A logic for probability in quantum systems

Ron van der Meyden and Manas Patra

School of Computer Science and Engineering
University of New South Wales, Sydney 2052, Australia
{meyden,manasp}@cse.unsw.edu.au

Abstract. Quantum computation deals with projective measurements and unitary transformations in finite dimensional Hilbert spaces. The paper presents a propositional logic designed to describe quantum computation at an operational level by supporting reasoning about the probabilities associated to such measurements: measurement probabilities, and transition probabilities (a quantum analogue of conditional probabilities). We present two axiomatizations, one for the logic as a whole and one for the fragment dealing just with measurement probabilities. These axiomatizations are proved to be sound and complete. The logic is also shown to be decidable, and we provide results characterizing its complexity in a number of cases.
Keywords:Probability logic, quantum computing.

1 Introduction

Quantum computing promises to open fresh vistas for computer science - almost 100 years after quantum mechanics revolutionized physics. We expect that logical methods will play a key role in the development of quantum computer systems, much like the role they have played in classical computing. (Pratt [Pra92] has also argued that logical support for reasoning about quantum effects may become essential in the next ten years to designers of classical hardware.) In this paper, we study what is potentially one of the building blocks of modal logics for quantum computing, by developing a logic for expressing properties of quantum states, in the same way that propositional logic, which expresses properties of classical states, provides the basis for modal logics of computation.

A new propositional basis is required for a logic of quantum computation because quantum mechanical description does not fit in the classical paradigm being inherently probabilistic rather than deterministic. There already exists an extensive body of literature on logics for reasoning about (classical) probability [AH94,Bac90,Car50,FHM90,Nil86]. Of these works, relatively few concern explicit statements about probability values; the most expressive and most fully analyzed framework that does admit such statements is that of Fagin et al [FHM90], which permits statements such as $\Sigma_{i=1\ldots k} a_i P(\phi_i) \leq a_{k+1}$, where the ϕ_i are propositional formulas and the a_i are integer constants.

However, these existing results cannot be directly applied to reasoning about probabilities in the context of quantum computation. One of the obstacles is

that the space of propositions in quantum mechanics has a significantly more complicated structure than the space of classical propositions. Unlike its classical physics counterpart measurements of observables often disturb a quantum system and there are incompatible obsevables that can not be measured simultaneously. In such cases one can only make probabilisitic predictions. These probabilities are calculated from non-linear equation over the complex number field. The subject of "quantum logic" [BvN36] studies the algebraic structure of the subspaces of the quantum state space that are associated with measurements[1]. This algebra turns out to have a non-boolean structure in which the the distributive law fails. "Quantum probability" theory [Gud89] goes on to define a revised notion of probability space based on these non-boolean algebraic spaces.

Our approach in this paper will be somewhat more pragmatic: we will take the Hilbert space formalization for granted, and focus on the operationally observable probabilities of quantum measurement outcomes. We take *finite dimensional* Hilbert spaces as our semantic basis; the restriction to finite dimensions is precisely that used in quantum computation. We consider two probability operators: a monadic operator P and a dyadic operator T. The operator P resembles a standard probability operator. Unlike quantum logic, which permits boolean combinations of incompatible propositions, we restrict the application of this probability operator to boolean combinations of a set of compatible propositions. A consequence of this is that the logic of this probability operator is similar to the logic of the classical probability operator. The second type of probability operator T that we consider resembles a classical conditional probability operator: in the quantum case, this notion corresponds to the probablity of a transition between subspaces taking place when a measurement is performed.

The main results of the paper are completeness theorems for two axiomatizations. The first deals with the fragment of the logic containing only the operator P, and permitting the expression of linear inequalities over probability values. The complete axiomatization in this case is wholly propositional (i.e. does not require quantification), and consists of a set of axioms concerning the interaction of the probability operators and boolean logic, together with a set of axioms for reasoning about linear inequalities. The second axiomatization is for the full language, with both operators P and T. When axiomatizing reasoning about classical conditional probabilities, one needs an axiomatization of real closed fields [Tar51]. For our logic, we need an extended theory of algebraically closed field with real closed field embedded in it.

In addition to the completeness results, we show that the satisfiability problem is decidable for both languages we consider, and we characterize its complexity. The complexity classes we identify for the satisfiability problem turn out to be the same classes as in the complexity results of [FHM90] for the classical case, viz., NP complete for the language with just the operator P and linear

[1] The term "quantum logic" is a somewhat of a misnomer, since it is concerned not with logic in the sense of inferential relations on syntactic expressions, but the with the analogue of boolean algebra in the quantum world.

constraints, and in exponential space for the language with both operators P and T and with polynomial equations and quantification over numbers.

The structure of the paper is as follows. Section 2 provides an overview of the basic definitions of quantum mechanics. We introduce the syntax of the language in section 3.1, and provide its semantics in Section 3.2. Section 4 provides a few illustrations of what can be expressed in the logic. The axiomatizations and completeness results are presented in Section 5.1 (for the logic based on P), and Section 5.2 (for the logic based on both P and T.) Section 6 concludes by discussing some questions raised by these results and sketching future work. Full proofs of the results are provided in the appendices for the interested reader.

2 Quantum Theory

The most complete description of a physical system is given by its state. According to quantum theory the state of system is a unit vector in a Hilbert space. Thus, let S be system. Associated with S is a Hilbert space, that is complex vector space with an inner product. We shall restrict ourselves to finite-dimensional spaces, which are adequate for quantum computing and our logic. We assume that all states are pure states, as described below. However, we could easily extend the syntax and semantics to "mixed" states which are positive, normalised combination of pure states.

Postulate 1 *Associated to S is a finite dimensional complex Hilbert space* $\{H,\ \langle\rangle\}$ *called the state space. The dimension n is determined by the system.*

We identify H with C^n with standard inner product; if $|\alpha\rangle = (x_1 \dots x_n),\ |\beta\rangle = (y_1 \dots y_n)$ then $\langle\alpha|\beta\rangle = \sum \overline{x_i} y_i$ where $\langle\alpha|$ is the conjugate vector $(\overline{x_1}, \cdots, \overline{x_n})$. The inner product satisfies $\langle\alpha|\beta_1 + \beta_2\rangle = \langle\alpha|\beta_1\rangle + \langle\alpha|\beta_2\rangle$ and $\langle\alpha|\beta\rangle = \overline{\langle\beta|\alpha\rangle}$ and $\langle\alpha|\alpha\rangle \geq 0$. The quantity $\||\alpha\rangle\| = \sqrt{\langle\alpha|\alpha\rangle}$ is called the length of $|\alpha\rangle$. If it is 1 then α is called a unit vector. Note that the length or more generally $|\langle\alpha|\beta\rangle|$ is invariant w.r.t. multiplication of $|\alpha\rangle$ and $|\beta\rangle$ by arbitrary complex constants of modulus 1. With this notation we extend Postulate 1.

Postulate 2 *The state of the system is given by a unit vector, determined up to a scalar multiple of modulus 1. Moreover, each such vector is realisable as a state.*

Thus $|\alpha\rangle$ and $|\beta\rangle$ represent the same state iff $|\alpha\rangle = e^{ic}|\beta\rangle \quad c$ real.

A basis $\mathbf{b} = \{\alpha_1,\ \cdots,\ \alpha_n\}$ of H is a linearly independent set of vectors such that every vector in H is a (unique) linear combination of the $|\alpha_i\rangle$'s. It is orthonormal iff $\langle\alpha_i|\alpha_j\rangle = \delta_{ij}$ where $\delta_{ij} = 1$ if $i = j$ and 0 otherwise. From any set of n linearly independent vectors we can construct an orthonormal basis. It is the set of orthonormal vectors which correspond to the classical notion of states. Their occurence in any test can be considered as mutually exclusive events. Henceforth basis will mean an orthonormal one.

Postulate 3 *Any orthornormal basis represents a realisable maximal test.*

Let n be the maximum number of different outcomes possible in a given system for any test. For example we may test for value of the z-component of spin of an electron or polarisation of a photon. We imagine we have large number of similarly prepared systems called an ensemble and we test for the values of different measurable quantities like spin etc.

For a spin-1/2 system we always get a maximum of 2 outcomes ('up' and 'down') for any test. So $n = 2$. This number is a property of the system and according to the postulate equals the dimension of the state space. In general, we postulate that for an ensemble in an arbitrary state, it is always possible to devise a test that yields the n outcomes corresponding to an orthonormal basis with definite probability.

Postulate 4 *If the system is prepared in state $|\alpha\rangle$ and a maximal test corresponding to a basis $\mathbf{b} = \{|\beta_i\rangle|\ i = 1, \cdots, n\}$ is performed, the probability that the outcome will correspond to $|\beta_i\rangle$ is given by $p_i = |\langle\alpha|\beta_i\rangle|^2$.*

Since one of the outcomes must occur, $\sum p_i = 1$. In the relative frequency interpretation of probability this means that if we have an ensemble of N systems and perform a maximal test corresponding to $\{|\beta_j\rangle\}$ then if the frequency of outcome corresponding to $|\beta_i\rangle$ is n_i, we have $p_i = \lim_{N\to\infty} \frac{n_i}{N}$.

If the system is known to be in one of the states in a basis $\{|\beta_i\rangle\}$, say $|\beta_1\rangle$, then $p_1 = 1$ and $p_i = 0$ for $i \neq 1$. That is, we can predict the outcome with certainty for this maximal test. This is the case that corresponds to the classical theory. However, if we choose a different maximal test corresponding to a different basis then the outcomes become random.

We note that if H is a Hilbert space with inner product $\langle\ ,\ \rangle$, then H is isomorphic to the dual space of linear functionals (i.e. complex valued functions) on H. Thus for each $|\alpha\rangle$ let $\langle\alpha|$ denote its image under this isomorphism, called the dual. Then $(\langle\alpha|)(|\beta\rangle) = \langle\alpha|\beta\rangle$ by definition. Further$(|\alpha\rangle\langle\beta|)(|\gamma\rangle) \stackrel{\text{def}}{=} (\langle\beta|\gamma\rangle)|\alpha\rangle$ is a linear operator on H. Let $\mathcal{L}(\mathcal{H})$ denote the space of linear operators on H. An operator $A \in \mathcal{L}(\mathcal{H})$ is hermitian if $\langle\alpha|A\beta\rangle = \langle A\alpha|\beta\rangle$ for all $|\alpha\rangle$ and $|\beta\rangle$. An operator U is called unitary if $\langle U\alpha|U\beta\rangle = \langle\alpha|\beta\rangle$ for all $|\alpha\rangle$ and $|\beta\rangle$. In matrix notation let $B^\dagger$ denote the transposed conjugate of a square matrix B. Then B is hermitian if $B = B^\dagger$ and U is unitary if $U^{-1} = U^\dagger$. In particular a unitary operator is invertible. Hermitian and unitary matrices play a crucial role in quantum theory.

Let the system be in a state $|\alpha_i\rangle$ where $\{|\alpha_i\rangle\,|\,i = 1, \cdots, n\}$ is an orthonormal basis. Let $\{|\beta_i\rangle\,|\,i = 1 \cdots, n\}$ be another orthonormal basis. Then if we do a maximal test with respect to $\{|\beta_i\rangle\}$ then the probability of obtaining result $|\beta_j\rangle$ is $p_{ij} = |\langle\alpha_i|\beta_j\rangle|^2$. This can also be written as $\mathtt{Tr}((|\alpha_i\rangle\langle\alpha_i|)(|\beta_i\rangle\langle\beta_i|))$ where the *trace* $\mathtt{Tr}$ is the sum of the diagonal elements of a square matrix, which is independent of the representation.

The p_{ij} are called the transition probabilities. Let $U = (u_{ij} = \langle\alpha_i|\beta_j\rangle)$ be a matrix. Then U is unitary. It is the matrix which expresses the change of basis and $p_{ij} = |u_{ij}|^2$. We thus see that the transition probability matrix is doubly

stochastic, i.e., $\sum_i p_{ij} = \sum_j p_{ij} = 1$. But an arbitrary doubly stochastic matrix (for example appearing in classical Markhov processes) may not correspond to transition probability matrix in quantum theory because it may not satisfy $p_{ij} = |u_{ij}|^2$ for some unitary $U = (u_{ij})$. Such matrices (p_{ij}) are called orthostochastic. Thus the p_{ij} must satisfy some relations. We thus see an important difference with classical probability theory. We can not make arbitrary probability assignments (satisfying of course the usual probability constraints) but the probabilities must satisfy certain nonlinear inequalities. This also true of the probabilities p_i introduced earlier.

3 Syntax and Semantics

We now present the syntax and semantics of our logic of quantum probabilities.

3.1 Syntax

For each dimension $n \geq 1$ we define two languages interpreted with respect to n-dimensional Hilbert space: $\mathcal{L}_n(P)$ and $\mathcal{L}_n(P,T)$. (We write $\mathcal{L}_n(X)$ when making assertions that apply to both languages.) We begin by describing the language $\mathcal{L}_n(P)$, which is based on the probability operator P.

Maximal measurements correspond to orthonormal bases of the Hilbert space, which are related by unitary transformations, as discussed above. Bases are represented in both languages by means of *basis variables* $\mathtt{b}, \mathtt{c}, \mathtt{d}, \ldots$. A *basis component* of $\mathcal{L}_n(X)$ is an expression of the form $\mathtt{b}_i$ where $1 \leq i \leq n$ and $\mathtt{b}$ is a basis variable.[2] Semantically, basis components correspond to the elements of an orthonormal basis of the n-dimensional Hilbert space.

The probability operators in our language will apply to formulas expressing properties of the outcome of a maximal measurement. We capture these properties by $\mathtt{b}$-*formulas*, where $\mathtt{b}$ is a basis variable representing the measurement. A $\mathtt{b}$-formula is a Boolean combination of $\mathtt{b}$-components, i.e., an expression of the form $\mathtt{b}_i$, or $\alpha \wedge \alpha'$, or $\neg\alpha$, where α and α' are $\mathtt{b}$-formulas. We define $\alpha \vee \alpha' as \neg(\neg\alpha \wedge \neg\alpha')$. Note that all the basis components in a $\mathtt{b}$-formula must be constructed from the same basis variable $\mathtt{b}$; if t and t' are distinct basis terms then $\mathtt{b}_1 \wedge \mathtt{b}'_1$ is not a $\mathtt{b}$-formula. Intuitively, this restriction ensures that $\mathtt{b}$-formulas describe the outcomes of measurements compatible with the basis $\mathtt{b}$, and prevents construction of formulas combining results of incompatible measurements.

A *probability term* is an expression of the form $P(\alpha)$ where α is a $\mathtt{b}$-formula for some basis variable $\mathtt{b}$. A *linear probability atom* is an expression of the form $a_1 \cdot P(\alpha_1) + \ldots + a_k \cdot P(\alpha_k) \leq c$, where each a_i is an integer, c is an integer, and each α_i is a $\mathtt{b}^i$-formula for some basis constant $\mathtt{b}^i$. The formulas of the language $\mathcal{L}_n(P)$ are all the boolean combinations of linear probability atoms i.e., each

[2] Note that we do not use subscripting to distinguish basis variables: $\mathtt{b}_1$ and $\mathtt{b}_2$ always denote components of the same basis $\mathtt{b}$, rather than two distinct basis variables. We use superscripting to denote distinct basis variables when use of distinct letters for the basis variables do not suffice.

linear probability atom is a formula of $\mathcal{L}_n(P)$, and if ϕ_1 and ϕ_2 are formulas of $\mathcal{L}_n(P)$ then so are $\neg\phi_1$, and $\phi_1 \wedge \phi_2$. The constructions $\phi_1 \vee \phi_2$, $\phi_1 \Rightarrow \phi_2$, $\phi_1 \Leftrightarrow \phi_2$ may be defined in this language as usual. Expressions such as $X < Y$, $X = Y$, where X, Y are linear combinations of probability terms are also definable in this language.

For the language $\mathcal{L}_n(P,T)$, we add *transition probability terms*, which are expressions of the form $T(\alpha, \beta)$, where α is a $\mathtt{b}$-formula for some basis variable $\mathtt{b}$ and β is a $\mathtt{c}$-formula for some basis variable $\mathtt{c}$. Intuitively, these are a kind of conditional probability, expressing the probability that a measurement in basis $\mathtt{c}$ will have outcome satisfying β, given that the current state is α. A *transition probability atom* is an expression of the form $p \leq 0$, where p is a polynomial expression with integer coefficients over probability terms and transition probability terms. Note that linear probability atoms are a special case of transition probability atoms. As above, comparison operators other than '$\leq$' are definable. For Fagin et al, [FHM90], the shift from linear inequalities over probability atoms to polynomial inequalities was motivated by the fact that conditional probabilities are defined as a quotient of probabilities, which leads to a polynomial when the quotients are multiplied out. For us, there is the additional motivation that quantum probabilities are inherently quadratic. Define a *simple transition probability formula* to be a boolean combination of transition probability atoms. For the language to be expressive enough we need quantification over both real and complex numbers and add a new type of term, denoting a complex number, to represent the entries of unitary matrices.

The proof theory for $\mathcal{L}(P,T)$ presented below will make use of results concerning the first order language $\mathcal{L}_{\{+,\cdot,=\}}$ with equality the only predicate symbol and function symbols representing addition and multiplication. The language $\mathcal{L}_{\{+,\cdot,=\}}$ leads to a recursively axiomatizable (in fact, decidable) theory both when interpreted with respect to the real field $\mathbf{R}$ and the complex field $\mathbf{C}$ [Tar51]. For our logic, it is convenient to first define the sorted first order language $\mathcal{L}_{\mathbf{RC}}$ with two sorts $\mathbf{R}$ and $\mathbf{C}$, with $\mathbf{R}$ a subsort of $\mathbf{C}$. The language $\mathcal{L}_{\mathbf{RC}}$ has equality as its only predicate symbol, a constant symbol c (of sort $\mathbf{R}$) for each integer, and the (infix) binary functions $+$ and $\cdot$ as its only function symbols. Both function symbols are overloaded: if t_1, t_2 are terms of sort $\mathbf{R}$ (respectively, $\mathbf{C}$), then so are $t_1 + t_2$ and $t_1 \cdot t_2$. We write $\forall x : \mathbf{R}.(\phi)$ and $\forall x : \mathbf{C}.(\phi)$ for universal quantification over the reals and complex numbers respectively. In this language, we may define operations such as complex conjugation $\overline{x + iy} = x - iy$, and the modulus of a complex number $|x + iy| = \sqrt{x^2 + y^2}$ (where x and y are real), so we use such operations freely. The inequality $x \leq y$ on real terms x, y is also definable (by $\exists z : R.(y = x + z^2)$).

The language $\mathcal{L}_n(P,T)$ is defined to be the extension of $\mathcal{L}_{\mathbf{RC}}$ in which we add probability terms and transition probability terms as terms of sort $\mathbf{R}$, as well as the terms $m_{ij}(\mathtt{b}, \mathtt{c})$, of sort $\mathbf{C}$, for $1 \leq i, j \leq n$ and basis variables $\mathtt{b}, \mathtt{c}$. Intuitively, $m_{ij}(\mathtt{b}, \mathtt{c})$ denotes the ij-th entry of the unitary matrix that transforms the basis denoted by $\mathtt{b}$ into the basis denoted by $\mathtt{c}$.

3.2 Semantics

We now present the semantics for the language $\mathcal{L}_n(P,T)$ (and consequently for the sublanguage $\mathcal{L}_n(P)$). Although there are no explicit modal operators, the semantics has some resemblences to Kripke semantics. In particular, we interpret formulas at a state within a collection of states, with respect to an interpretation of the atomic symbols.

A *structure* for $\mathcal{L}_n(P,T)$ is an n-dimensional Hilbert space H. A *state* within this structure is a unit vector ψ in H. An *interpretation* of $\mathcal{L}_n(P,T)$ in a structure H is function π, such that

1. for each basis variable $\mathtt{b}$, $\pi(\mathtt{b})$ is an orthonormal basis $\psi_1,\ldots,\psi_n$ of H; (we write $\pi(\mathtt{b})_i$ for ψ_i)
2. for each real variable x, $\pi(x)$ is a real number;
3. for each complex variable X, $\pi(X)$ is a complex number.

If $M=(m_{ij})$ is an $n\times n$ unitary matrix and $B=\psi_1,\ldots,\psi_n$ is a sequence of vectors of H, we write MB for the sequence of vectors $\psi'_1,\ldots,\psi'_n$, where $\psi'_i=\Sigma_{i=1}^n m_{ik}\psi_i$. If B is an orthonormal basis of H then so is MB.

We extend the interpretation π to terms $\mathbf{t}$ of various sorts as follows. Given the term $\mathbf{t}$, a state ψ and an interpretation π, we define the interpretation $[\![\mathbf{t}]\!]_{\pi,\psi}$ of X with respect to π and ψ as follows. Basis variables are interpreted as bases:

1. $[\![\mathtt{b}]\!]_{\pi,\psi}=\pi(\mathtt{b})$, when $\mathtt{b}$ is a basis variable.

When $\mathtt{b}$ is a basis variable, we interpret $\mathtt{b}$-formulas as projection operators on H (these may also be understood as representing the subspaces of H onto which they project):

2. $[\![\mathtt{b}_i]\!]_{\pi,|\psi\rangle}=|\psi'\rangle\langle\psi'|$, where $\psi'=\pi(\mathtt{b})_i$;
3. $[\![\alpha_1\wedge\alpha_2]\!]_{\pi,\psi}=[\![\alpha_1]\!]_{\pi,\psi}\cdot[\![\alpha_2]\!]_{\pi,\psi}$ (this is the projection operator projecting onto intersection of the subspaces of H that are the images of the projectors $[\![\alpha_1]\!]_{\pi,\psi}$ and $[\![\alpha_1]\!]_{\pi,\psi}$) which could be written as the product of these projectors.;
4. $[\![\neg\alpha]\!]_{\pi,\psi}=[\![\alpha]\!]^{\perp}_{\pi,\psi}$ is the projection operator projecting onto the orthogonal complement of the image of H under $[\![\alpha]\!]_{\pi,\psi}$.

(We note that the reason we have taken $\pi(\mathtt{b})$ to be a basis rather than sequence of projectors is in order to give semantics to the terms $m_{ij}(\mathtt{b},\mathtt{c})$.) Terms of sort $\mathbf{R}$, including probability terms and transition probability terms, are interpreted as real numbers, and terms of sort $\mathbf{C}$, including the unitary matrix entry terms $m_{ij}(\mathtt{b},\mathtt{c})$, are interpreted as complex numbers:

5. $[\![x]\!]_{\pi,\psi}=\pi(x)$, when x is real or complex variable;
6. $[\![k]\!]_{\pi,\psi}=k$, when k is an integer;
7. $[\![P(\alpha)]\!]_{\pi,\psi}=\|[\![\alpha]\!]_{\pi,\psi}(\psi)\|^2$;
8. $[\![T(\alpha,\beta)]\!]_{\pi,\psi}=\mathtt{Tr}([\![\beta]\!]_{\pi,\psi}[\![\alpha]\!]_{\pi,\psi})$
9. $[\![m_{ij}(\mathtt{b},\mathtt{c})]\!]_{\pi,\psi}=c_{ij}$, where $M=(c_{ij})$ is the $n\times n$ (unitary) complex array such that $M\pi(\mathtt{b})=\pi(\mathtt{c})$;

10. $[\![X \cdot Y]\!]_{\pi,\psi} = [\![X]\!]_{\pi,\psi} \cdot [\![X]\!]_{\pi,\psi}$
11. $[\![X + Y]\!]_{\pi,\psi} = [\![X]\!]_{\pi,\psi} + [\![Y]\!]_{\pi,\psi}$

To give semantics to formulas of $\mathcal{L}_n(P,T)$, we define a relation of satisfaction of a formula ϕ at a state ψ in a structure H, with respect to an interpretation π, denoted by $H, \pi, \psi \models \phi$. The definition is by the following induction:

1. $H, \pi, \psi \models X = Y$ if $[\![X]\!]_{\pi,\psi} = [\![Y]\!]_{\pi,\psi}$ (in case of $\mathcal{L}_n(P)$, this clause is replaced by $H, \pi, \psi \models X \leq c$ if $[\![X]\!]_{\pi,\psi} \leq c$);
2. $H, \pi, \psi \models \neg\phi$ if not $H, \pi, \psi \models \phi$;
3. $H, \pi, \psi \models \phi_1 \wedge \phi_2$ if $H, \pi, \psi \models \phi_1$ and $H, \pi, \psi \models \phi_2$;
4. $H, \pi, \psi \models \exists x : \mathbf{R}.(\phi)$ if there is a real number r such that $H, \pi[r/x], \psi \models \phi$;
5. $H, \pi, \psi \models \exists x : \mathbf{C}.(\phi)$ if there is a complex number c such that $H, \pi[c/x], \psi \models \phi$;

A formula ϕ of $\mathcal{L}_n(P,T)$ is *satisfiable* (in the n-dimensional Hilbert space H) if there exists an interpretation π and a state ψ such that $H, \pi, \psi \models \phi$. A formula ϕ is *valid* (in H) if $H, \pi, \psi \models \phi$ for all interpretations π and a states ψ.

4 Examples

We give some examples of formulas in our language which express important concepts of quantum mechanics.

Superposition: A vector $|\alpha\rangle$ is a *superposition* of two vectors $|\beta_1\rangle$ and $|\beta_2\rangle$ if it is a linear combination of the two, i.e., $|\alpha\rangle = c_1|\beta_1\rangle + c_2|\beta_2\rangle$ for some complex numbers c_1, c_2. Consider the formula $T(\mathtt{b}_1, \mathtt{b}'_1 \vee \mathtt{b}'_2) = 1$. If $\pi(\mathtt{b}_1) = |\alpha\rangle$, $\pi(\mathtt{b}'_1) = |\beta_1\rangle$ and $\pi(\mathtt{b}'_1) = |\beta_2\rangle$ then $H, \pi, \psi \models T(\mathtt{b}_1, \mathtt{b}'_1 \vee \mathtt{b}'_2) = 1$ iff $\mathbf{Tr}(|\alpha\rangle\langle\alpha|(|\beta_1\rangle\langle\beta_1| + |\beta_2\rangle\langle\beta_2|)) = 1$. This is equivalent to $|\langle\beta_1|\alpha\rangle|^2 + |\langle\beta_2|\alpha\rangle|^2 = 1$, which is true iff the state $|\alpha\rangle$ is a superposition of the states $|\beta_1\rangle$ and $|\beta_2\rangle$. That is, the formula expresses that "$\mathtt{b}_1$ is a superposition of $\mathtt{b}'_1$ and $\mathtt{b}'_2$".

Phase Relations: Let $\mathtt{b}^0, \ldots, \mathtt{b}^k$ be $k+1$ bases. Then the following formula states a relation between $\mathtt{b}^0$ and the $\mathtt{b}^j$, for $j = 1 \ldots k$.

$$\begin{aligned}\mathbf{MP}_k \quad & \forall x_1 \ldots x_n : \mathbf{R}.(\textstyle\bigwedge_{i=1}^n P(\mathtt{b}_i^0) = x_i^2 \Rightarrow \\ & \exists z_1 \ldots z_n : \mathbf{C}(\textstyle\bigwedge_{i=1}^n |z_i| = 1 \wedge \\ & \textstyle\bigwedge_{j=1}^k \bigwedge_{i=1}^n P(\mathtt{b}_i^j) = |\Sigma_{r=1}^n m_{ir}(\mathtt{b}^0, \mathtt{b}^j) x_r z_r|^2))\end{aligned}$$

Proposition 1. *The formula* $\mathbf{MP}_k$ *is valid for all* $k \geq 1$.

Proof. Let π be any interpretation and $|\psi\rangle$ any vector in H_n. If $[\![P(\mathtt{b}_i^0)]\!]_{\pi,|\psi\rangle} = \pi(x_i)^2$, then we may write $|\psi\rangle = \sum_{i=1}^n c_i \pi(x_i) \pi(\mathtt{b}^0)_i$, where the c_i are complex numbers with $|c_i| = 1$. Define $\pi(z_i) = c_i$. We can then calculate the probabilities with respect to other bases as follows:

$$\begin{aligned}[\![P(\mathtt{b}_i^j)]\!]_{\pi,|\psi\rangle} &= |\langle \pi(\mathtt{b}^j)_i \mid \psi\rangle|^2 \\ &= |\langle \textstyle\sum_{r=1}^n [\![m_{ir}(\mathtt{b}^0, \mathtt{b}^j)]\!]_{\pi,|\psi\rangle} \cdot \pi(\mathtt{b}^0)_r \mid \psi\rangle|^2 \\ &= |\textstyle\sum_{r=1}^n [\![m_{ir}(\mathtt{b}^0, \mathtt{b}^j)]\!]_{\pi,|\psi\rangle} \cdot \pi(x_r) \cdot \pi(\mathtt{b}^0)_r|^2\end{aligned}$$

from which it can be seen that $\mathbf{MP}_k$ holds.

Quantum State Tomography: Suppose we are given a collection of identically prepared systems (an ensemble), which corresponds to an unknown quantum state. Quantum state tomography (QST) addresses the problem of determining this unknown state. By measuring the ensemble in a single basis, we may determine a probability distribution over the outcomes associated to the basis elements. To determine the phases we divide the original collection of systems into subcollections and subject each to maximal measurements corresponding to an appropriately chosen bases. We get sets of probability distributions related by unitary transforms of bases. For an appropriate choice of measurements,bases this set of relations suffices to compute the state. The following formula expresses this fact. Let $\mathbf{u}$ be the sequence of variables u_{ij}^k where $1 \leq i, j, k \leq n$.

$$\begin{array}{l}\exists \mathbf{u} : \mathbf{C}[\ \bigwedge_{1\leq i,j,k\leq n} m_{ij}(\mathtt{b}, \mathtt{c}^k) = u_{ij}^k \Rightarrow \\ \forall z_1 \ldots z_n : \mathbf{C}(\bigwedge_{1\leq i,k\leq n} P(\mathtt{c}_i{}^k) = |\sum_j u_{ij}^k z_j \sqrt{P(\mathtt{b}_j)}|^2 \Rightarrow \\ \bigwedge_i P(\mathtt{b}_i{}') = |\sum_j m_{ij}(\mathtt{b}, \mathtt{b}') z_j \sqrt{P(\mathtt{b}_j)}|^2 \ \ )\ ]\,.\end{array}$$

This formula is valid. It expresses the fact that there is a "pattern of interrelation" between a set of bases $\mathtt{b}$ and $\mathtt{c}^1, \mathtt{c}^2, \ldots \mathtt{c}^n$, captured by the values $\mathbf{u}$, such that for any vector ψ, the probabilities of measurements associated to a set of bases related in this pattern provide sufficient information to calculate the probabilities of measurements with respect to any other basis. Note that by the discussion of the formula MP_k above, it is always possible to find values for $z_1, \ldots z_k$ such that

$$\bigwedge_{1\leq i,k\leq n} P(\mathtt{c}_i{}^k) = |\sum_j u_{ij}^k z_j \sqrt{P(\mathtt{b}_j)}|^2 \tag{1}$$

is satisfied. Thus the universally quantified formula in the conclusion is never true vacuously. The formula therefore expresses that given an appropriately related set of bases $\mathtt{b}$ and $\mathtt{c}^1, \mathtt{c}^2, \ldots \mathtt{c}^n$, it is possible, given any basis $\mathtt{b}'$, to calculate the values $P(\mathtt{b}_i')$ from the values u_{ij}^k, $P(\mathtt{b}_i)$, $P(\mathtt{c}_i^k)$ and $m_{ij}(\mathtt{b}, \mathtt{b}')$. We do this by first solving the equation (1) for the phase values $z_1, \ldots, z_n$, and then computing $P(\mathtt{b}_i')$ as $|\sum_j m_{ij}(\mathtt{b}, \mathtt{b}') z_j \sqrt{P(\mathtt{b}_j)}|^2$.

Uncertainty Relations: We say that bases $\mathtt{b}$ and $\mathtt{b}'$ are complementary if $nT(\mathtt{b}_i, \mathtt{b}_j{}') = 1$ holds for all $i, j = 1 \ldots n$. Let $n = 2$. Then the formula

$$\begin{array}{c}\bigwedge_i 2T(\mathtt{b}_i, \mathtt{b}_j{}') = 1 \ \wedge\ P(\mathtt{b}_1) = x_1^2 \ \wedge\ P(\mathtt{b}_2) = x_2^2 \ \Rightarrow \\ (x_1 - x_2)^2 \leq 2P(\mathtt{b}_j)' \leq (x_1 + x_2)^2\end{array}$$

expresses an uncertainty relation. For example if $x_1 = 1$ then there is no uncertainity in the result for a maximal test with respect to the $\mathtt{b}$-basis. But then we get the probability for both results in the $\mathtt{b}'$-basis equal to one half. Thus, there is maximum uncertainty.

Quantum Gates: The formula $T(\mathtt{b}_1, \mathtt{c}_2) = 1$of $\mathcal{L}_2(P, T)$ represents the quantum not gate. The standard representation of quantum not gate is by a unitary

matrix that "flips" the qubits taking $|\alpha\rangle = (1\ 0)$ to $|\beta\rangle = (0\ 1)$. Our representation essentially expresses the same thing. If a state vector represented in the $\mathtt{b}$-basis is measured later in the $\mathtt{c}$-basis then it has exactly the same effect: $|\alpha\rangle = 1 \cdot \pi(\mathtt{b}_1) + 0 \cdot \pi(\mathtt{b}_2)$ yields $P(\mathtt{c}_2) = 1$. Thus it is easily seen that the following is a valid formula of $\mathcal{L}_2(P, T)$:

$$T(\mathtt{b}_1, \mathtt{c}_2) = 1 \Rightarrow (P(\mathtt{b}_1) = 1 \Rightarrow P(\mathtt{c}_1) = 0) \wedge (P(\mathtt{b}_2) = 1 \Rightarrow P(\mathtt{c}_2) = 0).$$

5 Axiomatization

We now present axiomatizations and state the completeness results for the languages $\mathcal{L}_n(P)$ and $\mathcal{L}_n(P, T)$.

5.1 Axiomatizing $\mathcal{L}_n(P)$

The axiomatization of $\mathcal{L}_n(P)$ consists of a number of parts, each dealing with one of the syntactic constructs of the language.

The first fragment of our axiomatization deals with the boolean logic of the $\mathtt{b}$-formulas. As this is slightly richer than propositional logic, we identify for each basis variable $\mathtt{b}$ a fragment of the proof theory that deals only with $\mathtt{b}$-formulas. The axioms of this fragment can be taken to be any complete axiomatization of propositional logic over the atomic formulas $\mathtt{b}_1, \ldots, \mathtt{b}_n$, with, e.g., Modus Ponens as the proof rule, plus the following axioms that capture the fact that we are dealing with an n-dimensional Hilbert space:

B1 $\mathtt{b}_1 \vee \ldots \vee \mathtt{b}_n$

B2 $\neg(\mathtt{b}_i \wedge \mathtt{b}_j)$ for $i \neq j$

We say that a $\mathtt{b}$-formula ϕ is a $\mathtt{b}$-tautology, and write $\vdash_{\mathtt{b}} \phi$ if it can be derived from these axioms alone. Note that these definitions isolate reasoning about $\mathtt{b}$-formulas from reasoning about $\mathtt{c}$-formulas when $\mathtt{b}$ and $\mathtt{c}$ are distinct.

Next, we have some axioms capturing the properties of the probability operator. The following axioms correspond very closely to the axioms W1-W4 of Fagin et al [FHM90], but with the difference that we need to be careful to respect the syntactic constraints on probability terms. In the following, we require that there exists a basis term $\mathtt{b}$ such that ϕ, ϕ_1 and ϕ_2 are $\mathtt{b}$-formulas:

P1 $0 \leq P(\phi) \leq 1$

P2 $P(\phi) = 1$ if ϕ is a $\mathtt{b}$-tautology

P3 $P(\phi_1 \wedge \phi_2) + P(\phi_1 \wedge \neg\phi_2) = P(\phi_1)$

P4 $P(\phi_1) = P(\phi_2)$ if $\phi_1 \Leftrightarrow \phi_2$ is a $\mathtt{b}$-tautology

Note that in P2 and P4, we deal with $\mathtt{b}$-tautologies where Fagin et al have tautologies of propositional logic. The countable additivity axiom is not needed since the number of atomic events is finite (=n).

In addition to the above axioms, we also need a set of axioms that capture reasoning about linear inequalities. That is, we need to be able to derive formulas such as $(2P(\phi_1) \leq 3 \wedge 4P(\phi_2) \leq 1) \Rightarrow P(\phi_1) + 2P(\phi_2) \leq 2$, the validity of which follows just from the meaning of these operations on real numbers, rather than

the meaning of the probability terms. We refer the reader to Fagin et al [FHM90] for such an axiomatization $\mathtt{AX}_{\mathtt{INEQ}}$ of such reasoning, and leave it as an exercise to construct an axiomatization $\mathtt{AX}_{\mathtt{INEQ}}{}'$ suited to $\mathcal{L}_n(P)$ (the difference is to replace all variable occurences by probability terms.)

Let $\mathtt{AX}_{\mathtt{n}}(\mathtt{P})$ be the abovementioned axioms and rules of inference. Then we have the following:

Theorem 1. $\mathtt{AX}_{\mathtt{n}}(\mathtt{P})$ *is a sound and complete axiomatization of* $\mathcal{L}_n(P)$.

The axiomatization $\mathtt{AX}_{\mathtt{n}}(\mathtt{P})$ is almost identical to Fagin et al's axiomatization of for linear inequalities over classical probabilities — the main difference is the syntactic restrictions relating to $\mathtt{b}$-formulas. Thus, from the point of view of the language $\mathcal{L}_n(P)$, quantum probabilities behave similarly to classical probabilities. The similarity is also reflected in the complexity of the logic:

Theorem 2. *Satisfiability of a formula of* $\mathcal{L}_n(P)$ *in* n*-dimensional Hilbert space (with* $n \geq 2$*) is NP-complete.*

Precisely the same complexity was obtained by FHM for their logic of classical probabilities.

Interestingly, the proof of Theorem 1 shows that probabilities with respect to different bases act independently. More precisely, the completeness proof can be used to establish the following:

Proposition 2. *Let* $\phi_1, \ldots, \phi_m$ *be formulas and* $\mathtt{b}^1, \ldots, \mathtt{b}^m$ *be distinct basis variables such that for each* $j = 1, \ldots, n$*, the only probability terms occuring in* ϕ_j *are* $\mathtt{b}^j$ *probability terms. Then* $\phi_1 \wedge \ldots \wedge \phi_m$ *is satisfiable iff each* ϕ_j *is satisfiable.*

Thus, unlike quantum logic, $\mathcal{L}_n(P)$ is unable to express constraints on the ways that incompatible propositions are "pasted together". To capture such constraints, we need to turn to our richer logic, dealing with transition probabilities.

5.2 Axiomatizing $\mathcal{L}_n(P, T)$

We now present the axiomatization of $\mathcal{L}_n(P, T)$.

To capture the properties of the probability operator P, the axiomatization contains the axiomatization of $\mathtt{b}$-formulas used above, and the probability axioms P1-P4. We need a similar set of axioms for the transition probabilities. In the following, ϕ, ϕ_1, ϕ_2 are $\mathtt{b}$-formulas for some basis variable $\mathtt{b}$, and ϕ', ϕ'_1, ϕ'_2 are $\mathtt{b}'$-formulas for some basis variable $\mathtt{b}'$. For a fixed $\mathtt{b}$-formula ϕ, the probabilities of a transition to a $\mathtt{b}'$-formula satisfy four properties directly analogous to P1-P4 above:

T1 $T(\phi, \phi') \geq 0$

T2 $T(\phi, \phi') = 1$ when ϕ' is a $\mathtt{b}'$-tautology

T3 $T(\phi, \phi'_1 \wedge \phi'_2) + T(\phi, \phi'_1 \wedge \neg\phi'_2) = T(\phi, \phi'_1)$

T4 $T(\phi, \phi'_1) = T(\phi, \phi'_2)$ if $\phi'_1 \Leftrightarrow \phi'_2$ is a $\mathtt{b}'$-tautology

These properties allow us to decompose a transition probability term into an equivalent expression in transition probability terms in which the second argument contains only atomic basis formulas. A similar decomposition with respect to the first argument can be obtained using the following property:

T5 $T(\phi, \phi') = T(\phi', \phi)$

Additionally, we have the following properties concerning a number of special cases of transitions. The first concerns transitions within a given basis:

T6a $T(\mathtt{b}_i, \mathtt{b}_j) = 0$ when $i \neq j$

T6b $T(\mathtt{b}_i, \mathtt{b}_i) = 1$

Next, note that the formula $P(\mathtt{b}_i) = 1$ can be understood as saying that the state ψ at which the formula is being evaluated is equal to the i-th vector in the basis $\mathtt{b}$. The following property can be understood as stating that transition probabilities for transitions from the current state reduce to simple probabilities:

T7 $P(\mathtt{b}_i) = 1 \Rightarrow T(\mathtt{b}_i, \phi) = P(\phi)$

For $\mathcal{L}_n(P)$ our axiomatization used a set of axioms for reasoning about linear inequalities. In the case of $\mathcal{L}_n(P, T)$, we need to reason about non-linear polynomials. Moreover, to capture the quantum nature of the probabilities, we need to reason about complex numbers. This leads us to include in the axiomatization a set of axioms for reasoning about real and complex numbers. The following proposition follows from the fact that the complex numbers may be represented as pairs of real numbers, that the operations of complex addition and multiplication may be defined as operations on these pairs, and that the language $\mathcal{L}_{\{+,\cdot,=\}}$ has an axiomatizable theory with respect to the standard model $\mathbf{R}$ [Tar51].

Proposition 3. *The set of valid formulas of* $\mathcal{L}_{\mathbf{RC}}$ *has a recursive axiomatization* $\mathtt{AX}_{\mathtt{RC}}$.

The rules of inference of $\mathtt{AX}_{\mathtt{RC}}$ are the usual rules for first order logic with equality. For reasons of space we do not list the axioms of $\mathtt{AX}_{\mathtt{RC}}$ here. We include these axioms and rules of inference in our axiomatization.

The language $\mathcal{L}_n(P, T)$ contains the terms $m_{ij}(\mathtt{b}, \mathtt{c})$, of complex number sort, to represent the unitary operators associated with basis transformations. The following properties are direct from the definition of these terms:

M1 $m_{ij}(\mathtt{b}, \mathtt{c}) = \overline{m_{ji}(\mathtt{c}, \mathtt{b})}$

The fact that transformation from a basis to itself corresponds to the identity matrix, and that consecutive basis transformations correspond to matrix multiplication, are captured by the next two properties:

M2a $m_{ij}(\mathtt{b}, \mathtt{b}) = 1$ if $i = j$

M2b $m_{ij}(\mathtt{b}, \mathtt{b}) = 0$ if $i \neq j$

M3 $m_{ij}(\mathtt{b}, \mathtt{d}) = \Sigma_{k=1}^{n} m_{ik}(\mathtt{b}, \mathtt{c}) m_{kj}(\mathtt{c}, \mathtt{d})$

We note that the following property, expressing unitarity of the transformation, follows from M1-M3:

M4 $\Sigma_{k=1}^{n} m_{ik}(\mathtt{b}, \mathtt{c}) \overline{m_{jk}(\mathtt{b}, \mathtt{c})} = 1$

These matrices are connected to probabilities by the following axiom:

MT $T(\mathtt{b}_i, \mathtt{c}_j) = |m_{ij}(\mathtt{b}, \mathtt{c})|^2$

We note that M1-M3 and MT imply some of the properties of transition probabilities noted above. In particular, T1, T2 and T6 become derivable, as does the case $T(\mathtt{b}_i, \mathtt{b}_j) = T(\mathtt{b}_j, \mathtt{b}_i)$ of T5.

Let the axiomatization $\mathtt{AX_n(P,T)}$ consist of the propositional component with **B1**-**B2** for the b-formulas, the axioms **P1**-**P4**, **T1**-**T7**, the axioms and rules of $\mathtt{AX_{RC}}$ (including the usual rules of inference for first order logic), **M1**-**M3**, **MT** and the axiom $\mathbf{MP}_k$ (see Section 4) for all $k \leq n^2 - n + 1$. Then we have the following:

Theorem 3. $\mathtt{AX_n(P,T)}$ *is a sound and complete axiomatization for the language* $\mathcal{L}_n(P,T)$.

Note that although we have shown that $\mathbf{MP}_k$ is sound for all $k \geq 1$, we have only included its instances for $k \leq n^2 - n + 1$ in the set of axioms. Indeed, as part of the completeness proof we show that it is not necessary to include $\mathbf{MP}_k$ for larger k since it already follows:

Theorem 4. *For every number* $k \geq 1$*, the formula* $\mathbf{MP}_k$ *is a theorem of* $\mathtt{AX_n(P,T)}$.

We have stated this result as a theorem because we feel that it is of significance for physics as well as the logic of quantum probabilities. It shows that to determine whether a set of numbers can have arisen as the probabilities associated to a set of k bases in n-dimensional Hilbert space, it suffices to check the probabilities associated to every subset of size $n^2 - n + 1$.

As for the language $\mathcal{L}_n(P)$, we also can also obtain from the completeness proof some complexity bounds for $\mathcal{L}_n(P,T)$. These bounds are once again identical to those obtained by FHM for their corresponding classical language.

Theorem 5. *Satisfiability of a formula in* $\mathcal{L}_n(P,T)$ *can be decided in exponential space. If the formula is quantifier free, then its satisfiability can be decided in polynomial space.*

The proof of this result makes use of results of Ben-Or, Kozen and Reif [BKR] for the full language, and of Canny [Canny88] for the quantifier free case.

6 Conclusion

A topic that has been of some interest in the quantum mechanics literature is the extent to which it is possible to eliminate the use of complex numbers, and to reason about quantum probabilities purely as real numbers. This requires the characterization of the relationships between the quantum probabilities that follow from their Hilbert space definition. These relationships have been characterized in some low dimensions [Per95], but their charaterization in general remains an open problem. Our work may provide an avenue to address this problem, by applying quantifier elimination to our axiomatization.

We have shown our logic to be to be decidable. An interesting topic for further research is to determine the extent to which it is possible to further enrich

the logic while retaining decidability/axiomatizability. Extensions that suggest themselves are temporal logic, dynamic logic and the logic of knowledge. Even before embarking on a study of such modal extensions, a variety of constructs dealing only with a single state are worthy of study. Constructs such as quantification over bases and unitary transformations, can also be added while keeping the language decidable. One construct that is of critical significance for quantum computing is the tensor product. (We can already handle this to some extent simply by applying our language to the case where the dimension n is a product $n_1 \cdot n_2$, but it is desirable to have the tensor product as a more integral part of the language.) We plan to study such extensions in future work.

References

[AH94] M. Abadi and J.Y. Halpern. Decidability and expressiveness for first-order logics of probability. *Information and Computation*, 112(1):1–36, 1994.

[Bac90] F. Bacchus. *Representing and Reasoning with Probabilistic Knowledge*. MIT Press, Cambridge, Mass., 1990.

[BKR] M. Ben-Or, D. Kozen and J. H. Reif. The complexity of elementary algebra and geometry. *Journal of Computer and System Sciences*, 32(1):251-264, 1986.

[BvN36] G. Birkhoff and J. von Neumann. The logic of quantum mechanics. *Annals of Mathematics*, (37):823–843, 1936.

[Canny88] J. F. Canny. Some algebraic and geometric computations in PSPACE. In *Proc. 20th ACM Symp. on Theory of Computing*, 460-467, 1988.

[Car50] R. Carnap. *Logical Foundations of Probability*. University of Chicago Press, Chicago, 1950.

[FHM90] R. Fagin, J. Y. Halpern, and N. Megiddo. A logic for reasoning about probabilities. *Information and Computation*, 87(1/2):78–128, 1990.

[GPSS80] D. Gabbay, A. Pnueli, S. Shelah, and J. Stavi. On the temporal analysis of fairness. In *Proc. 7th ACM Symp. on Principles of Programming Languages*, pages 163–173, 1980.

[Gud89] S. Gudder. *Quantum Probability Theory*. Academic Press, San Diego, 1989.

[HM90] J. Y. Halpern and Y. Moses. Knowledge and common knowledge in a distributed environment. *Journal of the ACM*, 37(3):549–587, 1990.

[Nil86] N. Nilsson. Probabilistic logic. *Artificial Intelligence*, 28:71–87, 1986.

[Per95] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, Dordrecht, 1995.

[Pra76] V. R. Pratt. Semantical considerations on Floyd-Hoare logic. In *Proc. 17th IEEE Symp. on Foundations of Computer Science*, pages 109–121, 1976.

[Pra92] V.R. Pratt. Linear logic for generalized quantum mechanics. In *Proc. of Workshop on Physics and Computation (PhysComp'92)*, pages 166–180, Dallas, Oct 1992. IEEE.

[Tar51] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. Univ. of California Press, 2nd edition, 1951.

Optional Appendices: Full Proofs of Results

A Deductions.

In the following we make several simple deductions in $\mathtt{Ax}_n(P)$ and $\mathtt{Ax}_n(P,T)$. These results are useful for later purposes. The deductions are informal but could be easily formalised.

D1. Let ϕ be the formula $\mathtt{b}_{i_1} \vee \mathtt{b}_{i_2} \vee \ldots \vee \mathtt{b}_{i_k}$. Then

$$\vdash_{\mathtt{b}} \neg\phi \Leftrightarrow \mathtt{b}_{j_1} \vee \mathtt{b}_{j_2} \vee \ldots \vee \mathtt{b}_{j_{n-k}} \tag{2}$$

where $\{j_1, j_2, \cdots j_{n-k}\}$ is the complement of $\{i_1, i_2, \cdots i_k\}$ in $\{1, 2, \ldots n\}$.

For the proof, note that by **B1**,

$$\begin{aligned}\neg\phi &\Leftrightarrow \neg\phi \wedge (\mathtt{b}_1 \vee \ldots \vee \mathtt{b}_n)\\ &\Leftrightarrow (\neg\mathtt{b}_{i_1} \wedge \ldots \wedge \neg\mathtt{b}_{i_k}) \wedge (\mathtt{b}_1 \vee \ldots \vee \mathtt{b}_n)\\ &\Leftrightarrow \bigvee_{j=1}^{n} ((\neg\mathtt{b}_{i_1} \wedge \ldots \wedge \neg\mathtt{b}_{i_k}) \wedge \mathtt{b}_j)\end{aligned}$$

Now by **B2**, we have that $\vdash \mathtt{b}_j \Rightarrow \neg\mathtt{b}_i$ for $i \neq j$. It follows that each term $(\neg\mathtt{b}_{i_1} \wedge \ldots \wedge \mathtt{b}_{i_k}) \wedge \mathtt{b}_j$ is provably equivalent to $\mathtt{b}_j$ if $j \in \{i_1, \ldots, i_k\}$ and provably false otherwise. This yields the result.

D2. For two disjoint subsets I and J of $\{1, 2, \cdots, n\}$ we have $\vdash_{\mathtt{b}} \neg\left((\bigvee_{i\in I} \mathtt{b}_i) \wedge (\bigvee_{j\in J} \mathtt{b}_j)\right)$

This is an easy consequence of **B2** and the distributive laws.

D3. If $\vdash_{\mathtt{b}} \neg\phi$ then $\vdash P(\phi) = 0$.

This is obtained by taking ϕ_1 to be any $\mathtt{b}$-tautology and ϕ_2 equal to ϕ in **P3**. Noting that by **P4** we have $\vdash P(\phi_1 \wedge \psi) = P(\psi)$ for any $\mathtt{b}$-formula ψ, we obtain $\vdash P(\phi) + P(\neg\phi) = P(\phi_1)$. By **P2**, we have $\vdash P(\phi_1) = 1$ Similarly, by **P2**, if $\neg\phi$ is a $\mathtt{b}$-tautology also, we have $\vdash P(\neg\phi) = 1$. It follows that $\vdash P(\phi) = 0$ by reasoning about linear inequalities.

D4. If $\phi = \mathtt{b}_{i_1} \vee \mathtt{b}_{i_2} \vee \ldots \vee \mathtt{b}_{i_k}$ and $\psi = \mathtt{b}_{j_1} \vee \mathtt{b}_{j_2} \vee \ldots \vee \mathtt{b}_{j_m}$ then $\vdash \phi \wedge \psi \Leftrightarrow \mathtt{b}_{r_1} \vee \mathtt{b}_{r_2} \vee \ldots \vee \mathtt{b}_{r_s}$ where $\{r_1, r_2, \cdots, r_s\} = \{i_1, i_2, \cdots, i_k\} \cap \{j_1, j_2, \cdots, j_m\}$.

The proof uses the distributive laws and **B2**.

D5. For every $\mathtt{b}$-formula ϕ there exists a $\mathtt{b}$-formula ψ of the form $\mathtt{b}_{i_1} \vee \mathtt{b}_{i_2} \vee \ldots \vee \mathtt{b}_{i_k}$ such that $\vdash_{\mathtt{b}} \phi \Leftrightarrow \psi$.

The proof is by induction on the construction of ϕ. We assume that ϕ is expressed using conjunction and negation only. The base case, of a formula of the form $\mathtt{b}_i$, is trivial. The inductive case for negations is handled using **D1** and the inductive case for conjunctions is handled using **D4**.

D6. If $\vdash_{\mathtt{b}} \phi = \mathtt{b}_{i_1} \vee \mathtt{b}_{i_2} \vee \ldots \vee \mathtt{b}_{i_k}$ then $\vdash P(\phi) = P(\mathtt{b}_{i_1}) + P(\mathtt{b}_{i_2}) + \ldots + P(\mathtt{b}_{i_k})$.

For the proof, consider the instance of **P3** obtained by choosing $\phi_1 = \phi \vee \psi$ and $\phi_2 = \phi$:

$$P((\phi \vee \psi) \wedge \phi) + P((\phi \vee \psi) \wedge \neg\phi) = P(\phi \vee \psi)$$

Using **P4**, the first term in this equation is equal to $P(\phi)$. Similarly, if $\vdash_{\mathtt{b}} \neg(\phi \wedge \psi)$, then the second term is equal to $P(\psi)$. This shows $P(\phi) + P(\psi) = P(\phi \vee \psi)$ when $\vdash_{\mathtt{b}} \neg(\phi \wedge \psi)$. We apply this fact, together with **B2**, to obtain the result.

D7. If $\phi \Leftrightarrow \bigvee_k \mathtt{b}_{i_k}$ and $\phi' \Leftrightarrow \bigvee_m \mathtt{b}_{j_m}$ then $\vdash T(\phi, \phi') = \sum_{k,m} T(\mathtt{b}_{i_k}, \mathtt{b}_{j_m})$.

The proof is by a similar argument to the above, using T-axioms.

B Completeness

Our arguments for completeness have some similarity to those of [FHM90] for the logic of classical probabilities, but there are also some fundamental differences between the classical and the quantum case. To explain the differences, we first give a brief account of the classical case. We loosely follow [FHM90], and assume some familiarity with the basic definitions of measure theory. (We confine this discussion to the case when the basic propositions are measurable.)

Let Φ be the set of primitive propositions. For simplicity assume Φ to be the finite set $\{p_1, p_2, \ldots, p_m\}$. A *probability structure* is a pair consisting of a measure space (S, Ξ, μ) and a function $\mathbf{M} : \Phi \to 2^S$, where S is a set, Ξ is a Boolean ring of subsets of S closed under complimentation and countable unions, and μ is a measure on Ξ. We also assume that each $\mathbf{M}(p_i)$ is measurable. The set $\mathbf{M}(p_i)$ is to be understood as the subset of S on which event p_i occurs (or p_i is true). The probability assigned to the basic proposition p_i in a probability structure is written $W(p_i)$, and defined to be the value $\mu(\mathbf{M}(p_i))$.

A formula ϕ (expressing a boolean combination of linear inequalities over probability terms) is defined to be satisfiable in the classical theory if there exists a probability structure with respect to which ϕ is true. The completeness proof proceeds by constructing a probability structure satisfying a given consistent formula ϕ. In particular, in this construction, one has a large degree of freedom in the choice of the measure space (S, Ξ, μ), as well as the interpretation function $\mathbf{M}$. This freedom is used to advantage in the completeness proof. Its is first shown that the formula ϕ is equivalent to a formula ϕ' in which the basic probability terms are of the form $W(l_1 \wedge \ldots \wedge l_m)$ where each l_i is either p_i or $\neg p_i$. A set of 2^m real variables $x_1, \ldots, x_{2^m}$ are introduced to correspond to these terms. Replacing these terms in ϕ' by their corresonding variables, and conjoining the constraints

$x_i \geq 0$ and $\sum_{i=1}^{m} x_i = 1$, we obtain a consistent formula ϕ'' concerning just the real variables $x_1, \ldots, x_{2^m}$. *Any* values of the x_i satisfying ϕ'' can be used to construct a probability structure satisfying ϕ'' and the correspondence formulas $W(l_1 \wedge \ldots \wedge l_m) = x_i$, and hence ϕ. We refer to FHM for the details.

Our arguments for the quantum case (for both $\mathcal{L}_n(P)$ and $\mathcal{L}_n(P,T)$) follow a similar structure, in that we also first reduce the construction of a model for a given consistent formula to the problem of finding a set of real values x_i that correspond to a set of probabilities. However, once we obtain the values x_i we are somewhat more constrained in the way we construct a model. Our probabilities arise not from a completely undetermined measure space, but from vectors and bases in the (essentially unique) Hilbert space H_n of dimension n. Instead of constructing a measure space, we need to construct a vector and a set of bases that give rise to the values x_i through the inner product.

B.1 The Case of $\mathcal{L}_n(P)$

We first deal with completeness for the language $\mathcal{L}_n(P)$.

Lemma 1. *For every basic formula α of $\mathcal{L}_n(P)$, with basis symbols amongst $\mathtt{b}^1, \ldots, \mathtt{b}^m$, it is possible to construct in time $O(|\alpha| \cdot n)$ a basic formula α^* of the form $\sum_{k=1}^{m} \sum_{j=1}^{n} c_{jk} P(\mathtt{b}_j^k) \sim d$, where '$\sim$' stands for either '$\leq$' or '$<$', and the c_{jk} and d are integers, such that $\vdash \alpha \Leftrightarrow \alpha^*$.*

Proof. If α is an atomic formula, it has the form $\sum_{j=1}^{n} a_j P(\phi_j) \sim d$, where the a_j and d are integers. Let $\mathtt{b}$ be the basis symbol such that ϕ_j is a $\mathtt{b}$-formula. By **D5**, there exists a set $\{i_1, \ldots, i_r\}$ such that $\vdash_{\mathtt{b}} \phi_j \Leftrightarrow \mathtt{b}_{i_1} \vee \mathtt{b}_{i_2} \vee \ldots \vee \mathtt{b}_{i_r}$. Using **D1** and **D4**, the computation of this set can be done in time $O(|\phi_j| \cdot n)$, following the inductive construction of ϕ_j. By **D6** and the axiom **P4**, we have $P(\phi_j) = \sum_{r=1}^{n} P(\mathtt{b}_{i_r})$. Using reasoning about linear inequalities, we can now (in time $O(|\alpha| \cdot n)$ substitute the right hand side of these equations equations in α, collect terms of the form $aP(\mathtt{b}_j^k)$ with the same basis term $\mathtt{b}_j^k$ into a single term of this form, and add coefficients $c_{jk} = 0$ for those j such that the corresponding $\mathtt{b}_j^k$ does not appear. This turns α into a basic formula of the required form.

Theorem 1: $\mathtt{AX_n(P)}$ *is a sound and complete axiomatization for $\mathcal{L}_n(P)$.*

Proof. Soundness is straightforward and left to the reader. It will suffice to show that if ϕ is a consistent formula of $\mathcal{L}_n(P)$ then it is satisfiable. Let $\mathtt{b}^1, \ldots \mathtt{b}^k$ be the basis symbols in ϕ. By Lemma 1, ϕ is provably equivalent to a formula ϕ^* in which all probability terms are of the form $P(\mathtt{b}_i^j)$. If ϕ is consistent, then so is ϕ^*, and by soundness, any model of ϕ^* is a model of ϕ. It therefore suffices to show that ϕ^* is satisfiable. For each term $P(\mathtt{b}_i^j)$ let y_i^j be a new variable of real type. Write $\mathbf{y}^j$ for the sequence of variables $y_1^j, \ldots, y_n^j$. Let $\phi'(\mathbf{y}^1, \ldots, \mathbf{y}^k)$ denote the formula obtained from ϕ^* by replacing each occurrence of $P(\mathtt{b}_i^j)$ in ϕ^* by y_i^j. Write $\mathtt{Prob}(\mathbf{y}^j)$ formula

$$\bigwedge_{i=1}^{n} y_i^j \geq 0 \ \wedge \ \sum_{i=1}^{n} y_i^j = 1$$

and $\mathtt{Prob}(\mathbf{y}^1,\ldots,\mathbf{y}^k)$ for $\bigwedge_{j=1}^{k}\mathtt{Prob}(\mathbf{y}^j)$. The formula $\phi'(\mathbf{y}^1,\ldots,\mathbf{y}^k)\wedge\mathtt{Prob}(\mathbf{y}^1,\ldots,\mathbf{y}^k)$ is a consistent formula of the theory of linear contraints. To see this, note first that ϕ^* is provably equivalent in $\mathtt{AX_n(P)}$ to its conjunction with the formulas $P(\mathtt{b}_i^j)\geq 0$ and the formulas $\sum_{i=1}^{n}P(\mathtt{b}_i^j)=1$, since these formulas are derivable, the former by **P1**, and the latter by **B1** and **D6**. Since all substitution instances of axioms and rules of inferences of the theory of linear constraints are in $\mathtt{AX_n(P)}$, if $\phi'(\mathbf{y}^1,\ldots,\mathbf{y}^k)\wedge\mathtt{Prob}(\mathbf{y}^1,\ldots,\mathbf{y}^k)$ were inconsistent, then ϕ^* would be inconsistent. Since the theory of linear constraints is sound and complete, it follows that there exists an assignment π' of real numbers to the variables $\mathbf{y}^1,\ldots,\mathbf{y}^k$ satisfying $\phi'(\mathbf{y}^1,\ldots,\mathbf{y}^k)\wedge\mathtt{Prob}(\mathbf{y}^1,\ldots,\mathbf{y}^k)$. We now use this satisfying assignment to construct a unit vector $|\psi\rangle$ in H_n, and an assignment π of orthonormal bases in H_n to the basis symbols $\mathtt{b}^1,\ldots\mathtt{b}^k$, such that $H_n,\pi,|\psi\rangle\models\phi^*$. Clearly, it suffices to show that for each variable y_i^j, we have $[\![P(\mathtt{b}_i^j)]\!]_{\pi,\psi}=\pi'(y_i^j)$. We proceed as follows.

We start by choosing $\pi(\mathtt{b}^1)$ to be equal to an arbitrary orthonormal basis $A=|\epsilon_1\rangle,|\epsilon_2\rangle,\ldots,|\epsilon_n\rangle$. Write r_i^j for $\pi'(y_i^j)$. Since we have $r_i^j\geq 0$, we may define the vectors

$$|\psi_j\rangle=\sum_{i=1}^{n}\sqrt{r_i^1}|\epsilon_i\rangle. \tag{3}$$

Note that because $\sum_{i=1}^{n}r_i^j=1$, each $|\psi_j\rangle$ is a unit vector. Take $|\psi\rangle$ to be equal to $|\psi_1\rangle$. For $i=1\ldots n$ we have $[\![P(\mathtt{b}_i^1)]\!]_{\pi,|\psi\rangle}=\|\langle\epsilon_i|\psi_1\rangle\|^2=r_i^1$, as required. For $\mathtt{b}^2,\ldots,\mathtt{b}^k$, we proceed as follows. First, for each $j=1\ldots k$, take $B_j=|\beta_1^j\rangle,\ldots,|\beta_n^j\rangle$ to be any orthonormal basis such that $|\beta_1^j\rangle=|\psi_j\rangle$. For each $j=1\ldots k$, let U^j be the unitary transformation such that $U^jB_1=B_j$. Now define $\pi(\mathtt{b}^j)$ to be the basis $(U^j)^{-1}A$. Then we have

$$\begin{aligned}
[\![P(\mathtt{b}_i^j)]\!]_{\pi,|\psi\rangle} &= \|\langle\pi(\mathtt{b}^j)_i\mid\psi\rangle\|^2\\
&= \|\langle(U^j)^{-1}\epsilon_i\mid\psi_1\rangle\|^2\\
&= \|\langle\epsilon_i\mid U^j\psi_1\rangle\|^2\\
&= \|\langle\epsilon_i\mid\psi_j\rangle\|^2\\
&= r_i^j\\
&= \pi'(y_i^j)
\end{aligned}$$

as required.

Proposition 2: *Let $\phi_1,\ldots,\phi_m$ be formulas and $\mathtt{b}^1,\ldots,\mathtt{b}^m$ be distinct basis variables such that for each $j=1,\ldots,n$, the only probability terms occuring in ϕ_j are $\mathtt{b}^j$ probability terms. Then $\phi_1\wedge\ldots\wedge\phi_m$ is satisfiable iff each ϕ_j is satisfiable.*

Proof. It is trivial that if $\phi_1\wedge\ldots\wedge\phi_m$ is satisfiable then each ϕ_j is satisfiable. Suppose each ϕ_j is satisfiable. Then each ϕ_j is consistent, and we may apply the construction of the proof of Theorem 1. Note that the construction can start with any given vector $|\psi\rangle$, so we may choose the same vector ψ for each ϕ_j. This yields a pair $\pi,|\psi\rangle$ with respect to which $\phi_1\wedge\ldots\wedge\phi_m$ is satisfied.

Theorem 2: *Satisfiability of a formula of $\mathcal{L}_n(P)$ in n-dimensional Hilbert space (with $n \geq 2$) is NP-complete.*

Proof. We first show NP-hardness, by means of a reduction from $\mathtt{SAT}$. Let α be a formula of propositional logic. We asssume without loss of generality that negation and conjunction are the only propositional operators used. We define a formula α^* of $\mathcal{L}_n(P)$ such that $\alpha \in \mathtt{SAT}$ iff α^* is satisfiable in n-dimensional Hilbert space. Let the propositional constants of α be $p_1, \ldots, p_m$. Corresponding to each, let $\mathtt{b}^1, \ldots, \mathtt{b}^m$ be a collection of distinct basis symbols. We define α^* by induction on the construction of α, as follows:

$$\begin{aligned} p_i^* &= P(\mathtt{b}_1^i) = 1, \\ (\neg\alpha_1)^* &= \neg\alpha_1^*, \\ (\alpha_1 \wedge \alpha_2)^* &= \alpha_1^* \wedge \alpha_2^*. \end{aligned}$$

We now show that $\alpha \in \mathtt{SAT}$ iff α^* is satisfiable. Its is easily seen that if α^* is satisfiable then so is α. For, suppose that $H_n, \pi, \psi \models \alpha^*$. Then it is immediate that the assignment $V : \{p_1, \ldots, p_m\} \to \{0, 1\}$ defined by $V(p_i) = 1$ iff $H_n, \pi, \psi \models p_i^*$ is a satisfying assignment for α. Conversely, suppose that α is satisfiable, and let V be a satisfying assignment. We construct a vector ψ in H_n and an interpretation π of the basis symbols $\mathtt{b}^1, \ldots, \mathtt{b}^m$ such that $H_n, \pi, \psi \models \alpha^*$. For this, let $B_1 = \psi_1, \ldots, \psi_n$ be any orthonormal basis of H_n. Let B_2 be the sequence of vectors obtained by swapping ψ_1 and ψ_2 in B_1. Clearly, B_2 is also an orthonormal basis. By definition, $\langle\psi_1|\psi_2\rangle = 0$. We now take $\psi = \psi_1$, and define π as follows: for each $i = 1 \ldots m$, we let $\pi(\mathtt{b}^i) = B_1$ if $V(p_i) = 1$ and $\pi(\mathtt{b}^i) = B_2$ otherwise. It is now straightforward to check that $H_n, \pi, \psi \models p_i^*$ iff $V(p_i) = 1$, from which it follows that $H_n, \pi, \psi \models \alpha^*$.

To see that satisfiability of ϕ can be determined in NP, we use the construction of Theorem 1. By Lemma 1, the formulas ϕ^* and hence $\phi'(\mathbf{y}^1, \ldots, \mathbf{y}^k)$ may be constructed in time $O(|\phi| \cdot n)$, as may the formula $\mathtt{Prob}(\mathbf{y}^1, \ldots, \mathbf{y}^k)$. Hence we also obtain the formula $\phi'(\mathbf{y}^1, \ldots, \mathbf{y}^k) \wedge \mathtt{Prob}(\mathbf{y}^1, \ldots, \mathbf{y}^k)$ in time $O(|\phi| \cdot n)$. The arguments of Theorem 1 are cast in terms of consistency, but we may see by similar arguments that ϕ is satisfiable iff $\phi'(\mathbf{y}^1, \ldots, \mathbf{y}^k) \wedge \mathtt{Prob}(\mathbf{y}^1, \ldots, \mathbf{y}^k)$ is satisfiable. The latter is a boolean combination of linear constraints. It follows from the fact that linear programming is in PTIME [**?**] that satisfiability of such formulas is in NP. Thus, satisfiability of ϕ in $\mathcal{L}_n(P)$ is also in NP.

B.2 Dealing with $\mathcal{L}_n(P, T)$

We now deal with the general case. Here the nonlinearity of quantum probabilities come into picture. Let Φ be formula of $\mathcal{L}_n(P, T)$, with $\mathtt{b}^0, \mathtt{b}^1, ..., \mathtt{b}^k$ the basis symbols that occur in Φ.

Lemma 2. *Let ϕ be a formula of $\mathcal{L}_n(P, T)$ containing the basis constants $\mathtt{b}^1, \ldots, \mathtt{b}^m$. Then it is possible to construct in polynomial time a formula ϕ^* such that $\vdash \phi \Leftrightarrow \phi^*$ such that all atomic subformulas of ϕ^* are of the form $p = 0$ where p is a polynomial with integer coefficients over terms of the form $P(\mathtt{b}_i^r)$, or $m_{ij}(\mathtt{b}^1, \mathtt{b}^r)$, with $1 \leq r \leq k$ and $1 \leq i, j \leq n$.*

Proof. It suffices to show that each atomic subformula α of ϕ is equivalent to a formula α^* of the required form. First, we note that by the arguments of Lemma 1, all probability terms $P(\gamma)$, with γ a $\mathtt{b}_r$ formula, are provably equal to a sum of terms of the form $P(\mathtt{b}_i^r)$. It therefore suffices to consider terms of the form $T(\gamma, \delta)$, where γ is a $\mathtt{b}^r$-formula and δ is a $\mathtt{b}^s$-formula. Using **T1**-**T4**, **B1**-**B2** and arguments very similar to those of Lemma 1, we may show that $T(\gamma, \delta)$ is provably equal to a sum of terms of the form $T(\gamma, \mathtt{b}_i^s)$. By **T5**, each such term is provably equal to $T(\mathtt{b}_i^s, \gamma)$. Now, using **T1**-**T4**, **B1**-**B2** again, each term of the latter form can be shown to be provably equal to a sum of terms of the form $T(\mathtt{b}_i^s, \mathtt{b}_j^r)$. It follows that the original term $T(\gamma, \delta)$ is provably equal to a sum of terms of the form $T(\mathtt{b}_i^s, \mathtt{b}_j^r)$. By **MT**, each term of the latter form equals $|m_{ij}(\mathtt{b}^s, \mathtt{b}^r)|^2$. Using **M3**, we may express the terms $m_{ij}(\mathtt{b}^s, \mathtt{b}^r)$ as a sum of terms of the form $m_{ik}(\mathtt{b}^s, \mathtt{b}^1) \cdot m_{ki}(\mathtt{b}^1, \mathtt{b}^r)$. By **M1**, the terms $m_{ik}(\mathtt{b}^s, \mathtt{b}^1)$ are equal to $\overline{m_{ki}(\mathtt{b}^1, \mathtt{b}^s)}$.

The result of these transformations is to show that α is equivalent to an atomic formula of the form $p = 0$, where p is composed from real and complex variables and terms of the form $P(\mathtt{b}_i^r)$ and $m_{ij}(\mathtt{b}^1, \mathtt{b}^r)$ using addition, multiplication and conjugation. We now use the fact that $\phi(\overline{y})$ is an abbreviation for $\exists x : \mathbf{C}.(\phi(x) \wedge \exists a, b : \mathbf{R}.\exists z : \mathbf{C}.(z^2 + 1 = 0 \ \wedge \ y = a + bz \ \wedge \ x = a - bz))$ to eliminate the use of conjugation. This leaves a formula in the required form.

We can now prove the completeness result for $\mathcal{L}_n(P, T)$ using a similar argument to that above. We assume that ϕ is a consistent formula of $\mathcal{L}_n(P, T)$ containing the basis symbols $\mathtt{b}^1, \ldots, \mathtt{b}^k$, and construct a vector and basis interpretation in H_n with respect to which ϕ is satisfied. Using Lemma 2, it suffices to show that ϕ^* is satisfiable. For $1 \leq j \leq k$ and $1 \leq i \leq n$, let x_i^j be a variable of real type. For each $1 \leq j \leq k$ and $1 \leq i, r \leq n$, let y_{ir}^j be a variable of complex type. Write $\mathbf{x}$ for the sequence of variables x_i^j and write $\mathbf{y}$ for the sequence of variables y_{ir}^j. Let θ be the substitution that substitutes $P(\mathtt{b}_i^j)$ for each x_i^j, and substitutes $m_{ir}(\mathtt{b}^1, \mathtt{b}^j)$ for each y_{ir}^j. At this point of the proof we make use of the following lemma, whose proof we defer to later.

Lemma 3. *There exists a formula Ψ of $\mathcal{L}_{\mathbf{RC}}$ with free variables amongst $\mathbf{x}, \mathbf{y}$ such that*

1. *Ψ is constructible in time polynomial in $|\mathbf{x}, \mathbf{y}|$,*
2. *$\vdash \Psi\theta$,*
3. *if π' is an interpretation of the real and complex variables $\mathbf{x}$ and $\mathbf{y}$ that satisfies Ψ, then there exists a vector $|\psi\rangle$ of H_n and an interpretation π for the basis symbols $\mathtt{b}^1, \ldots, \mathtt{b}^k$ in H_n, such that*
   (a) *$[\![P(\mathtt{b}_i^j)]\!]_{\pi, |\psi\rangle} = \pi'(x_i^j)$ for $1 \leq j \leq k$ and $1 \leq i \leq n$, and*
   (b) *$[\![m_{ir}(\mathtt{b}^1, \mathtt{b}^j)]\!]_{\pi, |\psi\rangle} = \pi'(y_{ir}^j)$ for $1 \leq j \leq k$ and $1 \leq i, r \leq n$.*

To construct an interpretation satisfying ϕ^*, we proceed as follows. Since ϕ^* is consistent, and $\vdash \Psi\theta$, the formula $\phi^* \wedge \Psi\theta$ is consistent. Let $\phi'(\mathbf{x}, \mathbf{y})$ be the formula of $\mathcal{L}_{\mathbf{RC}}$ such that $\phi^* = \phi'(\mathbf{x}, \mathbf{y})\theta$. Since $\mathtt{AX}_n(P, T)$ contains all substitution instances of a sound and complete proof theory for $\mathcal{L}_{\mathbf{RC}}$, it follows that

$\phi'(\mathbf{x}, \mathbf{y}) \wedge \Psi$ is a consistent formula with respect to the latter proof theory. By completeness, there exists an interpretation π' of the variables $\mathbf{x}$ and $\mathbf{y}$ as real and complex numbers, with respect to which this formula is satisfied. In particular, Ψ is satisfied with respect to π'. It follows by Lemma 3 that there exists a vector $|\psi\rangle$ of H_n and an interpretation π for the basis symbols $\mathtt{b}^1, \ldots, \mathtt{b}^k$ in H_n, such that the conditions of the lemma are satisfied. It follows from these conditions, and the fact that $\phi'(\mathbf{x}, \mathbf{y})$ is satisfied with respect to π', that $H_n, \pi, |\psi\rangle \models \phi^*$, hence $H_n, \pi, |\psi\rangle \models \phi$. This completes the proof. An inspection of the argument shows that it also yields a complexity result:

Theorem 5: *Satisfiability of a formula in $\mathcal{L}_n(P, T)$ can be decided in exponential space. If the formula is quantifier free, then its satisfiability can be decided in polynomial space.*

Proof. We note that similar reasoning to that above shows that $\phi'(\mathbf{x}, \mathbf{y}) \wedge \Psi$ is satisfiable iff ϕ is satisfiable. This formula may be constructed in time polynomial in $|\phi|$. Thus, the satisfiability problem reduces to that for $\mathcal{L}_{\mathbf{RC}}$. We now show that there exists a further reduction of this decision problem to that for $\mathcal{L}_{\mathbf{R}}$, i.e., the language of the theory of real closed fields.

Define the operator $\tau : \mathcal{L}_{\mathbf{RC}} \to \mathcal{L}_{\mathbf{R}}$ by induction, as follows. To each complex variable x, associate two variables x_r, x_c of real type. For convenience, we extend this notation to real variables and integers, by treating x_r as a notation for x x_c as a notation for 0, when x is either a real variable or an integer. Without loss of generality, we assume that all atomic formulas of $\phi \in \mathcal{L}_{\mathbf{RC}}$ are of the form $z = x + y$ or $z = x \cdot y$, where z is a variable and x and y are either variables or integers. We define $\tau(\phi)$ (which we also write as ϕ^τ) by induction on the construction of ϕ:

1. $(z = x + y)^\tau$ is $z_r = x_r + y_r \ \wedge \ z_c = x_c + y_c$,
2. $(z = x \cdot y)^\tau$ is $z_r = x_r \cdot y_r - x_c \cdot y_c \ \wedge \ z_c = x_c \cdot y_r + x_r \cdot y_c$,
3. $(\phi_1 \wedge \phi_2)^\tau$ is $\phi_1^\tau \wedge \phi_2^\tau$
4. $(\neg\phi)^\tau$ is $\neg\phi^\tau$,
5. $(\exists x : \mathbf{R}.\phi)^\tau$ is $\exists x(\phi^\tau)$,
6. $(\exists x : \mathbf{C}.\phi)^\tau$ is $\exists x_r \exists x_c(\phi^\tau)$.

Using the well-known interpretation of complex numbers as pairs of reals, it is readily seen that ϕ is satisfiable iff ϕ^τ is satisfiable. The result now follows from the result of Ben-Or, Kozen and Reif [BKR] that the theory of real closed fields (which is equal to the theory of the reals) is decidable in exponential space.

In the quantifier free case, we note that $\phi'(\mathbf{x}, \mathbf{y})$ may contain quantifiers arising from the elimination of conjugation. However, by avoiding the conjugation elimination step we may assume that $\phi'(\mathbf{x}, \mathbf{y})$ expresses conjugation by means of basic formulas of the form $z = \overline{x}$. The translation τ may be extended to formulas containing such atoms by defining $(z = \overline{x})^\tau$ as $z_r = x_r \ \wedge z_c = -x_c$. This makes ϕ^τ a quantifier free formula, satisfiable iff ϕ is satisfiable. By a result of Canny [Canny88], satisfiability of ϕ^τ can be decided in polynomial space.

To complete the proof, we now turn to the omitted proof of Lemma 3. A key part of the proof of this lemma turns on the following result, which we state as a theorem given its non-trivial nature and independent interest.

Theorem 4: *For every number $k \geq 1$, the formula $\mathbf{MP}_k$ is a theorem of $\mathtt{AX_n(P,T)}$.*

Proof. First, if $k \leq n^2 - n + 1$ then the formula $\mathbf{MP}_k$ is an axiom. We show that for larger k, the formula also follows from instances of $\mathbf{P}$. It does so in a way that depends only upon algebraic reasoning. It therefore suffices to present a purely semantic argument, and rely upon the fact that $\mathtt{AX}_n(P,T)$ contains all instances of valid formulas of $\mathcal{L}_{\mathbf{RC}}$.

We introduce some notation. We write ι for $\sqrt{-1}$. Let $y_i^j = \sqrt{P(\mathfrak{b}_i^j)}$ — as we have already noted in the proof of Proposition 1, the sign of the x_i is irrelevant to the truth of $\mathbf{MP}_k$, so we may assume that in the case $j = 0$ we have $y_i^0 = x_i$. Let $m_{ij}(\mathfrak{b}^1, \mathfrak{b}^j) = p_{ij}^j \cdot e^{\iota\beta_{ij}}$, with $p_{ij}^j \geq 0$ be the polar form of the entries of the unitary matrix. To show that the desired formula is valid, we need to show that a set of equations in the z_i has a solution. One set of these equations states the z_i have norm 1, so without loss of generality, we may write $z_i = e^{\iota\theta_i}$.

Then each remaining equation in the conjunction we need to prove can be represented as follows

$$\| \sum_r p_{ir}^j e^{\iota(\beta_{ir}+\theta_r)} y_r^0 \|^2 \;=\; (y_i^j)^2 \tag{4}$$

where $1 \leq i, r \leq n$ and $1 \leq j \leq k$. This equation can be written as

$$\begin{array}{c} \sum_{r<s} p_{ir}^j p_{is}^j y_r^0 y_s^0 \cos(\beta_{ir} - \beta_{is} + \theta_r - \theta_s) \\ = \frac{1}{2}((y_j^i)^2 - \sum_r (p_{ir}^j)^2 (y_r^0)^2) \end{array}$$

Writing the rhs of the above equation as q_i^j we rewrite it as

$$\begin{array}{c} \sum_{r<s} p_{ir}^j p_{is}^j y_r^0 y_s^0 (\cos(\beta_{ir} - \beta_{is}) \cos(\theta_r - \theta_s) \\ - \sin(\beta_{ir} - \beta_{is}) \sin(\theta_r - \theta_s)) = q_j^i. \end{array} \tag{5}$$

If we treat $\cos(\theta_r - \theta_s)$ and $sin(\theta_r - \theta_s)$, for $1 \leq r < s \leq n$, as independent variables then (5) represents a set of linear equations. However, these variables are quadratically constrained by the relations $\cos^2(\theta_r - \theta_s) + \sin^2(\theta_r - \theta_s) = 1$ and the (quadratic) relations among $cos(\theta_r - \theta_s)$ and $\sin(\theta_r - \theta_s)$) and $cos(\theta_r)$, $\cos(\theta_s)$ $\sin(\theta_r)$, and $\sin(\theta_s)$. Thus despite the appearance of transcendental functions $cos(\theta_r - \theta_s)$, the equations (5) is a set of algebraic (in fact quadratic) equations. There are $n(n-1)/2$ variables each of type $cos(\theta_r - \theta_s)$ and $\sin(\theta_r - \theta_s)$, thus a total of $n(n-1)$ variables. We call the n linear equations arising for a fixed value of j (corresponding to transition from $\mathfrak{b}^0$ to $\mathfrak{b}^j$) a *block*. Notice that for each block, we also have a set of quadratic equations, but these are identical from block to block.

Now suppose that the entire set of equations does not have a solution. We prove a contradiction. Since there are $n(n-1)$ variables in the blocks, the maximum dimension of the set of solutions of some subset of the linear equations is

$n(n-1)$. Adding a block to a set of linear equations either decreases the dimension, or leaves the solutions space invariant. Thus, we can find a set of at most $n(n-1)+1$ blocks that does not have a solution. But this contradicts the axiom **MP**.

We are now in a position to provide the proof omitted above.

Proof. **(Of Lemma 3)** Write $\mathbf{y}^j$ for the sequence of variables $y_1^j, \ldots, y_n^j$. We reuse the formula $\mathtt{Prob}(\mathbf{x}^j)$ defined in the proof of Theorem 1. Additionally, for each $j = 1 \ldots, k$, define $\mathtt{Unitary}(\mathbf{y}^j)$ to be the result of eliminating conjugation from the formula $\bigwedge_{i=1}^n \bigwedge_{r=1}^n \sum_{k=1}^n y_{ik}^j \cdot \overline{y_{rk}^j} = \delta_{ir}$. Define $\mathtt{Phase}(z_1, \ldots, z_n, \mathbf{x}, \mathbf{y})$, where the z_i are variables of complex type, to be the formula

$$\bigwedge_{i=1}^{n} (\|z_i\| = 1) \;\; \wedge \;\; \bigwedge_{j=2}^{k} \bigwedge_{i=1}^{n} \| \sum_{r=1}^{n} y_{ir}^j z_r \sqrt{x_r^1} \|^2 = \|x_i^j\|^2.$$

We now take $\Psi(\mathbf{x}, \mathbf{y})$ to be the conjunction of the formulas $\mathtt{Prob}(\mathbf{x}^j) \wedge \mathtt{Unitary}(\mathbf{y}^j)$, for $j = 1 \ldots k$, with the formula $\exists z_1, \ldots, z_n : \mathbf{C}.(\mathtt{Phase}(z_1, \ldots, z_n, \mathbf{x}, \mathbf{y}))$. Clearly $\Psi(\mathbf{x}, \mathbf{y})$ can be constructed in time polynomial in $|\mathbf{x}, \mathbf{y}|$, so the first condition of the lemma is satisfied.

We now show that the third condition is satisfied. Let π' be an assignment of real and complex numbers to the variables $\mathbf{x}$ and $\mathbf{y}$ such that $\Phi(\mathbf{x}, \mathbf{y})$ is satisfied. Morever, suppose that π' assigns complex numbers to the variables $z_1, \ldots, z_n$ such that the formula $\mathtt{Phase}(z_1, \ldots, z_n, \mathbf{x}, \mathbf{y})$ is satisfied.

Construct the interpretation π for $\mathtt{b}^1, \ldots, \mathtt{b}^k$ in H_n and the vector $|\psi\rangle$ in H_n as follows. For $\pi(\mathtt{b}^1)$ take any othonormal basis $|\epsilon_1\rangle, \ldots, |\epsilon_n\rangle$. For the remaining bases $\mathtt{b}^j$, with $2 \leq j \leq k$, we define

$$\pi(\mathtt{b}^j)_i = \sum_{r=1}^{n} \pi'(y_{ir}^j) \cdot |\epsilon_r\rangle.$$

We take

$$|\psi\rangle = \sum_{r=1}^{n} \pi'(z_r) \cdot \sqrt{\pi'(x_r^j)} \cdot |\epsilon_r\rangle.$$

This is a unit vector because, by assumption, we have that $\|\pi'(z_r)\| = 1$ and $\sum_{i=1}^n \pi'(x_r^j) = 1$.

We show that the two parts of condition (3) of Lemma 3 are satisfied. The second part is immediate from the definition of the $\pi(\mathtt{b}^j)_i$. For the first part, note that

$$\begin{aligned}
&[\![P(\mathtt{b}_i^j)]\!]_{\pi,|\psi\rangle} \\
&\quad = \|\langle \pi(\mathtt{b}_i^j)|\psi\rangle\|^2 \\
&\quad = \|\langle \; \textstyle\sum_{r=1}^n \pi'(y_{ir}^j) \cdot |\epsilon_r\rangle \;\; | \\
&\qquad\qquad \textstyle\sum_{r=1}^n \pi'(z_r) \cdot \sqrt{\pi'(x_r^j)} \cdot |\epsilon_r\rangle \; \rangle\|^2 \\
&\quad = \| \; \textstyle\sum_{r=1}^n \pi'(y_{ir}^j) \cdot \pi'(z_r) \cdot \sqrt{\pi'(x_r^j)} \; \|^2 \\
&\quad = \pi'(x_i^j)
\end{aligned}$$

where the last step follows from the fact that π' satisfies $\texttt{Phase}(z_1, \ldots, z_n, \mathbf{x}, \mathbf{y})$.

It remains to show that $\Psi\theta$ is derivable. By **D6** and **P1, P2**, we have that $\vdash \texttt{Prob}(\mathbf{x}^j)\theta$ for each $j = 1 \ldots k$. It follows from **M1** and **M4** that $\vdash \texttt{Unitary}(\mathbf{y}^j)\theta$ for each $j = 1 \ldots k$. By Theorem 4 we have $\vdash \exists z_1 \ldots z_n(\texttt{Phase}(z_1, \ldots, z_n, \mathbf{x}, \mathbf{y})\theta$. Thus, each of the conjuncts of $\Psi\theta$ is derivable, so this formula itself is derivable.