A Logical Analysis of Quantum Voting Protocols

Soroush Rafiee Rad* Elahe Shirinkalam† Sonja Smets‡

Abstract

In this paper we provide a logical analysis of the Quantum Voting Protocol for Anonymous Surveying as developed by Horoshko and Kilin in [16]. In particular we make use of the probabilistic logic of quantum programs as developed in [7] to provide a formal specification of the protocol and to derive its correctness. Our analysis is part of a wider program on the application of quantum logics to the formal verification of protocols in quantum communication and quantum computation.

1 Introduction

We focus in this paper on the logical analysis of quantum electronic voting. The literature on quantum voting protocols has seen an expansion over the last decade and shows different possible ways in which quantum voting procedures can be specified. The differences in these procedures refer to the use of specific quantum states to encode the voting ballots, to the use of measurements or unitary operators to model the casting of votes and to the presence and actions of an authority or so-called tallyman. All such protocols aim to guarantee at least the correctness of the voting procedure by ensuring that a) the identity of the voters cannot be matched with their votes and b) all votes are correctly accounted for, so that nobody has voted more than once and nobody can change someone else's vote. The first property is what is known as 'privacy' or 'anonymity of voting', while the later property has been called 'non-exaggeration' or also 'non-reusability' in the literature. In addition one may want to ask for other properties which allow each voter to verify that their vote has been correctly accounted for or to guarantee that only eligible voters have participated in the voting procedure. But even when numerous claims are made about the secure features of such protocols in the literature, the question remains whether these claims can survive a logic-based formal verification process? What is needed for a logic-based verification process is an expressive quantum logical language that can provide a proof of the correctness of these protocols. In this paper we provide such an analysis and derive the correctness of the so-called Quantum Voting Protocol for Anonymous Surveying as developed by Horoshko and Kilin in [16].

Our analysis in this paper is based on the Probabilistic Logic of Quantum Programs (PLQP) [7]. PLQP is a logical setting that has already been used for expressing and deriving the correctness of a wide range of different quantum protocols. As a logical setting, PLQP combines the intuitions and techniques from modal logic and probability logic with

*Institute for Logic, Language and Computation, UvA

†Department of Mathematics, Shahid Beheshti University

‡Institute for Logic, Language and Computation, UvA. The contributions by S. Smets and S. Rafiee Rad are supported by FP7/2007-2013/ERC Grant agreement no.283963.

the traditional formalisms of quantum logic. This work is part of the dynamic turn in the study of quantum logic, which follows on the developments in [1, 3, 4, 5, 7]. Characteristic for this approach is the fact that from a conceptual point of view, the non-classicality of quantum behavior is modeled as due to the non-classical dynamics of quantum information rather than to the non-classical behavior of its static properties. From a more technical point of view, this logical setting is particularly suitable for expressing different quantum protocols and allows for a rigorous analysis of their correctness.

In the following sections we first introduce an overview of the main ideas of quantum dynamic logic as formally introduced in [2, 3, 7] and conceptually further explained in [4, 5], before we turn to PLQP which further extends these settings by introducing a probabilistic modality which can capture the probability that a given test (of a quantum-testable property) will succeed. In the last section we apply the logic PLQP to the formal verification of the quantum electronic voting protocol.

2 Probabilistic Logic of Quantum Programs (PLQP)

In the Logic of Quantum Actions (LQA), the Logic of Quantum Programs (LQP) and its probabilistic successor PLQP, Baltag and Smets [2, 3, 7] introduce a new logical perspective on the behaviour of quantum systems. In this approach quantum logic gives a special treatment to the non-classical flow of quantum information. This view divides the structure that governs the interaction between propositions into a static and a dynamic part. The static part of this logical setting captures the static properties of the system in a given state. The dynamic part of the logical setting captures quantum tests and evolutions that can change the state of the system and consequently can change the static properties that are true of the current state of the system.

As explained in [4, 5], conceptually, the aim is to gain a better intuition into the nature of the non-classicality of quantum properties and to account for the strange behaviour of quantum systems in contrast to classical ones. What is more, the static part of this logical settings may well behave classically: this allows for the reintroduction of classical connectives such as disjunction and negation (which have a different meaning in standard quantum logic) to expand the range of properties of the system that can be captured in the logical language. The underlying idea comes from the observation that the physical meaning of the quantum connectives is essentially dynamic: it deals with what will happen to the system as a result of actions such as tests or evolutions of the system. In this view, the move to dynamic logics, that have been studied extensively for modelling dynamic systems (e.g transition systems), for capturing the behaviour of the quantum logical connectives seems a natural step.

In standard quantum logic, a quantum system is modelled by a (infinite dimensional) Hilbert space, say $\mathcal{H}$, and the testable properties of the system will correspond to the closed linear subspaces of $\mathcal{H}$, [14]. The main notion of experiment in quantum mechanics is that of a measurement. In the Hilbert space formalisation, the measurements are modelled by a family of projectors onto mutually orthogonal subspaces of $\mathcal{H}$. More specifically, we can view every such measurement as consisting of a combination of binary yes/no measurements. A binary measurement is represented by a single pair of projectors, one onto a given linear subspace P of $\mathcal{H}$, and the other onto its orthogonal complement, denoted by $P^{\perp}$. Following the line of work of C. Piron, it is indicated in [5] that such a binary measurement can be thought of as a yes/no question where the positive answer corresponds to property P holding after the measurement and the negative answer cor-

responds to property $P^{\perp}$. It is important to notice, however, that the answer "yes" to a test of property P corresponds to the property P holding *after* the measurement has been performed. The measurements on a quantum system can typically change the state of the system, thus a successful test of the property P (or its orthocomplement) only guarantees that the property P (respectively, $P^{\perp}$) holds in the (new) state of the system, after the measurement has been performed. In particular it gives no information as to whether or not P holds in the current state of the system.

In our logical language, we shall write $P?$ for the successful test of property P i.e. the projector onto the closed linear subspace (corresponding to) P. For a system in a state σ, the state of the system after a successful test of property P, is given by projecting σ into the closed linear subspace P, $P?(\sigma)$. So, a successful test of the property P will ensure that the state of the system, after the test, lies in the subspace P and thus guarantees that P will hold for the outcome state $P?(\sigma)$ (but not for the initial state σ). Note also that, the quantum measurements are mostly non-deterministic. That means that the initial state cannot guarantee the outcome of a test either way as long as both projections $P?$ and $P^{\perp}?$ are non-zero.

To see the dynamic nature of the connectives in quantum logic, first consider the property defined by ortho-complementation, $P^{\perp}$. We shall use the syntactic construct $\sim P$ in our language to refer to this property. The operational meaning of $\sim P$ as a property of the state σ is that a test of P, is guaranteed to fail at σ. We note that this is stronger than the assertion that P is false at σ as it is possible for P to be false at σ and yet for a test of P to have a positive probability of success, namely where σ is neither in P nor in $P^{\perp}$. It now becomes clear how the move to dynamic logics can be beneficial: we can, for example, capture the meaning of the ortho-complement using a dynamic formula: for an action π and a property P, the dynamic modality $[\pi]$ is used to capture the performing of action π and the formula $[\pi]P$ captures the assertion that after performing π, property P will hold. In this setting the meaning of $\sim P$ can be captured by a dynamic formula $[P?]\perp$ which guarantees the impossibility of performing a successful test of P. In a similar fashion, following [5], one can work out the operational meaning of the conjunction: a state σ satisfies the conjunction of two testable properties P and Q if and only if both testable properties hold at σ. This means that both tests $P?$ and $Q?$ are certain to succeed at σ. Note in the dynamic logic setting that for two actions, π_1 and π_2, the action $\pi_1 \cup \pi_2$ corresponds to a non-deterministic choice between them, and the identity $[\pi_1 \cup \pi_2]P = [\pi_1]P \wedge [\pi_2]P$, essentially asserts that P holds after a non-deterministic choice of π_1 and π_2 if and only if it holds after performing either of them. Thus $P \wedge Q = \sim\sim P \wedge \sim\sim Q = [(\sim P)?]\perp \wedge [(\sim Q)?]\perp = [(\sim P)? \cup (\sim Q)?]\perp$. Similar arguments can be made for the quantum join and quantum implication. The dynamic nature of these connectives is one of the main motivating reasons for adopting the dynamic turn in the study of quantum logic by Baltag and Smets which we shall further review below.

The way quantum information is viewed in this framework, has made it possible to provide an informational-logical characterization of quantum properties such as 'separability' and 'entanglement' in epistemic logical terms. In the formal setting below we use an epistemic operator $K_I P$ with the intended meaning that subsytem I carries the information that property P holds. This corresponds to a specific type of implicit knowledge, whose semantics as provided in the next section is in line with [8]. Within the latest developments in quantum logic, this approach ties in closely to the work on epistemic quantum structures in [10, 11, 12, 18] where it is shown that quantum computational structures are

intrinsically connected to epistemic problems, interpreting for instance basic epistemic operations as special kinds of Hilbert-space operations. Going one step further on the dynamic logic side does yield a quantum version of Dynamic Epistemic Logic (DEL) that can be used to talk about the informational effects of both classical and quantum measurements [9]. For this paper we will however restrict ourselves to the setting in which we do not yet model the epistemic states of classical agents but use the epistemic operators only to represent non-classical quantum information.

2.1 Syntax of PLQP

In this and the following section we follow [7] to introduce the basics of the formal system PLQP, but refer the reader to [7] for a fully detailed exposition. The syntax of PLQP is an extension of the classical syntax for Propositional Dynamic Logic (PDL), with epistemic as well probabilistic modalities. The set of formulas φ and the set of programs π are defined inductively as:

$$\varphi ::= p|\neg\varphi|\varphi \wedge \varphi|\varphi_I|[\pi]\varphi|K_I\varphi|P^{\geq r}\varphi$$

$$\pi ::= \varphi?|u|\pi^{\top}|\pi \cup \pi|\pi;\pi$$

where $p \in \mathcal{A}t$ are given atomic sentences, $u \in U$ are given unitaries, N is a set of natural numbers and $I \subseteq N$ and $r \in [0,1]$. The $\neg\phi$ and $\phi \wedge \phi$ denote the classical negation and conjunction. To see the intended meaning of ϕ_I and $K_I\phi$ take the given set of natural numbers N and a family of Hilbert spaces $\{\mathcal{H}_i\}_{i\in N}$ and consider $\mathcal{H} = \bigotimes_{i\in N}\mathcal{H}_i$. Then each $I \subseteq N$ corresponds to a subsystem of $\mathcal{H}$ that is made up of those components $\mathcal{H}_i$ with $i \in I$. The formula ϕ_I intuitively refers to the information that the subsystem I has about ϕ. This means that if ϕ_I is true, no local measurement at subsystem I can refute ϕ. The formula $K_I\phi$ is intended to mean that ϕ holds at the subsystem corresponding to I. The probabilistic modality $P^{\geq r}\phi$ has the meaning that testing property ϕ will succeed with probability at least r. The $\phi?$ denotes a successful test of ϕ, $u \in \mathcal{U}$ are basic actions (in physical terms they capture unitaries) and $\pi \cup \pi$ and $\pi;\pi$ denote the non-deterministic choice and the sequential composition respectively.

Quantum negation, quantum join as well as classical conjunction and implication are definable in this syntax, as are a range of other obvious probabilistic formulas:

$$\begin{array}{lll}
\bot := \phi \wedge \neg\phi & \sim\phi := [\phi?]\bot & \phi \sqcup \psi := \sim(\sim\phi \wedge \sim\psi) \\
P^{\leq r}\phi := P^{\geq(1-r)} \sim\phi & P^{>r}\phi := \neg P^{\leq r}\phi & P^{<r}\phi := \neg P^{\geq r}\phi \\
T(\phi) := \sim\sim\phi \equiv \phi & I(\phi) := \phi \equiv \phi_I &
\end{array}$$

where predicate T is interpreted as testability, thus $T(\phi)$ captures that ϕ is a testable property.

2.2 Semantics of PLQP

Fix a Hilbert space $\mathcal{H}$ and let $\Sigma_{\mathcal{H}}$ denote the set of one dimensional subspaces of $\mathcal{H}$. The semantics of PLQP is defined by an assignment, $\|\cdot\|$, assigning a set $\|p\| \subseteq \Sigma_{\mathcal{H}}$ (which, we will identify with the closed linear subspace of $\mathcal{H}$ spanned by it) to each

atomic proposition p and a unitary relation $\|u\| \subset \Sigma_{\mathcal{H}} \times \Sigma_{\mathcal{H}}$ to each basic action u. This assignment is then recursively extended to all sentences and programs. The intuition here is to view the system as a transition system where $\Sigma_{\mathcal{H}}$ is the set of states. The interpretation of formulas specify which formula is true at each state. The interpretation of programs as relations between states captures the transition from a state to another as a result of an action.

For a relation $R \subset \Sigma_{\mathcal{H}} \times \Sigma_{\mathcal{H}}$ and $\sigma \in \Sigma_{\mathcal{H}}$, let $R(\sigma) = \{\delta \in \Sigma_{\mathcal{H}} \,|\, (\sigma, \delta) \in R\}$ and for a closed linear subspace S of $\mathcal{H}$ let $Proj_S : \mathcal{H} \to \mathcal{H}$ be the projection on S.

$$\|\neg\phi\| = \Sigma_{\mathcal{H}} - \|\phi\| \qquad \|\phi \wedge \psi\| = \|\phi\| \cap \|\psi\|$$
$$\|[u]\phi\| = \{\sigma \mid \|u\|(\sigma) \subseteq \|\phi\|)\} \qquad \|[\phi?]\psi\| = \{\sigma \,|\, Proj_{\|\phi\|}(\sigma) \in \|\psi\|\}$$
$$\|[\pi_1;\pi_2]\phi\| = \|[\pi_2][\pi_1]\phi\| \qquad \|[\pi_1 \cup \pi_2]\phi\| = \|[\pi_1]\phi\| \cap \|[\pi_2]\phi\|$$

Take the Hilbert space $\mathcal{H} = \bigotimes_{i\in N} \mathcal{H}_i$ and let $U : \mathcal{H} \to \mathcal{H}$ be a unitary transformation of the form $U = Id_I \otimes V$ where $Id_I : \bigotimes_{i\in I} \mathcal{H}_i \to \bigotimes_{i\in I} \mathcal{H}_i$ is the identity map on I and $V : \bigotimes_{i\in N-I} \mathcal{H}_i \to \bigotimes_{i\in N-I} \mathcal{H}_i$ is a unitary transformation. Then U is called I-remote and we denote the set of I-remote transformations by $U_{Rem(I)}$.

$$\|\phi_I\| = \{\sigma_I \otimes \sigma_{N-I} \,|\, \sigma_I \otimes \delta_{N-I} \in \|\phi\| \text{ for some } \delta_{N-I}\} \quad \|K_I\phi\| = \{\sigma \,|\, \forall U \in U_{Rem(I)} U(\sigma) \subseteq \|\phi\|\}$$
$$\left\|P^{\geq r}\phi\right\| = \{\sigma \,|\, \langle v|Proj_{\|\phi\|}|v\rangle \geq r \text{ for all unit } v \in \sigma\}$$

With this semantics, at state σ, $K_I\phi$ is true if and only if ϕ is true at any other state that is indistinguishable from σ for the subsystem I. The interpretation of the probabilistic modality is given, as expected, by Bohr's formula which regulates the collapse of the quantum state to a new state with probability $\geq r$ during a quantum measurement.

2.2.1 Proof System of PLQP

The proof system for PLQP is developed in [13] and extends the earlier work in [2]. It consists of three rules.

- Modus Ponens $\frac{\phi \quad \phi\to\psi}{\psi}$
- Necessitation $\frac{\phi}{[\pi]\phi}$
- Substitution $\frac{\phi(p)}{\phi[q/p]}$

We extend the list of axioms in [13] by adding the axioms for a spatial-epistemic operator K. First we introduce the standard axioms for propositional dynamic logic,

$$\textit{All propositional tautologies} \qquad \vdash [\pi_1;\pi_2]p \leftrightarrow [\pi_2][\pi_1]p$$
$$\vdash [\pi_1 \cup \pi_2]p \leftrightarrow [\pi_1]p \wedge [\pi_2]p$$

Next we add the basic axioms for quantum systems, where we use the abbreviations $\top = \neg\bot$, $\langle\pi\rangle\phi = \neg[\pi]\neg\phi$, $\Box\phi =\sim \neg\phi$ and $\Diamond\phi = \neg\Box\neg\phi$

$\vdash \langle q?\rangle p \to \langle p?\rangle\top$ $(testability)$
$\vdash (p \wedge q) \to \langle p?\rangle q$ $(Adequacy)$
$\vdash p \to [u; u^T]p$ $(UnitaryBijectivity1)$
$\vdash \langle\pi\rangle\Box\Box p \to [\pi']p$ $(ProperSuperpositions)$
$\vdash \neg[p?]q \to [p?]\neg q$ $(PartialFunctionality)$
$\vdash T(p) \to [p?]p$ $(Repeatability)$
$\vdash p \to [u^T; u]p$ $(UnitaryBijectivity2)$
$\vdash p \to [q?]\Box\langle q?\rangle\Diamond p$ $(Adjointness)$

and the axioms for the local formulas and Spatial-Knowledge modality

$\vdash I(\phi) \to \phi_{N-I} \equiv \top$ $(I1)$
$\vdash K_I\phi \to \phi$ $(K1)$
$\vdash J(\phi) \to (\phi \to K_I\phi)$ $for\ all\ J \subseteq I$ (KI)
$\vdash (\phi \wedge \psi)_I \equiv \phi_I \wedge \psi_I$ $(I2)$
$\vdash K_I(\phi \to \psi) \to (K_I\phi \to K_I\psi)$ $(K2)$

And finally we add the axioms about local and probabilistic formulas, where $P^{=r}\phi = P^{\geq r}\phi \wedge P^{\leq r}\phi$,

$\vdash P^{\geq 0}\phi$ $\vdash P^{=1}\top$ $\vdash P^{=0}\phi \leftrightarrow\sim \phi$
$\vdash (\phi \equiv \psi) \to (P^{=r}\phi \leftrightarrow P^{=r}\psi)$
$\vdash \Box\Box(\phi \to\sim \psi) \to (P^r(\phi \sqcup \psi) \to (P^{=s}\phi \to P^{=r-s}\psi))$
$\vdash \Box\Box(\phi \to \psi) \wedge P^{=r}\psi \wedge [\psi?]P^{=s}\phi \to P^{=rs}\phi$
$\vdash (\Box\Box(p \to\sim q) \wedge P^{>0}p \wedge P^{>0}q) \to P^{>0}(P^{=r}p \wedge P^{=1-r}q)$

A proof is defined in the usual way. The first set of axioms are standard in propositional dynamic logic and capture the intended meaning of non-deterministic choice and sequential composition. In the axioms for quantum systems, as explained in [3, 2], *Testability* asserts that any property that can be realized by performing a measurement is a testable property. *Adequacy* asserts that testing a true property does not change the state and *Repeatability* ensures that after testing a property, it will hold true and thus any successive test of the same property will be guaranteed to succeed. The Unitary Bijectivities correspond to unitaries being invertible functions whose transpose is their inverse and *superposition* and the *Adjointness* axiom correspond to projectors being Hermitian self adjoints operators on the Hilbert space. For the probabilistic axioms, the first two correspond to probabilities being in the interval [0, 1] and that a test of ϕ is guaranteed to fail exactly when the a test of $\sim \phi$ is guaranteed to succeed. The third axiom asserts that equivalent formulas should have equal probabilities and the forth axiom captures the additivity of the probabilities (notice that here ϕ and ψ) and the fifth captures the law of conditional probabilities: the probability of $\phi \wedge \psi$ is equal to probability ϕ given ψ times probability of ψ. The last axiom is the probabilistic assertion of the superposition axiom: for every two states there is a state that is the superposition of the two and thus have complementary probability of collapsing on each one the two states.

Theorem 2.1. *All the axioms above are sound with respect to the given Hilbert space semantics.*

Proof.
We show the soundness of the axiom (KI). See [13] and [2] for a proof the soundness of other axioms. Suppose ϕ is J-local, $J \subseteq I$, and that $\sigma \in \|\phi\|$. We will show that $\sigma \in \|K_I\phi\|$. Let U be an arbitrary I-remote operation, then $U = Id_I \otimes V_{N-I}$. Since ϕ is J remote $\|\phi\| = \|\phi_J\| = \{\sigma_J \otimes \sigma_{N-J} \mid \sigma_J \otimes \delta_{N-I} \in \|\phi\| \text{ for some } \delta_{N-I}\}$. Then for $\sigma \in \|\phi\|$, if $\gamma \in U(\sigma)$ then $\gamma = \sigma_J \otimes \sigma_{I-J} \otimes \delta_{N-I}$ for some δ_{N-I}. Thus $\gamma \in \|\phi_J\|$ by definition since $\sigma_J \otimes \sigma_{N-J} \in \|\phi_J\| = \|\phi\|$. Thus $\gamma \in \|\phi\|$ and hence $U(\sigma) \subseteq \|\phi\|$. Since U was *any* I-remote operation we have $\sigma \in \|K_I\phi\|$ as required.

Proposition 2.2. *The following formulae are derivable.*
$(i). \vdash p \to \sim\sim p \quad (ii). (p \to q) \to (\sim q \to \sim p) \quad (iii). \vdash (p \to q) \to (Pr^{\geq r}p \to P^{\geq r}q)$
$(iv). \vdash T(\phi) \to (\phi \leftrightarrow P^{=1}\phi) \quad (v). \vdash T(\phi) \wedge T(\psi) \to T(\phi \sqcup \psi)$
(vi). For all n the following formula is derivable.

$$\vdash \left(\bigwedge_{i<j\leq n} b_i \perp b_j \right) \to \left(P^{=r} \bigsqcup_{i\leq n} b_i \wedge P^{=r_i} b_i \to P^{=r-r_i} \bigsqcup_{j\neq i,\, j\leq n} b_j \right)$$

See [13] for proofs.

Proposition 2.3.

$$\vdash \left(\bigsqcup_{i=1}^{n} \phi_i \wedge \bigwedge_{i\neq j} (\phi_{i,I} \perp \phi_{j,I}) \right) \to \bigwedge_{i=1}^{n} (K_I\phi_{i,I} \to K_{N-I}\phi_{i,N-I})$$

Proof.

1. $\vdash K_I\phi_{i,I} \to \phi_{i,I}$ (K1)
2. $\vdash \bigwedge_{j\neq i}(\phi_{i,I} \perp \phi_{j,I}) \to (K_I\phi_{i,I} \to \bigwedge_{j\neq i} \sim \phi_{j,I})$ (2)
3. $\vdash \bigwedge_{j\neq i} \phi_{i,I} \perp \phi_{j,I} \to (K_I\phi_{i,I} \to \bigwedge_{j\neq i} P^{=0}\phi_{j,I})$ (P. 2.2)
4. $\vdash \bigwedge_{i=1}^{n}(\phi_j \to \phi_{j,I})$
5. $\vdash \bigwedge_{i=1}^{n}(P^{>0}\phi_j \to P^{>0}\phi_{j,I})$ (P. 2.2)
6. $\vdash \bigwedge_{j\neq i} \phi_{i,I} \perp \phi_{j,I} \to (K_I\phi_{i,I} \to \bigwedge_{j\neq i} P^{=0}\phi_j)$ (3, 5)
7. $\vdash \bigsqcup_{i=1}^{n} \phi_i \wedge \bigwedge_{j\neq i} \phi_{i,I} \perp \phi_{j,I} \to (K_I\phi_{i,I} \to \phi_i)$ (6, P. 2.2)
8. $\vdash \phi_i \to \phi_{i,N-I}$
9. $\vdash \bigsqcup_{i=1}^{n} \phi_i \wedge \bigwedge_{j\neq i} \phi_{i,I} \perp \phi_{j,I} \to (K_I\phi_{i,I} \to \phi_{i,N-I})$ (7, 8)
10. $\vdash N - I(\phi_{i,N-I})$ (since $\phi_{i,N-I}$ is $N-I$ local)
11. $\vdash \phi_{i,N-I} \to K_{N-I}\phi_{i,N-I}$ (10, KI)
12. $\vdash \bigsqcup_{i=1}^{n} \phi_i \wedge \bigwedge_{j\neq i} \phi_{i,I} \perp \phi_{j,I} \to (K_I\phi_{i,I} \to K_{N-I}\phi_{i,N-I})$ (9, 11)

Proposition 2.4. *For a finite set of formula $\mathcal{B} = \{b_1, \ldots, b_n\}$, let $SubBasis(\mathcal{B}) = \left(\bigwedge_{b\in\mathcal{B}} b \not\equiv \perp\right) \wedge \bigwedge_{b_i\neq b_j\in\mathcal{B}}(b_i \perp b_j) \wedge \left(\bigsqcup_{b\in\mathcal{B}} b \equiv T\right)$. Then the following formula is derivable.*

$$\vdash SubBasis(\mathcal{B}) \to \bigwedge_{b_i\in\mathcal{B}} (P^{=r_i} b_i \to P^{=1-r_i} \bigsqcup_{j\neq i, j\in\mathcal{B}} b_j)$$

The proof follows directly from Proposition 2.2.

3 Deriving the Correctness of Quantum Voting Protocols

The logic PLQP has been developed as a logic for quantum programs. Baltag et al. investigated the application of PLQP to quantum protocols in [7] by showing that this logical setting can express and analyse, for example, the protocol for the *quantum leader election*. Bergfield and Sack, expanded this direction in [13] by developing the proof system given in the previous section and used PLQP to express and formally derive the correctness of the *BB84* protcol in the given proof system. Our goal here is to extend their analysis to the application of this logic to study quantum anonymous voting protocols. In particular we can express and formally verify the correctness of the *Quantum Voting Protocol for Anonymous Surveying* developed by Horoshko and Kilin [16] as well as the *Quantum Secret Ballot* developed by Dolev, Pitowsky, and Tamir [15]. We will focus here only on the *Quantum Voting Protocol for Anonymous Surveying* as it is the more involved of the two.

3.1 Quantum Voting Protocol for Anonymous Surveying

The *Quantum Voting Protocol for Anonymous Surveying* is developed by Horoshko and Kilin [16]. First the description of the protocol:

The Protocol: Let $V = \{v_1, ..., v_n\}$ be n legal voters who participate in a voting process and let state $|0, ..., 0\rangle$ be an initial state in a compound system $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$. Let $\Psi_{ij}^{\pm}$ and $\Phi_{ij}^{\pm}$ denote the following Bell states

$$\Psi_{ij}^{\pm} := \frac{1}{\sqrt{2}}(|0_i 1_j\rangle \pm |1_i 0_j\rangle), \quad \Phi_{ij}^{\pm} := \frac{1}{\sqrt{2}}(|0_i 0_j\rangle \pm |1_i 1_j\rangle).$$

Each voter makes a decision to vote or to check for anonymity. This divides the voters into two groups A_1 and A_2:

a) $i \in A_1$ if and only if v_i wants to votes. Let a_i denote the vote of voter v_i where $a_i = 0$ corresponds to **no** and $a_i = 1$ to **yes**. To encode her vote, the voter applies the operator X^{a_i} on the i-th qubit (thus $X_i^0 = I_i$ (identity operator) if the vote is no and $X_i^1 = X_i$ if the vote is yes).

b) $i \in A_2$ if and only if v_i wants to check for anonymity. In this case v_i cooperates with another voter who also wants to check for anonymity, say voter v_j. Let $A_2' = \{(i, j) \mid i, j \in A_2\}$ such that each $i \in A_2$ appears in exactly one pair in A_2'. So A_2' is the pairs of agents that have chosen to cooperate for an anonymity check. For each $(i, j) \in A_2'$, v_i and v_j encode their pair of qubits in the Bell state $\Psi_{ij}^{+} = \frac{1}{\sqrt{2}}(|0\rangle_i|1\rangle_j + |1\rangle_i|0\rangle_j)$.
The program π_v corresponding to the voting process can be described as

$$\pi_v := \bigwedge_{(i,j)\in A_2'} (\Psi_{ij}^{+}?); \bigwedge_{i\in A_1} (X_i^{a_i})$$

The votes are then sent to the tallyman together with the identities of these voters. The identities are used by the tallyman to check that all voters are legitimate and

that each have voted only once, although this process is not part of the protocol. The tallyman then calculates the number of **yes** votes by applying to the n-qubit system the projector valued measure

$$\widehat{P}(s) = \sum_{\pi} |m(s,\pi)\rangle\langle m(s,\pi)|$$

where $|m(s,\pi)\rangle$ is a product state of n qubits in the computational basis, having exactly s $1's$ in the order determined by the permutation variable π. Next, the tallyman send the qubits back to the voters and they perform a ballot test to ensure that the votes have not been tampered with:

a) For each $i \in A_1$, v_i measures her qubit in the computational basis. If the state of this qubit is different from the a_i she announces the ballot test failure. The program $\pi_{A_1} = \bigwedge_{i\in A_1}(b_i?)$ describes this action.

b) For each $(i,j) \in A_2'$, voters v_i and v_j measure their pair of qubits in the Bell basis. The program $\pi_{A_2} := \bigwedge_{(i,j)\in A_2'}(\Psi_{ij}^+? \cup \Psi_{ij}^-? \cup \Phi_{ij}^+? \cup \Phi_{ij}^-?)$ describes this action. If the result of their measurement is different from Ψ^+, they announce a ballot test failure. The program corresponding to the whole process of voting by agents, counting by the tallyman and rechecking by agents can be described by

$$\pi := \bigwedge_{(i,j)\in A_2'} (\Psi_{ij}^+? \cup \Psi_{ij}^-? \cup \Phi_{ij}^+? \cup \Phi_{ij}^-?); \bigwedge_{i\in A_1} (b_i?); \widehat{P}(s); \pi_v$$

3.1.1 Simple Attacks

The simplest type of attack for the tallyman is to make a measurement on the i-th qubit. This measurement is represented in our setting as $\pi_{SA} := (0_i)? \cup (1_i)?$. Let $\Pi = \{0,1\}^n$ and let Π_s be the subset of Π with sequences with exactly s 1's. For each $i \in \{1,...,n\}$, we add propositional variables $0_i, 1_i$ to denote the proposition that the state of the i-th qubit is $|0\rangle_i$ or $|1\rangle_i$ respectively. Moreover, let the propositional variables $\sigma_{s,\pi}$, $1 \leq s \leq n, \pi \in \Pi_s$, denote the ballot states with exactly s 1's in the positions specified by π. And for the ease of notation we take propositional variables $\Psi_{ij}^{\pm}$ and $\Phi_{ij}^{\pm}$ to denote that the i-th and j-th qubits are in the respective Bell states. If v_i has chosen to vote, this attack will pass unnoticed. However, if v_i has chosen to check for anonymity (in cooperation with, say v_j), the attack will be detected with a positive probability. What this means is that the tallyman cannot safely execute the simple attack described above. Let's assume all other voters (except from v_i and v_j) have chosen to vote, with k voting yes. The ballot state will then be

$$\frac{1}{\sqrt{2}}(|m(k+1,\pi)\rangle + |m(k+1,\pi')\rangle)$$

where π and π' agree on every position except i and j where they differ. This state is described in our setting by the formula

$$\theta := (\sigma_{k+1,\pi} \sqcup \sigma_{k+1,\pi'}) \wedge (P^{=r}\sigma_{k+1,\pi} \leftrightarrow P^{=r}\sigma_{k+1,\pi'}).$$

Notice that θ implies Ψ_{ij}^+ and that the Bell states are testable and local properties. So for $I = \{i,j\}$

$$\vdash \theta \rightarrow \Psi_{ij}^+ \qquad \vdash T(\Psi_{ij}^+) \wedge T(\Psi_{ij}^-) \qquad \vdash I(\Psi_{ij}^{\pm}) \tag{1}$$

After the attack, the state of the ij subsystem, which was Ψ^+_{ij}, will collapse into $|0\rangle_i|1\rangle_j$ or $|1\rangle_i|0\rangle_j$

$$\vdash \Psi^+_{ij} \to [(0_i)? \cup (1_i)?]((0_i \wedge 1_j) \vee (1_i \wedge 0_j)).$$

When the voters check the validity of the ballot state, v_i and v_j run a measurement in the Bell basis. In this basis the states $|0\rangle_i|1\rangle_j$ and $|1\rangle_i|0\rangle_j$ are both superpositions of Ψ^+_{ij} and Ψ^-_{ij} and upon a Bell measurement they will collapse on either Ψ^+_{ij} or Ψ^-_{ij} with equal probability.

$$\vdash (0_i \wedge 1_j) \to \big((\Psi^+_{ij} \sqcup \Psi^-_{ij}) \wedge (P^{=r}\Psi^+_{ij} \leftrightarrow P^{=r}\Psi^-_{ij})\big) \tag{2}$$

So when the measurement is preformed by v_i and v_j, they will observe either Ψ^+_{ij} or Ψ^-_{ij} with equal probabilities. If the probability of observing Ψ^-_{ij} is positive it means a positive probability of the ballot test failure. Remember that π_{SA} is the simple attack $(0_i? \cup 1_i?)$ and π_B is the measurement in Bell basis $(\Psi^+_{ij}? \cup \Psi^-_{ij}? \cup \Phi^+_{ij}? \cup \Phi^-_{ij}?)$. We prove that, if the simple attack (π_{SA}) is made on the ballot state described by θ, the ballot test (π_{A_2}) by v_i and v_j will fail with a positive probability. To this end, we show

$$\vdash \theta \to [\pi_{SA}]P^{>0}[\pi_{A_2}]K_{A_2}\neg\theta$$

1. $\vdash \theta \to \Psi^+_{ij}$.
2. $\vdash \Psi^+_{ij} \to [\pi_{SA}]((0_i \wedge 1_j) \vee (1_i \wedge 0_j))$
3. $\vdash (1_i \wedge 0_j) \to (\Psi^+ \sqcup \Psi^-)$ (Eq (2))
4. $\vdash (0_i \wedge 1_j) \to (\Psi^+ \sqcup \Psi^-)$ (Eq (2))
5. $\vdash T(\phi) \wedge T(\psi) \to T(\phi \sqcup \psi)$ (P. 2.2)
6. $\vdash T(\Psi^+_{ij}) \wedge T(\Psi^-_{ij})$ (Eq 1)
7. $\vdash P^{=1}(\Psi^+_{ij} \sqcup \Psi^-_{ij}) \leftrightarrow (\Psi^+_{ij} \sqcup \Psi^-_{ij})$ (5, 6, Pr. 2.2)
8. $\vdash (0_i \wedge 1_j) \to P^{=1}(\Psi^+ \sqcup \Psi^-)$ (4, 7)
9. $\vdash P^{=1}(\Psi^+_{ij} \sqcup \Psi^-_{ij}) \to (P^{=0}\Psi^+_{ij} \to P^{=1}\Psi^-_{ij})$ (P. 2.2)
10. $\vdash (0_i \wedge 1_j) \to (P^{=1}\Psi^+_{ij} \to P^{=0}\Psi^-_{ij})$ (8, 9)
11. $\vdash (0_i \wedge 1_j) \to (\neg P^{=0}\Psi^-_{ij} \to \neg P^{=1}\Psi^+_{ij})$ (11)
12. $\vdash (0_i \wedge 1_j) \to (P^{=r}\Psi^-_{ij} \to P^{=r}\Psi^+_{ij})$ (Eq 2)
13. $\vdash (0_i \wedge 1_j) \to (P^{=0}\Psi^-_{ij} \to P^{=0}\Psi^+_{ij})$ (13)
14. $\vdash (0_i \wedge 1_j) \to (P^{=0}\Psi^-_{ij} \to \neg P^{=1}\Psi^+_{ij})$ (14)
15. $\vdash (0_i \wedge 1_j) \to (P^{=0}\Psi^-_{ij} \vee \neg P^{=0}\Psi^-_{ij})$ (Prop. Logic)
16. $\vdash (0_i \wedge 1_j) \to \neg P^{=1}\Psi^+_{ij}$. (12, 15, 16)
17. $\vdash (0_i \wedge 1_j) \to P^{<1}\Psi^+_{ij}$ (17)
18. $\vdash (1_i \wedge 0_j) \to P^{<1}\Psi^+_{ij}$ (similarly)
19. $\vdash ((0_i \wedge 1_j) \vee (1_i \wedge 0_j)) \to P^{<1}\Psi^+_{ij}$ (18, 19)
20. $\vdash \Psi^+_{ij} \sqcup \Psi^-_{ij} \to (P^{=0}\Psi^-_{ij} \to P^{=1}\Psi^+_{ij})$ (P. 2.2)
21. $\vdash ((0_i \wedge 1_j) \vee (1_i \wedge 0_j)) \to \neg P^{=0}\Psi^-_{ij}$ (3,4, 20, 21)
22. $\vdash \Psi^-_{ij} \to [\pi_{A_2}]\Psi^-_{ij}$ (from Adequacy)
23. $\vdash P^{>0}\Psi^-_{ij} \to P^{>0}[\pi_{A_2}]\Psi^-_{ij}$ (P. 2.2)
24. $\vdash ((0_i \wedge 1_j) \vee (1_i \wedge 0_j)) \to P^{>0}[\pi_{A_2}]\Psi^-_{ij}$ (22, 24)
25. $\vdash \theta \to [\pi_{SA}]P^{>0}[\pi_{A_2}]\Psi^-_{ij}$ (1, 2, 25)
26. $\vdash \{i,j\}(\Psi^-_{ij})$. ($\Psi^-_{ij}$ is local to i,j-subsystem)
27. $\vdash \Psi^-_{ij} \to K_{A_2}\Psi^-_{ij}$ (27, KI)
28. $\vdash \theta \to [\pi_{SA}]P^{>0}[\pi_{A_2}]K_{A_2}\Psi^-_{ij}$ (26, 28)
29. $\vdash \theta \to [\pi_{SA}]P^{>0}[\pi_{A_2}]K_{A_2}\neg\Psi^+_{ij}$
30. $\vdash \theta \to [\pi_{SA}]P^{>0}[\pi_{A_2}]K_{A_2}\neg\theta$. (1, 30)

Which yields

$$\vdash \theta \to [\pi_{SA}]P^{>0}[\pi_{A_2}]K_{A_2}\neg\theta$$

as required.

3.1.2 General Attack

Assume that the tallyman wants to make a measurement on the ballot state. Let's call the system of n qubits the Ballot, B. The most general type of measurement on B consists in first attaching to it another quantum system of at least the same dimensionality, the Apparatus A. Next to perform a unitary transformation U_{BA} of both the Ballot and the Apparatus. And finally, to analyse the resulting state of the Apparatus.
The unitary transformation can be determined by its action on the basis states:

$$U_{BA}|m(s,\pi)\rangle_B|a_0\rangle_A = \sum_{\pi'} |m(s,\pi')\rangle_B|a_{\pi\pi'}\rangle_A \tag{3}$$

Where $|a_0\rangle_A$ is the initial state of the apparatus and $|a_{\pi\pi'}\rangle_A$ are its final states. The claim is that any interference of this general sort by the tallyman has a positive probability of detection, in the sense that for any attack by the tallyman, there is some ballot state in which the tallyman's attack can result in a ballot test failure.
More precisely, it is proved in [16], that for any measurement, defined by the apparatus states, there is a ballot state for which the probability of ballot test failure is non-zero unless all the states of the apparatus satisfy $|a_{\pi\pi'}\rangle_A = |a\rangle_A$. This effectively renders the apparatus uninformative.

3.1.3 Verification for the General Attack

The security of the protocol is claimed probabilistically; it is not the case that any attack by the tallyman *will* be detected, but that any such attack *might* be detected. Thus the protocol ensures that there is no *safe* way for the tallyman to intervene with the ballot state.
Consider the compound system of the ballot and the apparatus given in $\mathcal{H}$. We shall call the subsystem referring to the ballot by B and the one for the apparatus by A, $\mathcal{H} = \mathcal{H}_B \otimes \mathcal{H}_A$. Let the propositional variables $\sigma_{s,\pi}$ denote the ballot state with s 1's in the positions specified by π as before and δ_0 denote the proposition that the initial state of the apparatus is $|a_0\rangle$. Let $\delta_{\pi,\pi'}$ be the set of propositional variables denoting the possible final states of the apparatus $|a_{\pi,\pi'}\rangle$ that form an orthonormal basis for $\mathcal{H}_A$. Notice that $\Sigma_s = \{\sigma_{s,\pi} \,|\, \pi\}$ forms a basis for a $\binom{n}{s}$ dimensional subspace of $\mathcal{H}_B$. The formulas $\sigma_{s,\pi}$ and $\delta_{\pi,\pi'}$ are thus local to subsystems B and A respectively. Remembering that for a subsystem I, $I(\phi) := \phi \equiv \phi_I$, expresses that ϕ is local to subsystem I, we write these as

$$\bigwedge_{s=1}^{n} \bigwedge_{\pi\in\Pi_s} B(\sigma_{s,\pi'}), \qquad \bigwedge_{s=1}^{n} \bigwedge_{\pi,\pi'\in\Pi_s} A(\delta_{\pi,\pi'}).$$

First suppose we know that there are $\pi \neq \pi'$ and a possible non-zero final state $|a_{\pi,\pi'}\rangle \neq 0$ for the apparatus, denoted by $\delta_{\pi,\pi'}$, i.e, $[U]P^{>0}K_A\delta_{\pi,\pi'}$. We consider two cases: In the first case all voters have decided to vote and the ballot state is given by $|m(s,\pi)\rangle = \sigma_{s,\pi}$. The tallyman will be safe from detection if after the attack, no measurement available to subsystem B (which is accessible to agents) can detect that the state has changed (i.e. refute $\sigma_{s,\pi}$). In other words, the tallyman will be safe if after the attack $\neg K_B\neg\sigma_{s,\pi}$ holds. We will thus show that this fails with a positive probability, which ensures a positive probability of the ballot test will failure after the attack. To this end we show that, after the attack, $P^{>0}K_B\neg\sigma_{s,\pi}$ holds true.

Proof. By 3,

$$\sigma_{s,\pi} \wedge \delta_0 \rightarrow [U_{BA}] \bigsqcup_{\pi'} (\sigma_{s,\pi'} \wedge \delta_{\pi,\pi'}).$$

So

1. $\vdash \sigma_{s,\pi} \wedge \delta_0 \rightarrow [U] \bigsqcup_{\pi'} (\sigma_{s,\pi'} \wedge \delta_{\pi\,\pi'})$
2. $\vdash \bigwedge_{s=1}^{n} \bigwedge_{\pi \in \Pi_s} B(\sigma_{s,\pi'})$
3. $\vdash \bigwedge_{s=1}^{n} \bigwedge_{\pi,\pi' \in \Pi_s} A(\delta_{\pi,\pi'})$
4. $\vdash \bigwedge_{\pi' \in \Pi_s} ((\sigma_{s,\pi'} \wedge \delta_{\pi,\pi'})_B \equiv \sigma_{s,\pi'})$
5. $\vdash \bigwedge_{\pi' \in \Pi_s} ((\sigma_{s,\pi'} \wedge \delta_{\pi,\pi'})_A \equiv \delta_{\pi,\pi'})$
6. $\vdash SubBasis(\Sigma_s)$
7. $\vdash SubBasis(\Delta)$
8. $\vdash \bigwedge_{\pi \neq \pi' \in \Pi_s} \sigma_{s,\pi} \perp \sigma_{s,\pi'}$ (6)
9. $\vdash \bigwedge_{\pi' \neq \pi'' \in \Pi_s} \delta_{\pi,\pi'} \perp \delta_{\pi,\pi''}$ (7)
10. $\vdash \bigwedge_{\pi' \neq \pi'' \in \Pi_s} (\sigma_{s,\pi'} \wedge \delta_{\pi,\pi'})_A \perp (\sigma_{s,\pi''} \wedge \delta_{\pi,\pi''})_A$ (5, 9) □
11. $\vdash \bigsqcup_{\pi' \in \Pi_s} (\sigma_{s,\pi'} \wedge \delta_{\pi,\pi'}) \rightarrow (K_A \delta_{\pi,\pi'} \rightarrow K_B \sigma_{s,\pi'})$ (5, 10, P. 2.3)
12. $\vdash \sigma_{s,\pi} \wedge \delta_0 \rightarrow [U](K_A \delta_{\pi,\pi'} \rightarrow K_B \sigma_{s,\pi'})$ (1, 11)
13. $\vdash \sigma_{s,\pi} \wedge \delta_0 \rightarrow [U](P^{>0} K_A \delta_{\pi,\pi'} \rightarrow P^{>0} K_B \sigma_{s,\pi'})$ (12, P. 2.2)
14. $\vdash [U] P^{>0} K_A \delta_{\pi,\pi'}$ (by assumption)
15. $\vdash \sigma_{s,\pi} \wedge \delta_0 \rightarrow [U] P^{>0} K_B \sigma_{s,\pi'}$ (13,14)
16. $\vdash \sigma_{s,\pi} \wedge \delta_0 \rightarrow [U] P^{>0} K_B \sim \sigma_{s,\pi}$ (8, 15)
17. $\vdash \sigma_{s,\pi} \wedge \delta_0 \rightarrow [U] P^{>0} K_B \neg \sigma_{s,\pi}$ (16)

So for $\pi \neq \pi'$, $P^{>0} K_A \delta_{\pi,\pi'}$ results in a positive probability of a ballot test failure. Next suppose $|a_{\pi,\pi}\rangle \neq |a_{\pi',\pi'}\rangle$, denoted by $\delta_{\pi,\pi}$ and $\delta_{\pi',\pi'}$, are two possible non-zero final states of the apparatus, i.e., $[U](P^{>0} K_A \delta_{\pi,\pi} \wedge P^{>0} K_A \delta_{\pi',\pi'})$. Assume that π and π' differ in k places. Take the voting profile in which k voters, specified by those coordinates in which π and π' differ, choose to make anonymity check and the rest vote according to π (or π' as they agree on the remaining places). Let Π^k denote the set of 2^k, π which agree on fixed $n - k$ places. The ballot state will then be

$$E = \frac{1}{\sqrt{2^k}} \sum_{\pi \in \Pi^k} |m(k+l, \pi)\rangle$$

that is, the superposition of 2^k states which are denoted in our setting by $\sigma_{k+l,\pi}$, $\pi \in \Pi^k$. Let ψ be the formula denoting this superposition, $\psi = \bigsqcup_{\pi \in \Pi^k} \sigma_{k+l,\pi} \wedge \bigwedge_{\pi,\pi' \in \Pi^k} (P^{=r} \sigma_{k+l,\pi} \rightarrow P^{=r} \sigma_{k+l,\pi'})$. We have

$$U_{BA} |E\rangle_B |a_0\rangle_A = \frac{1}{\sqrt{2^k}} \sum_{\pi'} \sum_{\pi} |m(k+l, \pi)\rangle |a_{\pi\pi'}\rangle$$

Remember that by the discussion above, for $\pi \neq \pi'$ we have $P^{=0} K_A \delta_{\pi,\pi'}$ or there is already a positive probability of the ballot test failure and we are done. Thus $\psi \wedge \delta_0 \rightarrow [U] \bigsqcup_{\pi \in \Pi_{k+l}} (\sigma_{k+l,\pi} \wedge \delta_{\pi,\pi})$. We will now show that the tallyman's attack on this ballot state gives a non-zero probability of ballot test failure and thus can be detected with a

positive probability.

1. $\vdash \psi \wedge \delta_0 \rightarrow [U] \bigsqcup_{\pi} \sigma_{k+l,\pi} \wedge \delta_{\pi,\pi}$
2. $\bigwedge_{\pi' \neq \pi'' \in \Pi_s} (\sigma_{k+l,\pi'} \wedge \delta_{\pi,\pi'})_B \perp (\sigma_{k+l,\pi''} \wedge \delta_{\pi,\pi''})_B$
3. $\bigwedge_{\pi' \neq \pi'' \in \Pi_s} (\sigma_{s,\pi'} \wedge \delta_{\pi,\pi'})_A \perp (\sigma_{s,\pi''} \wedge \delta_{\pi,\pi''})_A$
4. $\vdash \bigsqcup_{\pi' \in \Pi_s} (\sigma_{s,\pi'} \wedge \delta_{\pi,\pi'}) \rightarrow (K_A \delta_{\pi,\pi'} \rightarrow K_B \sigma_{k+l,\pi'})$ (3, P. 2.3)
5. $\vdash \bigsqcup_{\pi' \in \Pi_s} (\sigma_{s,\pi'} \wedge \delta_{\pi,\pi'}) \rightarrow (P^{>0} K_A \delta_{\pi,\pi'} \rightarrow P^{>0} K_B \sigma_{k+l,\pi'})$ (4, P 2.2)
6. $\vdash [U] P^{>0} K_A \delta_{\pi',\pi'}$ (by assumption)
7. $\vdash \psi \wedge \delta_0 \rightarrow [U] P^{>0} K_B \sigma_{k+l,\pi'}$ (5, 6)
8. $\vdash \psi \wedge \delta_0 \rightarrow [U] P^{>0} K_B \neg \psi$ (7)

Hence, here again, after the tallyman's attack and upon performing the ballot test, the voters will know with a positive probability that the state is changed. That is a positive probability of the ballot test failure. Thus, again, from the assumption of having two different possible non-zero final states $|a_{\pi,\pi}\rangle \neq |a_{\pi',\pi'}\rangle$, we get a positive probability for detection of the tallyman's attacks. Hence the only way that tallyman's interference will be safely undetectable is when the apparatus has only a single possible non-zero final state $|a\rangle$ in which case the state of the apparatus will be uninformative and the tallyman's measurement does not provide her with any information regarding the ballot state.

References

[1] Baltag, A. and Smets, S. "The Logic of Quantum Programs", in the proceedings of the 2nd International Workshop on Quantum Programming Languages (QPL), *TUCS General Publication*, vol. 33, (2004)

[2] Baltag, A. and Smets, S. "LQP: The Dynamic Logic of Quantum Information", *Mathematical Structures in Computer Science*, Special Issue on Quantum Programming Languages, vol. 16(3): p.491-525, (2006)

[3] Baltag, A. and Smets, S. "Complete Axiomatizations for Quantum Actions", *Int. J. of Theoretical Physics*, vol. 44(12): p.2267-2282, (2005)

[4] Baltag, A. and Smets, S. "A Dynamic - Logical Perspective on Quantum Behavior", *Studia Logica*, I. Douven and L. Horsten (eds.) Special issue on Applied Logic in the Philosophy of Science, vol. 89: p.185-209, (2008)

[5] Baltag,A., and Smets., S. "Quantum Logic as a Dynamic Logic", *Synthese*, T. Kuipers, J. van Benthem and H. Visser (eds.) Special issue, (2011)

[6] Baltag,A., and Smets., S. "The Dynamic Turn in Quantum Logic", *Synthese*, vol. 186(3), (2012)

[7] Baltag, A., Bergfeld, J., Kishida, K., Smets, S., Sack, J. and Zhong, S. "PLQP & Company: Decidable Logics for Quantum Algorithms", *Int. J. of Theoretical Physics*, vol. 53(10): p. 3628-3647, (2014)

[8] Baltag, A. and Smets, S. "Correlated Knowledge, An Epistemic-Logic View on Quantum Entanglement", *Int. J. of Theoretical Physics*, vol. 49, (2010)

[9] Baltag, A. and Smets, S. "Modeling correlated information change: from conditional beliefs to quantum conditionals", *Soft Computing*, vol. 21: p.1523-1535 (2017)

[10] Beltrametti, E., Dalla Chiara, ML., Giuntini R, Leporini, R. and Sergioli, G. "Epistemic quantum computational structures in a Hilbert-space environment", *Fundam Inf*, vol. 115: p.1-14, (2012)

[11] Beltrametti, E., Dalla Chiara, ML., Giuntini, R. and Sergioli, G. "Quantum teleportation and quantum epistemic semantics", *Math Slovacca*, vol. 62(6): p.1-24, (2012)

[12] Beltrametti, E., Dalla Chiara, ML., Giuntini, R., Leporini, R. and Sergioli, G. "A quantum computational semantics for epistemic logical operators. Part I: epistemic structures", *Int. J. of Theoretical Physics*, vol. 53(10): p.3279-3292, (2014)

[13] Bergfeld, J.M. and Sack , J. "Deriving the Correctness of Quantum Protocols in the Probabilistic Logic for Quantum Programs", *Soft Computing*, vol. 21(6): p. 1421-1441, (2017)

[14] Birkhoff, G. and von Neumann, J. "The Logic of Quantum Mechanics", *Annals of Mathematics*, vol. 37: p.823-843, 1936, reprinted in C.A. Hooker (ed.), *The Logico-algebraic Approach to Quantum Mechanics*, vol. 1: p.1-26, (1975)

[15] Dolev, Sh. and Pitowsky, I. and Tamir, B. "A quantum secret ballot", *CoRR*, abs/quant-ph/0602087, (2006)

[16] Horoshko, D. and Kilin, S. "Quantum Anonymous Voting with Anonymity Check", *Physics Letters A*, vol. 375: p.1172-1175, (2011)

[17] Inamon, H., Lutkenhaus, N., Mayers, D. "Unconditional Security of Practical Quantum Key Disribution", *Eur. Phys. J. D*, vol. 41(3): p. 599-627, (2007)

[18] Sergioli, G. and Leporini, R. "Quantum approach to epistemic semantics", *Soft Computing*, vol. 21, (2017)