

Reasoning about faulty quantum programs

Paolo Zuliani
Computer Science Department
Carnegie Mellon University
Pittsburgh, PA 15213, USA
pzuliani@cs.cmu.edu

Abstract

We show how to use a programming language for formally describing and reasoning about errors in quantum computation. The formalisation is based on the concept of performing the correct operation with probability at least p , and the erroneous one with probability at most $1-p$. We apply the concept to two examples: Bell's inequalities and the Deutsch-Jozsa quantum algorithm. The former is a fundamental thought experiment aimed at showing that Quantum Mechanics is not "local and realist", and it is used in quantum cryptography protocols. We study it assuming faulty measurements, and we derive hardware reliability conditions that must be satisfied in order for the experiment to support its conclusions. The latter is a quantum algorithm for efficiently solving a classification problem for Boolean functions. The algorithm solves the problem with no error, but when we introduce faulty operations it becomes a two-sided error algorithm. Reasoning is accomplished via standard programming laws and quantum laws.

1 Introduction

In this paper we use the quantum programming language qGCL for reasoning about errors in quantum computation. The effects of faulty hardware on computation is an inherently important topic, which is even more important for quantum computation. As a matter of fact, the speed-up promised by quantum computers can be realised only by relatively error-free components. The presence of noise (via interaction with the environment) translates into errors for the quantum computer, which thus deviates from its proposed task. The fundamental threshold theorem for quantum computation states

that if the error rate is below a certain threshold, it is possible to carry out successfully an arbitrarily long quantum computation (by using suitable quantum error-correcting codes; see Chapter 10 of [15]). Therefore, from a theoretical point of view quantum computers are realisable. However, inadequacy of current technology severely limits the demonstration of feasibility of quantum computing.

qGCL [17] was developed as a superset of the *probabilistic* guarded-command language pGCL [14]. One of the most important features of pGCL is its treatment of both probabilistic choice and demonic choice, which is the basis for our work. Other quantum programming languages, such as Selinger’s QPL [18] or Altenkirch and Grattage’s QML [2], do not offer demonic choice (probabilistic choice is implicitly offered in the quantum model). For a survey of other quantum programming languages see [10].

A quantum computation is usually composed of initialisation followed by evolution and finally by finalisation. In this work we provide a simple model for faulty initialisation and finalisation (a model for error propagation in evolution is being investigated, and it is sketched in Section 6). The formalisation is based on the concept of performing the correct operation with probability *at least* p , and the erroneous one with probability *at most* $1 - p$. The technical foundation is provided by the combined treatment of probabilistic choice and demonic choice in pGCL. This enables a rigorous formalisation to be given of the error model.

We apply the concept to two examples: Bell’s inequalities and the Deutsch-Jozsa quantum algorithm. The former is a fundamental thought experiment aimed at showing that Quantum Mechanics cannot be “local and realist”, like Classical Mechanics. By local it is meant that any physical system cannot influence another at a speed greater than the speed of light. Realist means that any physical property of a system is well-determined at any one time, and in particular it does not depend on other, distant, systems. As known, Bell [4] devised a thought experiment and derived from it a set of inequalities which are true in any local and realist theory, but *fail* within Quantum Mechanics. Experiments performed by Aspect *et al.* [3] confirmed the violation of Bell inequalities, in the way predicted by quantum theory. Ekert [8] used the violation of Bell inequalities to detect eavesdropping in a quantum key-distribution protocol (in such a protocol keys are securely distributed between two partners, and then used as one-time pads). An implementation of Ekert’s protocol has been successfully tested over a freespace distance of 144km [19]. Recently, physicists have been able to transmit entangled photon pairs over the same distance [9], showing that multi-photons protocols (*e.g.*, quantum dense coding [5]) are also feasible over freespace

channels. We study Bell’s thought experiment assuming faulty measurements, and we derive hardware reliability conditions that must be satisfied in order for the experiment to violate the inequalities.

The Deutsch-Jozsa quantum algorithm [7] is one of the few known quantum algorithms and efficiently solves a classification problem: given a Boolean function f which is “promised” to be either constant or balanced, find which holds. A classical algorithm must evaluate f an exponential number of times in the worst case, while the Deutsch-Jozsa algorithm always needs only a *single* evaluation. The quantum algorithm solves the problem with no error, but when we introduce faulty operations it becomes a two-sided error algorithm. We also derive a lower bound on the probability that it replies correctly.

The aim of this work is not to provide a detailed model of faulty quantum computation, such as the superoperator quantum circuits of Aharonov *et al.* [1]. That is a very important approach useful for performing precise calculations about errors. We instead aim at giving a higher-level description which, while being more abstract, is nonetheless rigorous, allow mixing quantum and classical code, and makes use of programming laws (thus possibly looking more familiar to computer scientists).

2 Quantum programming

2.1 Quantum types

We define the type $\mathbf{B} \hat{=} \{0, 1\}$, which we will treat as Booleans or bits, depending on convenience. A classical register of size $n: \mathbf{N}^+$ is a vector of n Booleans. The type of all registers of size n is then defined to be the set of Boolean-valued functions on $\{0, 1, \dots, n - 1\}$, *i.e.* $\mathbf{B}^n \hat{=} [n] \longrightarrow \mathbf{B}$. The quantum analogue of \mathbf{B}^n is the set of complex-valued functions on \mathbf{B}^n whose squared modulus sum to 1:

$$q(\mathbf{B}^n) \hat{=} \{\chi: \mathbf{B}^n \longrightarrow \mathbf{C} \mid \sum_{x: \mathbf{B}^n} |\chi(x)|^2 = 1\}.$$

An element of $q(\mathbf{B})$ is called a *qubit* and that of $q(\mathbf{B}^n)$ a *qureg*. Classical state is embedded in its quantum analogue by the Dirac delta function:

$$\begin{aligned} \delta: \mathbf{B}^n &\longrightarrow q(\mathbf{B}^n) \\ \delta_x(y) &\hat{=} (y = x). \end{aligned}$$

The range of δ , $\{\delta_x \mid x:\mathbf{B}^n\}$, forms a *basis* for quantum states, that is:

$$\forall \chi \in q(\mathbf{B}^n) \quad \chi = \sum_{x:\mathbf{B}^n} \chi(x)\delta_x.$$

The Hilbert space $\mathbf{B}^n \longrightarrow \mathbf{C}$ (with the structure making it isomorphic to \mathbf{C}^{2^n}) is called the *enveloping space* of $q(\mathbf{B}^n)$. The usual scalar product becomes the application $\langle \cdot, \cdot \rangle : q(\mathbf{B}^n) \times q(\mathbf{B}^n) \rightarrow \mathbf{C}$ defined by:

$$\langle \psi, \phi \rangle \hat{=} \sum_{x:\mathbf{B}^n} \psi(x)^* \phi(x)$$

where z^* is the complex conjugate of $z:\mathbf{C}$. The *length* of ψ is defined $\|\psi\| \hat{=} \langle \psi, \psi \rangle^{\frac{1}{2}}$.

In standard computation we can describe the state space of a program having multiple component variables as the Cartesian product of the single components. In quantum computation the analogue construction is represented by the *tensor product* of the components. The tensor product of (standard) registers is defined

$$\begin{aligned} \otimes : \mathbf{B}^m \times \mathbf{B}^n &\rightarrow \mathbf{B}^{m+n} \\ (x \otimes y)(i) &\hat{=} x(i \operatorname{div} n) \cdot y(i \operatorname{mod} n) \end{aligned}$$

and readily shown to be surjective. That definition lifts, via δ and linearity, to quantum registers

$$\otimes : q(\mathbf{B}^m) \times q(\mathbf{B}^n) \rightarrow q(\mathbf{B}^{m+n}).$$

For sets E and F of quregs we write

$$E \otimes F \hat{=} \{\chi \otimes \xi \mid \chi \in E \wedge \xi \in F\}.$$

The following isomorphism is easy to prove

$$q(\mathbf{B}^m \times \mathbf{B}^n) \cong q(\mathbf{B}^m) \otimes q(\mathbf{B}^n).$$

In order to simplify notation, we shall not write the tensor symbol for the elements of the standard basis $\{\delta_x \mid x:\mathbf{B}^n\}$. For example, in $q(\mathbf{B}^2)$ we shall write δ_{01} for $\delta_0 \otimes \delta_1$.

Next tensor product of functions on registers is defined

$$\begin{aligned} \otimes : (\mathbf{B}^m \rightarrow \mathbf{B}^m) \times (\mathbf{B}^n \rightarrow \mathbf{B}^n) &\rightarrow (\mathbf{B}^{m+n} \rightarrow \mathbf{B}^{m+n}) \\ (A \otimes B)(x \otimes y) &\hat{=} A(x) \otimes B(y). \end{aligned}$$

Finally \otimes is extended by linearity to functions on quantum registers, for which we follow tradition and use the same symbol yet again

$$\otimes : q(\mathbf{B}^m \rightarrow \mathbf{B}^m) \times q(\mathbf{B}^n \rightarrow \mathbf{B}^n) \rightarrow q(\mathbf{B}^{m+n} \rightarrow \mathbf{B}^{m+n}).$$

More facts on the tensor product are provided in Appendix C.

2.2 Quantum language qGCL

qGCL is an extension of pGCL [14], which in turn extends Dijkstra's guarded-command language with a probabilistic choice constructor in order to address probabilism. The syntax of pGCL (without iteration) is:

$$\begin{aligned} prg \hat{=} & \text{ skip } | \text{ abort } | x := e | prg ; prg | \text{ if } \square b_i \rightarrow prg_i \text{ fi } | prg \sqcap prg \\ & | \text{ var } v:D \bullet prg \text{ rav } | prg \oplus_p prg \end{aligned}$$

The probabilistic combinator \oplus_p executes its LHS (RHS) with probability p (\bar{p}). For probability p we define $\bar{p} \hat{=} 1 - p$. Both probabilistic and non-deterministic choice may be written using a prefix notation. Let $\{(P_j, r_j)\}$ for $j \in [m]$ be a finite indexed family of (program, number) pairs with $\sum r_j = 1$, then the probabilistic choice in which P_j is chosen with probability r_j is written in prefix form: $[P_j @ r_j \mid j \in [m]]$. For nondeterministic choice the notation is similar. Semantics for pGCL can be given in terms of expectation-transformers, which is a generalisation of the usual predicate-transformer semantics (see Appendix B for more details).

A *quantum program* is a pGCL program invoking quantum procedures and the resulting language is called qGCL. Quantum procedures can be of three different kinds: *Initialisation* (or state preparation) followed by *Evolution* and finally by *Finalisation* (or observation).

Initialisation prepares a qureg for further computation, via a simple assignment: e.g. $\chi := \frac{1}{\sqrt{2}}(\delta_{00} - \delta_{11})$, where $\chi:q(\mathbf{B}^2)$.

Quantum-mechanical systems evolve over time under the action of *unitary* transformations:

$$\begin{aligned} U:q(\mathbf{B}^n) & \rightarrow q(\mathbf{B}^n), \text{ linear} \\ U \text{ unitary} & \text{ iff } \|U\psi\| = \|\psi\| \text{ iff } UU^\dagger = U^\dagger U = I \end{aligned}$$

where I is the identity transform and U^\dagger is the conjugate transpose of U (in matrix representation). *Evolution* consists of iteration of unitary transformations on quantum state. In our formalism, evolution of qureg χ under unitary operator U is described by the assignment:

$$\chi := U\chi.$$

The content of a qureg can be read (measured) through quantum procedure *Finalisation* and suitable *observables*. In general, an observable is represented by a self-adjoint operator and the measurable values are exactly the eigenvalues of that operator (we recall that the eigenvalues of a self-adjoint operator are real numbers). By the well-known spectral theorem the

eigenspaces of a self-adjoint operator are pairwise orthogonal and complete in the enveloping space. The axioms of quantum mechanics assert that the measurement reduces the state vector $\chi:q(\mathbf{B}^n)$ to state $\frac{P_i\chi}{\|P_i\chi\|}$ with probability $\langle\chi, P_i\chi\rangle$, where P_i is the projector over the eigenspace corresponding to eigenvalue i . In our notation we write $\mathbf{Fin}(\mathcal{O}, r, \chi)$ for the measurement of \mathcal{O} on a quantum system described by state $\chi:q(\mathbf{B}^n)$; r holds the return eigenvalue. Finalisation is therefore defined

Definition 2.1.

$$\mathbf{Fin}(\mathcal{O}, r, \chi) \hat{=} \left[\left(r, \chi := i, \frac{P_i\chi}{\|P_i\chi\|} \right) @ \langle\chi, P_i\chi\rangle \mid i \in \Lambda_{\mathcal{O}} \right]$$

where $\Lambda_{\mathcal{O}}$ is the set of eigenvalues of \mathcal{O} .

An observable is said *degenerate* when at least one of its eigenspaces has dimension greater than one - *i.e.* the associated eigenvalue is degenerate in the usual sense.

2.3 Probabilistic and demonic nondeterminism

In pGCL refinement $P \sqsubseteq Q$ means that Q is at least as deterministic as P :

$$P \sqsubseteq Q \quad \text{iff} \quad P \sqcap Q = P \tag{1}$$

In pGCL (demonic) nondeterminism is expressed semantically as the combination of all possible probabilistic resolutions

$$P \sqcap Q = \sqcap \{ P \text{ }_r\oplus Q \mid 0 \leq r \leq 1 \}. \tag{2}$$

Thus a (demonic) nondeterministic choice between two programs is refined by any probabilistic choice between them

$$\forall r \in [0, 1] \quad P \sqcap Q \sqsubseteq P \text{ }_r\oplus Q. \tag{3}$$

We introduce an important notation which we use in the paper: $P \geq_r \oplus Q$ is equal to P with probability *at least* r and otherwise is equal to Q .

Definition 2.2. For any $r \in [0, 1]$

$$P \geq_r \oplus Q \hat{=} \sqcap \{ P \text{ }_p\oplus Q \mid r \leq p \leq 1 \}$$

It can be proved that $P \geq_r \oplus Q = (P \text{ }_r\oplus Q) \sqcap P$.

3 Faulty measurement

In this section we study the situation in which the quantum measurement devices are faulty. In our formalism, a measurement device being faulty means that procedure **Fin** deviates from standard Definition 2.1. We restrict our model to *nondegenerate* observables.

We start by defining the worst measurement: it is the nondeterministic choice among all possible outcomes and final states. The possible outcomes form a finite set, so a nondeterministic choice (assignment) among them is readily defined. The state after finalisation is instead a vector belonging to some eigenspace, thus an infinite set. An unbounded nondeterministic assignment does not semantically correspond to any pGCL code, so it cannot be defined. However, the axioms of Quantum Mechanics come to help. Let \mathcal{O} be a nondegenerate observable, λ an eigenvalue and μ an associated (normalised) eigenvector. Since \mathcal{O} is nondegenerate, the eigenspace associated to λ is unidimensional, thus spanned by μ . If we measure \mathcal{O} in state v we know that the final state is (see Definition 2.1):

$$\frac{P_\lambda v}{\|P_\lambda v\|} = \frac{\mu \langle \mu, v \rangle}{\|\mu \langle \mu, v \rangle\|} = \frac{\mu \langle \mu, v \rangle}{|\langle \mu, v \rangle| \|\mu\|} = \frac{\mu \langle \mu, v \rangle}{|\langle \mu, v \rangle|}.$$

But $\frac{\langle \mu, v \rangle}{|\langle \mu, v \rangle|}$ is a complex number of modulus 1, and Quantum Mechanics tells us that when we multiply a vector by an arbitrary complex number of modulus 1 we obtain an “equivalent” vector. That is, there is no measurement that could distinguish between the two states so, for all practical purposes they represent the same state (see (9) in Appendix C). Therefore, the final state is just μ , independent from v . Of course the choice of μ is arbitrary but again, any other normalised λ -eigenvector is a multiple of μ , thus indistinguishable from it. Finally, we know that by the spectral theorem we can always find an orthonormal basis made of eigenvectors.

We can now define the worst measurement.

Definition 3.1. For nondegenerate observable \mathcal{O} over qureg χ , the worst (most nondeterministic) measurement is

$$\mathbf{Fin}_\square(\mathcal{O}, r, \chi) \hat{=} \square [r, \chi := i, \mu_i \mid i \in \Lambda_{\mathcal{O}}]$$

where $\Lambda_{\mathcal{O}}$ is the set of eigenvalues of \mathcal{O} and μ_i the (normalised) eigenvector associated to eigenvalue i .

The faulty measurement is defined as follows.

Definition 3.2. For any $c \in [0, 1]$ and nondegenerate observable \mathcal{O} , the faulty measurement is

$$\mathbf{Fin}_c(\mathcal{O}, r, \chi) \hat{=} \mathbf{Fin}(\mathcal{O}, r, \chi) \underset{c}{\oplus} \mathbf{Fin}_\square(\mathcal{O}, r, \chi).$$

Because nondeterministic choice is refined by any probabilistic choice, we have that the standard measurement \mathbf{Fin} refines the worst measurement \mathbf{Fin}_\square , as we now show. In order to simplify notation, we omit signatures when equal (although we shall write them when needed in proofs).

Lemma 3.1. *For any nondegenerate observable*

$$\mathbf{Fin}_\square \sqsubseteq \mathbf{Fin}$$

Proof. We reason:

$$\begin{aligned} & \mathbf{Fin}(\mathcal{O}, r, \chi) \\ &= && \text{definition of } \mathbf{Fin} \\ & \left[\left(r, \chi := i, \frac{P_i \chi}{\|P_i \chi\|} \right) @ \langle \chi, P_i \chi \rangle \mid i \in \Lambda_{\mathcal{O}} \right] \\ &= && \text{definition of projector} \\ & \left[\left(r, \chi := i, \frac{\mu_i \langle \mu_i, \chi \rangle}{\|\mu_i \langle \mu_i, \chi \rangle\|} \right) @ \langle \chi, P_i \chi \rangle \mid i \in \Lambda_{\mathcal{O}} \right] \\ &= && \mu_i \text{ normalised, } \frac{\langle \mu_i, \chi \rangle}{\|\mu_i \langle \mu_i, \chi \rangle\|} \text{ has modulus 1} \\ & \left[(r, \chi := i, \mu_i) @ \langle \chi, P_i \chi \rangle \mid i \in \Lambda_{\mathcal{O}} \right] \\ & \sqsupseteq && \underset{p}{\oplus} \text{ refines } \square \text{ (3), def of } \mathbf{Fin}_\square \\ & \mathbf{Fin}_\square(\mathcal{O}, r, \chi) \end{aligned}$$

□

By Lemma 3.1 and law P-1 we immediately have

Corollary 3.2. *For any $c \in [0, 1]$ and nondegenerate observable*

$$\mathbf{Fin}_c \sqsubseteq \mathbf{Fin}.$$

The use of the “approximate” probabilistic choice $\underset{c}{\geq} \oplus$ does not give a different definition of faulty measurement.

Theorem 3.3. *For any $c \in [0, 1]$ and nondegenerate observable*

$$\mathbf{Fin}_c = \mathbf{Fin} \underset{\geq c}{\oplus} \mathbf{Fin}_\square$$

Proof. We reason from the right-hand side:

$$\begin{aligned}
& \mathbf{Fin}_{\geq c} \oplus \mathbf{Fin}_{\sqcap} \\
& = && \text{definition of } \geq c \oplus \\
& (\mathbf{Fin}_c \oplus \mathbf{Fin}_{\sqcap}) \sqcap \mathbf{Fin}_{\sqcap} \\
& = && \sqcap \text{ commutative (law N-1) and law P-2} \\
& \mathbf{Fin}_{\sqcap} \sqcap (\mathbf{Fin}_{\sqcap} \oplus \mathbf{Fin}) \\
& = && \text{laws P-3 and P-2} \\
& \mathbf{Fin}_c \oplus (\mathbf{Fin}_{\sqcap} \sqcap \mathbf{Fin}_{\sqcap}) \\
& = && \text{Lemma 3.1 and (1)} \\
& \mathbf{Fin}_c \oplus \mathbf{Fin}_{\sqcap} \\
& = && \text{definition of } \mathbf{Fin}_c \\
& \mathbf{Fin}_c
\end{aligned}$$

□

We now present a few laws regarding the sequential composition of measurements.

Laws for measurements

$$\begin{aligned}
\mathbf{Fin} \circledast \mathbf{Fin} &= \mathbf{Fin} \\
\mathbf{Fin}_{\sqcap} \circledast \mathbf{Fin}_{\sqcap} &= \mathbf{Fin}_{\sqcap} \\
\mathbf{Fin} \circledast \mathbf{Fin}_{\sqcap} &= \mathbf{Fin}_{\sqcap} \\
\mathbf{Fin}_{\sqcap} \circledast \mathbf{Fin} &= \mathbf{Fin}_{\sqcap} \\
\mathbf{Fin}_c \circledast \mathbf{Fin}_c &= \mathbf{Fin}_{c^2}
\end{aligned}$$

From the first two laws we gather that \mathbf{Fin} and \mathbf{Fin}_{\sqcap} are idempotent; the next two laws express the fact that \mathbf{Fin}_{\sqcap} is both right and left zero for \mathbf{Fin} . The last law tells us that performing twice the same faulty measurement will decrease quadratically our chance to see the correct result. Proofs of the above laws can be found in Appendix A.

We observe that from the third and fourth law we get that $\mathbf{Fin}_{\sqcap} \circledast \mathbf{Fin} = \mathbf{Fin} \circledast \mathbf{Fin}_{\sqcap}$. This expresses some interesting behaviour of the combination of probabilistic and nondeterministic choice in this particular setting. In

general, it is known that

$$prg_1 \wp (prg_2 \text{ } r\oplus prg_3) \quad \sqsupseteq \quad (prg_1 \wp prg_2) \text{ } r\oplus (prg_1 \wp prg_3)$$

for (possibly nondeterministic) programs prg_1 , prg_2 , and prg_3 . In particular, equality between RHS and LHS is ruled out by the following simple example. Consider the two programs

$$\begin{aligned} P &\hat{=} (x := 0 \text{ } \frac{1}{2}\oplus x := 1) \wp y := 0 \sqcap y := 1 \\ Q &\hat{=} (y := 0 \sqcap y := 1) \wp x := 0 \text{ } \frac{1}{2}\oplus x := 1 . \end{aligned}$$

By using pGCL semantics with post-expectation $[x = y]$ (see Appendix B) we can show that program Q guarantees $x = y$ with probability at least $\frac{1}{2}$, while P cannot guarantee $x = y$ at all. This implies that $P \neq Q$, and that nondeterministic choice does not in general commute with probabilistic choice.

3.1 A simplified model

For our application we shall not need to perform further quantum evolutions after a measurement, so we define a variant of finalisation in which quantum state is left untouched. As a matter of fact, the principal quantum algorithms (*i.e.* Grover's, Deutsch-Jozsa's and Shor's) do not perform any unitary evolution after a finalisation, so update of the quantum state is irrelevant. Furthermore, the quantum circuit model assumes that there is only one measurement, at the end of the unitary evolution. This assumption is grounded in the *Principle of Deferred Measurement*, which states that all measurements can be moved at the end of a quantum computation, without affecting the output distribution [15, Section 4.4]. We therefore have the following definition.

Definition 3.3. For observable \mathcal{O} we define standard measurement as

$$\mathbf{fin}(\mathcal{O}, r, \chi) \hat{=} [r := i \text{ } @ \langle \chi, P_i \chi \rangle \mid i \in \Lambda_{\mathcal{O}}] .$$

We observe that Definition 3.3 is a special case of the well-known POVM formalism [15, Section 2.2.6], where the measurement operators are simply projectors. Our next definition does not have a counterpart in Quantum Mechanics, yet.

For any finite set S we write $s:S$ for $\sqcap [s := i \mid i \in S]$. The worst measurement simply returns any eigenvalue via demonic choice, and a faulty measurement is then defined as following.

Definition 3.4. For any $c \in [0, 1]$ and observable \mathcal{O} , the faulty measurement is

$$\mathbf{fn}_c(\mathcal{O}, r, \chi) \hat{=} \mathbf{fn}(\mathcal{O}, r, \chi) \text{ }_c\oplus \text{ } r:\Lambda_{\mathcal{O}} .$$

We have that \mathbf{fn}_c executes \mathbf{fn} (the correct behaviour) with probability c , and nondeterministically chooses any result with probability \bar{c} . Note that the definition is for any (possibly degenerate) observable. We implicitly assumed that the finalisation always returns an answer: for example, when a particle is fired towards a detector, that particle is always detected and the measured value returned. We do not consider here the case in which the detector does not detect anything at all.

Though simple, Definition 3.4 abstracts a large class of probabilistic faulty measurements.

Lemma 3.4. For any $c \in [0, 1]$

$$\mathbf{fn}_c(\mathcal{O}, r, \chi) = \mathbf{fn}(\mathcal{O}, r, \chi) \text{ }_{\geq c}\oplus \text{ } r:\Lambda_{\mathcal{O}} .$$

Proof. We first note that since a nondeterministic choice is refined by any probabilistic choice (see (3)), we have that $r:\Lambda_{\mathcal{O}} \sqsubseteq \mathbf{fn}(\mathcal{O}, r, \chi)$. The proof now follows the same steps of that of theorem 3.3, except that instead of lemma 3.1 we use the fact $r:\Lambda_{\mathcal{O}} \sqsubseteq \mathbf{fn}(\mathcal{O}, r, \chi)$. \square

Also, if $\{p_i\}$ is any probability distribution (possibly dependent on χ) over the eigenvalues, it follows straightly from Lemma 3.4 and (3) that

$$\mathbf{fn}_c(\mathcal{O}, r, \chi) \sqsubseteq \mathbf{fn}(\mathcal{O}, r, \chi) \text{ }_{\geq c}\oplus \text{ } [r := j \text{ } @ \text{ } p_j \mid j \in \Lambda_{\mathcal{O}}] .$$

The informal meaning is that any behaviour exhibited by the RHS cannot be worse than that of \mathbf{fn}_c .

4 Example: Bell's inequalities

In this section we model Bell's thought experiment in qGCL, assuming that the quantum measurements are faulty. Since real-world conditions seldom correspond to ideal ones, it makes sense to study whether we could establish Quantum Mechanics as a non local-realist theory even with faulty apparatuses. Our aim is to derive hardware reliability conditions that must be satisfied in order for the experiment to violate the Bell inequalities. In particular, we consider a variant of Bell's experiment due to Clauser, Horne, Shimony, and Holt [6], which is also known as the CHSH experiment.

The experiment assumes a source emitting pairs of photons polarised in the “singlet” state $\frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10})$. The photons are arranged to move away from each other in opposite directions, towards observers Alice and Bob. Now, Alice and Bob measure the polarisation of their incoming photon along different directions: Alice may choose to measure along a or a' , while Bob along b or b' . In any case, the result of their measurements is either “vertical” or “horizontal” polarisation, which correspond to values -1 and 1 respectively. Next, a series of repeated measurements is performed on pairs of photons prepared in the singlet state.

If we are to model this experiment by a “realist-local” theory, one assumes that each photon has a well defined value at any time for any direction of measurement, independent on the alteration of a remote measuring equipment. We denote by a_n the polarisation measured by Alice along direction a in the n -th repetition of the experiment, similarly for b_n and Bob.

The Bell inequalities are derived studying the correlation between measurements made by Alice and Bob along the four directions. For directions a, b that is defined as:

$$C(a, b) \hat{=} \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N a_n b_n$$

and similarly for the three remaining pairs. Note that if the measured polarisations are always correlated then $C(a, b) = 1$, while $C(a, b) = -1$ if they are always anticorrelated, and $C(a, b) = 0$ if they are uncorrelated. Now, the quantity

$$c_n \hat{=} a_n b_n + a_n b'_n + a'_n b_n - a'_n b'_n \quad (4)$$

can be easily proved to evaluate only to ± 2 (each term of the sum can only be ± 1). Therefore we can write

$$\left| \frac{1}{N} \sum_{n=1}^N c_n \right| = \left| \frac{1}{N} \sum_{n=1}^N a_n b_n + \frac{1}{N} \sum_{n=1}^N a_n b'_n + \frac{1}{N} \sum_{n=1}^N a'_n b_n - \frac{1}{N} \sum_{n=1}^N a'_n b'_n \right| \leq 2.$$

Taking the limit $N \rightarrow \infty$ we have the Bell inequality:

$$|C(a, b) + C(a', b) + C(a, b') - C(a', b')| \leq 2. \quad (5)$$

4.1 Inequality violation in Quantum Mechanics

We now describe how Quantum Mechanics violates inequality (5). The polarisation of a photon can be described by a qubit; the measurement of

polarisation along a direction at angle θ with the incident photon is described by the self-adjoint operator:

$$S_\theta \hat{=} \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$$

whose eigenvalues are 1 (horizontal polarisation) and -1 (vertical), and the corresponding eigenvectors are

$$h_\theta \hat{=} \cos \theta \delta_0 + \sin \theta \delta_1 \quad v_\theta \hat{=} -\sin \theta \delta_0 + \cos \theta \delta_1 .$$

A measurement of a photon in state δ_0 will return 1 with probability

$$\langle \delta_0, P_{h_\theta} \delta_0 \rangle = \langle \delta_0, h_\theta \langle h_\theta, \delta_0 \rangle \rangle = \cos^2 \theta$$

and therefore will return -1 with probability $\sin^2 \theta$.

A pair of photons is thus described by $\chi:q(\mathbf{B}^2)$ and the singlet state is $\chi = \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10})$. Each observer can obviously measure its photon only, so the joint observables for Alice and Bob are respectively $S_a \otimes I$ and $I \otimes S_b$, where a and b are the angles and I is the identity transform on a qubit. For the distributivity of tensor products over matrix multiplication we have that:

$$(S_a \otimes I) \cdot (I \otimes S_b) = (I \otimes S_b) \cdot (S_a \otimes I) = S_a \otimes S_b \quad (6)$$

which amounts to say that observables S_a and S_b are *simultaneously measurable* (*i.e.* the order in which they are measured does not affect the final outcome), and their joint operator is $S_a \otimes S_b$; we shall denote the joint observable by S_{ab} .

The eigenvalues of S_{ab} are the product of the eigenvalues of S_a, S_b , therefore they are just $\{1, -1\}$, thus degenerate. Eigenvalue 1 represents the fact that the detectors have measured the same polarisation ($1 = (\pm 1)^2$), while eigenvalue -1 the fact that they measure different polarisations ($-1 = (\pm 1) \cdot (\mp 1)$). The eigenvectors are given by the tensor products of the eigenvectors of S_a, S_b :

$$\begin{aligned} \mu_1 &\hat{=} h_a \otimes h_b & \mu_2 &\hat{=} v_a \otimes v_b \\ \lambda_1 &\hat{=} h_a \otimes v_b & \lambda_2 &\hat{=} v_a \otimes h_b \end{aligned}$$

where of course $\{\mu_1, \mu_2\}$ are associated to eigenvalue 1, while $\{\lambda_1, \lambda_2\}$ to -1 . Since the eigenvectors are pairwise orthogonal, we define the projectors for the joint observable S_{ab} :

$$\begin{aligned} P_{ab}^+ &\hat{=} P_{\mu_1} + P_{\mu_2} \\ P_{ab}^- &\hat{=} P_{\lambda_1} + P_{\lambda_2} \end{aligned}$$

where for a vector v the projector over the span of v is defined by

$$\forall w \bullet P_v w \hat{=} v \langle v, w \rangle .$$

With these definitions the probability that Alice and Bob measure correlated values (*i.e.* a measurement of S_{ab} returns 1) in the singlet state is

$$\begin{aligned} \text{Prob}(\text{Alice and Bob correlated}) &= \langle \chi, P_{ab}^+ \chi \rangle \\ &= \langle \chi, (P_{\mu_1} + P_{\mu_2}) \chi \rangle \\ &= \langle \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}), (P_{\mu_1} + P_{\mu_2}) \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}) \rangle \\ &= \sin^2(b - a) \end{aligned}$$

which of course implies that $\text{Prob}(\text{Alice and Bob anticorrelated}) = \cos^2(b - a)$. Finally, the correlation between the measurements is simply the expected value

$$C_q(a, b) = 1 \cdot \sin^2(b - a) + (-1) \cdot \cos^2(b - a) = -\cos 2(b - a)$$

from which we define the quantity B

$$B \hat{=} |C_q(a, b) + C_q(a', b) + C_q(a, b') - C_q(a', b')| . \quad (7)$$

By choosing $b - a = b - a' = b' - a = \frac{\pi}{8}$ and $b' - a' = \frac{3\pi}{8}$ we have that $B = 2\sqrt{2}$, thus violating inequality (5). Aspect *et al.* [3] actually performed this experiment in the laboratory, obtaining a violation of the Bell inequality for the amount predicted by Quantum Mechanics.

The recent work of Ursin *et al.* [19] confirmed the same results in an open-space experiment where Alice and Bob were separated by 144km.

The correlation between measurements can also be obtained by computing the expected value of S_{ab} . For an observable \mathcal{O} and state ψ , the expected value of the result of measuring \mathcal{O} on a system in state ψ is $\langle \psi, \mathcal{O} \psi \rangle$ (see Appendix C). Recalling that by the spectral theorem any self-adjoint operator can be decomposed as a sum of the projectors over its eigenspaces, we get that $\langle \chi, S_{ab} \chi \rangle = C_q(a, b)$, as it should be. We took the longer route in order to give a step-by-step explanation of the quantum rule.

4.2 Quantum program and faulty measurement

We model in qGCL the photon experiment, with one (not significant) difference. Instead of considering the observable S_{ab} , whose eigenvalues are -1 and 1 , we consider

$$\mathcal{O}_{ab} \hat{=} S_{ab} + 1$$

i.e. we simply add 1 to the outcome of a measurement of S_{ab} . Thus, a measurement of \mathcal{O}_{ab} will return either 0 or 2 (we have defined a so-called *function of an operator*, see again Appendix C). In particular, the self-adjoint operator corresponding to \mathcal{O}_{ab} is $S_a \otimes S_b + I$, where I is the identity transform over $q(\mathbf{B}^2)$.

It is straightforward to check that the eigenvalues of \mathcal{O}_{ab} are 0 and 2, and its expected value in the singlet state is

$$\langle \mathcal{O}_{ab} \rangle_\chi = \langle S_a \otimes S_b + I \rangle_\chi = \langle S_a \otimes S_b \rangle_\chi + \langle I \rangle_\chi = C_q(a, b) + 1$$

which is thus greater or equal to 0, since $-1 \leq C_q(a, b) \leq 1$. The projectors over the eigenspaces remain unchanged:

$$P_{ab}^2 \hat{=} P_{ab}^+, \quad P_{ab}^0 \hat{=} P_{ab}^-.$$

The positivity of the return values (the eigenvalues) is required by our future program manipulation involving pGCL's expectation-transformer semantics, in which possibly negative variables might conflict with the semantic requirement for positive expectations (see Appendix B for further details). Ours is actually an example in which negative variables do cause problems, as we later report.

Program E describes the measurement of polarisation made by Alice and Bob along any two directions at angles a and b :

$$E \hat{=} \left(\begin{array}{l} \mathbf{var} \ \chi:q(\mathbf{B}^2), r:\{0, 2\} \bullet \\ \chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}) \ ; \ \mathbf{fin}(\mathcal{O}_{ab}, r, \chi) \\ \mathbf{rav} \end{array} \right)$$

It is a straightforward application of pGCL laws to prove that E correctly implements the experiment. However, we are more interested in studying the behaviour of E when \mathbf{fin} is replaced by \mathbf{fin}_c , its faulty companion. Our aim is to find the range of values for parameter c for which the quantum predictions of the experiments are satisfied, thereby showing that Quantum Mechanics is not realist-local. The faulty version of E is program E_c

$$E_c \hat{=} \left(\begin{array}{l} \mathbf{var} \ \chi:q(\mathbf{B}^2), r:\{0, 2\} \bullet \\ \chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}) \ ; \ \mathbf{fin}_c(\mathcal{O}_{ab}, r, \chi) \\ \mathbf{rav} \end{array} \right)$$

where c is an arbitrary probability. We now reason:

$$\begin{aligned}
& E_c \\
& = \text{definition of } \mathbf{fin}_c \\
& \chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}) \mathbin{\text{\$}} \mathbf{fin}(\mathcal{O}_{ab}, r, \chi) \text{ } c \oplus r:\{0, 2\} \\
& = \text{law A-1} \\
& \left(\chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}) \mathbin{\text{\$}} \mathbf{fin}(\mathcal{O}_{ab}, r, \chi) \right) \text{ } c \oplus \left(\chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}) \mathbin{\text{\$}} r:\{0, 2\} \right) \\
& = \text{definition of } \mathbf{fin} \text{ and law A-1} \\
& \left[\left(\chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}) \mathbin{\text{\$}} r := i \right) \text{ } @ \frac{1}{2} \langle \delta_{01} - \delta_{10}, P_{ab}^i(\delta_{01} - \delta_{10}) \rangle \mid i \in \{0, 2\} \right] \text{ } c \oplus \\
& \left(\chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}) \mathbin{\text{\$}} r:\{0, 2\} \right) \\
& \sqsupseteq \text{de-initialise } \chi \text{ and linear algebra} \\
& (r := 2 \sin^2(b-a) \oplus r := 0) \text{ } c \oplus r:\{0, 2\} \\
& = \text{law P-4 and notation} \\
& \left| \begin{array}{l} r := 2 \quad @ \quad c \cdot \sin^2(b-a) \\ r := 0 \quad @ \quad c \cdot \cos^2(b-a) \\ r:\{0, 2\} \quad @ \quad \bar{c}. \end{array} \right. \\
& \cong \text{definition} \\
& E'_c
\end{aligned}$$

We note that the abstraction introduced in the penultimate step is due to χ so, as far as r is concerned, no determinism is “lost”. We now want to calculate the minimal value of c for which the faulty quantum program violates Bell’s inequality.

Proposition 4.1. *Bell’s inequality is violated only for $c > \frac{2}{1+\sqrt{2}} \approx 83\%$.*

Proof. We first calculate the expected value of r after the execution of E'_c , depending on the angles a, b and parameter c . Next we calculate the quantity B_c , defined analogously to quantity B of (7), which will depend on the four angles a, b, a', b' and parameter c . Finally, we fix the angles in B_c at the four values giving $B = 2\sqrt{2}$, and calculate a lower bound on c by imposing a violation of Bell’s inequality (which will be slightly modified, since the return values are “shifted” by 1).

We now calculate the expected value of r , by simply applying the semantics of E'_c to the post-expectation r . We reason on E'_c :

$$wp.E'_c.r$$

$$\begin{aligned}
&= && \text{definition of } E'_c, \text{ semantics of } {}_p\oplus \\
& c \cdot \sin^2(b-a) \cdot wp.(r := 2).r \\
& + c \cdot \cos^2(b-a) \cdot wp.(r := 0).r \\
& + \bar{c} \cdot (wp.(r := 2).r \sqcap wp.(r := 0).r) \\
&= && \text{assignment semantics} \\
& c \cdot \sin^2(b-a) \cdot r[r \setminus 2] \\
& + c \cdot \cos^2(b-a) \cdot r[r \setminus 0] \\
& + \bar{c} \cdot (r[r \setminus 2] \sqcap r[r \setminus 0]) \\
&= && \text{arithmetic} \\
& 2c \cdot \sin^2(b-a) \\
&= && \text{trigonometry} \\
& -c \cos 2(b-a) + c \\
&= && \text{definition of } C_q \\
& c(C_q(a, b) + 1).
\end{aligned}$$

The quantity B_c is thus defined analogously to B (7), by summing the four correlations $c(C_q(a, b) + 1)$:

$$B_c \hat{=} |c(C_q(a, b) + C_q(a', b) + C_q(a', b') - C_q(a, b')) + 2c| . \quad (8)$$

Since we calculated the quantum correlation of Alice and Bob's results plus one, we cannot directly compare that with inequality (5). The proper inequality is derived by considering, analogously to c_n in (4), the sum

$$a_n b_n + 1 + a'_n b_n + 1 + a'_n b'_n + 1 - a_n b'_n - 1 = c_n + 2$$

which evaluates either 0 or 4, since c_n is ± 2 . The Bell inequality thus becomes:

$$0 \leq C(a, b) + C(a', b) + C(a, b') - C(a', b') \leq 4 .$$

Finally, we fix as before the angles $b-a = b-a' = b'-a = \frac{\pi}{8}$ and $b'-a' = \frac{3\pi}{8}$, and we have that $B_c = c2\sqrt{2} + 2c$. To violate Bell's inequality $B_c > 4$, which implies $c > \frac{2}{1+\sqrt{2}} \approx 0.828$. \square

We note that the detectors used in Aspect *et al.*'s experiment [3] had an efficiency between 0.92 and 0.95, so well above the required value.

One can verify that if we had used the observable S_{ab} we would have obtained that c should be greater than $\frac{1}{\sqrt{2}} \approx 0.707$. Therefore, we would have not only applied pGCL semantics erroneously, but we would have obtained a more relaxed, thus wrong, bound on c .

4.3 Informal reasoning

The same result can be obtained in a less formal, though rigorous, way. We could compute the minimum and maximum probabilities of obtaining $r = 1$ and $r = -1$. Then, we calculate the usual expected value of r and study when it is minimum (*i.e.* the worst case). Finally, we fix the four angles and compare the minimum expectation of r with Bell's inequality (5) to derive a lower bound for c .

Consider a program which behaves like

$$\left| \begin{array}{l} r := 1 \quad @ \quad c \cdot \sin^2(b - a) \\ r := -1 \quad @ \quad c \cdot \cos^2(b - a) \\ r:\{1, -1\} \quad @ \quad \bar{c} \end{array} \right.$$

that is, it performs the correct operation with probability c and chooses nondeterministically with probability \bar{c} (we can keep r in $\{1, -1\}$ because we shall not use pGCL semantics). Now, notwithstanding the action of the demon, we must have that

$$\text{Prob}(r = 1) \geq c \cdot \sin^2(b - a) \hat{=} p_{min}^+$$

which implies that

$$\text{Prob}(r = -1) \leq \bar{c} \cdot \sin^2(b - a) \hat{=} p_{max}^- .$$

Given any distribution r over $\{1, -1\}$ defined by probabilities p^+, p^- , the expected value $E[r]$ is

$$E[r] = 1 \cdot p^+ + (-1)p^- = p^+ - p^- .$$

The demon works against us, so it tries to lower our expectation over r . It is easy to show that the minimal value for $E[r]$ is

$$\begin{aligned} E[r]_{min} &= p_{min}^+ - p_{max}^- \\ &= c \cdot \sin^2(b - a) - 1 + c \cdot \sin^2(b - a) \\ &= 2c \cdot \sin^2(b - a) - 1 \\ &= c \cdot C_q(a, b) + c - 1 . \end{aligned}$$

The sum of the four correlations would then be

$$B'_c \hat{=} |c(C_q(a, b) + C_q(a', b) + C_q(a', b') - C_q(a, b')) + 2c - 2|$$

and by fixing the usual four “violating” angles we get that $B'_c = c2\sqrt{2} + 2c - 2$. In order to violate Bell’s inequality, B'_c has to be greater than 2, which implies $c > \frac{2}{1+\sqrt{2}}$, as before.

We observe that using a formal method such as qGCL, instead of the *ad hoc* argument above, is not a pure exercise of style. The interplay between probabilistic and demonic nondeterminism can be quite subtle, and counter-intuitive quantum effects further complicate the setting. It is therefore important to have a general, formal framework in which to cast our reasonings - this is indeed the reason why so much effort has been (and is still being) devoted in studying formal methods for computing systems.

4.4 Comparison with deterministic probabilism

It is useful to compare our model for faulty measurement with one in which (demonic) nondeterminism is absent, *i.e.* errors are purely probabilistic. For example, we could define a faulty measurement for which erroneous behaviour is represented by the toss of a fair coin:

$$\mathbf{fin}'_c(\mathcal{O}, r, \chi) \hat{=} \mathbf{fin}(\mathcal{O}, r, \chi) \text{ }_c\oplus (r := 0 \text{ }_{\frac{1}{2}}\oplus 2) .$$

We plug this definition into program E and by using a similar reasoning as in Proposition 4.1 we obtain the following program D :

$$D \hat{=} \left| \begin{array}{ll} r := 2 & @ \quad c \cdot \sin^2(b - a) \\ r := 0 & @ \quad c \cdot \cos^2(b - a) \\ r := 0 \text{ }_{\frac{1}{2}}\oplus 2 & @ \quad \bar{c} . \end{array} \right.$$

The expected value of r is again calculated as $wp.D.r$:

$$\begin{aligned} & wp.D.r \\ = & \hspace{15em} \text{definition of } D, \text{ semantics of } \text{ }_p\oplus \\ & c \cdot \sin^2(b - a) \cdot wp.(r := 2).r + c \cdot \cos^2(b - a) \cdot wp.(r := 0).r \\ & + \bar{c} \cdot (wp.(r := 0 \text{ }_{\frac{1}{2}}\oplus 2).r) \\ = & \hspace{15em} \text{semantics of assignment and } \text{ }_p\oplus \\ & 2c \cdot \sin^2(b - a) + \frac{\bar{c}}{2}(wp.(r := 0).r + wp.(r := 2).r) \end{aligned}$$

$$\begin{aligned}
&= && \text{assignment semantics} \\
&2c \cdot \sin^2(b - a) + \bar{c} \\
&= && \text{definition of } C_q \\
&cC_q(a, b) + 1.
\end{aligned}$$

By summing the four correlations set at the known four angles we get the quantity

$$c2\sqrt{2} + 2$$

which has to be greater than 4 if we want to violate Bell's inequality, and that implies $c > \frac{1}{\sqrt{2}} \approx 0.707$.

5 Faulty initialisation

In this section we provide a model for the case of error-prone quantum initialisations. A correct initialisation of qureg χ is modelled by the assignment $\chi := v$, where v is some constant qureg. A faulty initialisation is modelled by the probabilistic choice in which to χ is assigned v with probability *at least* p , and some other v' with probability *at most* \bar{p} . In our notation

$$\chi := v \gg_p \oplus \chi := v'.$$

We now study the sequential composition of a faulty initialisation and a faulty measurement.

The following lemma is a straightforward application of law A-1.

Lemma 5.1. *For any $c \in [0, 1]$*

$$\chi := v \mathbin{\text{\$}} \mathbf{fn}_c(\mathcal{O}, r, \chi) = \chi := v \mathbin{\text{\$}} \mathbf{fn}_c(\mathcal{O}, r, v).$$

Proof. We reason from the LHS:

$$\begin{aligned}
&\chi := v \mathbin{\text{\$}} \mathbf{fn}_c(\mathcal{O}, r, \chi) \\
&= && \text{definition of } \mathbf{fn}_c \text{ and law A-1} \\
&\chi := v \mathbin{\text{\$}} \mathbf{fn}(\mathcal{O}, r, \chi) \text{ }_c \oplus \chi := v \mathbin{\text{\$}} \mathbf{fn}_{\top}(\mathcal{O}, r, \chi) \\
&= && \text{definition of } \mathbf{fn} \text{ and law A-1} \\
&[(\chi := v \mathbin{\text{\$}} r := i) @ \langle v, P_i v \rangle \mid i \in \Lambda_{\mathcal{O}}] \text{ }_c \oplus \chi := v \mathbin{\text{\$}} \mathbf{fn}_{\top}(\mathcal{O}, r, \chi) \\
&= && \text{law A-1} \\
&\chi := v \mathbin{\text{\$}} [r := i @ \langle v, P_i v \rangle \mid i \in \Lambda_{\mathcal{O}}] \text{ }_c \oplus \chi := v \mathbin{\text{\$}} \mathbf{fn}_{\top}(\mathcal{O}, r, \chi)
\end{aligned}$$

$$\begin{aligned}
&= && \text{definition of } \mathbf{fin} \\
\chi := v \ ; \ \mathbf{fin}(\mathcal{O}, r, \chi) \ c \oplus \ \chi := v \ ; \ \mathbf{fin}_{\sqcap}(\mathcal{O}, r, \chi) \\
&= && \text{law A-1 and definition of } \mathbf{fin}_c \\
\chi := v \ ; \ \mathbf{fin}_c(\mathcal{O}, r, v)
\end{aligned}$$

□

Lemma 5.2. *Let Q be the program defined as*

$$Q \hat{=} (\chi := v \ \geq_p \oplus \ \chi := v' \ ; \ \mathbf{fin}_c(\mathcal{O}, r, \chi)) .$$

Then:

$$\forall i \in \Lambda_{\mathcal{O}} \bullet \text{Prob}(\text{after } Q \ r = i) \geq ct_i + c\bar{p}(0 \sqcap (t'_i - t_i))$$

where $t_i \hat{=} \langle v, P_i v \rangle$ and $t'_i \hat{=} \langle v', P_i v' \rangle$.

Proof. First we reason on Q , then we use pGCL semantics to calculate the required probability:

$$\begin{aligned}
&\chi := v \ \geq_p \oplus \ \chi := v' \ ; \ \mathbf{fin}_c(\mathcal{O}, r, \chi) \\
&= && \text{law S-3} \\
&\chi := v \ ; \ \mathbf{fin}_c(\mathcal{O}, r, \chi) \ \geq_p \oplus \ \chi := v' \ ; \ \mathbf{fin}_c(\mathcal{O}, r, \chi) \\
&= && \text{lemma 5.1} \\
&\chi := v \ ; \ \mathbf{fin}_c(\mathcal{O}, r, v) \ \geq_p \oplus \ \chi := v' \ ; \ \mathbf{fin}_c(\mathcal{O}, r, v') \\
&\sqsupseteq && \text{de-initialise } \chi \\
&\mathbf{fin}_c(\mathcal{O}, r, v) \ \geq_p \oplus \ \mathbf{fin}_c(\mathcal{O}, r, v') \\
&= && \text{definition of } \mathbf{fin}_c \\
&(\mathbf{fin}(\mathcal{O}, r, v) \ c \oplus \ r:\Lambda_{\mathcal{O}}) \ \geq_p \oplus \ (\mathbf{fin}(\mathcal{O}, r, v') \ c \oplus \ r:\Lambda_{\mathcal{O}}) \\
&= && \text{law S-4} \\
&(\mathbf{fin}(\mathcal{O}, r, v) \ \geq_p \oplus \ \mathbf{fin}(\mathcal{O}, r, v')) \ c \oplus \ r:\Lambda_{\mathcal{O}} \\
&= && \text{definition of } \geq_p \oplus \\
&(\mathbf{fin}(\mathcal{O}, r, v) \ p \oplus \ \mathbf{fin}(\mathcal{O}, r, v) \ \sqcap \ \mathbf{fin}(\mathcal{O}, r, v')) \ c \oplus \ r:\Lambda_{\mathcal{O}} \\
&= && \text{law P-4 and notation} \\
&\left| \begin{array}{ll} \mathbf{fin}(\mathcal{O}, r, v) & @ \ cp \\ \mathbf{fin}(\mathcal{O}, r, v) \ \sqcap \ \mathbf{fin}(\mathcal{O}, r, v') & @ \ c\bar{p} \\ r:\Lambda_{\mathcal{O}} & @ \ \bar{c} . \end{array} \right.
\end{aligned}$$

$$\begin{array}{l} \hat{=} \\ Q' \end{array} \quad \text{define } Q'$$

so that we have $Q \sqsupseteq Q'$. Again, since we are only interested in the final value of r , there is no harm in using Q' instead of Q . In particular, the probability that after executing Q' r equals i is calculated as the expectation-transformer semantics of Q' applied to the post-expectation $[r = i]$ (see Appendix B), that is

$$\text{Prob}(\text{after } Q' \ r = i) \geq wp.Q'.[r = i].$$

We reason:

$$\begin{array}{l} wp.Q'.[r = i] \\ = \quad \text{semantics of } \oplus_p \\ cp \cdot wp.\mathbf{fn}(\mathcal{O}, r, v).[r = i] \\ + c\bar{p} \cdot wp.(\mathbf{fn}(\mathcal{O}, r, v) \sqcap \mathbf{fn}(\mathcal{O}, r, v')).[r = i] \\ + \bar{c} \cdot wp.r:\Lambda_{\mathcal{O}}.[r = i] \\ = \quad \text{semantics of } \sqcap \\ cp \cdot wp.\mathbf{fn}(\mathcal{O}, r, v).[r = i] \\ + c\bar{p} \cdot (wp.\mathbf{fn}(\mathcal{O}, r, v).[r = i] \sqcap wp.\mathbf{fn}(\mathcal{O}, r, v').[r = i]) \\ + \bar{c} \cdot wp.r:\Lambda_{\mathcal{O}}.[r = i] \\ = \quad \text{definition of } \mathbf{fn} \text{ and semantics of } \oplus_p \\ cp \cdot \langle v, P_i v \rangle \\ + c\bar{p} \cdot (\langle v, P_i v \rangle \sqcap \langle v', P_i v' \rangle) \\ + \bar{c} \cdot wp.r:\Lambda_{\mathcal{O}}.[r = i] \\ = \quad \text{definition of } r:\Lambda_{\mathcal{O}} \text{ and semantics of } \sqcap \\ cp \cdot \langle v, P_i v \rangle + c\bar{p} \cdot (\langle v, P_i v \rangle \sqcap \langle v', P_i v' \rangle) \\ + \bar{c} \cdot \sqcap_{j \in \Lambda_{\mathcal{O}}} \{wp.r := j.[r = i]\} \\ = \quad \text{semantics of assignment and logic} \\ cp \cdot \langle v, P_i v \rangle + c\bar{p} \cdot (\langle v, P_i v \rangle \sqcap \langle v', P_i v' \rangle) \\ = \quad a \sqcap b = a + (0 \sqcap (b - a)) \\ c \cdot \langle v, P_i v \rangle + c\bar{p} \cdot (0 \sqcap (\langle v', P_i v' \rangle - \langle v, P_i v \rangle)) \\ = \quad \text{definition of } t_i, t'_i \end{array}$$

$$ct_i + c\bar{p}(0 \sqcap (t'_i - t_i)).$$

□

It is worth noting that the left-hand summand does not depend on p , the minimal probability of a correct initialisation. Such dependency is only present in the right-hand summand via \bar{p} , and it is proportional to the (truncated) difference between the perturbed and correct probabilities. This confirms intuition: since the demon always tries to lower the post-expectation, the faulty initialisation is effective only when the demon can take advantage of it (*i.e.*, when $t'_i - t_i < 0$).

5.1 Example: Deutsch-Jozsa quantum algorithm

We apply the concepts of faulty initialisation and measurements to the Deutsch-Jozsa algorithm [7]. For $n \in \mathbf{N}^+$, a function $f: \mathbf{B}^n \rightarrow \mathbf{B}$ is *constant* iff it takes only a single value. It is *balanced* iff it takes 0 and 1 equally often, *i.e.* $\# f^{-1}(0) = \# f^{-1}(1)$. Any constant Boolean function f is not balanced, and any balanced function is not constant. The Deutsch-Jozsa classification problem is to decide, for a given function which is either constant or balanced, which actually holds. The quantum algorithm is expressed in qGCL:

$$DJ \hat{=} \left(\begin{array}{l} \mathbf{var} \ \chi: q(\mathbf{B}^n), \ r: \mathbf{B} \bullet \\ \chi := \frac{1}{\sqrt{2^n}} \sum_{i \in \mathbf{B}^n} \delta_i \mathfrak{?} \\ \chi := T_f \chi \mathfrak{?} \\ \mathbf{fin}(\mathcal{V}, r, \chi) \\ \mathbf{rav} \end{array} \right)$$

where Boolean finalisation \mathcal{V} is defined by the family of spaces $\{V_0, V_1\}$, with $V_0 \hat{=} \mathbf{C} \sum_{y \in \mathbf{B}^n} \delta_y$ and V_1 the orthogonal complement of V_0 (note that V_0 is a unidimensional complex space, so V_1 is a $(n - 1)$ -dimensional complex space). Initialisation is efficiently accomplished by the Hadamard transform (see [17] for details). Transformation $T_f: q(\mathbf{B}^n) \rightarrow q(\mathbf{B}^n)$ is defined by

$$\forall i \in \mathbf{B}^n \quad T_f \chi(i) \hat{=} (-1)^{f(i)} \chi(i)$$

that is, T_f inverts the sign of $\chi(i)$ if $f(i) = 1$ and leaves it unchanged otherwise; T_f is clearly unitary. The output of the algorithm is encoded in variable r : 0 indicates “constant”, 1 indicates “balanced”.

The quantum algorithm thus solves the Deutsch-Jozsa problem with a *single* evaluation of f (that of T_f). A standard algorithm instead evaluates f at least $O(2^n)$ times in the worst case and on average evaluates f thrice.

Let us now consider the faulty version of this algorithm. We replace **Fin** with **fin_c**; with respect to initialisation and T_f evolution, we simplify things by composing both assignments into one and then replacing that by a single faulty assignment:

$$DJ' \hat{=} \chi := w \underset{\geq p}{\oplus} w' \ ; \ \mathbf{fin}_c(\mathcal{V}, r, \chi)$$

where $w = \frac{1}{\sqrt{2^n}} \sum_{i \in \mathbf{B}^n} (-1)^{f(i)} \delta_i$ and w' is the erroneous value (which will in general depend on f). It is obviously $DJ' \subseteq DJ$.

By applying Lemma 5.2 we can calculate the probabilities of program DJ' giving the correct results. They are:

$$\begin{array}{ll} \text{if } f \text{ constant} & \text{Prob}(r = 0) \geq c + c\bar{p}(t'_0 - 1) = cp + c\bar{p}t'_0 \\ \text{if } f \text{ balanced} & \text{Prob}(r = 1) \geq c + c\bar{p}(t'_1 - 1) = cp + c\bar{p}t'_1 \end{array}$$

where $t'_i = \langle w', P_i w' \rangle$. Since $(t'_i - 1)$ is in general negative, it follows that DJ' is guaranteed to be correct only with probability smaller than c , thus making it a two-sided error algorithm.

When the t'_i 's are bounded by some positive constant ϵ (*i.e.*, $0 < t'_i < \epsilon$), we can use the relations above to find bounds on the parameters p and c . Since we are now dealing with a probabilistic algorithm, we may just ask for DJ' to be correct with some probability q greater than $\frac{1}{2}$, so we would need to have

$$cp + c\bar{p}\epsilon \geq q$$

which for example implies that

$$c \geq \frac{q}{p + \bar{p}\epsilon} .$$

6 Faulty evolution

In this section we sketch a model for the case of error-prone quantum evolutions. A correct evolution of unitary U is modelled by the assignment $\chi := U\chi$. A faulty evolution is modelled by the probabilistic choice in which U gets executed with *at least* probability p , and some other unitary U' gets executed with probability *at most* $1 - p$. In our notation we write

$$\chi := U\chi \underset{\geq p}{\oplus} \chi := U'\chi .$$

Before considering the sequential composition of two faulty gates we need the following lemma.

Lemma 6.1. *For programs $prg_1, prg_2, prg_3, prg_4$ and probabilities p, q we have*

$$\begin{aligned} & (prg_1 \geq_q \oplus prg_2) \geq_p \oplus (prg_3 \geq_q \oplus prg_4) \\ & \sqsupseteq \\ & prg_1 \geq_{pq} \oplus (prg_2 \sqcap prg_3 \sqcap prg_4). \end{aligned}$$

Proof. See Appendix B. □

Proposition 6.2. *For unitaries U, V, U', V' and probabilities p, q we have*

$$\begin{aligned} & \chi := U\chi \geq_p \oplus \chi := U'\chi \ ; \ \chi := V\chi \geq_q \oplus \chi := V'\chi \\ & \sqsupseteq \\ & \chi := VU\chi \geq_{pq} \oplus (\chi := V'U\chi \sqcap \chi := VU'\chi \sqcap \chi := V'U'\chi). \end{aligned}$$

Proof. We reason:

$$\begin{aligned} & \chi := U\chi \geq_p \oplus \chi := U'\chi \ ; \ \chi := V\chi \geq_q \oplus \chi := V'\chi \\ & = \text{law S-3} \\ & \chi := U\chi \ ; \ (\chi := V\chi \geq_q \oplus \chi := V'\chi) \geq_p \oplus \\ & \quad \chi := U'\chi \ ; \ (\chi := V\chi \geq_q \oplus \chi := V'\chi) \\ & = \text{laws A-4 and A-3} \\ & (\chi := VU\chi \geq_q \oplus \chi := V'U\chi) \geq_p \oplus (\chi := VU'\chi \geq_q \oplus \chi := V'U'\chi) \\ & \sqsupseteq \text{Lemma 6.1} \\ & \chi := VU\chi \geq_{pq} \oplus (\chi := V'U\chi \sqcap \chi := VU'\chi \sqcap \chi := V'U'\chi) \end{aligned}$$

□

We now perform a faulty finalisation (with no quantum state update, as per Definition 3.4) after the two faulty evolutions.

Proposition 6.3. *For unitaries U, V, U', V' , observable \mathcal{O} , and probabilities p, q, c we have*

$$\begin{aligned} & (\chi := U\chi \geq_p \oplus \chi := U'\chi) \ ; \ (\chi := V\chi \geq_q \oplus \chi := V'\chi) \ ; \ \mathbf{fin}_c(\mathcal{O}, r, \chi) \\ & \sqsupseteq \\ & (\mathbf{fin}(\mathcal{O}, r, VU\chi) \geq_{pq} \oplus (\mathbf{fin}(\mathcal{O}, r, V'U\chi) \sqcap \mathbf{fin}(\mathcal{O}, r, VU'\chi) \sqcap \mathbf{fin}(\mathcal{O}, r, V'U'\chi))) \\ & \quad \text{c} \oplus r : \Lambda_{\mathcal{O}}. \end{aligned}$$

Proof. For simplicity we abbreviate $\mathbf{fin}_c(\mathcal{O}, r, \chi)$ and $\mathbf{fin}(\mathcal{O}, r, \chi)$ by $\mathbf{fin}_c(\chi)$ and $\mathbf{fin}(\chi)$ respectively. We reason from the LHS:

$$\begin{aligned}
& (\chi := U\chi \gg_p \oplus \chi := U'\chi) \mathbin{\&}; (\chi := V\chi \gg_q \oplus \chi := V'\chi) \mathbin{\&}; \mathbf{fin}_c(\chi) \\
& \sqsupseteq \text{Proposition 6.2} \\
& \chi := VU\chi \gg_{pq} \oplus (\chi := V'U\chi \sqcap \chi := VU'\chi \sqcap \chi := V'U'\chi) \mathbin{\&}; \mathbf{fin}_c(\chi) \\
& = \text{law S-3} \\
& \chi := VU\chi \mathbin{\&}; \mathbf{fin}_c(\chi) \gg_{pq} \oplus (\chi := V'U\chi \sqcap \\
& \chi := VU'\chi \sqcap \chi := V'U'\chi \mathbin{\&}; \mathbf{fin}_c(\chi)) \\
& = \text{law S-2} \\
& \chi := VU\chi \mathbin{\&}; \mathbf{fin}_c(\chi) \gg_{pq} \oplus ((\chi := V'U\chi \mathbin{\&}; \mathbf{fin}_c(\chi)) \sqcap \\
& (\chi := VU'\chi \mathbin{\&}; \mathbf{fin}_c(\chi)) \sqcap (\chi := V'U'\chi \mathbin{\&}; \mathbf{fin}_c(\chi))) \\
& = \text{Lemma 5.1} \\
& \chi := VU\chi \mathbin{\&}; \mathbf{fin}_c(VU\chi) \gg_{pq} \oplus ((\chi := V'U\chi \mathbin{\&}; \mathbf{fin}_c(V'U\chi)) \sqcap \\
& (\chi := VU'\chi \mathbin{\&}; \mathbf{fin}_c(VU'\chi)) \sqcap (\chi := V'U'\chi \mathbin{\&}; \mathbf{fin}_c(V'U'\chi))) \\
& \sqsupseteq \text{de-initialise } \chi \\
& \mathbf{fin}_c(VU\chi) \gg_{pq} \oplus (\mathbf{fin}_c(V'U\chi) \sqcap \mathbf{fin}_c(VU'\chi) \sqcap \mathbf{fin}_c(V'U'\chi)) \\
& = \text{definition of } \mathbf{fin}_c \\
& \mathbf{fin}_c(VU\chi) \gg_{pq} \oplus ((\mathbf{fin}(V'U\chi) \mathbin{\&} r:\Lambda_{\mathcal{O}}) \sqcap \\
& (\mathbf{fin}(VU'\chi) \mathbin{\&} r:\Lambda_{\mathcal{O}}) \sqcap (\mathbf{fin}(V'U'\chi) \mathbin{\&} r:\Lambda_{\mathcal{O}})) \\
& = \text{law P-3 twice} \\
& \mathbf{fin}_c(VU\chi) \gg_{pq} \oplus ((\mathbf{fin}(V'U\chi) \sqcap \mathbf{fin}(VU'\chi) \sqcap \mathbf{fin}(V'U'\chi)) \mathbin{\&} r:\Lambda_{\mathcal{O}}) \\
& = \text{definition of } \mathbf{fin}_c \\
& (\mathbf{fin}(VU\chi) \mathbin{\&} r:\Lambda_{\mathcal{O}}) \gg_{pq} \oplus ((\mathbf{fin}(V'U\chi) \sqcap \\
& \mathbf{fin}(VU'\chi) \sqcap \mathbf{fin}(V'U'\chi)) \mathbin{\&} r:\Lambda_{\mathcal{O}}) \\
& = \text{law S-4} \\
& (\mathbf{fin}(VU\chi) \gg_{pq} \oplus (\mathbf{fin}(V'U\chi) \sqcap \mathbf{fin}(VU'\chi) \sqcap \mathbf{fin}(V'U'\chi))) \mathbin{\&} r:\Lambda_{\mathcal{O}}
\end{aligned}$$

□

We see that the correct operation $\mathbf{fin}(\mathcal{O}, r, VU\chi)$ is executed with probability at least cpq , and therefore the erroneous behaviour has overall probability at most $1 - cpq$. However, the erroneous behaviour due to faulty

evolutions has probability at most $c(1 - pq)$, while erroneous (fully nondeterministic) behaviour due to the faulty measurement has probability $1 - c$.

To quantify the difference between the “correct” and “wrong” measurement statistics one usually employs the total variation distance of the output distributions. For distributions $\{a_i\}$ and $\{b_i\}$ over some finite set S , their total variation distance is $\sum_{i \in S} |a_i - b_i|$. Aharonov *et al.* [1] proved that maximal total variation distance between two distributions taken over all possible observables equals the trace distance between the density matrices representing the quantum states. However, this approach cannot be readily applied to our case, since our computations feature demonic nondeterminism. The challenge is therefore to extend Aharonov *et al.*'s approach to cope with demonic nondeterminism.

7 Conclusions

In this paper we have provided a starting point for a high-level description and analysis of faulty quantum programs, based on the quantum programming language qGCL. In particular, we have described a simple model for faulty initialisation and quantum measurements, based on the operation “execute the correct behaviour with probability at least p ”. We have applied it to an example of Bell inequalities and to the Deutsch-Jozsa quantum algorithm. In the former we have derived a hardware efficiency bound in order for the experiment to be successful. In the latter we have calculated lower bounds on the probability of success of the faulty algorithm. In conclusion, it seems possible to provide an abstract treatment for faulty quantum programs. An important aspect of our approach is that both the correct and faulty program can be reasoned about in the same environment, thus benefiting from well-established programming laws and “classical” concepts such as refinement and abstraction.

8 Acknowledgements

This work has been carried out while the author was at the Oxford University Computing Laboratory, supported by a *Marie Curie Outgoing International Fellowship* of the European Commission's 6th Framework Programme. The author wishes to thank Jeff Sanders for many stimulating discussions and for commenting a draft of this paper. The author also thanks an anonymous referee for suggesting many improvements to the paper.

References

- [1] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *STOC '98: Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 20–30, 1998.
- [2] T. Altenkirch and J. Grattage. A functional quantum programming language. In *LICS '05: Proceedings of the 20th Annual IEEE Symposium on Logic in Computer Science*, pages 249–258, 2005.
- [3] A. Aspect, P. Graingier, and G. Roger. Experimental realization of EPR Gedankenexperiment: A new violation of Bell's inequalities. *Physical Review Letters*, 49:91–94, 1982.
- [4] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.
- [5] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992.
- [6] J. F. Clauser, M. A. Horne, A. Shimony, and R.A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969.
- [7] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London*, A439:553–558, 1992.
- [8] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.
- [9] A. Fedrizzi *et al.* High-fidelity transmission of entanglement over a high-loss freespace channel. *Nature Physics*, 5:389–392, 2009.
- [10] S. J. Gay. Quantum programming languages: survey and bibliography. *Mathematical Structures in Computer Science*, 16(4):581–600, 2006.
- [11] J. He, A. McIver, and K. Seidel. Probabilistic models for the guarded command language. *Science of Computer Programming*, 28:171–192, 1997.
- [12] C. J. Isham. *Lectures on quantum theory*. Imperial College Press, 1997.

- [13] A. McIver and C. C. Morgan. *Abstraction, Refinement and Proof for Probabilistic Systems*. Springer, 2005.
- [14] C. C. Morgan, A. McIver, and K. Seidel. Probabilistic predicate transformers. *ACM Transactions on Programming Languages and Systems*, 18(3):325–353, May 1996.
- [15] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.
- [16] M. Reed and B. Simon. *Methods of Mathematical Physics. I:Functional Analysis*. Acamedic Press, 1972.
- [17] J. W. Sanders and P. Zuliani. Quantum programming. In *MPC '00: Mathematics of Program Construction, Springer LNCS*, volume 1837, pages 80–99, 2000.
- [18] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.
- [19] R. Ursin *et al.* Entanglement-based quantum communication over 144 km. *Nature Physics*, 3:481–486, 2007.
- [20] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, 1955.

A Proofs of measurement laws

We prove the following laws for faulty measurements that were given in Section 3:

Law F-1	$\mathbf{Fin} \circledast \mathbf{Fin} = \mathbf{Fin}$
Law F-2	$\mathbf{Fin}_{\square} \circledast \mathbf{Fin}_{\square} = \mathbf{Fin}_{\square}$
Law F-3	$\mathbf{Fin} \circledast \mathbf{Fin}_{\square} = \mathbf{Fin}_{\square}$
Law F-4	$\mathbf{Fin}_{\square} \circledast \mathbf{Fin} = \mathbf{Fin}_{\square}$
Law F-5	$\mathbf{Fin}_c \circledast \mathbf{Fin}_c = \mathbf{Fin}_{c^2}$
Law F-2a	$\mathbf{Fin}_{\square}(\mathcal{A}) \circledast \mathbf{Fin}_{\square}(\mathcal{B}) = \mathbf{Fin}_{\square}(\mathcal{B})$
Law F-3a	$\mathbf{Fin}(\mathcal{A}) \circledast \mathbf{Fin}_{\square}(\mathcal{B}) = \mathbf{Fin}_{\square}(\mathcal{B})$.

Theorem A.1. [Law F-1] *For any (possibly degenerate) observable:*

$$\mathbf{Fin} \circledast \mathbf{Fin} = \mathbf{Fin}.$$

Proof. Let \mathcal{O} denote our observable. We reason from the left-hand side:

$$\begin{aligned}
& \mathbf{Fin} \mathbin{\text{\textcircled{;}}} \mathbf{Fin} \\
& = \text{definition of } \mathbf{Fin} \\
& \left[\left(r, \chi := i, \frac{P_i \chi}{\|P_i \chi\|} \right) \text{\textcircled{@}} \langle \chi, P_i \chi \rangle \mid i \in \Lambda_{\mathcal{O}} \right] \mathbin{\text{\textcircled{;}}} \mathbf{Fin} \\
& = \text{law S-1} \\
& \left[\left(r, \chi := i, \frac{P_i \chi}{\|P_i \chi\|} \mathbin{\text{\textcircled{;}}} \mathbf{Fin} \right) \text{\textcircled{@}} \langle \chi, P_i \chi \rangle \mid i \in \Lambda_{\mathcal{O}} \right] \\
& = \text{definition of } \mathbf{Fin} \\
& \left[\left(\left(r, \chi := i, \frac{P_i \chi}{\|P_i \chi\|} \mathbin{\text{\textcircled{;}}} \left[\left(r, \chi := j, \frac{P_j \chi}{\|P_j \chi\|} \right) \text{\textcircled{@}} \langle \chi, P_j \chi \rangle \mid j \in \Lambda_{\mathcal{O}} \right] \right) \text{\textcircled{@}} \langle \chi, P_i \chi \rangle \mid i \in \Lambda_{\mathcal{O}} \right) \right] \\
& = \text{law A-1} \\
& \left[\left[\left(r, \chi := j, \frac{P_j P_i \chi}{\|P_j P_i \chi\|} \right) \text{\textcircled{@}} \langle P_i \chi, P_j P_i \chi \rangle \mid j \in \Lambda_{\mathcal{O}} \right] \text{\textcircled{@}} \langle \chi, P_i \chi \rangle \mid i \in \Lambda_{\mathcal{O}} \right] \\
& = P_i P_j = 0 \text{ if } i \neq j, P_i \text{ idempotent} \\
& \left[\left(r, \chi := i, \frac{P_i \chi}{\|P_i \chi\|} \right) \text{\textcircled{@}} \langle \chi, P_i \chi \rangle \mid i \in \Lambda_{\mathcal{O}} \right] \\
& = \text{definition of } \mathbf{Fin} \\
& \mathbf{Fin}
\end{aligned}$$

□

Lemma A.2. *For any nondegenerate observable \mathcal{A} :*

$$r, \chi := E, F \mathbin{\text{\textcircled{;}}} \mathbf{Fin}_{\sqcap}(\mathcal{A}, r, \chi) = \mathbf{Fin}_{\sqcap}(\mathcal{A}, r, \chi)$$

where E is an expression ranging over \mathcal{A} 's return values, and F is an expression of type qureg .

Proof. Let a_i denote the orthonormal eigenvector basis of \mathcal{A} :

$$\begin{aligned}
& r, \chi := E, F \mathbin{\text{\textcircled{;}}} \mathbf{Fin}_{\sqcap}(\mathcal{A}, r, \chi) \\
& = \text{definition of } \mathbf{Fin}_{\sqcap} \\
& r, \chi := E, F \mathbin{\text{\textcircled{;}}} \sqcap [r, \chi := i, \mu_i \mid i \in \Lambda_{\mathcal{A}}] \\
& = \text{law A-2} \\
& \sqcap [(r, \chi := E, F \mathbin{\text{\textcircled{;}}} r, \chi := i, \mu_i) \mid i \in \Lambda_{\mathcal{A}}] \\
& = \text{law A-3 (} i \text{ and } \mu_i \text{ are constants)}
\end{aligned}$$

$$\begin{aligned}
& \sqcap[r, \chi := i, \mu_i \mid i \in \Lambda_{\mathcal{A}}] \\
& = \text{definition of } \mathbf{Fin}_{\sqcap} \\
& \mathbf{Fin}_{\sqcap}
\end{aligned}$$

□

The law $\mathbf{Fin}_{\sqcap} \circledast \mathbf{Fin}_{\sqcap} = \mathbf{Fin}_{\sqcap}$ can be generalised to two observables.

Theorem A.3. [Law F-2a] *For nondegenerate observables \mathcal{A}, \mathcal{B} :*

$$\mathbf{Fin}_{\sqcap}(\mathcal{A}, r, \chi) \circledast \mathbf{Fin}_{\sqcap}(\mathcal{B}, r, \chi) = \mathbf{Fin}_{\sqcap}(\mathcal{B}, r, \chi)$$

Proof. Let a_i, b_j denote respectively the orthonormal eigenvector basis of \mathcal{A}, \mathcal{B} . We reason from the left-hand side:

$$\begin{aligned}
& \mathbf{Fin}_{\sqcap}(\mathcal{A}, r, \chi) \circledast \mathbf{Fin}_{\sqcap}(\mathcal{B}, r, \chi) \\
& = \text{definition of } \mathbf{Fin}_{\sqcap} \\
& \sqcap[r, \chi := i, a_i \mid i \in \Lambda_{\mathcal{A}}] \circledast \mathbf{Fin}_{\sqcap}(\mathcal{B}, r, \chi) \\
& = \text{law S-2} \\
& \sqcap[r, \chi := i, a_i \circledast \mathbf{Fin}_{\sqcap}(\mathcal{B}, r, \chi) \mid i \in \Lambda_{\mathcal{A}}] \\
& = \text{Lemma A.2} \\
& \sqcap[\mathbf{Fin}_{\sqcap}(\mathcal{B}, r, \chi) \mid i \in \Lambda_{\mathcal{A}}] \\
& = \text{law S-2 and skip identity} \\
& \mathbf{Fin}_{\sqcap}(\mathcal{B}, r, \chi)
\end{aligned}$$

□

When $\mathcal{A} = \mathcal{B}$ we get of course law F-2.

Theorem A.4. [Law F-3a] *For any observable \mathcal{A} and nondegenerate observable \mathcal{B} :*

$$\mathbf{Fin}(\mathcal{A}, r, \chi) \circledast \mathbf{Fin}_{\sqcap}(\mathcal{B}, r, \chi) = \mathbf{Fin}_{\sqcap}(\mathcal{B}, r, \chi)$$

Proof. We reason:

$$\begin{aligned}
& \mathbf{Fin}(\mathcal{A}, r, \chi) \circledast \mathbf{Fin}_{\sqcap}(\mathcal{B}, r, \chi) \\
& = \text{definition of } \mathbf{Fin} \\
& \left[\left(r, \chi := i, \frac{P_i \chi}{\|P_i \chi\|} \right) @ \langle \chi, P_i \chi \rangle \mid i \in \Lambda_{\mathcal{A}} \right] \circledast \mathbf{Fin}_{\sqcap}(\mathcal{B}, r, \chi)
\end{aligned}$$

$$\begin{aligned}
&= \text{law S-1} \\
&\left[\left(r, \chi := i, \frac{P_i \chi}{\|P_i \chi\|} \circledast \mathbf{Fin}_\square(\mathcal{B}, r, \chi) \right) @ \langle \chi, P_i \chi \rangle \mid i \in \Lambda_{\mathcal{A}} \right] \\
&= \text{Lemma A.2} \\
&\left[\mathbf{Fin}_\square(\mathcal{B}, r, \chi) @ \langle \chi, P_i \chi \rangle \mid i \in \Lambda_{\mathcal{A}} \right] \\
&= \text{law S-1 and skip identity} \\
&\mathbf{Fin}_\square(\mathcal{B}, r, \chi)
\end{aligned}$$

□

Again, law F-3 is deduced when $\mathcal{A} = \mathcal{B}$.

Theorem A.5. [Law F-4] *For any nondegenerate observable:*

$$\mathbf{Fin}_\square \circledast \mathbf{Fin} = \mathbf{Fin}_\square$$

Proof. Let a_i denote the orthonormal eigenvector basis of some nondegenerate observable \mathcal{A} . We reason:

$$\begin{aligned}
&\mathbf{Fin}_\square(\mathcal{A}, r, \chi) \circledast \mathbf{Fin}(\mathcal{A}, r, \chi) \\
&= \text{definition of } \mathbf{Fin}_\square \text{ and law S-2} \\
&\square \left[r, \chi := i, a_i \circledast \mathbf{Fin}(\mathcal{A}, r, \chi) \mid i \in \Lambda_{\mathcal{A}} \right] \\
&= \text{definition of } \mathbf{Fin} \\
&\square \left[r, \chi := i, a_i \circledast \left[\left(r, \chi := j, \frac{P_j \chi}{\|P_j \chi\|} \right) @ \langle \chi, P_j \chi \rangle \mid j \in \Lambda_{\mathcal{A}} \right] \mid i \in \Lambda_{\mathcal{A}} \right] \\
&= \text{law A-1} \\
&\square \left[\left[\left(r, \chi := i, a_i \circledast r, \chi := j, \frac{P_j \chi}{\|P_j \chi\|} \right) @ \langle a_i, P_j a_i \rangle \mid j \in \Lambda_{\mathcal{A}} \right] \mid i \in \Lambda_{\mathcal{A}} \right] \\
&= P_j \perp a_i \text{ if } i \neq j \\
&\square \left[\left(r, \chi := i, a_i \circledast r, \chi := i, \frac{P_i \chi}{\|P_i \chi\|} \right) \mid i \in \Lambda_{\mathcal{A}} \right] \\
&= \text{law A-3} \\
&\square \left[\left(r, \chi := i, \frac{P_i a_i}{\|P_i a_i\|} \right) \mid i \in \Lambda_{\mathcal{A}} \right] \\
&= P_i a_i = a_i \text{ and definition of } \mathbf{Fin}_\square \\
&\mathbf{Fin}_\square(\mathcal{A}, r, \chi)
\end{aligned}$$

□

Lemma A.6. *For any $c \in [0, 1]$ and nondegenerate observable:*

$$\mathbf{Fin}_\square \circledast \mathbf{Fin}_c = \mathbf{Fin}_\square$$

Proof. We prove equality by showing refinement and abstraction. We begin with refinement:

$$\begin{aligned} & \mathbf{Fin}_\square \circledast \mathbf{Fin}_c \\ & \sqsubseteq && \mathbf{Fin}_c \sqsubseteq \mathbf{Fin} \text{ (Corollary 3.2)} \\ & \mathbf{Fin}_\square \circledast \mathbf{Fin} \\ & = && \text{Theorem A.5} \\ & \mathbf{Fin}_\square . \end{aligned}$$

Abstraction is

$$\begin{aligned} & \mathbf{Fin}_\square \\ & = && \text{Theorem A.3} \\ & \mathbf{Fin}_\square \circledast \mathbf{Fin}_\square \\ & = && \text{law P-1} \\ & \mathbf{Fin}_\square \circledast (\mathbf{Fin}_\square \oplus_c \mathbf{Fin}_\square) \\ & \sqsubseteq && \mathbf{Fin} \sqsubseteq \mathbf{Fin}_\square \text{ (Lemma 3.1)} \\ & \mathbf{Fin}_\square \circledast (\mathbf{Fin}_c \oplus \mathbf{Fin}_\square) \\ & = && \text{definition of } \mathbf{Fin}_c \\ & \mathbf{Fin}_\square \circledast \mathbf{Fin}_c \end{aligned}$$

□

We can prove our last law.

Theorem A.7. [Law F-5] *For any $c \in [0, 1]$ and nondegenerate observable:*

$$\mathbf{Fin}_c \circledast \mathbf{Fin}_c = \mathbf{Fin}_{c^2}$$

Proof. We reason:

$$\begin{aligned} & \mathbf{Fin}_c \circledast \mathbf{Fin}_c \\ & = && \text{definition of } \mathbf{Fin}_c \\ & (\mathbf{Fin}_c \oplus \mathbf{Fin}_\square) \circledast \mathbf{Fin}_c \end{aligned}$$

$$\begin{aligned}
&= && \text{law S-1} \\
&(\mathbf{Fin} \mathbin{\text{;}} \mathbf{Fin}_c)_c \oplus (\mathbf{Fin}_\square \mathbin{\text{;}} \mathbf{Fin}_c) \\
&= && \text{Lemma A.6} \\
&(\mathbf{Fin} \mathbin{\text{;}} \mathbf{Fin}_c)_c \oplus \mathbf{Fin}_\square \\
&= && \text{definition of } \mathbf{Fin}_c \\
&(\mathbf{Fin} \mathbin{\text{;}} \mathbf{Fin}_c \oplus \mathbf{Fin}_\square)_c \oplus \mathbf{Fin}_\square \\
&= && \text{law F-3} \\
&(\mathbf{Fin} \mathbin{\text{;}} \mathbf{Fin}_c \oplus \mathbf{Fin} \mathbin{\text{;}} \mathbf{Fin}_\square)_c \oplus \mathbf{Fin}_\square \\
&= && \text{Theorems A.1 and A.4} \\
&(\mathbf{Fin}_c \oplus \mathbf{Fin}_\square)_c \oplus \mathbf{Fin}_\square \\
&= && \text{law P-4} \\
&\mathbf{Fin}_{c^2} \oplus \mathbf{Fin}_\square \\
&= && \text{definition of } \mathbf{Fin}_c \\
&\mathbf{Fin}_{c^2}
\end{aligned}$$

□

B Semantics and programming laws

Semantics for pGCL (and in turn for qGCL) can be given either relationally [11] or in terms of expectation transformers [14]. The former relates each initial state to a set of final distributions. The latter extends pre- and post-conditions to pre- and post-*expectations*: real-valued random variables. The two models are related by a Galois connection embedding the relational in the transformer [14].

We briefly present the main definitions and concepts of the transformer model. An *expectation* is a \mathbf{R}^+ -valued function on a state space X . The set \mathcal{Q} of all expectations is $\mathcal{Q} \hat{=} X \rightarrow \mathbf{R}^+$. Expectations can be ordered using the standard pointwise functional ordering for which we shall use the symbol \Rightarrow . Standard predicates are easily embedded in \mathcal{Q} by identifying *true* with expectation $\mathbf{1}$ and *false* with $\mathbf{0}$. For standard predicate p we shall write $[p]$ for its embedding.

An expectation transformer represent a computation by mapping post-expectations to their greatest pre-expectations. The expectation-transformer semantics for the pGCL commands used in the paper is (we retain the *wp*

prefix for convenience):

$$\begin{aligned}
wp.(x := E).q &\hat{=} q[x \setminus E] \\
wp.(prg_1 \sqcap prg_2).q &\hat{=} (wp.prg_1.q) \sqcap (wp.prg_2.q) \\
wp.(prg_1 \oplus_r prg_2).q &\hat{=} p \cdot (wp.prg_1.q) + \bar{p} \cdot (wp.prg_2.q)
\end{aligned}$$

where $q \in \mathcal{Q}$, $x \in X$, $p \in [0, 1]$; $q[x \setminus E]$ denotes the expectation obtained after replacing all free occurrences of x in q by expression E ; \sqcap denotes the greatest lower bound.

pGCL enjoys a refinement calculus, which derives from the semantics above; when we say that program Q refines program P , written $P \sqsubseteq Q$, we mean:

$$P \sqsubseteq Q \hat{=} \forall q: \mathcal{Q} \bullet wp.P.q \Rightarrow wp.Q.q .$$

Intuitively, $P \sqsubseteq Q$ means that Q is at least as deterministic as P . The converse of refinement is *abstraction* and it is denoted by \sqsupseteq . When $P \sqsupseteq Q$ and $P \sqsubseteq Q$ then P and Q are equal programs and we write $P = Q$.

We list a few algebraic laws which hold for pGCL programs; for more laws see Appendix B of [13].

Law (skip identity). $prg \ ; \ \mathbf{skip} = \mathbf{skip} \ ; \ prg = prg$

Law (N-1). $prg \sqcap prg = prg$

Law (N-2). $prg_1 \sqcap prg_2 = prg_2 \sqcap prg_1$

Law (P-1). $prg \oplus_r prg = prg$

Law (P-2). $prg_1 \oplus_r prg_2 = prg_2 \oplus_{\bar{r}} prg_1$

Law (P-3). $(prg_1 \sqcap prg_2) \oplus_r prg_3 = (prg_1 \oplus_r prg_3) \sqcap (prg_2 \oplus_r prg_3)$

Law (P-4). $(prg_1 \oplus_p prg_2) \oplus_q (prg_3 \oplus_r prg_4) = \begin{array}{l} prg_1 \quad @ \quad pq \\ prg_2 \quad @ \quad \bar{p}q \\ prg_3 \quad @ \quad \bar{q}r \\ prg_4 \quad @ \quad \bar{q}\bar{r} \end{array}$

Law (S-1). $(prg_1 \oplus_r prg_2) \ ; \ prg_3 = (prg_1 \ ; \ prg_3) \oplus_r (prg_2 \ ; \ prg_3)$

Law (S-2). $(prg_1 \sqcap prg_2) \ ; \ prg_3 = (prg_1 \ ; \ prg_3) \sqcap (prg_2 \ ; \ prg_3)$

Law (S-3). $(prg_1 \geq_r \oplus prg_2) \ ; \ prg_3 = (prg_1 \ ; \ prg_3) \geq_r \oplus (prg_2 \ ; \ prg_3)$

Law (S-4). $(prg_1 \oplus_r prg_2) \geq_s \oplus (prg_3 \oplus_r prg_2) = (prg_1 \geq_s \oplus prg_3) \oplus_r prg_2$

Law (A-1). $x := e \ ; (prg_1 \ r \oplus \ prg_2) = (x := e \ ; prg_1) \ r[x \setminus e] \oplus (x := e \ ; prg_2)$

Law (A-2). $x := e \ ; (prg_1 \ \sqcap \ prg_2) = (x := e \ ; prg_1) \ \sqcap \ (x := e \ ; prg_2)$

Law (A-3). $(x := e \ ; x := f) = x := f[x \setminus e]$

Law (A-4). $x := e \ ; (prg_1 \ \succcurlyeq_r \oplus \ prg_2) = (x := e \ ; prg_1) \ \succcurlyeq_{r[x \setminus e]} \oplus (x := e \ ; prg_2)$

Expression $r[x \setminus e]$ is obtained replacing all free occurrences of x in r by e .

Proof of Lemma 6.1. We reason from the LHS:

$$\begin{aligned}
& (prg_1 \ \succcurlyeq_q \oplus \ prg_2) \ \succcurlyeq_p \oplus \ (prg_3 \ \succcurlyeq_q \oplus \ prg_4) \\
= & \hspace{15em} \text{definition of } \succcurlyeq \oplus \\
& (prg_1 \ \succcurlyeq_q \oplus \ prg_2) \ \oplus_p \ ((prg_1 \ \succcurlyeq_q \oplus \ prg_2) \ \sqcap \ (prg_3 \ \succcurlyeq_q \oplus \ prg_4)) \\
= & \hspace{15em} \text{definition of } \succcurlyeq \oplus \\
& (prg_1 \ \oplus_q \ (prg_1 \ \sqcap \ prg_2)) \ \oplus_p \ ((prg_1 \ \succcurlyeq_q \oplus \ prg_2) \ \sqcap \ (prg_3 \ \succcurlyeq_q \oplus \ prg_4)) \\
= & \hspace{10em} \text{rearrange with } r = \frac{p-pq}{1-pq} \\
& prg_1 \ \oplus_{pq} \ ((prg_1 \ \sqcap \ prg_2) \ \oplus_r \ ((prg_1 \ \succcurlyeq_q \oplus \ prg_2) \ \sqcap \ (prg_3 \ \succcurlyeq_q \oplus \ prg_4))) \\
\sqsubseteq & \hspace{15em} \succcurlyeq \oplus \ \text{refines } \sqcap \\
& prg_1 \ \oplus_{pq} \ (prg_1 \ \sqcap \ prg_2 \ \sqcap \ prg_1 \ \sqcap \ prg_2 \ \sqcap \ prg_3 \ \sqcap \ prg_4) \\
= & \hspace{10em} \sqcap \ \text{idempotent and commutative (laws N-1, N-2)} \\
& prg_1 \ \oplus_{pq} \ (prg_1 \ \sqcap \ prg_2 \ \sqcap \ prg_3 \ \sqcap \ prg_4) \\
= & \hspace{15em} \text{definition of } \succcurlyeq \oplus \\
& prg_1 \ \succcurlyeq_{pq} \oplus \ (prg_2 \ \sqcap \ prg_3 \ \sqcap \ prg_4)
\end{aligned}$$

□

C Quantum mechanics

Quantum computing theory relies on von Neumann's approach to quantum mechanics [20], that is the theory of linear operators over Hilbert spaces. A good self-contained exposition of this theory can be found in [12], for example.

C.1 Basic concepts

A Hilbert space \mathcal{H} is a vector space equipped with a scalar product making it a complete inner product space. Here we consider only complex vector spaces \mathbf{C}^n , for $n \in \mathbf{N}$. The scalar product is therefore the application $\langle \cdot, \cdot \rangle: \mathbf{C}^n \times \mathbf{C}^n \rightarrow \mathbf{C}$ defined by:

$$\langle \psi, \phi \rangle \hat{=} \sum_{0 \leq i < n} \psi_i^* \phi_i$$

where ψ_i is the i -th component of $\psi \in \mathbf{C}^n$, and z^* is the complex conjugate of $z \in \mathbf{C}$. The *length* of a vector ψ is defined $\|\psi\| \hat{=} \langle \psi, \psi \rangle^{\frac{1}{2}}$; ψ is *normalised* if $\|\psi\|^2 = 1$.

A linear function $A: \mathcal{H} \rightarrow \mathcal{H}$ is also called an *operator*. The *adjoint* (or *hermitian conjugate*) of an operator A is the operator A^\dagger defined by:

$$\forall \psi, \phi \in \mathcal{H} \bullet \langle \psi, A^\dagger \phi \rangle = \langle A\psi, \phi \rangle.$$

A linear operator A is *self-adjoint* (or *hermitian*) if $A = A^\dagger$. In the case of infinite-dimensional Hilbert spaces there is a difference between self-adjointness and hermiticity, but since here we deal only with finite spaces we consider them equivalent. Also, we should check that A^\dagger defined above is actually an operator (which it is, as a matter of fact). All these mathematical details can be found in Reed and Simon's book [16], for example.

In von Neumann's approach to quantum mechanics the state of a physical system is modelled by a vector of some n -dimensional complex Hilbert space and state evolution is modelled by linear operators. As a consequence any quantum operator on \mathcal{H} can always be written as a $n \times n$ complex matrix.

Let A be a $n \times n$ matrix representing a quantum operator \mathcal{A} . Then, with respect to an orthonormal basis, the elements of the matrix representing \mathcal{A}^\dagger satisfy:

$$\forall i, j \in \{1, \dots, n\} \bullet (A^\dagger)_{ij} = A_{ji}^*.$$

We note that if \mathcal{A} is self-adjoint then $A_{ij} = A_{ji}^*$.

Quantum transformations satisfy also another property: they are *unitary*. Such an operator guarantees the existence of the inverse operator and preserves scalar products, that is for an operator U unitary we have:

$$\forall \psi, \phi \in \mathcal{H} \bullet \langle U\psi, U\phi \rangle = \langle \psi, \phi \rangle$$

In terms of matrices it means that the matrix U modelling the evolution of the system must satisfy:

$$U \cdot U^\dagger = U^\dagger \cdot U = \mathbf{1}$$

where $\mathbf{1}$ is the identity matrix of appropriate size. The set of complex unitary matrices forms a group with the usual matrix multiplication.

A (non-zero) vector $\psi:\mathcal{H}$ is an *eigenvector* of an operator A with *eigenvalue* $a:\mathbb{C}$ if:

$$A\psi = a\psi.$$

In quantum mechanics an *observable* is represented by a self-adjoint operator and the measurable values are exactly the eigenvalues of that operator. It is easy to show that the eigenvalues of a self-adjoint operator are real numbers.

For $\psi:\mathcal{H}$ we write P_ψ for the projector onto the one-dimensional subspace spanned by vector ψ :

$$\forall\phi:\mathcal{H} \bullet P_\psi(\phi) \hat{=} \frac{\psi}{\|\psi\|^2} \cdot \langle\psi, \phi\rangle.$$

For an observable \mathcal{O} we denote by $\Lambda_{\mathcal{O}}$ the set of its eigenvalues. For $\lambda \in \Lambda_{\mathcal{O}}$ we denote by $E_{\mathcal{O},\lambda}$ its eigenspace and by $P_{\mathcal{O}}^\lambda$ the projector over that space. The fundamental *spectral theorem* for self-adjoint operators on finite-dimensional Hilbert spaces states that the operator's eigenspaces are pairwise orthogonal and complete in the Hilbert space [12]. In other words, we have that

$$\mathcal{O} = \sum_{\lambda \in \Lambda_{\mathcal{O}}} \lambda \cdot P_{\mathcal{O}}^\lambda.$$

The rules of quantum theory state that if the state of a system is described by some normalised vector $\psi:\mathcal{H}$ then, if a measurement of observable \mathcal{O} is made, the probability that the result will be the particular eigenvalue λ is:

$$\text{Prob}(\mathcal{O} = \lambda \mid \psi) = \langle\psi, P_{\mathcal{O}}^\lambda\psi\rangle. \tag{9}$$

Note that the probability does not change if the state vector ψ is multiplied by an arbitrary complex number of modulus 1.

By the spectral theorem we deduce that the family of eigenspaces of an observable \mathcal{O} is a partition for \mathcal{H} and we have seen that to each eigenspace there is an associated projector $P_{\mathcal{O}}^\lambda$. A projector is a self-adjoint operator with just two eigenvalues, 0 and 1; therefore a measurement of an observable \mathcal{O} tells us in which subspace the state vector ψ has “fallen”, as a consequence of the measurement process.

The probability rule written above is a special case of the following rule, which holds even for observables with continuous eigenvalue spectrum. The

expected result $\langle \mathcal{O} \rangle_\psi$ of measuring \mathcal{O} on a system described by (normalised) state $\psi: \mathcal{H}$ is

$$\langle \mathcal{O} \rangle_\psi \hat{=} \langle \psi, \mathcal{O}\psi \rangle .$$

Alternatively, one can define an observable from a family of pairwise orthogonal subspaces which together span the whole space \mathcal{H} and then consider the projector of each subspace.

Finally, functions of operators can be defined, and we are in particular interested in functions of self-adjoint operators, *i.e.* functions of observables. For self-adjoint operator \mathcal{O} (whose eigenvalues are always real numbers) and function $f: \mathbf{R} \rightarrow \mathbf{R}$ we define

$$f(\mathcal{O}) \hat{=} \sum_{\lambda \in \Lambda_{\mathcal{O}}} f(\lambda) \cdot P_{\mathcal{O}}^\lambda .$$

Note that $f(\mathcal{O})$ is self-adjoint, since $f(\lambda)$ is real for all λ .

C.2 Tensor products

The state of a composite quantum system is described by the tensor product of Hilbert spaces. Consider two complex Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2$ of dimensions n_1, n_2 respectively. For any pair of vectors $\psi: \mathcal{H}_1, \phi: \mathcal{H}_2$, the *tensor vector* $\psi \otimes \phi$ is given by the map $(\cdot \otimes \cdot): \mathcal{H}_1 \times \mathcal{H}_2 \rightarrow \mathbf{C}^{n_1 \cdot n_2}$:

$$(\psi \otimes \phi)_i \hat{=} \psi_i \operatorname{div}_{n_2} \phi_{i \bmod n_2} \quad 0 \leq i < n_1 \cdot n_2 .$$

Tensor products are linear in each argument, that is:

$$\forall \alpha, \beta: \mathbf{C}, \psi, \phi: \mathcal{H}_1, \chi: \mathcal{H}_2 \bullet (\alpha\psi + \beta\phi) \otimes \chi = (\alpha\psi) \otimes \chi + (\beta\phi) \otimes \chi,$$

$$\forall \alpha, \beta: \mathbf{C}, \psi, \phi: \mathcal{H}_1, \chi: \mathcal{H}_2 \bullet \psi \otimes (\alpha\phi + \beta\chi) = \psi \otimes (\alpha\phi) + \psi \otimes (\beta\chi).$$

Multiplication by a complex number distributes across the tensor product:

$$\forall \alpha: \mathbf{C}, \psi: \mathcal{H}_1, \phi: \mathcal{H}_2 \bullet \alpha(\psi \otimes \phi) = (\alpha\psi) \otimes \phi = \psi \otimes (\alpha\phi).$$

Consider now the vector space $\mathbf{C}^{n_1 \cdot n_2}$: defining the scalar product $\langle \psi_1 \otimes \psi_2, \phi_1 \otimes \phi_2 \rangle \hat{=} \langle \psi_1, \phi_1 \rangle_{\mathcal{H}_1} \langle \psi_2, \phi_2 \rangle_{\mathcal{H}_2}$ enable us to define a new Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$, called the *tensor product* of \mathcal{H}_1 and \mathcal{H}_2 . Vectors in $\mathcal{H}_1 \otimes \mathcal{H}_2$ which cannot be written as a single product $\psi \otimes \phi$ for any $\psi: \mathcal{H}_1$ or $\phi: \mathcal{H}_2$, are called *entangled*. For example, in \mathbf{C}^4 the vector

$$\frac{1}{\sqrt{2}}(e_0 \otimes e_1 - e_1 \otimes e_0)$$

is entangled (e_0 and e_1 are the standard basis for \mathbf{C}^2). However, every vector in $\mathcal{H}_1 \otimes \mathcal{H}_2$ can be written as a *sum* of such product vectors.

The tensor product can be extended to linear operators over Hilbert spaces. Let $A_1: \mathcal{H}_1 \rightarrow \mathcal{H}_1$ and $A_2: \mathcal{H}_2 \rightarrow \mathcal{H}_2$ be two linear operators over Hilbert spaces \mathcal{H}_1 and \mathcal{H}_2 respectively. The operator $A_1 \otimes A_2: \mathcal{H}_1 \otimes \mathcal{H}_2 \rightarrow \mathcal{H}_1 \otimes \mathcal{H}_2$ is defined as:

$$(A_1 \otimes A_2)\psi_1 \otimes \psi_2 \hat{=} (A_1\psi_1) \otimes (A_2\psi_2)$$

where $\psi_1: \mathcal{H}_1$ and $\psi_2: \mathcal{H}_2$. By linearity it is extended to any vector in $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Since linear operators can be represented by matrices, the tensor product is readily available for them, too. Let $A = (a_{i,j})$ and B be two matrices of dimensions $m \times n$ and $p \times q$ respectively: the tensor product $A \otimes B$ is the $mp \times nq$ matrix:

$$\begin{pmatrix} a_{0,0}B & a_{0,1}B & \cdots & a_{0,n-1}B \\ a_{1,0}B & & & \\ \vdots & & & \vdots \\ a_{m-1,0}B & \cdots & a_{m-1,n-1}B \end{pmatrix}$$

The tensor product of matrices preserves unitarity and distributes over standard matrix multiplication, that is for operators M, N, L, P we have:

$$(M \cdot N) \otimes (L \cdot P) = (M \otimes L) \cdot (N \otimes P).$$