{QTS}, w \models \phi \wedge [\pi][\pi^*]\phi$.

3.4.5 Analysis

This approach is quite different to the two previously presented, as it is designed as a tool for proving correctness of quantum programs rather than as a tool for model checking. However, the addition of the knowledge operator does allow the examination of some epistemic properties of the systems. The main differences between this approach and the previous two are:

Abstraction. As a consequence of the logic being designed to prove properties of quantum computations in an abstract fashion, it is not possible to represent agents using the logic. The closest thing to a notion of agents in the system is the ability to consider subsystems of quantum systems in terms of a set of qubits.

Quantum Knowledge. The knowledge operator has a similar behaviour to that of quantum knowledge in the Qubit Message Passing Environments approach. It is stated by the authors of the work on Dynamic Epistemic Quantum Logic that the knowledge operator should not be regarded as the knowledge which could physically be gathered by an observer, but instead should be used to reason about the information in the rest of the system. This is because the equivalence relation for the knowledge operator is defined in terms of entanglement of the qubits of the subsystem under consideration. As a result, the knowledge operator provides a description of the correlation between the effects of measurement on one part of the system with its effects on another, non-local part of the system. Although this interpretation of the knowledge operator is far more plausible than one which suggests that agents know the state of any qubit, it is no more useful when considering distributed systems of agents.

As with the first two approaches described, this logic does not reason about probabilities of measurement results. Instead, any possible measurement results are considered. However, with further research, it may be possible to add to this logic to enable reasoning about probabilities.

Because this logic is intended as a proof-theoretic tool, it may be used for reasoning over any qubit values (by using a proposition such as ϕ_1, which denotes that qubit 1 has any testable property). This is a problem if epistemic properties are to be verified automatically, since the state space of a quantum program described using the logic is essentially infinite. In other words, there are an infinite number of possible worlds in the quantum transition system, each world having an infinite number of relations to other worlds. However, it may be possible to use the logic to produce proofs of epistemic properties, rather than by model checking.

Finally, it is noted by the authors that the logic is not necessarily complete with respect to the postulates of quantum mechanics. Because of this, it may not be possible to prove certain properties of quantum programs which are actually true. This will also apply to any proofs of epistemic properties.

3.5 Conclusion

In this chapter we have seen three approaches to modelling knowledge in quantum systems:

- The first approach to modelling knowledge involves using Qubit Message Passing Environments, which was developed independently of a semantics for quantum computation. This work is not a viable platform for further research, as it has numerous issues, including a lack of quantum gates, a flawed definition of knowledge, and no mechanism for specifying a quantum protocol from which the possible states may be algorithmically determined.
- The alternative approach to modelling knowledge is the DMC-based approach. This approach has the advantages of being grounded in a full semantics for distributed quantum computation, has a plausible notion of knowledge about quantum states, and probabilities may be determined from the execution semantics of DMC. This work is the most preferable base from which to perform further research.
- A more abstract approach to modelling knowledge in quantum systems is that of Dynamic Epistemic Quantum Logic. Although this approach is useful for verifying the correctness of quantum protocols, it is too abstract to be used to model knowledge in multi-agent quantum systems.

Further work starting from the DMC-based approach may involve:

- Addition of probabilities to the logic. The probability of a transition to a particular configuration may easily be determined from the execution semantics of DMC. A logic which reasons about probabilities over these configurations may be very similar to Probabilistic Computational Tree Logic (PCTL) [32], since the current definition of the logic over configurations is very similar to Computational Tree Logic [35].
- Implementation of a model checker. Since the semantics of DMC are already defined, it is possible to implement a model checker which generates the configurations automatically based on the execution semantics of DMC. Standard model checking techniques may be used to verify epistemic formulae over these configurations.

- Use of the implementation to verify other quantum protocols. Generating the specification of a network and the epistemic properties to be verified requires very little work. Once a model checker has been implemented, it could be used to model check quantum protocols easily - variations of attacks may be checked using only a small amount of human time, since the quantum network may easily be modified to specify different attacks on a protocol.

Chapter 4

Epistemic Verification of the Quantum Teleportation Protocol

4.1 Introduction

In this section, we use each of the three approaches described in the previous chapter to verify epistemic properties of the Quantum Teleportation protocol. The process of verification is described and used to highlight some of the characteristics of each approach. First, the Quantum Teleportation protocol is described in detail. Subsequently, the protocol is verified using each of the three formalisms.

4.2 The Quantum Teleportation Protocol

The Quantum Teleportation protocol was first presented in [11]. The protocol achieves the transmission of the state of an arbitrary qubit from an agent A (Alice) to another agent B (Bob) using only a classical channel, and an entangled pair of qubits. Figure 4.1 shows a quantum circuit which implements the Quantum Teleportation protocol.

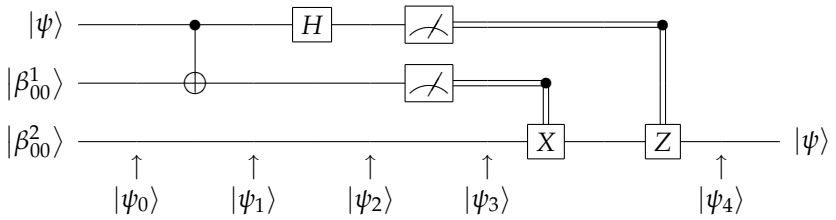


Figure 4.1: A quantum circuit for the Quantum Teleportation protocol.

Alice wishes to send a qubit to Bob without using a quantum channel, only using a classical channel. Alice holds the top two qubits (call them $|\phi_1\rangle$ and $|\phi_2\rangle$, and Bob holds the third qubit (called $|\phi_3\rangle$). $|\phi_2\rangle$ and $|\phi_3\rangle$ are in the entangled state $|\beta_{00}\rangle$. The states $|\phi_1\rangle$ and $|\beta_{00}\rangle$ are:

$$\begin{aligned} |\phi_1\rangle &= \alpha|0\rangle + \beta|1\rangle \\ |\beta_{00}\rangle &= \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle] \end{aligned}$$

Alice will "teleport" the state of $|\phi_1\rangle$ to Bob so that he eventually has a qubit which is in the state $\alpha|0\rangle + \beta|1\rangle$. The state of the whole system in the initial state is given by

$$\begin{aligned} |\psi_0\rangle &= |\phi_1\rangle \otimes |\phi_2\rangle \otimes |\phi_3\rangle \\ &= \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)] \end{aligned} \tag{4.1}$$

Alice sends her qubits through a $CNOT$ gate, giving

$$\begin{aligned}
|\psi_1\rangle &= (CNOT \otimes I)|\psi_0\rangle \\
&= \frac{\alpha}{\sqrt{2}}[(CNOT(|00\rangle) \otimes I|0\rangle + CNOT(|01\rangle) \otimes I(|1\rangle)] \\
&+ \frac{\beta}{\sqrt{2}}[(CNOT(|10\rangle) \otimes I|0\rangle + CNOT(|11\rangle) \otimes I(|1\rangle)] \\
&= \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|110\rangle + |101\rangle) \qquad (4.2)
\end{aligned}$$

Alice then sends her first qubit through a Hadamard gate, giving

$$\begin{aligned}
|\psi_2\rangle &= (H \otimes I \otimes I)|\psi_1\rangle \\
&= \frac{\alpha}{\sqrt{2}}(H|0\rangle \otimes (I \otimes I)|00\rangle + H|0\rangle \otimes (I \otimes I)|11\rangle \\
&+ \frac{\beta}{\sqrt{2}}(H|1\rangle \otimes (I \otimes I)|10\rangle + H|1\rangle \otimes (I \otimes I)|01\rangle \\
&= \frac{\alpha}{\sqrt{2}}H|0\rangle(|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}}H|1\rangle(|10\rangle + |01\rangle) \\
&= \frac{\alpha}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes (|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes (|10\rangle + |01\rangle) \\
&= \frac{\alpha}{2}(|000\rangle + |011\rangle + |111\rangle) + \frac{\beta}{2}(|010\rangle + |001\rangle - |110\rangle - |101\rangle)
\end{aligned}$$

Before we examine how the measurement outcome affects the state, we can re-arrange $|\psi_2\rangle$ so that we can see more easily how the measurement outcome affects qubit 3:

$$\begin{aligned}
|\psi_2\rangle &= \frac{\alpha}{2}(|000\rangle + |011\rangle + |111\rangle) + \frac{\beta}{2}(|010\rangle + |001\rangle - |110\rangle - |101\rangle) \\
&= \frac{\alpha}{2}|000\rangle + \frac{\beta}{2}|001\rangle + \frac{\beta}{2}|010\rangle + \frac{\alpha}{2}|011\rangle + \frac{\alpha}{2}|100\rangle - \frac{\beta}{2}|101\rangle - \frac{\beta}{2}|110\rangle + \frac{\alpha}{2}|111\rangle \\
&= \frac{1}{2}[|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + |01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) \\
&+ |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + |11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle)] \qquad (4.3)
\end{aligned}$$

Alice then measures her qubits, which will give her one of four measurement outcomes with equal probability, either $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$. It can be seen from inspection of Equation 4.3 that the third qubit will be left in a state $\alpha|0\rangle + \beta|1\rangle$, $\alpha|1\rangle + \beta|0\rangle$, $\alpha|0\rangle - \beta|1\rangle$ or $\alpha|1\rangle - \beta|0\rangle$, corresponding to the measurement outcome. The system is now in one of the four states given by:

$$|\psi_3\rangle = \begin{cases} |00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) & \text{with probability } \frac{1}{4} \\ |01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) & \text{with probability } \frac{1}{4} \\ |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) & \text{with probability } \frac{1}{4} \\ |11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle) & \text{with probability } \frac{1}{4} \end{cases} \qquad (4.4)$$

Alice then sends two classical bits, m and n to Bob which tell him the measurement outcome. m is equal to the measurement result of the first qubit, and n is equal to the measurement result of the second qubit.

- In the case where Alice's measurement outcome was $|00\rangle$, then Bob's qubit is already in state $\alpha|0\rangle + \beta|1\rangle$ so he needs take no further action. In the quantum circuit, this is realised because $Z^m X^n = Z^0 X^0 = I^2 = I$.

- In the case where Alice's measurement outcome was $|01\rangle$, $m = 0$ and $n = 1$. The transformation Bob applies is equal to X. As Bob's qubit is in the state $\alpha|1\rangle + \beta|0\rangle$, the application of the X gate transforms his qubit to state $\alpha|0\rangle + \beta|1\rangle$.

- In the case where Alice's measurement outcome was $|10\rangle$, $m = 1$ and $n = 0$. The transformation Bob applies is equal to Z. As Bob's qubit is in the state $\alpha|0\rangle - \beta|1\rangle$, the application of the Z gate transforms his qubit to state $\alpha|0\rangle + \beta|1\rangle$.

- Finally, In the case where Alice's measurement outcome was $|11\rangle$, $m = 1$ and $n = 1$. The transformation Bob applies is equal to ZX. As Bob's qubit is in the state $\alpha|1\rangle - \beta|0\rangle$, the application of the X gate and subsequently the Z gate transforms his qubit to state $\alpha|0\rangle + \beta|1\rangle$.

After Bob has applied the necessary quantum gates, the state of the system is now:

$$\begin{aligned} |\psi_4\rangle &= (I \otimes I \otimes Z^m X^n)|\psi_3\rangle \\ &= |mn\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) \end{aligned} \tag{4.5}$$

Hence we can see that Bob's qubit is in the state $\alpha|0\rangle + \beta|1\rangle$ - Alice has successfully "teleported" her first qubit to Bob without making use of a quantum channel!

4.3 Verification Using Qubit Message Passing Environments

4.3.1 A New Action

In order to represent the Quantum Teleportation protocol using Qubit Message Passing Environments, we must augment the definition of Qubit Message Passing Environments with a new action, called $\texttt{gate}(g, L)$: An agent i applies the gate g to qubits in the tuple L. This may only occur when $\forall n \in L, \texttt{loc}(n) = i$, i.e. an agent may only operate on qubits in its possession.

4.3.2 Verification

There are two agents, A and B. They have no variables. There are three qubits in the environment, the first two held by A and the third by B. The initial state (call it s_0) is given by:

$$\begin{aligned} \texttt{Var}_0 &= \emptyset \\ \texttt{loc}_0(0) = \texttt{loc}_0(1) &= A \\ \texttt{loc}_0(2) &= B \\ \texttt{chan}_0(A, B) = \texttt{chan}_0(B, A) &= \perp \\ \texttt{res}_0 &= \emptyset \end{aligned}$$

$$\begin{aligned} s_0^c &= \langle \texttt{Var}_0, \texttt{loc}_0, \texttt{chan}_0, \texttt{res}_0 \rangle \\ s_0^q &= |\psi_0\rangle \\ s_0 &= \langle s_0^q, s_0^c \rangle \end{aligned}$$

Between this state and the next state, Alice performs the action $\texttt{gate}(CNOT, \langle 0, 1\rangle)$. Bob performs no action (If it were required that an agent must perform an action, he could do a $\texttt{send}_{B,B}(\perp)$, to transmit an empty message to himself). We get the state s_1:

$$
\begin{aligned}
\mathtt{Var}_1 &= \emptyset \\
\mathtt{loc}_1(0) = \mathtt{loc}_1(1) &= A \\
\mathtt{loc}_1(2) &= B \\
\mathtt{chan}_1(A,B) = \mathtt{chan}_1(B,A) &= \perp \\
\mathtt{res}_1 &= \emptyset
\end{aligned}
$$

$$
\begin{aligned}
s_1^c &= \langle \mathtt{Var}_1, \mathtt{loc}_1, \mathtt{chan}_1, \mathtt{res}_1 \rangle \\
s_1^q &= |\psi_1\rangle \\
s_1 &= \langle s_1^q, s_1^c \rangle
\end{aligned}
$$

Between this state and the next state, Alice performs the action $\mathtt{gate}(H,1)$, and Bob transmits himself another empty message. We then get the state s_2:

$$
\begin{aligned}
\mathtt{Var}_2 &= \emptyset \\
\mathtt{loc}_2(0) = \mathtt{loc}_2(1) &= A \\
\mathtt{loc}_2(2) &= B \\
\mathtt{chan}_2(A,B) = \mathtt{chan}_2(B,A) &= \perp \\
\mathtt{res}_2 &= \emptyset
\end{aligned}
$$

$$
\begin{aligned}
s_2^c &= \langle \mathtt{Var}_2, \mathtt{loc}_2, \mathtt{chan}_2, \mathtt{res}_2 \rangle \\
s_2^q &= |\psi_2\rangle \\
s_2 &= \langle s_2^q, s_2^c \rangle
\end{aligned}
$$

Between this state and the next state, Alice performs a measurement, M on her qubits, measuring them in the basis $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. Therefore,

$$
M_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad M_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad M_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}
$$

Her measurement outcome is recorded in m and n where m stores the result from the first qubit and n stores the outcome from the second qubit. Again Bob transmits an empty message to himself. We now have the state s_3:

$$
\begin{aligned}
\mathtt{Var}_3 &= \emptyset \\
\mathtt{loc}_3(0) = \mathtt{loc}_3(1) &= A \\
\mathtt{loc}_3(2) &= B \\
\mathtt{chan}_3(A,B) = \mathtt{chan}_3(B,A) &= \perp \\
\mathtt{res}_{3A} &= \langle \{M, m, n\} \rangle \\
\mathtt{res}_{3B} &= \emptyset
\end{aligned}
$$

$$
\begin{aligned}
s_3^c &= \langle \mathtt{Var}_3, \mathtt{loc}_3, \mathtt{chan}_3, \mathtt{res}_3 \rangle \\
s_3^q &= |\psi_3\rangle \\
s_3 &= \langle s_3^q, s_3^c \rangle
\end{aligned}
$$

There are actually four distinct states for s_3, which each differ in the measurement outcomes. These may be referred to as s_{3-0} when $m = n = 0$, s_{3-1} when $m = 0, n = 1$, s_{3-2} when $m = 1, n = 0$ and s_{3-3}

when $m = n = 1$. After this state Alice performs a $\texttt{send}_{A,B}(\{m,n\})$ action, and Bob transmits himself an empty message. We now have the states s_4:

$$\begin{aligned}
\texttt{Var}_4 &= \emptyset \\
\texttt{loc}_4(0) = \texttt{loc}_4(1) &= A \\
\texttt{loc}_4(2) &= B \\
\texttt{chan}_4(A,B) &= \{m,n\} \\
\texttt{chan}_4(B,A) &= \bot \\
\texttt{res}_{4A} &= \langle\{M,m,n\}\rangle \\
\texttt{res}_{4B} &= \emptyset \\
\\
s_4^c &= \langle \texttt{Var}_4, \texttt{loc}_4, \texttt{chan}_4, \texttt{res}_4 \rangle \\
s_4^q &= |\psi_3\rangle \\
s_4 &= \langle s_4^q, s_4^c \rangle
\end{aligned}$$

Again there are four s_4 states, which each correspond to one of the measurement outcomes earlier - s_{4-0} when $m = n = 0$, s_{4-1} when $m = 0, n = 1$, s_{4-2} when $m = 1, n = 0$ and s_{4-3} when $m = n = 1$. Alice's next action is to transmit herself an empty message. Bob's next action depends on the earlier measurement outcome. In state s_{4-0}, he performs the identity transformation on his qubit, i.e. $\texttt{gate}(I,2)$. In state s_{4-1}, he performs $\texttt{gate}(Z,2)$. In state s_{4-2}, he performs $\texttt{gate}(X,2)$. In state s_{4-3}, he performs $\texttt{gate}(ZX,2)$. This assumes that he is able to apply a gate which performs the X and Z actions successively between two states. We now have the state s_5:

$$\begin{aligned}
\texttt{Var}_5 &= \emptyset \\
\texttt{loc}_5(0) = \texttt{loc}_5(1) &= A \\
\texttt{loc}_5(2) &= B \\
\texttt{chan}_5(A,B) &= \{m,n\} \\
\texttt{chan}_5(B,A) &= \bot \\
\texttt{res}_{5A} &= \langle\{M,m,n\}\rangle \\
\texttt{res}_{5B} &= \emptyset \\
\\
s_5^c &= \langle \texttt{Var}_5, \texttt{loc}_5, \texttt{chan}_5, \texttt{res}_5 \rangle \\
s_5^q &= |\psi_4\rangle \\
s_5 &= \langle s_5^q, s_5^c \rangle
\end{aligned}$$

As before there are four s_5 states, each of which corresponds to a measurement outcome. We have reached the final state of the quantum teleportation protocol, and have described all the possible states of the system. We can now enumerate all the possible runs r of the system:

$$\begin{aligned}
r_0 &= \{s_0, s_1, s_2, s_{3-0}, s_{4-0}, s_{5-0}\} \\
r_1 &= \{s_0, s_1, s_2, s_{3-1}, s_{4-1}, s_{5-1}\} \\
r_2 &= \{s_0, s_1, s_2, s_{3-2}, s_{4-2}, s_{5-2}\} \\
r_3 &= \{s_0, s_1, s_2, s_{3-3}, s_{4-3}, s_{5-3}\}
\end{aligned} \tag{4.6}$$

We can now determine a model in which the runs exist. Figure 4.2 shows the possible states of the system and the temporal accessibility relation between them. Call this the model $\mathcal{M}$.

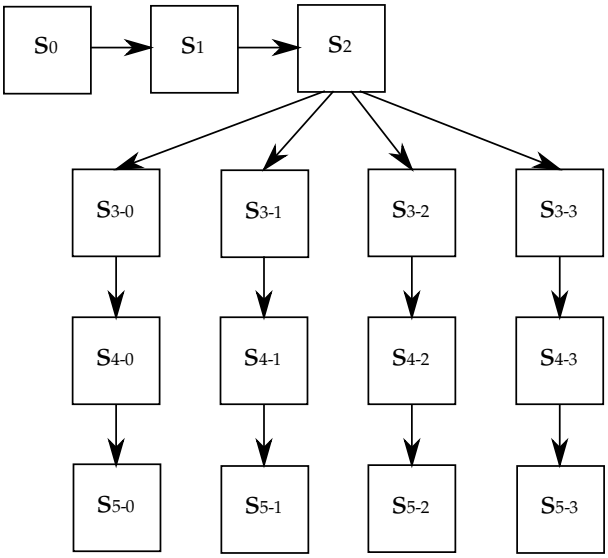


Figure 4.2: The model $\mathcal{M}$ - Possible worlds of the QT protocol and temporal accessibility relation

An interpretation function, π will now be defined on the model. Take p to be an atomic proposition which means "The state of qubit 1 is $\alpha|0\rangle + \beta|1\rangle$". This is true at state s_0 only. Therefore:

$$\pi(s, p) = \begin{cases} 1 & \text{when } s = s_0 \\ 0 & \text{otherwise} \end{cases} \tag{4.7}$$

Now we consider the epistemic accessibility relation for quantum knowledge. This is shown in Figure 4.3. In order to save drawing a large number of arcs between states, the epistemic relations are instead depicted by boxes. Any two states bounded by the same box are related by the epistemic accessibility relation of the agent whose knowledge it represents. The classical epistemic accessibility relation would be similar assuming that agents can recall what operations they have performed on their qubits. It is thought that this is a reasonable assumption to make.

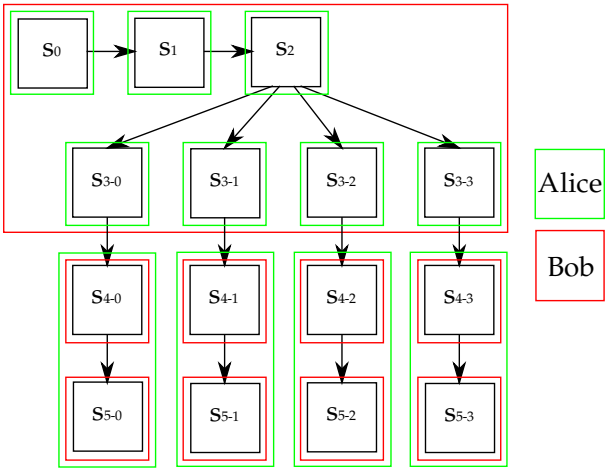


Figure 4.3: Epistemic accessibility relation between states in the QT protocol

The formula which we wish to verify that the QT protocol satisfies in the initial state (stated in [51]) is:

$$k_A^q p \wedge \neg k_B^q p \wedge \Diamond k_B^q \texttt{init}(p) \tag{4.8}$$

This formula states that Alice quantumly knows that the state of qubit 1 is $\alpha|0\rangle + \beta|1\rangle$, that Bob does not quantumly (and hence classically) know the state of qubit 1 is $\alpha|0\rangle + \beta|1\rangle$, but that eventually Bob

knows that the initial state of qubit 1 is $\alpha|0\rangle + \beta|1\rangle$. To verify that this formula is realised, we examine the initial state of each run of the protocol and check that it is satisfied there:

Checking $k_A^q p$. In every run, the initial state is the state s_0. The only epistemically-accessible state from s_0 for Alice is s_0. Therefore, we only need to check that $k_A^q p$ is true at s_0. $\pi(s_0, p) = 1$, as required.

Checking $\neg k_B^q p$. The epistemically-accessible states from s_0 for Bob are s_0, s_1, s_2, s_{3-0}, s_{3-1}, s_{3-2}, s_{3-3}. Since p is not true at all these states, it is the case that $\neg k_B^q p$ at s_0, as required.

Checking $\Diamond k_B^q \mathtt{init}(p)$. Clearly if p is true in the initial state then $\mathtt{init}(p)$ is true at all subsequent states. Therefore, $k_B^q \mathtt{init}(p)$ and $\Diamond k_B^q \mathtt{init}(p)$ will be true at all states. Although it is the case that Bob eventually does quantumly know $\mathtt{init}(p)$ (i.e. he eventually has a qubit in the state $|\psi\rangle$), it is not true in a physical system - Bob should not have quantum knowledge of the initial truth value of p until he has a qubit in the state $|\psi\rangle$, which is only true in the states s_5. In this example, the property $k_B^q \mathtt{init}(p)$ is verified as being correct even at states where it should not be true.

We may attempt to remedy this by altering the definitions given slightly - we may interpret $k_B^q \mathtt{init}(\phi)$ as a modality which is interpreted as being true at states where Bob's local state gives him enough information to compute the truth of the formula ϕ at the initial state. However, this definition is slightly flimsy in that it is somewhat arbitrary, and still leads to incorrect verification. Bob has enough information in his local state to compute the truth of p at the initial state when the states s_4 and s_5 have been reached. Since for Bob each state s_4 and s_5 is the only epistemically possible one when in that state, $k_B^q \mathtt{init}(\phi)$ is true at all of these states. However, since Bob quantumly knows the initial truth value of p in this states s_4, this interpretation also allows the incorrect verification of epistemic properties.

Since all the terms of the conjunction are realised in both potential interpretations, we can say that the formula $k_A^q p \wedge \neg k_B^q p \wedge \Diamond k_B^q \mathtt{init}(p)$ is realised by the quantum teleportation protocol. However, there are problems in this verification of the protocol using both definitions of quantum knowledge of an initial state, since it is considered that Bob already "knows" the truth of the proposition p in the states s_4, - this is not the case in a real implementation of the protocol, since Bob will not have a qubit in the same state as Alice's initial qubit until he has applied the gates to correct the value of his qubit. The fact that it has been possible to verify a property which is not true suggests that analyses performed using Qubit Message Passing Environments are not sound.

4.4 Verification Using Distributed Measurement Based Computation

The verification of some epistemic properties of the Quantum Teleportation protocol using the DMC-based approach is presented in [20]. We briefly reproduce this verification process here with a more detailed explanation than is presented in the original paper, and verify some additional epistemic properties which are felt to be relevant. In order to verify the Quantum Teleportation protocol, we must first convert the Quantum Teleportation circuit to a Quantum Network.

In the literature a slightly simplified notation is used in order to make it easier to read the configurations of the network, without any ambiguity. We will follow this convention in reproducing the analysis of the protocol. The simplifications include using $\mathtt{c}!x_1x_2$ as a shorthand for $\mathtt{c}!x_1\mathtt{c}!x_2$ and similarly for classical receive and quantum sending and receiving. Additionally in the event sequences, the measurement patterns have the computation space and sets of input and output qubits omitted, and only the operations performed on the qubits are stated. The equivalent quantum network to the quantum teleportation circuit is:

$$QT = \mathbf{A} : \{1,2\}.[(\mathtt{c}!s_2s_1).M_{12}^{0,0}] \mid \mathbf{B} : \{3\}.[X_3^{x_2}Z_3^{x_1}.(\mathtt{c}?x_2x_1)] \mid\mid E_{23}$$

When the measurement is performed by Alice (agent **A**), there are four possible measurement outcomes. Therefore, for each subsequent configuration of the network there are four possible configurations, parameterised by the measurement outcomes j_1 and j_2. This gives rise to the configurations:

$$
\begin{aligned}
C_1(|\psi\rangle) =& |\psi\rangle E_{23}; \emptyset, \mathbf{A} : \{1,2\}.[(\mathsf{c}!s_2 s_1).M_{12}^{0,0}] \mid \emptyset, \mathbf{B} : \{3\}.[X_3^{x_2} Z_3^{x_1}.(\mathsf{c}?x_2 x_1)] \\
C_2^{j_1 j_2}(|\psi\rangle) =& X^{j_2} Z^{j_1} |\psi\rangle; [s_1, s_2 \mapsto j_1, j_2], \mathbf{A}.(\mathsf{c}!s_2 s_1) | \emptyset, \mathbf{B} : \{3\}.[X_3^{x_2} Z_3^{x_1}.(\mathsf{c}?x_2 x_1)] \\
C_3^{j_1 j_2}(|\psi\rangle) =& X^{j_2} Z^{j_1} |\psi\rangle; [s_1, s_2 \mapsto j_1, j_2], \mathbf{A} \mid [x_1, x_2 \mapsto j_1, j_2], \mathbf{B} : \{3\}.X_3^{x_2} Z_3^{x_1}) \\
C_4^{j_1 j_2}(|\psi\rangle) =& |\psi\rangle; [s_1, s_2 \mapsto j_1, j_2], \mathbf{A} \mid [x_1, x_2 \mapsto j_1, j_2], \mathbf{B} : \{3\} \ .
\end{aligned}
$$

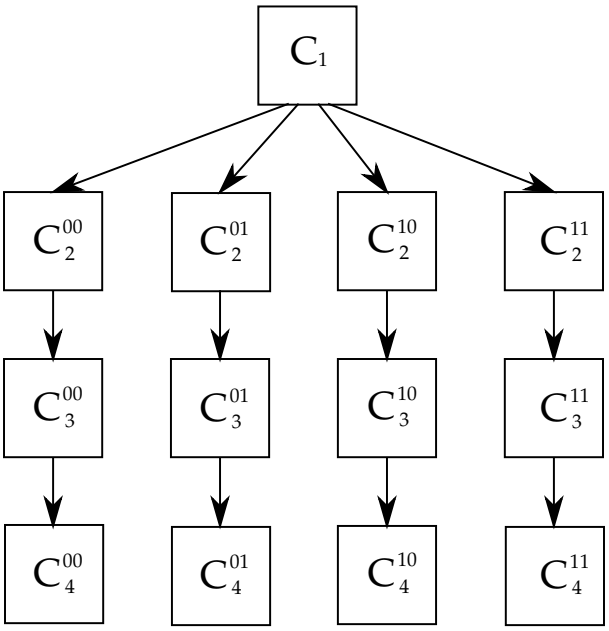


Figure 4.4: The model $\mathcal{CM}$ - Possible worlds (configurations) of the QT network and the temporal accessibility relation

Figure 4.4 gives a graphical representation of the possible configurations, and the temporal accessibility relation between them. We can determine the epistemic possibility relation between these worlds based on the local information which each agent has available at each configuration. First we determine the possibility relation $\sim_{\mathbf{A}}$, the relation for Alice:

- Between configuration C_1 and C_2, Alice has performed a measurement, so she does not consider C_1 to be a possible configuration when in the configuration C_2, and vice-versa.
- When in configuration C_2, the four possible measurement outcomes all differ between the four C_2 configurations. Therefore, when in one of the C_2 configurations, Alice does not consider any of the other four C_2 configurations to be possible.
- Between the configurations C_2 and C_3, Alice has sent classical information to Bob. She therefore does not consider any C_2 configuration possible from any C_3 configuration and vice-versa.
- Since in each the configurations C_3, Alice had different measurement outcomes previously, she has a different local state in each of the C_3 configurations. Therefore, when in a C_3 configuration, she does not consider any of the other C_3 configurations possible.
- Between configurations C_3 and C_4, Alice's local state does not change. Therefore, she considers C_4 configurations possible from C_3 configurations and vice-versa. In each configuration $C_3^{j_1 j_2}$ her local state is only equal to that of the configuration $C_4^{k_1 k_2}$ when $j_1 = k_1$ and $j_2 = k_2$. Therefore, she only considers $C_3^{j_1 j_2}$ to be possible when in configuration $C_4^{j_1 j_2}$ and vice versa.

We may also determine the possibility relation $\sim_{\mathbf{B}}$, the relation for Bob:

- Bob has the same local information in configuration C_1 and all the four possible configurations of C_2. Therefore, in any of these states, Bob considers all of these states possible.
- In each of the possible C_3 configurations, Bob has received some information from Alice, altering his local state. Therefore, he does not consider the configurations C_1 and C_2 possible when in configuration C_3. In each of the four C_3 configurations, he has received different classical information from Alice. Therefore, when in one of the particular C_3 states, he does not consider any of the other C_3 states possible.
- In the C_4 states, Bob has applied one of four different corrections in each of these states. As such, when in one of the C_4 states, he does not consider any other C_4 state to be possible. Additionally, because Bob has applied corrections between the configurations C_3 and C_4, he does not consider any of the C_4 configurations possible when in a C_3 configuration and vice-versa.

The epistemic possibility relations are shown in Figure 4.5.

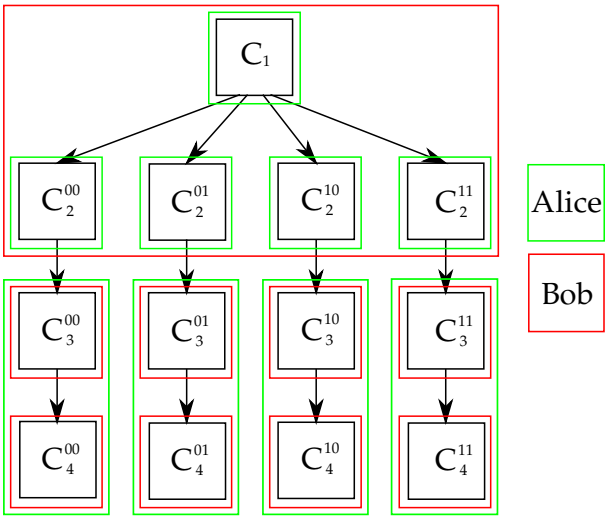


Figure 4.5: The epistemic accessibility relation of Alice and Bob between configurations of the QT network.

We may now define the interpretation of facts over this model. This can be done according to the specifications given in Section 3.3.3, Equations 3.1-3.5. Using these specifications, there are many facts which could possibly be defined over the configurations. However we will only describe the definition of facts which suffice to verify the properties we are interested in. These are:

- Assuming that the first qubit which Alice wishes to transmit is in an unknown quantum state, $|\psi\rangle$, we define the fact $(q_1 = |\psi\rangle)$. This is true only at the configuration C_1, as it is destroyed by Alice's measurement between configurations C_1 and C_2.
- In the initial state of all paths, $(q_1 = |\psi\rangle)$, so $(init(q_1) = |\psi\rangle)$ is true at all states.
- The final state of qubit 3 is equal to $|\psi\rangle$, which is a property that has been deduced throughout the execution of the network using the execution semantics. Therefore, we can define the fact $(q_3 = |\psi\rangle)$, which is true at all four of the configurations C_4.
- As $(q_3 = |\psi\rangle)$ is true at every final state on all paths, $(fin(q_3) = |\psi\rangle)$ is true at all states.
- Since $(init(q_1) = |\psi\rangle)$ is true everywhere and $(fin(q_3) = |\psi\rangle)$ is also true everywhere, $(init(q_1) = fin(q_3))$ is also true everywhere.

It is stated in [20] that the correctness of the QT network may be verified by the following formula, which does not use epistemic modalities:

$$C_1(|\psi\rangle), TP \models A\Diamond(fin(q_3) = init(q_1))$$

Although this formula does indeed verify the QT network, the diamond is somewhat redundant, since the fact $(fin(q_3) = init(q_1))$ is true everywhere. A more intuitive formula which verifies the QT network might be given by

$$C_1(|\psi\rangle), TP \models A\Diamond(q_3 = init(q_1))$$

This formula is satisfied since the fact $(q_3 = init(q_1))$ is eventually true on all paths (in the configuration C_4), but is not true at all configurations of all paths. We can also check epistemic properties of the network:

$$C_1(|\psi\rangle), TP \models \neg K_{\mathbf{A}}(q_1 = |\psi\rangle) \wedge \neg K_{\mathbf{B}}(q_1 = |\psi\rangle) \tag{4.9}$$

This formula states that neither Alice nor Bob ever knows the initial state of the first qubit, which is teleported. Since $|\psi\rangle$ is an arbitrary, unknown state, this is representative of a real-world situation in which the teleportation protocol is used to transmit an arbitrary qubit. This formula may be verified. It is obviously true that $C_1(|\psi\rangle), TP \models \neg K_{\mathbf{B}}(q_1 = |\psi\rangle)$, since $C_1 \sim_{\mathbf{B}} C_2$ and $C_2(|\psi\rangle), TP \models \neg(q_1 = |\psi\rangle)$. To check $C_1(|\psi\rangle), TP \models \neg K_{\mathbf{A}}(q_1 = |\psi\rangle)$, it must be noted that the state $C_1(|\psi\rangle)$ may be one of an infinite number of possible configurations, parameterised by the exact value of $|\psi\rangle$, which are all considered to be equivalent (and therefore possible) from the both agents' point of view. Therefore, we can then conclude that $C_1(|\psi\rangle), TP \models \neg K_{\mathbf{A}}(q_1 = |\psi\rangle)$ does hold, and that Equation 4.9 also holds. Another interesting epistemic property of the QT network may be verified by the formula:

$$C_1(|\psi\rangle), TP \models \neg E\Diamond K_{\mathbf{A}}(q_3 = |\psi\rangle) \wedge \neg E\Diamond K_{\mathbf{B}}(q_3 = |\psi\rangle)$$

This formula states that neither agent ever knows the exact state of the qubit. This is also a fact in a real-world teleportation scenario, so it should be expected that this may be verified in the QT network also. It may be verified in a similar manner to the previous formula, again by noting that there are an infinite number of possible configurations parameterised by $|\psi\rangle$ exist, which are all possible. However, we can verify that Bob eventually knows that the third qubit is equal to the initial state of the first qubit:

$$C_1(|\psi\rangle), TP \models A\Diamond K_{\mathbf{B}}(q_3 = init(q_1))$$

This formula is verified since at the final configuration of all paths, it is true that $(q_3 = init(q_1))$. Additionally, when Bob is in one of the final configurations, it is the only configuration which he considers to be possible. Finally, Alice never knows that $(q_3 = init(q_1))$:

$$C_1(|\psi\rangle), TP \models \neg E\Diamond K_{\mathbf{A}}(q_3 = init(q_1)) \tag{4.10}$$

This formula is verified since the configurations where $(q_3 = init(q_1))$ is true are the C_4 configurations. Alice cannot distinguish the C_4 configurations from the C_3 configurations, where $(q_3 = init(q_1))$ is not true. Therefore, Equation 4.10 holds.

It has been seen that using the DMC-based approach allows the verification of properties which essentially describe the correctness of the Quantum Teleportation protocol in terms of knowledge of the agents. This has been achieved without having to use a problematic interpretation of knowledge, unlike the previous approach.

4.5 Verification Using Dynamic Epistemic Quantum Logic

An LQP program which implements the quantum teleportation protocol is given in [3]. This program correctly performs the teleportation protocol; to show that this is the case, we will present a derivation of the program from the axioms of LQP. The theorems and axioms are as referred to in [3]. There is a full presentation of a proof theory for the logic given in [7], but in order to keep the derivation simple it is not used. In the derivation, we will also use "PL" to denote a tautology of propositional logic and

"PDL" to denote an axiom of Propositional Dynamic Logic (as all the axioms of PDL are admitted to LQP except for those pertaining to the test $\phi?$).

$$\vdash \phi_1 \rightarrow \phi_1 \qquad \text{(PL)}$$
$$\vdash \phi_1 \rightarrow [Z_1^x; Z_1^x]\phi_1 \qquad \text{(Unitary Bijectivity 1 since } Z = Z^\dagger\text{)}$$
$$\vdash \phi_1 \rightarrow [Z_1^x][Z_1^x]\phi_1 \qquad \text{(PDL)}$$
$$\vdash \phi_1 \rightarrow [Z_1^x][X_1^y; X_1^y][Z_1^x]\phi_1 \qquad \text{(Unitary Bijectivity 1 since } X = X^\dagger\text{)}$$
$$\vdash \phi_1 \rightarrow [Z_1^x; X_1^y][X_1^y; Z_1^x]\phi_1 \qquad \text{(PDL)}$$
$$\vdash \phi_1 \rightarrow [Z_1^x; X_1^y][Z_1^0; X_1^0][X_1^y; Z_1^x]\phi_1 \qquad \text{(Unitary Bijectivity 1 since } X^0 = Z^0 = I = I^\dagger\text{)}$$

Theorem 5 (the Teleportation Property, TP) states that for 1-local testable properties ϕ_1, $\vdash (\phi_1 \rightarrow [\pi_{(1)}; \sigma_{(1)}]q_1) \rightarrow (\phi_1 \wedge \overline{\sigma}_{23} \rightarrow [\overline{\pi}_{12}?]q_3)$. Therefore:

$$\vdash \phi_1 \wedge \overline{(Z_1^0; X_1^0)}_{23} \rightarrow [\overline{(Z_1^x; X_1^y)}_1 2?][X_1^y; Z_1^x]\phi_3 \qquad \text{(Modus Ponens \& TP)}$$

Proposition 14 (Bell States) states that the Bell formulae are defined as $\beta_{xy}^{ij} := \overline{(Z_1^x; X_1^y)}_{ij}$. Therefore:

$$\vdash \phi_1 \wedge \beta_{00}^{23} \rightarrow [\beta_{xy}^{12}?][X_1^y; Z_1^x]\phi_3 \qquad \text{(Bell States)}$$

The Corollary to Proposition 15 states that for distinct i, j and k, we have $\vdash \langle \beta_{xy}^{ij} \rangle p_k \leftrightarrow \langle CNOT_{ij}; H_i; (x_i \wedge y_j)? \rangle p_k$. We can use this to obtain:

$$\vdash \phi_1 \wedge \beta_{00}^{23} \rightarrow [CNOT_{12}; H_1; (x_1 \wedge y_2)?][X_1^y; Z_1^x]\phi_3 \qquad \text{(Corollary to Prop. 15)}$$

This is equivalent to:

$$\vdash \phi_1 \wedge \beta_{00}^{23} \rightarrow [\pi]\phi_3 \tag{4.11}$$

Until now the values over which x and y range have not been considered, as during the early part of this derivation their values did not matter. It is noted that there are four Bell states, β_{00}^{ij}, β_{01}^{ij}, β_{10}^{ij} and β_{11}^{ij}. Therefore, $x, y \in \{0, 1\}$. As a result, in Equation 4.11, we have that

$$\pi = \bigcup_{x,y \in \{0,1\}} (CNOT_{12}; H_1; (x_1 \wedge y_2)?; X_1^y; Z_1^x) \tag{4.12}$$

The non-deterministic choice between each of these four programs is required since we wish to always ensure that ϕ_3 holds after the execution of the program π. This allows the full specification of π to always execute to completion depending on the measured (tested) values of x and y. It should be noted that there is an obvious correlation between the six actions of the program π and the operations carried out in the quantum teleportation circuit.

Since it has been shown that Equation 4.11 is valid based on the axioms and theorems of LQP, this is also a proof that after the execution of the quantum teleportation protocol, the third qubit holds any testable property which the first qubit held. This implies that the state of the third qubit in the final world is equal to that of the first qubit in the initial world. Since the "if" part of the equation also includes β_{00}^{23}, it is essential that the second and third qubits are in the entangled Bell state prior to the execution of the program π.

A subset of the quantum model which includes the transition relations which are followed during the execution of the quantum teleportation protocol is shown in Figure 4.6. The initial world (at which ϕ_1 is assumed to hold) is denoted g_1. The final world (at which Equation 4.11 proves ϕ_3 holds) is denoted g_7. The other worlds are numbered arbitrarily.

Unfortunately this model of quantum teleportation has abstracted away the agents, and it is only possible to consider what can potentially be known based on the separated states of the qubits. This can be done by using the notion of separated subsystems. Here we define the subsystems

$$S = S_1 \otimes S_2$$

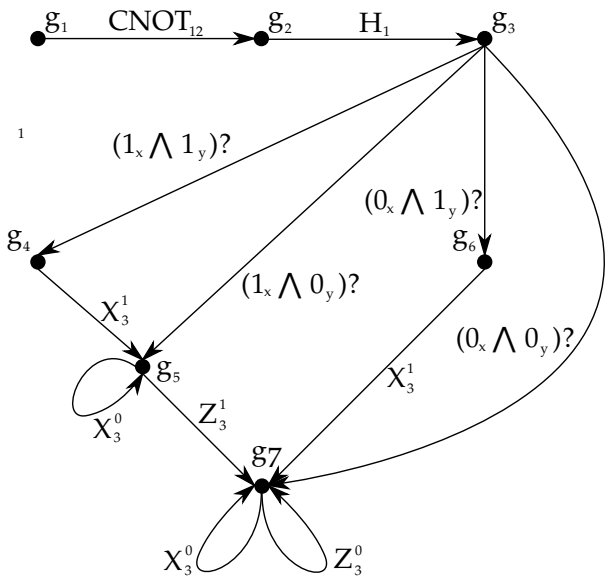


Figure 4.6: A subset of the quantum model $\mathcal{QTM}$ - Worlds of the quantum model and the transition relations.

where $S_1 = q_1 \otimes q_2$ and $S_2 = q_3$ since Alice is in possession of the first two qubits and Bob is in possession of the third qubit. Since there is not an explicit temporal notion in this logic we are restricted to evaluating the epistemic properties at specific worlds of the model. To do this we require an equivalence relation $\simeq_i$ for each subsystem. Of the worlds in the model, the epistemic similarity relation for subsystem S_1 is

$$\simeq_1 = \{(4,5),(4,6),(4,7),(5,4),(5,6),(5,7),(6,4),(6,5),(6,7),(7,4),(7,5),(7,6)\}$$

This is because after the quantum test $(x_1 \wedge y_2)?$ is executed, the entanglement is broken, and the subsystems are separated. Therefore, subsystem S_1 is not aware of changes which are made in subsystem S_2, which are the operations performed on qubit 3. Of the worlds in the model, the epistemic similarity relation for S_2 is simply $\simeq_2 = \{\}$. This is because with the exception of the first state, operations are performed on the first subsystem's qubits with which it is entangled, or local operations are performed on qubit 3, which are part of this subsystem. However, in the first state there are many more states which are epistemically possible according to subsystem S_2, since it is not entangled with qubit q_1, there are an infinite number of other possible states which the first qubit may be in which are also possible. Since there exists a 1-local unitary operation U such that $g_1' \simeq_2 U(g_1)$, there exists a state $g_1' \simeq_2 g_1$. Now that we have determined the worlds of the model and their relations, we may verify some properties of the protocol expressed in the logic:

- First we may verify that subsystem S_1 does not know that the third qubit now has the testable property which was originally a testable property of qubit 1 at the final state. This is given by the formula $\mathcal{QTM}, g_7 \not\models K_1\phi_3$ which is true since $g_7 \simeq_1 g_6$ and $\mathcal{QTM}, g_6 \not\models \phi_3$.
- We may also verify that the second subsystem does not know that the first qubit has the testable 1-local property ϕ. This is expressed by the formula $\mathcal{QTM}, g_1 \not\models K_2\phi_1$, which is true since $g_1' \simeq_2 g_1$. Since testable properties are not in general preserved by unitary transformations, $\mathcal{QTM}, g_1' \not\models \phi_1$.
- It is also interesting to verify that the subsystem S_2 does know that the qubit q_3 has the testable property ϕ_3 in the final world. This is modelled by the formula $\mathcal{QTM}, g_7 \models K_2\phi_3$. Since ϕ_3 is a testable 2-local property, subsystem S_2 does not consider any other world possible in which ϕ_3 may not hold - the only worlds it considers possible only differ in the 1-local properties. Therefore, the equation holds since $\forall g_7' \neq g_7 : g_7 \not\simeq_2 g_7'$ and $\mathcal{QTM}, g_7 \models \phi_3$.

Although these properties have been shown to be valid, the epistemic notion does not represent the knowledge which an agent may possibly know. The epistemic properties have provided a verification

of the correlations of effects between the two subsystems, rather than of the information which two agents in possession of the subsystem may be able to obtain.

4.6 Conclusion

We have seen the application of the three approaches to the epistemic verification of the Quantum Teleportation protocol.

- The Qubit Message Passing Environments-based approach has problems, as it verifies an epistemic property which is not correct. This is in addition to the problem of interpretation of qubits as ensembles for the Quantum Teleportation protocol.
- The DMC-based approach successfully verified epistemic properties of the protocol. There were no issues encountered in the verification process.
- Verification of the protocol using Dynamic Epistemic Quantum Logic proved properties of the protocol which are correct, but do not represent the knowledge of agents in a distributed system.

Chapter 5

Related Work

5.1 Introduction

In this chapter, we briefly describe other (epistemic and non-epistemic) approaches to verification of classical and quantum protocols. A short discussion of how additions may be made to some of the tools implementing these approaches to allow epistemic verification of quantum protocols is given.

5.2 Model Checking

5.2.1 QMC

Model checking tools such as Prism [36] and SPIN [34] have been used to perform model checking of the correctness of quantum protocols. In [47, 25], the BB84 Quantum Key Distribution protocol [9] is analysed using both these model checkers. The analyses demonstrated that the BB84 protocol was secure, by revealing that as the number of key bits increases, the probability of detecting an attacker becomes very close to 1, and also that the probability of an attacker (un-noticed or otherwise) only has a very small probability of recovering half of the key bits.

QMC [26] is a model checker which is able to check properties of a subset of quantum protocols. The properties which are checked are specified in the *Quantum CTL* (QCTL) logic. The quantum circuits which may be checked are restricted to those which may be expressed within the stabilizer formalism [29]. The stabilizer formulation only allows the specification of quantum circuits using the CNOT, Hadamard and Phase Gates. This restriction is required as stabilizer formalism circuits may be simulated in polynomial-time using only classical computation [2, 1]. The QMC tool is used to perform model checking of the Superdense Coding network [12], the Quantum Teleportation protocol [11], and Quantum Error Checking Codes (see [46], page 425). This work is presented in [27].

An interesting addition to QMC may be the addition of epistemic modalities to the properties which it may check. At present it does not consider properties of the quantum system which is composed of parts belonging to several agents. The addition of an epistemic modality would therefore require modification of QMC to allow the specification of which agents are in possession of which qubits, and primitives for transmission of qubits between agents.

5.2.2 MCMAS

MCMAS [39] is a symbolic model checking tool for the verification of multi-agent systems. MCMAS supports temporal logic and epistemic logic amongst others. A programming language, ISPL, is used to specify the system and the properties to be verified.

It is possible that functionality for verifying epistemic properties of quantum protocols may be added to MCMAS. Since epistemic logic and multi-agent systems are already supported, minimal changes may need to be made. The addition of the semantics of DMC may allow the configurations to be enumerated. The truth of propositions over these configurations may also be determined using the specifications for propositions given in Equations 3.1 to 3.5. The logic present in MCMAS which

performs model checking may then take over and determine the truth of epistemic properties of the specified system.

5.2.3 Adding an Epistemic Modality to Existing Model Checkers

The choice of defining an equivalence relation between states over which the modality operates for each agent must also be made. As it is not the case that agents may know the exact state of qubits which are in their possession in general, it seems sensible that the relation should only be based on the classical state of agents in the system. This would give an operator which behaves similarly to the knowledge operator in the DMC-based approach, and the classical knowledge operator in the Qubit Message Passing Environments-based approach. It may be useful for verification of protocols if a "knowledge" operator which has behaviour similar to that of the knowledge operator in the Logic of Quantum Information Flow or quantum knowledge in Qubit Message Passing Environments, but this operator should not be taken to necessarily represent the knowledge which an agent could possibly have based on the state of its qubits.

5.3 Quantum Process Algebras

An alternative method of verification of protocols involves using process algebras [48] to specify a protocol, and applying rules of the algebra to prove that the protocol is equivalent to a given specification (or that it is *not* equivalent!). One notion of equivalence between two processes in a process calculus is based on the existence of a *bisimulation relation* between them. The existence of the bisimulation relation between two processes implies that both processes make exactly the same transitions between their states. An alternative notion of equivalence is that of congruence. Two processes are congruent if, using the congruence axioms and theorems of the process algebra, the first process may be reduced to the second and vice-versa.

Attempts have been made to verify quantum protocols using classical process algebras. For example, the BB84 Quantum Key Distribution protocol [9] has been verified by expressing it as a set of CCS [44] formulae and testing it for bisimulation equivalence against a specification [45]. However, quantum processes may be modelled using classical process algebras to a limited extent, as they do not capture the non-classical dynamics of quantum computation.

In order to more succinctly model quantum processes, process algebras which combine classical and quantum computation have been developed. These include Communicating Quantum Processes [28], and the QPAlg process algebra [37]. Bisimilarity and congruence relations can be used for verification of QPAlg processes [38]. The DMC model described in Section 3.3 is quite similar to process algebras. This means that a two-fold verification of DMC networks may be performed: verification that the quantum network description meets a particular specification, and a subsequent verification of epistemic properties using the logic.

The process algebraic approach to verification is clearly quite different to a logic-based approach to verification. The process algebras also abstract away from the actual agents which participate in a computation. As such, the addition of epistemic properties to quantum process algebras is in general a difficult goal to achieve compared to that of adding them to already existing logic model checkers.

Chapter 6

Conclusions

We have seen three approaches to modelling knowledge in quantum systems, and their application to verification of epistemic properties of the Quantum Teleportation protocol. These approaches differ in their treatment of knowledge and the way in which they model a quantum system.

The first approach to model knowledge in quantum systems, using Qubit Message Passing Environments, is difficult to use for verification of quantum protocols. It has issues with its interpretation of quantum knowledge. Additionally, quantum knowledge verifies epistemic properties which do not hold in real-world systems.

The approach based on Distributed Measurement-Based Computation is a more sound approach - it has no problems with its interpretation of knowledge, since all knowledge is regarded as classical rather than quantum knowledge. The verification of properties of the Quantum Teleportation protocol using this approach did not lead to the verification of any false properties, and no other difficulties were encountered. The work based on this approach is a good starting point for further research.

Verification using the Dynamic Epistemic Quantum Logic based approach did not lead to any problems. However, the properties which may be verified using the logic are not useful models of knowledge in multi-agent systems, as this approach is too abstract.

Modelling knowledge in quantum systems fits into a wider context of quantum program verification, and should be used to complement the analyses of security properties used by these approaches. The security of a protocol may be assured with a greater certainty by using several different approaches to modelling attacks on the protocol.

6.1 Further Work

Further work based on the Distributed Measurement-Based Computation approach may include:

- Implementation of a model checker based on the existing published research. This implementation may be achieved without the necessity for further research.
- Verification of quantum protocols using an implementation of a model checker. The verification may be achieved by simulating attacks on protocols by providing different network specifications which model the actions of an eavesdropper or other malicious party.
- Addition of probabilities to the logic based on the probability of each measurement outcome. This will allow reasoning about the probability of particular knowledge states arising. This will allow the verification of properties such as “There is a 99.5% chance that agents will become aware of an eavesdropper during the execution of the protocol”, or “An eavesdropper only has a 0.5% chance of discovering all the bits of a key during the execution of a protocol”.

Bibliography

[1] Scott Aaronson and Daniel Gottesman. Improved Simulation of Stabilizer Circuits. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 70(5), 2004.

[2] Simon Anders and Hans J. Briegel. Fast Simulation of Stabilizer Circuits Using a Graph State Representation. *Physical Review A*, 73:022334, 2006.

[3] Alexandru Baltag and Sonja Smets. The Logic of Quantum Programs. In *Proceedings of the 2nd International Workshop on Quantum Programming Languages (QPL2004)*, pages 39–56. TUCS General Publication, 2004.

[4] Alexandru Baltag and Sonja Smets. Complete Axiomatizations for Quantum Actions. *International Journal of Theoretical Physics*, 44:2267–2282, December 2005.

[5] Alexandru Baltag and Sonja Smets. What Can Logic Learn from Quantum Mechanics? In *Proceedings of the European Computing and Philosophy Conference*, 2005.

[6] Alexandru Baltag and Sonja Smets. Lecture Notes on The Logic of Quantum Information Flow. Presented at ESSLLI 2006, 2006.

[7] Alexandru Baltag and Sonja Smets. LQP: The Dynamic Logic of Quantum Information. *Mathematical. Structures in Comp. Sci.*, 16(3):491–525, 2006.

[8] Alexandru Baltag and Sonja Smets. A Dynamic-Logical Perspective on Quantum Behavior. *Studia Logica*, 89(2):187–211, 2008.

[9] C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984.

[10] Charles H. Bennett. Quantum Cryptography Using Any Two Nonorthogonal States. *Physical Review Letters*, 68(21):3121+, May 1992.

[11] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. *Phys. Rev. Lett.*, 70(13):1895–1899, Mar 1993.

[12] Charles H. Bennett and Stephen J. Wiesner. Communication via One- and Two-particle Operators on Einstein-Podolsky-Rosen States. *Phys. Rev. Lett.*, 69(20):2881–2884, Nov 1992.

[13] Garrett Birkhoff and John Von Neumann. The Logic of Quantum Mechanics. *The Annals of Mathematics*, 37(4):823–843, 1936.

[14] Patrick Blackburn, Maarten de Rijke, and Yde Venema. *Modal Logic*. Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 2002.

[15] D.G. Cory, A.F. Fahmy, and T.F. Havel. Ensemble Quantum Computing by NMR Spectroscopy. In *Proceedings of the National Academy of Sciences*, volume 94, pages 1634–1639. National Acad Sciences, 1997.

[16] Vincent Danos and Ellie D'Hondt. Classical Knowledge for Quantum Cryptographic Reasoning. *Electron. Notes Theor. Comput. Sci.*, 192(3):39–58, 2008.

[17] Vincent Danos, Ellie D'Hondt, Elham Kashefi, and Prakash Panangaden. Distributed Measurement-based Quantum Computation. *Electron. Notes Theor. Comput. Sci.*, 170:73–94, 2007.

[18] Vincent Danos, Elham Kashefi, and Prakash Panangaden. The Measurement Calculus. *J. ACM*, 54(2):8, 2007.

[19] Ellie D'Hondt. *Distributed Quantum Computation - A Measurement-Based Approach*. PhD thesis, Vrije Universiteit Brussels, 2005.

[20] Ellie D'Hondt and Prakash Panangaden. Reasoning About Quantum Knowledge. *LNCS*, 3821:0544c, 2005.

[21] Ellie D'Hondt and Mehrnoosh Sadrzadeh. Classical Knowledge for Quantum Security. arXiv:0808.3574, Aug 2008. Comments: extended abstract, 13 pages.

[22] Artur K. Ekert. Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, 67(6):661+, 1991.

[23] Ronald Fagin, Joseph Y. Halpern, Moshe Y. Vardi, and Yoram Moses. *Reasoning About Knowledge*. MIT Press, Cambridge, MA, USA, 1995.

[24] Dov Gabbay, Kurt Engesser, and Daniel Lehmann. *A New Approach to Quantum Logic*. College Publications, 2007.

[25] Simon Gay, Rajagopal Nagarajan, and Nikolaos Papanikolaou. Probabilistic Model–Checking of Quantum Protocols, 2005.

[26] Simon Gay, Rajagopal Nagarajan, and Nikolaos Papanikolaou. QMC: A Model Checker for Quantum Systems, 2007.

[27] Simon Gay, Rajagopal Nagarajan, and Nikolaos Papanikolaou. Model Checking Quantum Protocols, 2008.

[28] Simon J. Gay and Rajagopal Nagarajan. Communicating Quantum Processes. *SIGPLAN Not.*, 40(1):145–157, 2005.

[29] D Gottesman. The Heisenberg Representation of Quantum Computers. In *the 1998 International Conference on Group Theoretic Methods in Physics, quant-ph/9807006*, pages 32–43. International Press, 1998.

[30] Daniel Gottesman and Hoi-Kwong LO. From Quantum Cheating to Quantum Security. *PHYSICS TODAY*, 53:22, 2001.

[31] Joseph Y. Halpern. A Little Knowledge Goes a Long Way: Simple Knowledge-based Derivations and Correctness Proofs for a Family of Protocols. In *PODC '87: Proceedings of the sixth annual ACM Symposium on Principles of distributed computing*, pages 269–280, New York, NY, USA, 1987. ACM.

[32] Hans Hansson and Bengt Jonsson. A Logic for Reasoning About Time and Reliability. *Formal Aspects of Computing*, 6:102–111, 1994.

[33] Jaakko Hintikka. *Knowledge and Belief - An Introduction to the Logic of the Two Notions*. Cornell University Press, 1962.

[34] Gerard Holzmann. *The SPIN Model Checker: Primer and Reference Manual*. Pearson Education, 2003.

[35] Michael Huth and Mark Ryan. *Logic in Computer Science: Modelling and Reasoning About Systems (Second Edition)*. Cambridge University Press, 2004.

[36] M. Kwiatkowska, G. Norman, and D. Parker. Quantitative Analysis With the Probabilistic Model Checker PRISM. *Electronic Notes in Theoretical Computer Science*, 153(2):5–31, 2005.

[37] M Lalire and P Jorrand. A Process Algebraic Approach to Concurrent and Distributed Quantum Computation: Operational Semantics. In *In: QPL*, pages 109–126, 2004.

[38] Marie Lalire. Relations Among Quantum Processes: Bisimilarity and Congruence. *Mathematical. Structures in Comp. Sci.*, 16(3):407–428, 2006.

[39] Alessio Lomuscio, Hongyang Qu, and Franco Raimondi. *MCMAS v0.9.7: User's Manual*. Imperial College London, 2009.

[40] Damian Markham and Barry C. Sanders. Graph States for Quantum Secret Sharing, Aug 2008.

[41] Dominic Mayers. Unconditional Security in Quantum Cryptography. *J. ACM*, 48(3):351–406, 2001.

[42] Norman D. Megill and Mladen Pavicic. Equations, States, and Lattices of Infinite-Dimensional Hilbert Spaces. *International Journal of Theoretical Physics*, 39:2337, 2000.

[43] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1996.

[44] Robin Milner. *Communication and Concurrency*. Prentice Hall International (UK) Ltd., Hertfordshire, UK, UK, 1995.

[45] Rajagopal Nagarajan and Simon Gay. Formal Verification of Quantum Protocols, 2002.

[46] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, October 2000.

[47] Nikolaos K. Papanikolaou. Techniques for Design and Validation of Quantum Protocols. Master's thesis, Department of Computer Science, University of Warwick, 2005.

[48] Benjamin Pierce. *Foundational Calculi for Programming Languages*, pages 2190–2207. CRC Press, Boca Raton, FL, 1995.

[49] R. Raussendorf, D.E. Browne, and H.J. Briegel. Measurement-based Quantum Computation on Cluster States. *Physical Review A*, 68(2):9418, 2003.

[50] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, Jan 1996.

[51] Ron van der Meyden and Manas Patra. Knowledge in Quantum Systems. In *TARK*, pages 104–117, 2003.