Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 210 (2008) 49–63

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Semantic Abstraction and Quantum Computation

Alessandra Di Pierro[1]

Dipartimento di Informatica
University of Pisa
Pisa, Italy

Herbert Wiklicky[2]

Department of Computing
Imperial College
London, UK

Abstract

We present a logico-algebraic approach to probabilistic abstract interpretation based on the ortholattice structure of the projective measurement operators in quantum mechanics. On this base, we present a novel interpretation of quantum measurement as a probabilistic abstraction showing that the measurement of a physical observable essentially corresponds to a static analysis of the observed property.

Keywords: Probabilistic abstract interpretation, quantum measurement, quantum computation.

1 Introduction

Some of the best known quantum algorithms, e.g. for the Deutsch problem or the phase estimation at the heart of Shor's quantum factorisation algorithm, ultimately aim in determining some properties of an unknown function f, represented by a black-box unitary operator $\mathbf{U}_f$.

Our treatment is not concerned with the specification and description of $\mathbf{U}_f$; in particular, it is not directed towards the immediate definition of a programming language for quantum computation. Instead we aim in investigating the mechanism at the base of the "detection", or analysis of properties of $\mathbf{U}_f$ and thus f, namely *quantum measurement*. We show that this aspect of quantum algorithms corresponds

[1] Email: dipierro@di.unipi.it

[2] Email: herbert@doc.ic.ac.uk

doi:10.1016/j.entcs.2008.04.017

to a particular static analysis technique, namely abstract interpretation, which is used in the classical setting for constructing approximations of the programs' semantics relatively to a given property of interest [7,8]; in addition, probabilistic abstract interpretation provides an estimation of such an approximation in terms of the distance between the analysis results and the concrete semantics [11,10].

This correspondence relies on a similar "logical structure" at the basis of both quantum measurement and probabilistic abstract interpretation. As is well-known in Quantum Mechanics, projection operators on a Hilbert space form a non-Boolean – in particular, non-distributive – lattice. This result dates back to the 1936 article by Birkhoff and von Neumann [3] where the authors' claimed objective was to "find a calculus of propositions which is formally indistinguishable from the calculus of linear subspaces of a Hilbert space with respect to *set products*, *linear sums* and *orthogonal complements*, and resembles the usual calculus of propositions with respect to *and*, *or* and *not*". In this paper we present a re-formulation of the theory of probabilistic abstract interpretation [11,10] in terms of orthogonal projections and we show that probabilistic abstractions possess the same lattice structure as the Birkhoff and von Neumann lattice of projections with respect to the ordering given by the inclusion relation on subspaces [21,3].

The intuitive reason why quantum physics and abstract interpretation require a similar non-standard logical treatment lies in the common characteristics of measurements and abstractions. In quantum physics it is well known that certain physical observables are not commensurable; this means that a simultaneous measurement of for example the position and the momentum of a particle is impossible, as measuring the position first "destroys" the information about the momentum and vice versa. The famous Heisenberg uncertainty relation can be expressed via the statement that the commutator between the position and momentum operator is not zero. In a similar way certain abstractions "destroy" information which makes a subsequent abstraction meaningless.

Based on the intrinsic similarity between quantum physics and probabilistic abstract interpretation, we show that the quantum measurement of a physical observable corresponds essentially to a static analysis of the observed property. More precisely, given a property the corresponding abstract domain (or equivalently the corresponding projection) can be seen as the result of the quantum measurement of an observable including the property; vice versa any physical observable (or equivalently any self-adjoint operator) can be seen as a linear combination of projections corresponding to some probabilistic abstract interpretations.

2 Semantical Abstractions

In this section, we recall some preliminary notions and results concerning the logic of projections in quantum mechanics, and introduce the ortholattice of probabilistic abstract interpretations.

2.1 The Lattice of Projections

If Y is a closed subspace of a Hilbert space[3] $\mathcal{H}$, each vector in $\mathcal{H}$ can be expressed uniquely in the form $y + z$ with $y \in Y$ and $z \in Y^\perp$, where $Y^\perp$ is a complementary subspace to Y (i.e. $Y \cup Y^\perp = \mathcal{H}$ and $Y \cap Y^\perp = \emptyset$). The linear operator $\mathbf{P} : \mathcal{H} \to Y$ defined by $\mathbf{P}(y+z) = y$ is called the *orthogonal projection*[4] from $\mathcal{H}$ onto Y. It is easy to show that projection operators $\mathbf{P}$ are bounded (their norm is always less than or equal to 1) idempotent ($\mathbf{P}^2 = \mathbf{P}$) and Hermitian. An operator $\mathbf{A}$ is said to be *self-adjoint* or *Hermitian* if it coincides with its adjoint $\mathbf{A}^*$, that is the unique operator such that the condition $\langle \mathbf{A}^* x, y\rangle = \langle x, \mathbf{A} y\rangle$ holds for all $x, y \in \mathcal{H}$ (cf. e.g.[15, Thm 2.4.2]). In particular, projections are a special kind of self-adjoint operators, that is positive operators. An operator $\mathbf{A}$ is called *positive*, denoted by $\mathbf{A} \sqsupseteq 0$, if there exists an operator $\mathbf{B}$ such that $\mathbf{A} = \mathbf{B}^*\mathbf{B}$. Projections can be identified with the closed subspaces of $\mathcal{H}$. In particular, as the range $Y_\mathbf{E} = \{\mathbf{E}x \mid x \in \mathcal{H}\}$ of an orthogonal projection is a closed subspace (cf. [6, Proposition II.3.2.b]), this correspondence is defined by associating to each projection on $\mathcal{H}$ its range $Y_\mathbf{E}$. The closed subspaces of $\mathcal{H}$ form a complete lattice under the operations of intersection and (closed linear span of) union. The one-to-one correspondence between this set and the collection $\mathcal{P}(\mathcal{H})$ of all orthogonal projections on $\mathcal{H}$ allows us to transfer the lattice structure of the set of all closed subspaces of $\mathcal{H}$ to $\mathcal{P}(\mathcal{H})$, thus turning the latter into a complete lattice.

A partial order on projections (and in general on self-adjoint operators) can be defined directly by: $\mathbf{E} \sqsubseteq \mathbf{F}$ iff $\mathbf{F} - \mathbf{E}$ is positive (e.g. [15, p105]). This is equivalent to the partial order defined via set inclusion on closed subspaces. More precisely, if $\mathbf{E}$ and $\mathbf{F}$ are projections from a Hilbert space $\mathcal{H}$ onto closed subspaces Y and Z respectively, then $\mathbf{E} \sqsubseteq \mathbf{F}$ iff $Y \subseteq Z$ (cf. [15, Proposition 2.5.2]).

The projections $\mathcal{P}(\mathcal{H})$ form a complete lattice with respect to this order, i.e. the least upper bound $\mathbf{E} \sqcup \mathbf{F}$ and the greatest lower bound $\mathbf{E} \sqcap \mathbf{F}$ always exist for any pair $\mathbf{E}$ and $\mathbf{F}$. The bottom element is given by the projection onto the null space, i.e. the operator mapping all vectors $x \in \mathcal{H}$ to the null vector, and the top element is the identity operator $\mathbf{I}$, i.e. the operator mapping each vector $x \in \mathcal{H}$ to itself. The concrete construction of $\mathbf{E} \sqcup \mathbf{F}$ and $\mathbf{E} \sqcap \mathbf{F}$ is in general not a trivial task. Only for commuting projections, i.e. $\mathbf{EF} = \mathbf{FE}$, we have (cf e.g. [15, Prop 2.5.3]):

$$\mathbf{E} \sqcup \mathbf{F} = \mathbf{E} + \mathbf{F} - \mathbf{EF} \text{ and } \mathbf{E} \sqcap \mathbf{F} = \mathbf{EF}.$$

A general way to construct $\mathbf{E} \sqcap \mathbf{F}$ (and by exploiting de Morgan's law also $\mathbf{E} \sqcup \mathbf{F}$) is via an infinite approximation sequence and has been suggested by Halmos [12, Problem 122]:

$$\mathbf{E} \sqcap \mathbf{F} = \lim_{n\to\infty} (\mathbf{EFE})^n.$$

For each projection $\mathbf{E}$, we can define an (ortho)complement $\mathbf{E}^\perp = \mathbf{I} - \mathbf{E}$; this corresponds to a projection into the closed subspace orthogonal to the image $Y_\mathbf{E}$

[3] A linear space is a Hilbert space if it has a scalar (or inner) product $\langle ., . \rangle$ and it is complete with respect to the norm generated by the scalar product.

[4] In operator theory and quantum physics "orthogonal" is often omitted, i.e. the term "projections" refers to "orthogonal projections".

of **E**. Thus, the orthogonal projection operators (and their corresponding closed subspaces of Hilbert spaces) form an *ortholattice* [2, Ex 10, II.10]. More precisely, $\mathcal{P}(\mathcal{H})$ is a complete orthomodular lattice [16, Proposition I.5.1].

Ortholattices can be seen as non-distributive analogs of Boolean algebras [2, I.10]. They are defined as follows (see e.g. [2, Def I.10] or [9, Def 2.1]):

Definition 2.1 An *ortholattice* $(L, \sqsubseteq, .^{\perp}, 0, 1)$ is a lattice $(L, \sqsubseteq)$ with universal bounds 0 and 1, i.e.

(i) $(L, \sqsubseteq)$ is a partial order (i.e. $\sqsubseteq$ is reflexive, antisymmetric, and transitive),

(ii) all pairs of elements $a, b \in L$ have a least upper bound or supremum, denoted by $a \sqcup b$, and a greatest lower bound or infimum, denoted by $a \sqcap b$,

(iii) $0 \sqsubseteq a$ and $a \sqsubseteq 1$ for all $a \in L$.

and a *complementation* operation $a \mapsto a^{\perp}$ satisfying:

(i) $a \sqcap a^{\perp} = 0$ and $a \sqcup a^{\perp} = 1$

(ii) $(a \sqcap b)^{\perp} = a^{\perp} \sqcup b^{\perp}$ and $(a \sqcup b)^{\perp} = a^{\perp} \sqcap b^{\perp}$

(iii) $(a^{\perp})^{\perp} = a$

In general $\sqcap$ and $\sqcup$ in an ortholattice are not distributive, in the sense that the relations

$$(a \sqcap b) \sqcup (a \sqcap c) \sqsubseteq a \sqcap (b \sqcup c) \text{ and } a \sqcup (b \sqcap c) \sqsubseteq (a \sqcup b) \sqcap (a \sqcup c)$$

are not in general equalities.

We say that two elements a and b in an ortholattice *commute*, denoted by $[a, b] = 0$, iff $a = (a \sqcap b) \sqcup (a \sqcap b^{\perp})$. An ortholattice is called an *orthomodular lattice* if $[a, b] = 0$ implies $[b, a] = 0$.

An important property of any ortholattice is given by the following proposition.

Proposition 2.2 ([2]) *In any ortholattice, $a \sqsubseteq b$ implies $[a, b] = 0$.*

In the ortholattice $\mathcal{P}(\mathcal{H})$ of orthogonal projections on a Hilbert space $\mathcal{H}$, two projections **E** and **F** commute, i.e. $\mathbf{EF} = \mathbf{FE}$, iff their associated closed subspaces commute (cf. [16, Lemma 4]). Thus, in this case $[Y_E, Y_F] = 0$ implies $[Y_F, Y_E] = 0$, and therefore $\mathcal{P}(\mathcal{H})$ is orthomodular.

2.2 Probabilistic Abstract Interpretation

Probabilistic Abstract Interpretation [11,10] is based on the notion of a categorical adjunction between Hilbert spaces defined by a bounded linear operator (representing the abstraction) and its Moore-Penrose pseudo-inverse (representing a concretisation operator). If $\mathcal{C}$ an $\mathcal{D}$ are two probabilistic domains, i.e. Hilbert spaces, and $\mathbf{A} : \mathcal{C} \to \mathcal{D}$ and $\mathbf{G} : \mathcal{D} \to \mathcal{C}$ are bounded linear operators between (the concrete domain) $\mathcal{C}$ and (the abstract domain) $\mathcal{D}$, such that $\mathbf{G}$ is the Moore-Penrose pseudo-inverse of $\mathbf{A}$, then we say that $(\mathcal{C}, \mathbf{A}, \mathcal{D}, \mathbf{G})$ forms a probabilistic abstract interpretation.

Definition 2.3 Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces and $\mathbf{A} : \mathcal{H}_1 \mapsto \mathcal{H}_2$ a bounded linear map between them. A bounded linear map $\mathbf{A}^\dagger = \mathbf{G} : \mathcal{H}_2 \mapsto \mathcal{H}_1$ is the *Moore-Penrose pseudo-inverse* of $\mathbf{A}$ iff

$$\mathbf{A} \circ \mathbf{G} = \mathbf{P}_\mathbf{A} \text{ and } \mathbf{G} \circ \mathbf{A} = \mathbf{P}_\mathbf{G},$$

where $\mathbf{P}_\mathbf{A}$ and $\mathbf{P}_\mathbf{G}$ denote orthogonal projections onto the ranges of $\mathbf{A}$ and $\mathbf{G}$.

Note that the multiplication of operators is usually denoted reversely to the corresponding function composition, i.e. $\mathbf{AB} = \mathbf{B} \circ \mathbf{A}$.

A necessary and sufficient condition for the existence of the Moore-Penrose pseudo-inverse for a bounded linear operator $\mathbf{A}$ on a Hilbert space $\mathcal{H}$ is that A is *normally solvable*, i.e. its range $\{\mathbf{A}x \mid x \in \mathcal{H}\}$ is closed [4, Thm 4.24]. All operators on a finite dimensional Hilbert space are Moore-Penrose invertible.

The properties of the Moore-Penrose pseudo-inverse (cf. e.g. [1]) guarantees a form of optimality of the abstractions constructed via PAI; in fact, they are the *closest* to the concrete semantics one can construct, where closeness is defined via the distance induced by the norm on the Hilbert space. As this is a numerical quantity, we can get an estimate of the information lost in the abstraction [11].

2.3 Ortholattice Structure of Probabilistic Abstract Interpretations

We can restrict w.l.o.g. to abstraction operators which are surjective, i.e. $\mathbf{A}(\mathcal{C}) = \mathcal{D}$. In fact, given a PAI $(\mathcal{C}, \mathbf{A}, \mathcal{D}, \mathbf{G})$, we can always partition the abstract domain $\mathcal{D}$ by identifying those elements with the same concrete meaning. In this way we can ensure that any abstract object in $\mathcal{D}$ is the image of a concrete object in $\mathcal{C}$, i.e. we reduce the abstract domain to one which does not contain redundant objects, or equivalently, we turn the abstraction operator $\mathbf{A}$ into a surjective one. In this case the closed subspace of $\mathcal{C}$ corresponding to the projection $\mathbf{G} \circ \mathbf{A} = \mathbf{P}_G$ is isomorphic to $\mathbf{A}(\mathcal{C})$; thus we can restrict ourselves to considering only probabilistic abstract interpretations of the form $(\mathcal{C}, \mathbf{P}_G, \mathbf{P}_G(\mathcal{C}), \mathbf{I})$. This will allow us to identify orthogonal projections on a Hilbert space $\mathcal{H}$ (or equivalently its closed subspaces) with all probabilistic abstract interpretations for the given concrete domain $\mathcal{H}$.

Proposition 2.4 *Let $\mathcal{H}$ be a Hilbert space and let $P \subseteq \mathcal{H}$ be a closed subspace of $\mathcal{H}$. Then $(\mathcal{H}, \mathbf{A}^\dagger \circ \mathbf{A}, P, \mathbf{I})$ is a PAI iff $\mathbf{A}^\dagger \circ \mathbf{A}(\mathcal{H}) = P$.*

Based on this identification, we can define the lattice of probabilistic abstract interpretations on a given Hilbert space $\mathcal{H}$ by means of the lattice of orthogonal projections introduced in Section 2.1. Since the projection $\mathbf{A}^\dagger \circ \mathbf{A}$ and the closed subspace of a Hilbert space $\mathcal{H}$ associated to it are uniquely determined by $\mathcal{H}$ and the abstraction operator $\mathbf{A}$ on $\mathcal{H}$, we can simply denote a probabilistic abstract interpretation by a pair $(\mathbf{A}, \mathcal{H})$ or its associated projection $\mathbf{A}^\dagger \circ \mathbf{A}$ on $\mathcal{H}$.

As already mentioned, the problem of constructing the least upper bound $\mathbf{E} \sqcup \mathbf{F}$ of two orthogonal projections $\mathbf{E}$ and $\mathbf{F}$ on $\mathcal{H}$ is in general considered as being not trivial. However, for commutative projections this can be constructed as $\mathbf{E} \sqcap \mathbf{F} = \mathbf{EF} = \mathbf{FE}$ and in the general case, using the Moore-Penrose pseudo-inverse, according to [1]:

$$\mathbf{E} \sqcap \mathbf{F} = 2\mathbf{E} : \mathbf{F} = 2\mathbf{E}(\mathbf{E} + \mathbf{F})^{\dagger}\mathbf{F}.$$

3 Probabilistic Abstraction and Quantum Measurement

The close relationship between probabilistic abstract interpretation and ortholattices — in effect the inherent logic of quantum physics [21,3] — allows us to develop a new interpretation and perhaps a better understanding of quantum physics, measurement and computation.

For a presentation of the basic model of quantum physics which goes back to von Neumann's work in the 1930 and which is based on a Hilbert space formulation see for example [14]. An arguably more elegant framework which generalises the Hilbert space based framework onto a C* algebraic level was developed in the 1950 [20,5]. We refer to [18,17] for an introduction to quantum computation and the common (notational) conventions.

One of the basic features of quantum physics is the fact that on the quantum level the state of a system is not directly accessible, instead the *observer* needs to perform a "measurement" on the quantum system in order to obtain information about the system. This measurement results in two effects: (i) the observer "measures" some value on his "instrument" and (ii) on the quantum level, the state is changed or "reduced" according to the result of the measurement. Which values can be observed and how the state might be reduced, depends on the *physical observable*. The postulates of quantum mechanics identify a physical observable $\mathbf{O}$ with a Hermitian or self-adjoint operator on the state space of the system being observed.

In general, even if there is no ambiguity about which state the system is in, it is left to chance which of several possible observations (together with the associate state reductions) will materialise. The probabilities of certain observations depend on the state observed and its relation to the intended observable $\mathbf{O}$ (see e.g. [14, p99] or [18, p88]):

(i) The value measured is an eigenvalue λ_m of $\mathbf{O}$

(ii) The probability for observing λ_m is $\langle x|\mathbf{P}_m x\rangle$ where $\mathbf{P}_m$ is a projection onto the eigenspace of $\mathbf{O}$ corresponding to λ_m.

(iii) The state $|x\rangle$ is reduced by projecting it onto the corresponding eigenspace $\frac{1}{\sqrt{\langle x|\mathbf{P}_m x\rangle}}\mathbf{P}_m\,|x\rangle$.

This formal model of quantum measurement, aka *projective measurement*[5], depends on the possibility of a spectral decomposition of observables, i.e. finite-dimensional self-adjoint operators (see e.g. [19, Thm 10.21] and for the general, infinite-dimensional case [15, Thm 5.2.2]).

Theorem 3.1 (Spectral Decomposition) *For a finite-dimensional self-adjoint*

[5] We are not concerned here with the more general notion of *POVM measurements* as in e.g. [18, 2.2.6].

operator $\mathbf{O}$*, the eigenvalues* λ_i *are real numbers and the projection operators* $\mathbf{P}_i$ *on the sub-spaces spanned by the eigenvectors corresponding to an eigenvalue* λ_i *are orthogonal and satisfy* $\sum_i \mathbf{P}_i = \mathbf{I}$ *and*

$$\mathbf{O} = \sum_i \lambda_i \mathbf{P}_i.$$

Considering the relation between the ortholattice of projections and the ortholattice of probabilistic abstract interpretations we can define observables out of PAI's:

Proposition 3.2 *Given a PAI* $(\mathbf{A}, \mathcal{H})$ *we can construct a corresponding physical observable* $\mathbf{O} = \lambda_\bullet \mathbf{A}\mathbf{A}^\dagger + \lambda_\circ(\mathbf{I} - \mathbf{A}\mathbf{A}^\dagger)$ *on* $\mathcal{H}$ *whose measurement in a state vector* $|x\rangle$ *returns either the value* $\lambda_\bullet$ *or the value* $\lambda_\circ$*.*

In this proposition we reverse the spectral decomposition in the sense that we take a projection $\mathbf{P} = \mathbf{A}\mathbf{A}^\dagger$ and construct its ortho-complement $\mathbf{P}^\perp = \mathbf{I} - \mathbf{P}$ such that $\mathbf{P} + \mathbf{P}^\perp = \mathbf{I}$. By choosing any real numbers $\lambda_\bullet$ and $\lambda_\circ$ as *measurement values* and constructing the linear combination of $\mathbf{P}$ and $\mathbf{P}^\perp$, we always end up with a self-adjoint operator, i.e. a physical observable.

The reverse of this construction is also possible; it is a simple consequence of the spectral decomposition theorem:

Proposition 3.3 *Given a physical observable* $\mathbf{O}$ *on* $\mathcal{H}$*, we can always define a set of PAI's* $(\mathbf{A}_i, \mathcal{H})$ *such that* $\mathbf{O} = \sum_i \lambda_i \mathbf{A}_i \mathbf{A}_i^\dagger$*, for some* $\lambda_i \in \mathbb{R}$*.*

From the spectral decomposition theorem we can always write a physical observable as a linear combination of projections. For projections we have $\mathbf{P} = \mathbf{P}^\dagger$; thus they can be seen directly as a PAI with $\mathbf{A} = \mathbf{G} = \mathbf{P}$ or $\mathbf{G} = \mathbf{I}|_{range(\mathbf{P})}$. However, this decomposition of projections into an abstraction $\mathbf{A}$ and concretisation $\mathbf{G}$, i.e. $\mathbf{P} = \mathbf{A}\mathbf{G}$, is not unique.

The decomposition of physical observables into PAI's also suggests a new philosophical interpretation of the measurement problem. A measurement can be interpreted as a probabilistic choice (depending on the state) among several different abstractions. This choice has two effects: (i) The measurement instrument indicates which measurement has happened (by displaying the corresponding measurement value, i.e. eigenvalue) and (ii) the state is abstracted accordingly and then again concretised (= projective reduction). The second effect could be seen as forcing the (world) state through the "eye of the needle" corresponding to the abstraction/concretisation pair representing the chosen abstraction.

4 Examples

In this section we demonstrate the results in the previous section by presenting examples of the translation of classical functions (and their properties) into a quantum computation setting and, vice versa, the classical interpretation of the measurement part of quantum algorithms.

4.1 Classical (Irreversible) Functions

Given a classical function $f : \{0, \dots , 2^n - 1\} \to \{0, \dots , 2^m - 1\}$ we first construct its representation as a unitary operator $\mathbf{U}_f$ on $m+n$ qubits such that $\mathbf{U}_f(|x\rangle\,|0\rangle) = |x\rangle\,|x \oplus f(x)\rangle$ with "$\oplus$" the bitwise sum operation, i.e. $x \oplus y = x + y \bmod 2$ (cf. e.g. [18]).

For example, for the classical (irreversible) function $f : \{0, \dots , 3\} \to \{0, 1\}$ defined below and represented by the matrix $\mathbf{F}$ such that $|x\rangle \cdot \mathbf{F} = |f(x)\rangle$, a (reversible) unitary representation is given by the operator $\mathbf{U}_f$

x	$f(x)$
0	1
1	0
2	0
3	1

$$\mathbf{F} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \mathbf{U}_f = \begin{bmatrix} 0&1&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{bmatrix}$$

Consider now the functions f_i represented by the following 8×4 matrices $\mathbf{F}_i$ (rows correspond to arguments $0, 1, \dots , 7$ and columns to results $0, 1, 2, 3$):

$$\mathbf{F}_1 = \begin{bmatrix} 0&1&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&1&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{bmatrix} \qquad \mathbf{F}_2 = \begin{bmatrix} 0&1&0&0 \\ 0&1&0&0 \\ 1&0&0&0 \\ 0&0&1&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 0&0&1&0 \\ 1&0&0&0 \end{bmatrix}$$

$$\mathbf{F}_3 = \begin{bmatrix} 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \\ 1&0&0&0 \end{bmatrix} \quad \mathbf{F}_4 = \begin{bmatrix} 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \end{bmatrix} \quad \mathbf{F}_5 = \begin{bmatrix} 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&0&0&1 \\ 0&0&0&1 \end{bmatrix}$$

The corresponding $\mathbf{U}_{f_i} = \mathbf{U}_i$ are 32×32 matrices which we will not explicitly write down as they would require a considerable amount of space.

We are interested in analysing the zero-ness of the functions f_i, that is the probability of getting a null value by applying f_i. A probabilistic abstraction corresponding to this property can be defined by the following matrix and its pseudo-inverse:

$$\mathbf{Z} = \begin{bmatrix} 1&0 \\ 0&1 \\ 0&1 \\ 0&1 \end{bmatrix} \quad \mathbf{Z}^\dagger = \begin{bmatrix} 1&0&0&0 \\ 0&\frac{1}{3}&\frac{1}{3}&\frac{1}{3} \end{bmatrix}.$$

The abstraction $\mathbf{Z}$ classifies the function outputs into "zero" and "non-zero" values. From this abstraction we can construct the projection

$$\mathbf{P}_Z = \mathbf{Z}\mathbf{Z}^\dagger = \begin{bmatrix} 1&0&0&0 \\ 0&\frac{1}{3}&\frac{1}{3}&\frac{1}{3} \\ 0&\frac{1}{3}&\frac{1}{3}&\frac{1}{3} \\ 0&\frac{1}{3}&\frac{1}{3}&\frac{1}{3} \end{bmatrix}$$

We now show that this corresponds to a physical observable for a quantum system associated to each $\mathbf{U}_i$.

We can construct a quantum circuit for $\mathbf{U}_i$ which starts with the 5 qubits input vector (i.e. a $32 = 2^5$ dimensional vector):

$$|x\rangle\,|0\rangle = |0\rangle\,|0\rangle\,|0\rangle\,|0\rangle\,|0\rangle\,.$$

To this we apply:

$$\mathbf{H} \otimes \mathbf{H} \otimes \mathbf{H} \otimes \mathbf{I} \otimes \mathbf{I}$$

where $\mathbf{H}$ is the Hadamard gate and $\mathbf{I}$ the identity, to get the superposition state:

$$\left(\frac{1}{\sqrt{8}} \sum_{i=0}^{7} |i\rangle\right) |0\rangle\,|0\rangle$$

Next we apply $\mathbf{U}_i$ to this vector in order to obtain

$$\frac{1}{\sqrt{8}}\sum_{i=0}^{7}|i\rangle\,|0 \oplus f(i)\rangle = \frac{1}{\sqrt{8}}\sum_{i=0}^{7}|i\rangle\,|f(i)\rangle$$

In short, the circuit corresponds to the unitary operator:

$$(\mathbf{H}\otimes\mathbf{H}\otimes\mathbf{H}\otimes\mathbf{I}\otimes\mathbf{I})\cdot\mathbf{U}_{f_i}.$$

We now apply the abstraction/measurement $\mathbf{P}_Z$ to the last two qubits register (we thus have to consider $\mathbf{I}\otimes\mathbf{I}\otimes\mathbf{I}\otimes\mathbf{P}_Z$ as our projection operator). Consider the output vector of the circuit for each of our functions f_i

$$|y_i\rangle = |0\rangle\,|0\rangle\,|0\rangle\,|0\rangle\,|0\rangle\cdot(\mathbf{H}\otimes\mathbf{H}\otimes\mathbf{H}\otimes\mathbf{I}\otimes\mathbf{I})\cdot\mathbf{U}_{f_i}.$$

In order to check their "zero-ness" we measure the physical observable:

$$\mathbf{A}_z = \lambda_Z\mathbf{P}_Z + \lambda_{Z^\perp}\mathbf{P}_Z^\perp = \lambda_Z\mathbf{P}_Z + \lambda_{Z^\perp}(\mathbf{I}-\mathbf{P}_Z)$$

with any two "measure values" λ_Z and $\lambda_{Z^\perp}$. We get the following probabilities of measuring λ_Z and $\lambda_{Z^\perp}$:

	$prob(\lambda_Z)$	$prob(\lambda_{Z^\perp})$
f_1	0.33333	0.66667
f_2	0.50000	0.50000
f_3	1.00000	0.00000
f_4	0.33333	0.66667
f_5	0.41667	0.58333

which we calculate as:

$$prob(\lambda_Z) = \langle y_i\mathbf{P}_Z|y_i\rangle \text{ and } prob(\lambda_{Z^\perp}) = \langle y_i(\mathbf{I}-\mathbf{P}_Z)|y_i\rangle\,.$$

As we only test for yes/no answers we have:

$$prob(\lambda_{Z^\perp}) = \langle y_i(\mathbf{I}-\mathbf{P}_Z)|y_i\rangle = \langle y_i|y_i\rangle - \langle y_i\mathbf{P}_Z|y_i\rangle = 1 - \langle y_i\mathbf{P}_Z|y_i\rangle\,.$$

As expected, these results show that the more often $f_i = 0$ holds the higher the probability that we measure λ_Z instead of $\lambda_{Z^\perp}$: In the case of the constant zero function $f_3 = 0$ this probability is 1.

4.2 The Deutsch Algorithm Revisited

The arguably best-known quantum algorithms are implemented essentially via a unitary transformation followed by a measurement in some appropriate base. Furthermore, they exploit various tricks to take advantage of the quantum parallelism and achieve a substantial speedup in comparison with corresponding classical algorithms.

By taking a semantic rather than a complexity theoretical viewpoint, we present a re-interpretation of the Deutsch algorithm which shows how these tricks can actually be seen as semantical abstractions aiming at "collecting" into an appropriate domain (base) the computational properties of interest.

We briefly recall the Deutsch problem and the quantum circuit for solving it. We consider here the case of a unary Boolean function, but the result can straightforwardly be generalised to the case of n-ary Boolean functions in the same way as the Deutsch algorithm can be generalised to the Deutsch-Jozsa algorithm (see e.g. [18]).

The problem solved by the Deutsch algorithm is to determine whether a function f is constant or balanced, where 'balanced' means that it returns 1 for half the domain and 0 for the other half. The quantum circuit implementing this algorithm takes two input qubits initialised to $|0\rangle$ and $|1\rangle$ respectively. It first applies Hadamard on the first qubit, forming all possible inputs; the second will be the answer qubit. Next, the circuit runs the operator $\mathbf{U}_f$ implementing the function (and given as a black box) once; this exclusive or's the result with the answer qubit. Finally, Hadamard is applied on the input qubit again, and the answer qubit is measured. If it is 0, the function is constant, otherwise the function is balanced.

Consider a function $f : \{0,1\} \rightarrow \{0,1\}$ and classify it either as constant – if $f(0) = f(1)$ – or balanced – if $f(0) \neq f(1)$. There are four possible pairs $(f(0), f(1)$ for a function f which we abstract into two classes c(onstant) and b(alanced). This abstraction from a four element concrete space $\{(0,0),(0,1),(1,0),(1,1)\}$ into a two element abstract space $\{c, b\}$ corresponds to a matrix $\mathbf{D}$ with its Moore-Penrose pseudo-inverse $\mathbf{D}^\dagger$ and the projection $\mathbf{P}_D = \mathbf{D}\mathbf{D}^\dagger$ given by:

$$\mathbf{D} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \mathbf{D}^\dagger = \begin{bmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \end{bmatrix} \qquad \mathbf{P}_D = \begin{bmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix}$$

Our aim is to show that $\mathbf{P}_D$ can be used to define a physical observable whose measurement is consistent with the final measurement in the Deutsch circuit. In fact, consider the physical observable

$$\mathbf{A} = \lambda_c \mathbf{P}_D + \lambda_b \mathbf{P}_D^\perp$$

and measure it on the output vector of the Deutsch circuit for the function f

$$|o_f\rangle = (|0\rangle\,|1\rangle) \cdot (\mathbf{H} \otimes \mathbf{H}) \cdot \mathbf{U}_f.$$

It turns out that we will get with probability one λ_c if the unknown function f is constant and λ_b in the case that f is a balanced function.

We can verify the result of this measurement on all four possible functions $f_i : \{0,1\} \rightarrow \{0,1\}$:

x	$f_1(x)$
0	1
1	1

$$\mathbf{F}_1 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \qquad \mathbf{U}_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

x	$f_2(x)$
0	0
1	1

$$\mathbf{F}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \mathbf{U}_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

x	$f_3(x)$
0	0
1	0

$$\mathbf{F}_3 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \qquad \mathbf{U}_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

x	$f_4(x)$
0	1
1	0

$$\mathbf{F}_4 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \mathbf{U}_4 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

We denote by o_i the output vector of the Deutsch circuit corresponding to f_i:

$$|o_i\rangle = (|0\rangle\,|1\rangle) \cdot (\mathbf{H} \otimes \mathbf{H}) \cdot \mathbf{U}_i$$

which in the concrete cases are given by:

$$|o_1\rangle = \left[\, -\tfrac{1}{2}\ \tfrac{1}{2}\ -\tfrac{1}{2}\ \tfrac{1}{2} \,\right]$$
$$|o_2\rangle = \left[\, \tfrac{1}{2}\ -\tfrac{1}{2}\ -\tfrac{1}{2}\ \tfrac{1}{2} \,\right]$$
$$|o_3\rangle = \left[\, \tfrac{1}{2}\ -\tfrac{1}{2}\ \tfrac{1}{2}\ -\tfrac{1}{2} \,\right]$$
$$|o_4\rangle = \left[\, -\tfrac{1}{2}\ \tfrac{1}{2}\ \tfrac{1}{2}\ -\tfrac{1}{2} \,\right]$$

If we compute the probabilities of obtaining λ_b and λ_c in the usual way we get:

$$\langle o_1 \mathbf{P}_D \mid o_1 \rangle = 0$$
$$\langle o_2 \mathbf{P}_D \mid o_2 \rangle = 1$$
$$\langle o_3 \mathbf{P}_D \mid o_3 \rangle = 0$$
$$\langle o_4 \mathbf{P}_D \mid o_4 \rangle = 1$$

which reflect the fact that f_1 and f_3 are indeed constant functions, while f_2 and f_4 are balanced.

Our presentation differs slightly from the usual presentation of the Deutsch circuit as:

$$(|0\rangle\,|1\rangle) \cdot (\mathbf{H} \otimes \mathbf{H}) \cdot \mathbf{U}_i \cdot (\mathbf{H} \otimes \mathbf{I})$$

In the notation of [18, p33] we measure $|\psi_3\rangle = (|0\rangle\,|1\rangle) \cdot (\mathbf{H} \otimes \mathbf{H}) \cdot \mathbf{U}_i$ instead of

$|\psi_4\rangle = (|0\rangle\,|1\rangle)\cdot(\mathbf{H}\otimes\mathbf{H})\cdot\mathbf{U}_i\cdot(\mathbf{H}\otimes\mathbf{I})$. The reason for this is that our measurement is with respect to a non-standard base given by the eigenvectors of $\mathbf{P}_D$:

$$|d_1\rangle = \left[\,0\ -\tfrac{1}{\sqrt{2}}\ \tfrac{1}{\sqrt{2}}\ 0\,\right]$$
$$|d_2\rangle = \left[\,\tfrac{1}{\sqrt{2}}\ 0\ 0\ -\tfrac{1}{\sqrt{2}}\,\right]$$
$$|d_3\rangle = \left[\,\tfrac{1}{\sqrt{2}}\ 0\ 0\ \tfrac{1}{\sqrt{2}}\,\right]$$
$$|d_4\rangle = \left[\,0\ \tfrac{1}{\sqrt{2}}\ \tfrac{1}{\sqrt{2}}\ 0\,\right]$$

and not $|0\rangle\,|0\rangle$, $|0\rangle\,|1\rangle$, $|1\rangle\,|0\rangle$, $|1\rangle\,|1\rangle$. The last Hadamard gate, i.e. $\mathbf{H}\otimes\mathbf{I}$ in the original Deutsch circuit has exactly the purpose of transforming $|\phi_3\rangle$ into the standard base.

5 Conclusion

In this paper we identified a close link between the logic of quantum measurements and probabilistic abstract interpretation. This is based on a re-interpretation of an abstraction $\mathbf{A}$ on a probabilistic domain $\mathcal{H}$ via the orthogonal projection $\mathbf{A}\mathbf{A}^\dagger$ on $\mathcal{H}$, where $\mathbf{A}^\dagger$ is a generalised inverse of $\mathbf{A}$.

The set of projections on a Hilbert space $\mathcal{H}$ (e.g. any finite dimensional vector space) is naturally equipped with two distinct structures: it is a subset of the algebra of bounded linear operators, and it carries a lattice structure which reflects the inclusion ordering among closed subspaces of $\mathcal{H}$. This means that we can use both algebraic operations (scalar product, vector addition and algebra product) and logical operations (intersection and union) in order to construct "new" projections from old ones.

Probabilistic abstract interpretations inherit both the linear algebra and the orthomodular structure of the set of projections on a Hilbert space. While the logical structure provides the theoretical basis for combining program analyses and for various refinement techniques in the classical and probabilistic programming languages setting, the algebraic structure allows us to define linear combinations of PAI's which correspond to "truly randomised" abstractions and cannot be formulated within the framework of classical abstract interpretation. These are at the base of a new philosophical interpretation of the measurement problem as the problem of probabilistically choosing among several properties (abstractions) to be observed.

We aim to investigate the relation between the lattice and algebraic structure of PAI's further. This will require in particular a more detailed study of the non-commutative situation, a better understanding of the vector lattice or Riesz space of positive operators which can be obtained by linear combination of projection operators, and the role of spectral theorems in decomposing (positive) operators into linear combinations of projections.

Such investigations may lead to new approaches to (measurement based) quantum computation; we will explore in particular the possibility of developing declarative-like quantum programming languages whose operational semantics exploits the idea of an incremental construction of observables starting from a set of possible, i.e. physically implementable, measurements. It appears that only algebraic operations are physically realisable but that logical combinations are conceptually easier to understand. It would therefore be important to understand how to bridge the gap in the non-commutative case, e.g. how to "compensate" for the difference between $\mathbf{P} \cap \mathbf{Q}$ and $\mathbf{PQ}$ in general and in particular cases.

References

[1] A. Ben-Israel and T.N.E. Greville. *Generalised Inverses — Theory and Applications*, volume 15 of *CMS Books in Mathematics*. Springer Verlag, New York, Berlin, second edition, 2003.

[2] G. Birkhoff. *Lattice Theory*, volume 25 of *Colloquium Publications*. American Mathematical Society, Providence, Rhode Island, second (revised) edition, 1948.

[3] G. Birkhoff and J. von Neumann. The logic of quantum mechanics. *Annals of Mathematics*, 37:823–843, 1936. in [13].

[4] A. Böttcher and B. Silbermann. *Introduction to Large Truncated Toeplitz Matrices*. Springer Verlag, New York, 1999.

[5] O. Bratteli and D.W. Robinson. *Operator Algebras and Quantum Statistical Mechanics*, volume 1 & 2. Springer Verlag, New York, Heidelberg, Berlin, 1979/81.

[6] J. Conway. *A Course in Functional Analysis*, volume 96 of *Graduate Texts in Mathematics*. Springer Verlag, second edition, 1990.

[7] P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proceedings of POPL'77*, pages 238–252, Los Angeles, 1977.

[8] P. Cousot and R. Cousot. Systematic design of program analysis frameworks. In *Proceedings of POPL'79*, pages 269–282, San Antonio, Texas, 1979.

[9] M.L. Della Chiara and R. Giuntini. Quantum logics. Technical Report, arXiv:quant-ph/0101028, January 2001. v2.

[10] A. Di Pierro and H. Wiklicky. Concurrent constraint programming: towards probabilistic abstract interpretation. In *Proceedings of PPDP'00*, pages 127–138. ACM, 2000.

[11] A. Di Pierro and H. Wiklicky. Measuring the precision of abstract interpretations. In *Proceedings of LOPSTR'00*, volume 2042 of *Lecture Notes in Computer Science*, pages 147–164. Springer Verlag, 2001.

[12] P.R. Halmos. *A Hilbert Space Problem Book*, volume 19 of *Graduate Texts in Mathematics*. Springer Verlag, Berlin, Heidelberg, New York, second edition, 1982.

[13] C.A. Hooker, editor. *The Logico-Algebraic Approach to Quantum Mechanics*, volume I: Historical Evolution. Reidel, Dordrecht, Boston, 1975.

[14] C.J. Isham. *Lectures on Quantum Theory*. Imperial College Press, 1995.

[15] R.V. Kadison and J.R. Ringrose. *Fundamentals of the Theory of Operator Algebras: Elementary Theory*, volume 15 of *Graduate Studies in Mathematics*. AMS, 1997. Reprint from Academic Press edition 1983.

[16] G. Kalmbach. *Orthomodular Lattices*. Academic Press, London, 1983.

[17] S.J. Lomonaco, editor. *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, volume 58 of *Proceedings of Symposia in Applied Mathematics*. AMS, Providence, Rhode Island, 2002.

[18] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[19] S. Roman. *Advanced Linear Algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer Verlag, second edition, 2005.

[20] W Thirring. *Quantum Mathematical Physics*. Springer, Berlin, Heidelberg, second edition, 2002.

[21] V.S. Varadarajan. *Geometry of Quantum Theory*, volume I. Van Nostrand, Princeton, 1968.