Programming Research Group

FORMAL REASONING FOR QUANTUM MECHANICAL NONLOCALITY

Paolo Zuliani

PRG-RR-01-05

Oxford University Computing Laboratory
Wolfson Building, Parks Road, Oxford OX1 3QD

Abstract

Nonlocality is an intriguing aspect of quantum mechanics which has puzzled scientists since the seminal work of Einstein, Podolsky and Rosen in 1935: events may have simultaneous effects, no matter how far one from the other they occur. Here we use a programming language developed for quantum computation, $qGCL$, to formalize and reason about the most famous examples of this phenomenon. $qGCL$ makes use of the modern programming techniques such as program refinement, abstraction and algebraic laws. Our formalism offers a unified rigorous treatment of various quantum systems, where all formal reasoning is accomplished by using algebraic laws rather than semantics, with corresponding simplicity and clarity.

1 Introduction

In this paper we shall show how it is possible to use a suitable programming language ($qGCL$) for reasoning about one of the strangest properties of quantum mechanics: nonlocality.

Nonlocality is the fact that an event occuring in one point of the universe can have a *simultaneous* effect in another part of the universe. The two parties may be arbitrarily distant, such that no signal can usefully travel directly between them.

The aim of this work is two-fold: to provide a further test for the suitability of $qGCL$ as a tool for describing and reasoning about quantum systems and thereby providing a rigorous treatment within Computation of various *Gedankenexperimente* from Quantum Physics.

$qGCL$ [18] is a general-purpose programming language for quantum computation developed as a superset of the *probabilistic* guarded-command language ($pGCL$). In particular, $qGCL$ extends $pGCL$ with four constructs:

- transformation q, that converts a classical bit register to its quantum analogue, a *qureg*;
- *initialisation*, which prepares a qureg for a quantum computation;
- *evolution*, which consists of iteration of unitary operators on quregs;
- *finalisation* or observation, which reads the content of a qureg.

$qGCL$ enjoys the same features of $pGCL$: it has a rigorous semantics and an associated refinement calculus (see for example [16, 17, 12]), which include program refinement, data refinement and combination of specifications with code. $qGCL$ has been successfully used to describe and reason about all known quantum algorithms and also to derive one of them (the Deutsch-Jozsa algorithm) from its specification [18].

The most famous example of nonlocality is the so called EPR paradox, named after a paper by Einstein, Podolsky and Rosen in 1935 [8]. Their Gedankenexperiment consists in a source emitting two spin-$\frac{1}{2}$ particles, whose total spin is zero. The two particles move away one from the other and the components of their spins are subsequently measured in the same direction by two observers, P and J say. Conservation of total spin entails that if P measures $+\frac{1}{2}$, then J will necessarily measure spin $-\frac{1}{2}$ and *vice versa*. The results are thus *anticorrelated*. The paradox lies in the fact that whoever between P and J measures the spin first, the outcome of the measurement will *simultaneously* constrain the measurement of the other party, no matter how far it is. Using $qGCL$ we shall write a program to formalize this paradox.

A possible solution to the paradox is to suppose the existence of "hidden variables" whose values are not possible to measure in the normal way but, working "behind the scenes", determine the actual measured values of what we normally regard as observables. Good examples are the microstates of classical thermodynamics: for a gas the values measured for observables like pressure, volume and temperature are ultimately determined by the values of the hidden variables representing the position and the energy of every single molecule composing the gas. The measurement of these hidden variables or microstates is not feasible in practice, due to the huge number of molecules present in the gas.

Hidden variable theories reproducing the results of quantum mechanics do in fact exist, although they exhibit a nonlocality as that discussed above. A result of Bell in 1964 [3] showed that this is not a problem of a particular hidden variable theory: any such theory which is expected to mimic quantum mechanics results will *necessarily* possess nonlocal features. In particular, he derived a set of inequalities which are true in any local physical theory consistent with quantum theory results, except quantum mechanics itself. Actual experiments performed by Aspect *et al.* [1] in the eighties confirmed the violation of Bell inequalities, in the way predicted by quantum theory.

Since Bell's original work, many other examples of "Bell inequalities" have been developed. We will here consider two examples by Mermin [13, 14]: the former is on the same line of Bell's work, describing a Gedankenexperiment which offer a statistical violation of some properties true in any local physical theory (statistical violation means that the properties are refuted only over a series of runs of the experiment). The latter offers a more dramatic violation of locality: a *single* run of his Gedankenexperiment suffices to rule out local theories wishing to mimic quantum theory results.

For both examples we shall write the corrisponding $qGCL$ program simulating the experiments; we shall also write the programs implementing the local theories constrained to reproduce the same results of quantum theory. Using algebraic laws and standard expectation-transformer semantics we will compare the quantum and the local programs on selected expectations, thus deriving the desired violation of locality.

Finally, we consider Bell's original proof of nonlocality, using $qGCL$ for formalizing one of his inequalities and showing how quantum mechanics violate that inequality.

2 Quantum programming

We give here a short presentation of the features of $qGCL$ (a full introduction can be found in [18]). $qGCL$ is an extension of $pGCL$ [16], which in turn extends Dijkstra's guarded-command language GCL [7] with probabilism.

We start the exposition with the data types required by quantum computation, then we introduce *pGCL* and successively *qGCL*'s quantum-related constructs.

2.1 Quantum types

We present a transformation q which maps a classical data type to its quantum analogue. All our later examples require the application of q only to registers, so we restrict ourselves to that case.

We define the type $\mathbb{B} := \{0, 1\}$, which we will treat as booleans or bits, depending on convenience. A classical register of size $n{:}\mathbb{N}$ 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 $\{0, 1, \ldots, n-1\}$:

$$\mathbb{B}^n := \{0, 1, \ldots, n-1\} \longrightarrow \mathbb{B}\,.$$

The quantum analogue of $\mathbb{B}^n$ is the set of complex-valued functions on $\mathbb{B}^n$ whose squared modulus sum to 1:

$$q(\mathbb{B}^n) := \{\chi{:}\mathbb{B}^n \longrightarrow \mathbb{C} \quad | \sum_{x:\mathbb{B}^n} |\chi(x)|^2 = 1\}\,.$$

An element of $q(\mathbb{B})$ is called a *qubit* [19] and that of $q(\mathbb{B}^n)$ a *qureg*. Classical state is embedded in its quantum analogue by the Dirac delta function:

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

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

$$\forall \chi{:}q(\mathbb{B}^n) \bullet \chi = \sum_{x:\mathbb{B}^n} \chi(x)\delta_x\,.$$

The Hilbert space $\mathbb{B}^n \longrightarrow \mathbb{C}$ (with the structure making it isomorphic to $\mathbb{C}^{2^n}$) is called the *enveloping space* of $q(\mathbb{B}^n)$.

2.2 Probabilistic language pGCL

A guarded-command language program is a sequence of assignments, **skip** and **abort** manipulated by the standard constructors of sequential composition, conditional selection, repetition and nondeterministic choice [7]. Assignments is in the form $x := e$, where x is a vector of program variables and e a vector of expressions whose evaluations always terminate with a single value. *pGCL* denotes the guarded-command language extended with the binary constructor ${}_p\oplus$ for $p{:}[0, 1]$, in order to deal with probabilism. We list all the other *pGCL* basic statements and constructors, though we shall use only a few of them in this paper:

- **skip**, which always terminates doing nothing;
- **abort**, which models divergence;

- **var**, variable declaration and begin local block;
- **rav**, end local block;
- sequential composition, $R \fatsemi S$, which firstly executes R and then, if R has terminated, executes S;
- iteration, **while** *cond* **do** S **od**, which executes S as long as predicate *cond* holds;
- binary conditional, $R \lhd cond \rhd S$, which executes R if predicate *cond* holds and executes S otherwise;
- nondeterministic choice, $R \sqcap S$, which executes R or S, according to some rule inaccessible to the program at the current level of abstraction;
- probabilistic choice, $R\,_p\!\oplus S$, which executes R with probability p and S with probability $1-p$;
- procedure declaration, **proc** $P(param) := body$, where *body* is a valid *pGCL* statement (including the specification statement, see below) and *param* is the parameter list, which may be empty. Parameters can be declared as **value**, **result** or **value result**, according to Morgan's notation [15]. As a quick explanation we will say that a **value** parameter is read-only, a **result** parameter is write-only and a **value result** parameter can be read and written. Procedure P is invoked by simply writing its name and filling the parameter list according to P's declaration.

For the probabilistic combinator $_p\oplus$ we allow p to be an expression whose evaluation returns a real in $[0,1]$. Both nondeterministic and probabilistic choice may be written using a prefix notation, in case the branches are more than two.

If E is a non empty set of expressions and x a program variable, then in *GCL* the assignment $x :\in E$ denotes the nondeterministic choice over all individual assignments of elements of E to x. In *pGCL* that choice is interpreted to occur with *uniform* probability.

For our purposes it is also useful to augment *pGCL* with the specification statement [15]:

$$x : [pre, post]\,.$$

It describes a computation which changes variable x in such a way that, if predicate *pre* holds on the initial value of x, termination is insured in a state satisfying predicate *post* over initial and final values of x; if *pre* does not hold the computation aborts.

2.3 Quantum language qGCL

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

Initialisation assigns to its qureg the uniform square-convex combination of all standard states:

$$\forall \chi{:}q(\mathbb{B}^n) \bullet \mathbf{In}(\chi) := \left(\chi := \frac{1}{\sqrt{2^n}} \sum_{x:\mathbb{B}^n} \delta_x \right),$$

and it is *feasible*, *i.e.* it can be achieved in practice [5].

Evolution is the iteration of unitary trasformations on quantum state. Since there are sets of universal quantum gates [2, 6], evolution is feasible.

Finalisation corresponds to physical observation (or state reduction). In quantum mechanics, an observable is represented by a self-adjoint operator and the measurable values are exactly the eigenvalues of that operator. Equivalently, we can define an observable from a family of pairwise orthogonal subspaces which together span the enveloping space (we shall give examples of both definitions in the following Gedankenexperimente). The axioms of quantum mechanics assert that the measurement reduces the state vector to lie in one of those subspaces with different probabilities. For an exposition of basic quantum theory see [11].

Let $\mathcal{O}$ be an observable defined by the family of pairwise orthogonal subspaces $\{S_i \mid 0 \leqslant i < m\}$. In our notation we write $\mathbf{Fin}[\mathcal{O}](i, \chi)$ for the measurement of $\mathcal{O}$ on a quantum system described by state $\chi{:}q(\mathbb{B}^n)$, where i is a result parameter determining the subspace to which state is reduced and χ is a value-result parameter giving that state.

Finalisation is entirely defined using the probabilistic combinator of $pGCL$ (see [18] for an unabridged treatment):

$$\mathbf{Fin}[\mathcal{O}](i, \chi) := \oplus[(i, \chi :\in \{j\}, S_j) \,@\, \langle \chi, P_{S_j}(\chi) \rangle \mid 0 \leqslant j < m],$$

where P_{S_j} denotes the projector onto subspace S_j, which will be formally defined in the next section.

2.3.1 Background quantum theory

To support our formalism we rely on von Neumann's approach to quantum mechanics [20], that is the theory of linear operators on Hilbert spaces. It is a well founded theory, since in nearly seventy years there has not been any discrepancy between theoretical predictions and experimental results.

Among its advantages is the uniform treatment given to observation and state evolution, which are treated as subclasses of linear operators. Furthermore, it is able to express in a formal way any quantum system, thus helping to carry out correct reasonings.

A good self-contained exposition of this theory can be found in [11] (it does not cover infinite quantum systems, but they require many mathematical subtleties and we need finite systems only).

3 The Einstein-Podolsky-Rosen paradox

In their paper [8] Einstein, Podolsky and Rosen questioned the completeness of quantum mechanics as a physical theory. In particular, they developed a Gedankenexperiment for which they could not find any *local* physical explanation. By local we mean that an event E occuring at a time t in one point of the universe is not affected by another event F occuring at the same time t in another part of the universe. Event E will "feel" the effects of event F only at time $t + \Delta t$, where Δt is the time needed by the light to cover the distance separating the two spatial locations where E and F take place. This because of Einstein's theory of special/general relativity and Maxwell's electromagnetic theory, in which every force propagates its effects no more than the speed c, the speed of light in the vacuum.

The Gedankenexperiment considered by Einstein, Podolsky and Rosen, can be summarized as a source emitting in opposite directions pairs of spin-$\frac{1}{2}$ particles whose total spin is zero. A subsequent observation of the particles' spins along the same direction always returns anticorrelated values.

In quantum mechanics the situation is formalised by considering a state χ formed as follows, called the EPR *singlet* state:

$$\chi := \frac{1}{\sqrt{2}}(v_\uparrow \otimes v_\downarrow - v_\downarrow \otimes v_\uparrow)$$

where $v_\uparrow, v_\downarrow$ are, without loss of generality, the eigenvectors for the spin along the spatial z direction for a single particle. As we can see χ is an *entangled* state, *i.e.* it cannot be decomposed as a single tensor product of two vectors. We note that entangled states are crucial for the advantage of quantum computation over classical.

From the structure of χ we see that the observer who first makes the measurement has an equal probability of measuring spin up and spin down, therefore χ will be reduced to either $v_\uparrow \otimes v_\downarrow$ or $v_\downarrow \otimes v_\uparrow$. In both cases a subsequent measurement performed by the second observer will respectively yields spin up, spin down with probability 1, as the state vector is now a product state.

The paradox lies in the fact that whoever between the two observers measures the spin first, the outcome of the measurement will *immediately* constrain the measurement's outcome of the other party, no matter how far it is. Einstein, Podolsky and Rosen could not explain how information about each observer's individual results "travels" to reach the other particle to guarantee that the result of the measurement performed by the second observer will be the correct one. Einstein was also preoccupied by the fact that a possible explanation might conflict with his theory of special relativity, in which the speed of light is the absolute maximum speed at which information can flow from one point to another.

We considered χ written in terms of the eigenvectors of the z-spin operator, but the argument remains valid if we consider the spin operator in other spatial directions. We can generalise saying that for any unit vector it is always possible to write χ as the sum of two anticorrelated terms formed by the eigenvectors of the projection of the spin operator along that vector.

3.1 EPR quantum program

The $qGCL$ program for the EPR paradox is:

$$EPR := \left(\begin{array}{l} \textbf{var}\ a, b{:}\mathbb{B}\ ;\ \chi{:}q(\mathbb{B}^2) \bullet \\ \quad \chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}); \\ \quad \left(\begin{array}{l} \textbf{Fin}[\mathcal{A}](a,\chi); \\ \textbf{Fin}[\mathcal{B}](b,\chi) \end{array} \right) \square \left(\begin{array}{l} \textbf{Fin}[\mathcal{B}](b,\chi); \\ \textbf{Fin}[\mathcal{A}](a,\chi) \end{array} \right) \\ \textbf{rav} \end{array} \right)$$

where the 2-qubit quantum register χ represents the state of the two particles. In [18] we required a quantum procedure to begin with initialisation **In**: this does not pose any problem, because we can achieve the required state applying some unitary transformation after **In** [21].

$\mathcal{A}$ and $\mathcal{B}$ are respectively the spin observables [11] for the lefthand and righthand particle and the corresponding self-adjoint operators are $(S_z \otimes \mathbb{1}_2)$, $(\mathbb{1}_2 \otimes S_z)$, where $\mathbb{1}_2$ is the 2×2 identity matrix and S_z is the spin matrix for a single particle (in physics it is known as the z-spin matrix):

$$S_z := \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The eigenvalues of S_z are $\frac{1}{2}, -\frac{1}{2}$ with eigenvectors respectively δ_0, δ_1. The set $\{\frac{1}{2}, -\frac{1}{2}\}$ can be easily mapped onto $\mathbb{B}$ via the bijection m defined by $m.\frac{1}{2} := 0$ and $m.(-\frac{1}{2}) := 1$, therefore we shall suppose the eigenvalues belonging to $\mathbb{B}$. Variables a, b will therefore store the outcome of the measurement performed by the two observers. For $i, j{:}\mathbb{B}$ we shall write δ_{ij} for $\delta_i \otimes \delta_j$.

With the assumptions above, the self-adjoint operators for observables $\mathcal{A}, \mathcal{B}$ have eigenvalues $\lambda{:}\mathbb{B}$. The eigenvectors are given in the following table:

observable	$\lambda = 0$	$\lambda = 1$
$\mathcal{A}$	δ_{00}, δ_{01}	δ_{10}, δ_{11}
$\mathcal{B}$	δ_{00}, δ_{10}	δ_{11}, δ_{01}

therefore observables $\mathcal{A}, \mathcal{B}$ are:

$$\begin{aligned} \mathcal{A} &:= [\mathbb{C}\delta_{00} \cup \mathbb{C}\delta_{01}, \mathbb{C}\delta_{10} \cup \mathbb{C}\delta_{11}], \\ \mathcal{B} &:= [\mathbb{C}\delta_{00} \cup \mathbb{C}\delta_{10}, \mathbb{C}\delta_{11} \cup \mathbb{C}\delta_{01}]. \end{aligned}$$

For a complex vector $v{:}\mathbb{C}^n$ we write P_v for the projector onto the one-dimensional subspace spanned by vector v:

$$\forall u{:}\mathbb{C}^n \bullet P_v \cdot u := \frac{v}{\|v\|^2} \cdot \langle v, u \rangle.$$

For an observable $\mathcal{O}$ and eigenvalue λ we denote by $E_{\mathcal{O},\lambda}$ the set of eigenvectors associated to eigenvalue λ; we write $P_{\mathcal{O}}^{\lambda}$ for the projector associated to eigenvalue λ:

$$P_{\mathcal{O}}^{\lambda} := P_{(\sum_{v:E_{\mathcal{O},\lambda}} v)} \ .$$

The projectors for $\mathcal{A}, \mathcal{B}$ are thus:

$$\begin{aligned} P^0_{\mathcal{A}} &= P_{\delta_{00}+\delta_{01}} & \qquad P^1_{\mathcal{A}} &= P_{\delta_{10}+\delta_{11}} \\ P^0_{\mathcal{B}} &= P_{\delta_{00}+\delta_{10}} & \qquad P^1_{\mathcal{B}} &= P_{\delta_{11}+\delta_{01}}. \end{aligned}$$

Tensor product distributes over standard matrix multiplication, that is for operators M, N, L, P we have:

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

As a special case, for any operator O the operator $(O \otimes \mathbb{1})$ commutes with $(\mathbb{1} \otimes O)$, so we can eliminate the nondeterministic choice on finalisation and keep just one of the branches. This could be viewed as an example of quantum program refinement, as it is derived from the laws of quantum mechanics rather than program semantics.

The EPR program can be therefore simplified:

$$EPR = \left(\begin{array}{l} \mathbf{var}\ a, b{:}\mathbb{B} \,;\, \chi{:}q(\mathbb{B}^2) \bullet \\ \quad \chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}); \\ \quad \mathbf{Fin}[\mathcal{A}](a, \chi); \\ \quad \mathbf{Fin}[\mathcal{B}](b, \chi) \\ \mathbf{rav} \end{array} \right).$$

3.2 Correctness

We now give a formal proof that program EPR is correct: the two observers always measure anticorrelated spin values. This could be accomplished using the expectation-transformer semantics of $qGCL$ and calculating $wp.EPR.[a = b]$ and $wp.EPR.[a \neq b]$; we expect the former to be 0 and the latter to be 1. However, this is a rather long route and we choose instead to use the algebraic laws of $qGCL$ to simplify program EPR, which will turn in a shorter and more elegant proof. Semantics arguments should be used only when algebraic laws cannot.

We shall now simplify program EPR:

$$\begin{array}{l} \mathbf{var}\ a, b{:}\mathbb{B} \,;\, \chi{:}q(\mathbb{B}^2) \bullet \\ \quad \chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}); \\ \quad \mathbf{Fin}[\mathcal{A}](a, \chi); \\ \quad \mathbf{Fin}[\mathcal{B}](b, \chi) \\ \mathbf{rav} \end{array}$$

$=$ def of **Fin**

$$\begin{array}{l} \mathbf{var}\ a, b{:}\mathbb{B} \,;\, \chi{:}q(\mathbb{B}^2) \bullet \\ \quad \chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}); \\ \quad (a, \chi := 0, P^0_{\mathcal{A}}\chi)\ {}_{\langle \chi, P^0_{\mathcal{A}}\chi \rangle}\!\oplus (a, \chi := 1, P^1_{\mathcal{A}}\chi); \\ \quad \mathbf{Fin}[\mathcal{B}](b, \chi) \\ \mathbf{rav} \end{array}$$

$=$ law A-1

$$
\begin{array}{l}
\textbf{var } a, b{:}\mathbb{B} \mathbin{⨾} \chi{:}q(\mathbb{B}^2)\bullet \\
\quad \left(a, \chi := 0, P^0_{\mathcal{A}} \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10})\right) {}_{\langle \chi, P^0_{\mathcal{A}}\chi\rangle[\chi \backslash \frac{1}{\sqrt{2}}(\delta_{01}-\delta_{10}]}\oplus \\
\quad \left(a, \chi := 1, P^1_{\mathcal{A}} \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10})\right) \mathbin{⨾} \\
\quad \mathbf{Fin}[\mathcal{B}](b, \chi) \\
\textbf{rav}
\end{array}
$$

$=$ logic

$$
\begin{array}{l}
\textbf{var } a, b{:}\mathbb{B} \mathbin{⨾} \chi{:}q(\mathbb{B}^2)\bullet \\
\quad (a, \chi := 0, \delta_{01}) \;{}_{\frac{1}{2}}\!\oplus (a, \chi := 1, -\delta_{10}) \mathbin{⨾} \\
\quad \mathbf{Fin}[\mathcal{B}](b, \chi) \\
\textbf{rav}
\end{array}
$$

$=$ law S-2

$$
\begin{array}{l}
\textbf{var } a, b{:}\mathbb{B} \mathbin{⨾} \chi{:}q(\mathbb{B}^2)\bullet \\
\quad (a, \chi := 0, \delta_{01} \mathbin{⨾} \mathbf{Fin}[\mathcal{B}](b, \chi)) \;{}_{\frac{1}{2}}\!\oplus (a, \chi := 1, -\delta_{10} \mathbin{⨾} \mathbf{Fin}[\mathcal{B}](b, \chi)) \\
\textbf{rav}
\end{array}
$$

$=$ def of **Fin**

$$
\begin{array}{l}
\textbf{var } a, b{:}\mathbb{B} \mathbin{⨾} \chi{:}q(\mathbb{B}^2)\bullet \\
\quad \left(\begin{array}{l} a, \chi := 0, \delta_{01} \mathbin{⨾} \\ (b, \chi := 0, P^0_{\mathcal{B}}\chi) \;{}_{\langle \chi, P^0_{\mathcal{B}}\chi\rangle}\!\oplus (b, \chi := 1, P^1_{\mathcal{B}}\chi) \end{array}\right) {}_{\frac{1}{2}}\!\oplus \\
\quad \left(\begin{array}{l} a, \chi := 1, -\delta_{10} \mathbin{⨾} \\ (b, \chi := 0, P^0_{\mathcal{B}}\chi) \;{}_{\langle \chi, P^0_{\mathcal{B}}\chi\rangle}\!\oplus (b, \chi := 1, P^1_{\mathcal{B}}\chi) \end{array}\right) \\
\textbf{rav}
\end{array}
$$

$=$ law A-1

$$
\begin{array}{l}
\textbf{var } a, b{:}\mathbb{B} \mathbin{⨾} \chi{:}q(\mathbb{B}^2)\bullet \\
\quad \left((a, b, \chi := 0, 0, P^0_{\mathcal{B}}\delta_{01}) \;{}_{\langle \chi, P^0_{\mathcal{B}}\chi\rangle[\chi\backslash\delta_{01}]}\!\oplus (a, b, \chi := 0, 1, P^1_{\mathcal{B}}\delta_{01}) \right) {}_{\frac{1}{2}}\!\oplus \\
\quad \left((a, b, \chi := 1, 0, -P^0_{\mathcal{B}}\delta_{10}) \;{}_{\langle \chi, P^0_{\mathcal{B}}\chi\rangle[\chi\backslash -\delta_{10}]}\!\oplus (a, b, \chi := 1, 1, -P^1_{\mathcal{B}}\delta_{10}) \right) \\
\textbf{rav}
\end{array}
$$

$=$ logic

$$
\begin{array}{l}
\textbf{var } a, b{:}\mathbb{B} \mathbin{⨾} \chi{:}q(\mathbb{B}^2)\bullet \\
\quad \left((a, b, \chi := 0, 0, 0) \;{}_{0}\!\oplus (a, b, \chi := 0, 1, \delta_{01}) \right) {}_{\frac{1}{2}}\!\oplus \\
\quad \left((a, b, \chi := 1, 0, -\delta_{10}) \;{}_{1}\!\oplus (a, b, \chi := 1, 1, 0) \right) \\
\textbf{rav}
\end{array}
$$

$=$ laws P-1,P-2

$$\begin{array}{l}\textbf{var } a, b{:}\mathbb{B} \,;\, \chi{:}q(\mathbb{B}^2)\bullet \\ \quad (a, b, \chi := 0, 1, \delta_{01}) \;{}_{\frac{1}{2}}\!\oplus\; (a, b, \chi := 1, 0, -\delta_{10}) \\ \textbf{rav}\end{array}$$

It is clear that a is always anticorrelated to b.

4 Mermin's two-particle experiment

Mermin's first Gedankenexperiment [13] offers a statistical violation of an inequality developed for a two-particle quantum system.

We consider a two spin-$\frac{1}{2}$ particle system (for example two electrons bound to a nucleus) in the EPR singlet state $\frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10})$. The particles are then arranged to move away from each other in the same trajectory, in opposite directions. A detector is put on each side of the trajectory, measuring the spin of the particles in the same three spatial directions u, v, z, each direction making a 120-degree angle with the other two. The detectors have a display such that for each of the three directions u, v, z, it will display 0 if spin up is measured, 1 if spin down. We now start firing pairs of particles, all in the singlet state, randomly changing each of the detectors independently to measure for spin in the u, v and z directions. For each firing we record the digits shown on the displays.

Quantum mechanics predicts that:

- when the detectors are set in the same direction, the displays always show different digits, a consequence of the antisimmetry of the EPR state;
- over all nine possible settings for the two detectors, the displays show different digits for exactly half the total number of particle pairs fired. This is a consequence of the 120-degree angle between directions.

We shall then build a classical theory consistent with the first prediction of quantum theory, but which will necessarily violate the second prediction, showing a higher degree of correlation between measurements.

4.1 Quantum program

The $qGCL$ program for the experiment is:

$$M2P_Q := \left(\begin{array}{l}\textbf{var } d_a, d_b{:}D, r_a, r_b{:}\mathbb{B}, \chi{:}q(\mathbb{B}^2)\bullet \\ \quad d_a, d_b :\in D; \\ \quad \chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}); \\ \quad \mathbf{Fin}[\mathcal{A}_{d_a}](r_a, \chi); \\ \quad \mathbf{Fin}[\mathcal{B}_{d_b}](r_b, \chi) \\ \textbf{rav}\end{array}\right)$$

where $D := \{u, v, z\}$; variables d_a, d_b and r_a, r_b represent respectively the random direction and result of measurement for the observers; χ is the state vector describing the two-particle system. $\mathcal{A}_{d_a}, \mathcal{B}_{d_b}$ are the spin observables for directions d_a, d_b, and their self-adjoint operators are respectively $(S_{d_a} \otimes \mathbb{1}_2), (\mathbb{1}_2 \otimes S_{d_b})$, where S_{d_a}, S_{d_b} denote the spin operators along directions d_a, d_b.

Using polar coordinates we write the spin operator S_n along the direction defined by the unit vector $n := (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$:

$$S_n := \frac{1}{2}\begin{pmatrix} \cos\theta & -e^{-i\phi}\sin\theta \\ e^{i\phi}\sin\theta & -\cos\theta \end{pmatrix}.$$

The eigenvalues of S_n are still $\frac{1}{2}, -\frac{1}{2}$ ("up" and "down") and the corresponding eigenvectors:

$$\chi_n^{\text{up}} := \begin{pmatrix} e^{-i\phi}\cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix}, \quad \chi_n^{\text{down}} := \begin{pmatrix} -\sin\frac{\theta}{2} \\ e^{i\phi}\cos\frac{\theta}{2} \end{pmatrix}.$$

The trajectories u, v, z correspond to the following polar angles:

$$u := (\phi = 0, \theta = 120), \quad v := (\phi = 120, \theta = 120), \quad z := (\phi = 0, \theta = 0).$$

For the distributivity of tensor products over matrix multiplication we have that:

$$(S_{d_a} \otimes \mathbb{1}_2) \cdot (\mathbb{1}_2 \otimes S_{d_b}) = (S_{d_a} \otimes S_{d_b})$$

which is the self-adjoint operator for $\mathcal{O}_{d_a d_b}$, the spin observable when the observers measure the spin of their particle along directions d_a, d_b; the eigenvalues of $\mathcal{O}_{d_a d_b}$ are the product of the eigenvalues of S_{d_a}, S_{d_b} therefore they are just $\frac{1}{4}, -\frac{1}{4}$, while the eigenvectors are given by the tensor products of the eigenvectors of S_{d_a}, S_{d_b}; the eigenvalues are clearly degenerate.

Eigenvalue $\frac{1}{4}$ represents the fact that the detectors have measured the same spin ($\frac{1}{4} = (\pm\frac{1}{2})^2$), while eigenvalue $-\frac{1}{4}$ the fact that they measure different spin values ($-\frac{1}{4} = (\pm\frac{1}{2}) \cdot (\mp\frac{1}{2})$). As before, we map the set $\{\frac{1}{4}, -\frac{1}{4}\}$ to $\mathbb{B}$ for convenience.

With the assumptions above we can simplify the program:

$$M2P_Q = \left(\begin{array}{l} \textbf{var } d_a, d_b{:}D, r{:}\mathbb{B}, \chi{:}q(\mathbb{B}^2)\bullet \\ \quad d_a, d_b :\in D\,; \\ \quad \chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10})\,; \\ \quad \textbf{Fin}[\mathcal{O}_{d_a d_b}](r, \chi) \\ \textbf{rav} \end{array}\right).$$

4.1.1 Correctness

We prove that program $M2P_Q$ is correct:

C_1 when they measure in the same direction the observers always disagree on the measured spin value;

C_2 over all detector settings the observers agree on the measured spin value half the time and disagree the other half.

Condition C_1 is formalized by $\mathrm{Prob}(r=1|d_a=d_b)=1$ at the end of program $M2P_Q$; condition C_2 by $\mathrm{Prob}(r=0)=\mathrm{Prob}(r=1)=\frac{1}{2}$. We reason:

$$
\begin{array}{l}
\mathbf{var}\ d_a, d_b{:}D, r{:}\mathbb{B}, \chi{:}q(\mathbb{B}^2)\bullet \\
\quad d_a, d_b :\in D ; \\
\quad \chi := \frac{1}{\sqrt{2}}(\delta_{01}-\delta_{10}) ; \\
\quad \mathbf{Fin}[\mathcal{O}_{d_a d_b}](r,\chi) \\
\mathbf{rav}
\end{array}
$$

$=$ def of prob assignment

$$
\begin{array}{l}
\mathbf{var}\ d_a, d_b{:}D, r{:}\mathbb{B}, \chi{:}q(\mathbb{B}^2)\bullet \\
\quad \oplus\left[(d_a, d_b := i,j)\ @\ \frac{1}{9}\ |\ i,j{:}D\right] ; \\
\quad \chi := \frac{1}{\sqrt{2}}(\delta_{01}-\delta_{10}) ; \\
\quad \mathbf{Fin}[\mathcal{O}_{d_a d_b}](r,\chi) \\
\mathbf{rav}
\end{array}
$$

$=$ law S-2

$$
\begin{array}{l}
\mathbf{var}\ d_a, d_b{:}D, r{:}\mathbb{B}, \chi{:}q(\mathbb{B}^2)\bullet \\
\quad \oplus\left[\left(\begin{array}{l} d_a, d_b := i,j ; \\ \chi := \frac{1}{\sqrt{2}}(\delta_{01}-\delta_{10}) ; \\ \mathbf{Fin}[\mathcal{O}_{d_a d_b}](r,\chi) \end{array}\right)\ @\ \frac{1}{9}\ |\ i,j{:}D\right] \\
\mathbf{rav}
\end{array}
$$

$=$ def of **Fin**

$$
\begin{array}{l}
\mathbf{var}\ d_a, d_b{:}D, r{:}\mathbb{B}, \chi{:}q(\mathbb{B}^2)\bullet \\
\quad \oplus\left[\left(\begin{array}{l} d_a, d_b := i,j ; \\ \chi := \frac{1}{\sqrt{2}}(\delta_{01}-\delta_{10}) ; \\ (r,\chi := 0, P^0_{\mathcal{O}_{d_a d_b}}\chi)\,{}_{\langle \chi, P^0_{\mathcal{O}_{d_a d_b}}\chi\rangle}\!\oplus \\ \qquad (r,\chi := 1, P^1_{\mathcal{O}_{d_a d_b}}\chi) \end{array}\right)\ @\ \frac{1}{9}\ |\ i,j{:}D\right] \\
\mathbf{rav}
\end{array}
$$

$=$ see Appendix for calculations

$$
\begin{array}{l}
\mathbf{var}\ d_a, d_b{:}D, r{:}\mathbb{B}, \chi{:}q(\mathbb{B}^2)\bullet \\
\quad \oplus\left[\begin{array}{l} R_{i,j}\ @\ \frac{1}{9}\ |\ i,j{:}D\bullet \\ R_{i,j} = \begin{cases} \left(\begin{array}{l} d_a, d_b := i,j ; \\ r,\chi := 1, P^1_{\mathcal{O}_{d_a d_b}}\frac{1}{\sqrt{2}}(\delta_{01}-\delta_{10}) \end{array}\right) & i=j, \\ \left(\begin{array}{l} d_a, d_b := i,j ; \\ (r,\chi := 0, P^0_{\mathcal{O}_{d_a d_b}}\frac{1}{\sqrt{2}}(\delta_{01}-\delta_{10}))\,{}_{\frac{3}{4}}\!\oplus \\ \qquad (r,\chi := 1, P^1_{\mathcal{O}_{d_a d_b}}\frac{1}{\sqrt{2}}(\delta_{01}-\delta_{10})) \end{array}\right) & i\neq j. \end{cases} \end{array}\right] \\
\mathbf{rav}
\end{array}
$$

Condition C_1 is satisfied as $i = j$ in the $M2P_Q$ program means that the detectors are measuring the spin in the same direction: in such a case r is always set to 1. With respect to condition C_2, it is a matter of simple probabilistic reasoning to show that $\text{Prob}(r = 0) = \frac{1}{9} \cdot \frac{3}{4} \cdot 6 = \frac{1}{2}$; by the same argument $\text{Prob}(r = 1) = \frac{1}{2}$, so the second prediction of quantum mechanics is satisfied as well.

4.2 Refutation of local theories

We shall now prove that any local theory which satisfies condition C_1 above necessarily violates condition C_2. By local theory [8] we mean a theory in which an object's property, such as the spin of an electron, is a considered a "local property", which cannot influence other objects at a speed faster than the speed of light. This is in sharp contrast with the EPR experiment, where after a measurement particles seem to send correlation signals faster than the speed of light. Therefore we shall now suppose that the spin of the two particles is a so-called element of "reality" that exists *before* it is measured.

In Mermin's Gedankenexperiment this hypothesis is formalized by supposing that each particle, after leaving the source, already "has" the spin components in the u, v, and z direction; furthermore, since the particle "does not know" in advance the detector's setting, it has to carry a sort of code that specifies the spin in each of the three possible directions of measurement. For example we might suppose the leftbound particle to carry the code 001 , which means that the spin components for u, v, z are respectively $0, 0, 1$.

A simple *reductio ad absurdum* argument shows that condition C_1 above implies that both particles in a pair must *always carry opposite codes*, that is if one particle carries 010, the other will necessarily carry 101. The $qGCL$ program implementing the required local theory is of course standard ($i.e$ non-quantum):

$$M2P_C := \left(\begin{array}{l} \textbf{var}\ u_1, v_1, z_1, u_2, v_2, z_2, a, b{:}\mathbb{B} \bullet \\ \quad \left(\begin{array}{l} u_1, v_1, z_1 := 0 \square 1, 0 \square 1, 0 \square 1 ; \\ u_2, v_2, z_2 := \neg u_1, \neg v_1, \neg z_1 \end{array} \right) \square \\ \qquad \left(\begin{array}{l} u_2, v_2, z_2 := 0 \square 1, 0 \square 1, 0 \square 1 ; \\ u_1, v_1, z_1 := \neg u_2, \neg v_2, \neg z_2 \end{array} \right) ; \\ \quad a, b :\in \{(s_1, s_2) \mid s_1{:}D_1,\ s_2{:}D_2\} \\ \textbf{rav} \end{array} \right)$$

where D_i is the set $\{u_i, v_i, z_i\}$ for $i = 1, 2$; the various indexed u, v, and z variables represent the spin components along the three spatial directions for the two particles; a, b represent the measurement outcome for the observers.

In order to violate the laws of quantum mechanics, we first simplify program $M2P_C$ and then calculate the minimum guaranteed probability that at the end of $M2P_C$ we find $a \neq b$, that is the observers measure different spin values. This amounts to calculate $wp.(M2P_C).[a \neq b]$, which will turn out to be greater than $\frac{1}{2}$, the corresponding quantum mechanical prediction.

We simplify program $M2P_C$:

$$
\begin{array}{l}
\textbf{var } u_1, v_1, z_1, u_2, v_2, z_2, a, b{:}\mathbb{B}\bullet \\
\quad \left(\begin{array}{l} u_1, v_1, z_1 := 0 \,\square\, 1, 0 \,\square\, 1, 0 \,\square\, 1 ; \\ u_2, v_2, z_2 := u_1, v_1, z_1 \end{array}\right) \square \\
\qquad \left(\begin{array}{l} u_2, v_2, z_2 := 0 \,\square\, 1, 0 \,\square\, 1, 0 \,\square\, 1 ; \\ u_1, v_1, z_1 := u_2, v_2, z_2 \end{array}\right) ; \\
\quad a, b :\in \{(s_1, s_2) \mid s_1{:}D_1,\ s_2{:}D_2\} \\
\textbf{rav}
\end{array}
$$

$=$ lemma A.1

$$
\begin{array}{l}
\textbf{var } u_1, v_1, z_1, u_2, v_2, z_2, a, b{:}\mathbb{B}\bullet \\
\quad u_1, v_1, z_1 := 0 \,\square\, 1, 0 \,\square\, 1, 0 \,\square\, 1 ; \\
\quad u_2, v_2, z_2 := \neg u_1, \neg v_1, \neg z_1 ; \\
\quad a, b :\in \{(s_1, s_2) \mid s_1{:}D_1, s_2{:}D_2\} \\
\textbf{rav}
\end{array}
$$

$=$ prob assignment and prefix notation

$$
\begin{array}{l}
\textbf{var } u_1, v_1, z_1, u_2, v_2, z_2, a, b{:}\mathbb{B}\bullet \\
\quad \square\,[u_1, v_1, z_1 := i, j, k \mid i, j, k{:}\mathbb{B}] ; \\
\quad u_2, v_2, z_2 := \neg u_1, \neg v_1, \neg z_1 ; \\
\quad \oplus\,[(a, b := s_1, s_2) \mathbin{@} \tfrac{1}{9} \mid s_1{:}D_1, s_2{:}D_2] \\
\textbf{rav}
\end{array}
$$

$=$ law S-1

$$
\begin{array}{l}
\textbf{var } u_1, v_1, z_1, u_2, v_2, z_2, a, b{:}\mathbb{B}\bullet \\
\quad \square \left[\left(\begin{array}{l} u_1, v_1, z_1 := i, j, k ; \\ u_2, v_2, z_2 := \neg u_1, \neg v_1, \neg z_1 ; \\ \oplus\,[(a, b := s_1, s_2) \mathbin{@} \frac{1}{9} \mid s_1{:}D_1, s_2{:}D_2 \end{array}\right) \mid i, j, k{:}\mathbb{B}\right] \\
\textbf{rav}
\end{array}
$$

$=$ law A-1

$$
\begin{array}{l}
\textbf{var } u_1, v_1, z_1, u_2, v_2, z_2, a, b{:}\mathbb{B}\bullet \\
\quad \square \left[\oplus \left[\left(\begin{array}{l} u_1, v_1, z_1 := i, j, k ; \\ u_2, v_2, z_2 := \neg u_1, \neg v_1, \neg z_1 ; \\ a, b := s_1, s_2 \end{array}\right) @\tfrac{1}{9} | s_1{:}D_1, s_2{:}D\right] \mid i, j, k{:}\mathbb{B}\right] \\
\textbf{rav}
\end{array}
$$

We now calculate $wp.(M2P_C).t$, where t is the expectation $[a = b]$:

$wp.(M2P_C).t$

$=$ $\square$ semantics

$$
\bigsqcap_{i,j,k:\mathbb{B}} \left\{ wp. \left(\oplus \left[\left(\begin{array}{l} u_1, v_1, z_1 := i, j, k ; \\ u_2, v_2, z_2 := \neg u_1, \neg v_1, \neg z_1 ; \\ a, b := s_1, s_2 \end{array} \right) @\, \tfrac{1}{9} \mid s_1{:}D_1, s_2{:}D_2 \right] \right) .t \right\}
$$

$=$ $\oplus$ semantics and def of t

$$\bigsqcap_{i,j,k:\mathbb{B}} \left\{ \tfrac{1}{9} \cdot \textstyle\sum_{s_1:D_1, s_2:D_2} wp. \left(\begin{array}{l} u_1, v_1, z_1 := i, j, k; \\ u_2, v_2, z_2 := \neg u_1, \neg v_1, \neg z_1; \\ a, b := s_1, s_2 \end{array} \right) .[a \neq b] \right\}$$

$=$ assignment semantics and logic

$$\bigsqcap_{i,j,k:\mathbb{B}} \left\{ \tfrac{1}{9} \cdot \textstyle\sum_{s_1:\{i,j,k\}, s_2:\{\neg i, \neg j, \neg k\}} [s_1 \neq s_2] \right\}$$

$=$ logic

$$\bigsqcap_{i,j,k:\mathbb{B}} \left\{ \tfrac{1}{9} \cdot (3 + 2[i \neq j] + 2[i \neq k] + 2[k \neq j]) \right\}$$

$=$ logic

$$\tfrac{5}{9}$$

5 Mermin's three-particle experiment

Mermin's second Gedankenexperiment offers a more dramatic violation of locality: a *single* run of his experiment suffices to rule out any local theory wishing to mimic quantum theory results.

This experiment offers us the possibility of dealing with a qureg bigger than 2 when describing the quantum system. Furthermore, when describing our putative local theory we shall introduce two new things:

- since no statistics is involved, we use the plain Guarded Command Language (*i.e* without probabilism). This entails that our reasoning will deal with standard predicates rather than expectations;
- for specifying the requirements that our local theory must satisfy we use the specification statement [15], which offers a superior expressivity than standard code.

We consider a source emitting three spin-$\frac{1}{2}$ particles in a particular entangled state. The particles fly apart one from each other and a detector is placed on their route. The detectors have a switch which enables the observation of the x component of the spin when set to "x" and the y component when set to "y". Each detector has a display which will show 0 if spin "up" is measured, 1 if spin "down" otherwise. The spatial directions x, y, and z form the usual Euclidean space.

We perform only experiments in which the numbers of detectors set to "x" is odd and we record the digits shown on the three displays. Possible experiments are thus four, with the following quantum mechanical predictions:

P_1 if just one detector is set to "x", then an odd number of 0's will always appear on the displays;

P_2 if all three detectors are set to "x", then an odd number of 0's is never seen on the displays.

Denoting by $a, b, c{:}\mathbb{B}$ the digits shown and defining $s := (a+b+c)_{\mathrm{mod}\,2}$, we can formalize the predictions above:

$$(s=0) \text{ iff } P_1, \quad (s=1) \text{ iff } P_2.$$

5.1 Quantum program

The $qGCL$ program for this experiment is:

$$M3P_Q := \left(\begin{array}{l} \mathbf{var}\ a,b,c{:}\{x,y\}, r{:}\mathbb{B},\ \chi{:}q(\mathbb{B}^3)\bullet \\ \quad \square\ [a,b,c := i,j,k \mid (i,j,k){:}W]\,\text{;} \\ \quad \chi := \frac{1}{\sqrt{2}}(\delta_{000} - \delta_{111})\,\text{;} \\ \quad \mathbf{Fin}[\mathcal{O}_{abc}](r,\chi) \\ \mathbf{rav} \end{array} \right)$$

where $W := \{(x,y,y),(y,x,y),(y,y,x),(x,x,x)\}$ is the set of the possible settings for the detectors.

Observable $\mathcal{O}_{abc}$ represents the detectors with their switch set to (a,b,c); its self-adjoint operator is therefore $S_a \otimes S_b \otimes S_c$, where the S_d denotes the spin matrix along direction $d{:}\{x,y,z\}$:

$$S_x := \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad S_y := \frac{1}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

matrix S_z has been already defined. They all have eigenvalues $\lambda{:}\{\frac{1}{2}, -\frac{1}{2}\}$; the eigenvectors are:

observable	$\lambda = \frac{1}{2}$	$\lambda = -\frac{1}{2}$
S_z	δ_0	δ_1
S_x	$\delta_0 + \delta_1$	$\delta_0 - \delta_1$
S_y	$\delta_0 + i\delta_1$	$\delta_0 - i\delta_1$

The (degenerate) eigenvalues of $S_a \otimes S_b \otimes S_c$ are just $\{\frac{1}{8}, -\frac{1}{8}\}$, which we will yet again map to $\mathbb{B}$.

Finally, we express conditions P_1, P_2 in terms of the simultaneous eigenvalues $r{:}\mathbb{B}$ of $\mathcal{O}_{abc}$. An odd number of 0's displayed means an odd number of eigenvalue $\frac{1}{2}$ (spin "up") observed, which in turn implies an even number of eigenvalues $-\frac{1}{2}$. Any product of triples of numbers of this type will yield $\frac{1}{8}$, which we mapped to 0: P_1 is therefore equivalent to $(r=0)$. A similar reasoning shows that P_2 is equivalent to $(r=1)$.

5.1.1 Correctness

We prove that program $M3P_Q$ is correct against predictions P_1 and P_2. We reason:

$$
\begin{array}{l}
\quad \textbf{var } a,b,c{:}\{x,y\}, r{:}\mathbb{B},\ \chi{:}q(\mathbb{B}^3)\bullet \\
\qquad \Box\ [a,b,c := i,j,k \mid (i,j,k){:}W]\,⨾ \\
\qquad \chi := \frac{1}{\sqrt{2}}(\delta_{000} - \delta_{111})⨾ \\
\qquad \mathbf{Fin}[\mathcal{O}_{abc}](r,\chi) \\
\quad \textbf{rav} \\
= \hfill \text{law S-1} \\
\quad \textbf{var } a,b,c{:}\{x,y\}, r{:}\mathbb{B},\ \chi{:}q(\mathbb{B}^3)\bullet \\
\qquad \Box \left[\left(\begin{array}{l} a,b,c := i,j,k⨾ \\ \chi := \frac{1}{\sqrt{2}}(\delta_{000} - \delta_{111})⨾ \\ \mathbf{Fin}[\mathcal{O}_{abc}](r,\chi) \end{array}\right) \mid (i,j,k){:}W\right] \\
\quad \textbf{rav} \\
= \hfill \text{def of } \mathbf{Fin} \text{ and law A-1} \\
\quad \textbf{var } a,b,c{:}\{x,y\}, r{:}\mathbb{B},\ \chi{:}q(\mathbb{B}^3)\bullet \\
\qquad \Box \left[\left(\begin{array}{l} a,b,c := i,j,k⨾ \\ (r,\chi := 0, P^0_{\mathcal{O}_{abc}}\frac{1}{\sqrt{2}}(\delta_{000} - \delta_{111})) \\ \qquad {}_{\langle\chi, P^0_{\mathcal{O}_{abc}}\chi\rangle[\chi\backslash\frac{1}{\sqrt{2}}(\delta_{000}-\delta_{111})]}\oplus \\ (r,\chi := 1, P^1_{\mathcal{O}_{abc}}\frac{1}{\sqrt{2}}(\delta_{000} - \delta_{111})) \end{array}\right) \mid (i,j,k){:}W\right] \\
\quad \textbf{rav} \\
= \hfill \text{see Appendix for calculations} \\
\quad \textbf{var } a,b,c{:}\{x,y\}, r{:}\mathbb{B},\ \chi{:}q(\mathbb{B}^3)\bullet \\
\qquad \Box \left[\left(\begin{array}{l} a,b,c := i,j,k⨾ \\ r,\chi := (a,b,c = x), \frac{1}{\sqrt{2}}(\delta_{000} - \delta_{111}) \end{array}\right) \mid (i,j,k){:}W\right] \\
\quad \textbf{rav}
\end{array}
$$

Correctness of program $M3P_Q$ follows from inspection (in the last step we wrote $(a,b,c = x)$ for $[(a = x) \wedge (b = x) \wedge (c = x)]$).

5.2 Refutation of local theories

We shall now prove that any theory which satisfies prediction P_1 necessarily violates prediction P_2. As in Mermin's first Gedankenexperiment, we suppose that the spin of the three particles is an element of "reality", that exists before it is measured. We shall therefore assume that the particles possess their spin components along the x and y direction just after they are emitted by the source.

When building our putative local theory we need to constrain it to satisfy prediction P_1. We shall use here an elegant and powerful tool, which generalize our first example of local theory: the specification statement [15].

The $qGCL$ program is:

$$M3P_C := \left(\begin{array}{l} \textbf{var } a_x, b_x, c_x, a_y, b_y, c_y{:}\mathbb{B} \bullet \\ \quad a_x, b_x, c_x, a_y, b_y, c_y : [post] \\ \textbf{rav} \end{array} \right)$$

where the various indexed variables represent the x and y spin components for the three particles; $post$ is the predicate defined as:

$$post := \left(\begin{array}{l} (a_x + b_y + c_y)_{\mathrm{mod}\,2} = (a_y + b_x + c_y)_{\mathrm{mod}\,2} = \\ (a_y + b_y + c_x)_{\mathrm{mod}\,2} = 0 \end{array} \right),$$

which formalizes prediction P_1.

To get a violation of prediction P_2 we calculate $wp.M3P_C.q$ where q is the boolean predicate:

$$q := ((a_x + b_x + c_x)_{\mathrm{mod}\,2} = 1).$$

We do not deal with expectations, as program $M3P_C$ does not use any probabilistic choice. We reason:

$$\begin{array}{ll}
& wp.M3P_C.q \\
= & \hfill \text{semantics of specification} \\
& \forall\, a_x, b_x, c_x, a_y, b_y, c_y \bullet post \Rightarrow q \\
= & \hfill \text{logic} \\
& \forall \begin{array}{l} a_x, b_x, c_x, \\ a_y, b_y, c_y \end{array} \bullet \left[\begin{array}{l} post \wedge \\ \left(post \Rightarrow \left(\begin{array}{l} (a_x + b_y + c_y)_{\mathrm{mod}\,2} \\ -(a_y + b_x + c_y)_{\mathrm{mod}\,2} \\ -(a_y + b_y + c_x)_{\mathrm{mod}\,2} \end{array} \right) = 0 \right) \end{array} \right] \Rightarrow q \\
= & \hfill \text{logic} \\
& \forall \begin{array}{l} a_x, b_x, c_x, \\ a_y, b_y, c_y \end{array} \bullet \left[\begin{array}{l} post \wedge \\ \left(post \Rightarrow \left(\begin{array}{l} (a_x + b_y + c_y)_{\mathrm{mod}\,2} \\ -(a_y + b_x + c_y)_{\mathrm{mod}\,2} \\ -(a_y + b_y + c_x)_{\mathrm{mod}\,2} \end{array} \right)_{\mathrm{mod}\,2} = 0 \right) \end{array} \right] \Rightarrow q \\
= & \hfill \text{logic and lemma A.2} \\
& \forall \begin{array}{l} a_x, b_x, c_x, \\ a_y, b_y, c_y \end{array} \bullet \left[\begin{array}{l} post \wedge \\ \left(post \Rightarrow \left(\begin{array}{l} a_x + b_y + c_y \\ -a_y - b_x - c_y \\ -a_y - b_y - c_x \end{array} \right)_{\mathrm{mod}\,2} = 0 \right) \end{array} \right] \Rightarrow q \\
= & \hfill \text{logic} \\
& \forall\, a_x, b_x, c_x, a_y \bullet \left[\begin{array}{l} post \wedge \\ (post \Rightarrow (a_x - 2a_y - b_x - c_x)_{\mathrm{mod}\,2} = 0) \end{array} \right] \Rightarrow q
\end{array}$$

$=$ logic

$$\forall a_x, b_x, c_x \bullet \begin{bmatrix} post \wedge \\ (post \Rightarrow (a_x - (b_x + c_x))_{\bmod 2} = 0) \end{bmatrix} \Rightarrow q$$

$=$ logic

$$\forall a_x, b_x, c_x \bullet \begin{bmatrix} post \wedge \\ (post \Rightarrow (a_x - (b_x + c_x) + 2(b_x + c_x))_{\bmod 2} = 0) \end{bmatrix} \Rightarrow q$$

$=$ logic

$$\forall a_x, b_x, c_x \bullet \begin{bmatrix} post \wedge \\ (post \Rightarrow (a_x + b_x + c_x)_{\bmod 2} = 0) \end{bmatrix} \Rightarrow q$$

$=$ logic and def of q

$false$

This entails that in any local theory we *never* have predictions P_1 and P_2 satisfied simultaneously.

6 Bell inequalities

The previous examples of nonlocality were derived considering what happens when two observers measure the spin of the particles along two (or three) different axes. Bell developed his inequalities considering two observers who measure their particles' spins along *any* two directions. In particular, we consider a pair of unit vectors a and a' for one observer, and another pair b and b' for the other. Now, we perform a series of repeated measurements on a two-spin-$\frac{1}{2}$ particle system prepared in the EPR singlet state. As we explained before, the "realist-local" hypothesis to test is that each particle always has a well defined value for any direction of spin, which does not depend on the alteration of a remote measuring equipment. As usual we map the spin values onto set $\mathbb{B}$; we denote by a_n the spin value along direction a for the first particle in the n-th repetition of the experiment.

The Bell inequalities are derived studying the correlation between measurements made by the two observers along these four directions. For directions a, b it is defined as:

$$C(a,b) := \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} (a_n + b_n)_{\bmod 2} \ .$$

Note that if the spins are always correlated then $C(a,b) = 0$, while $C(a,b) = 1$ if they are always anticorrelated.

The path leading to the refutation of classical theories is different from the previous examples: we shall first derive an inequality true in any realist-local theory and then prove its falsity within quantum theory.

The inequality to test is:

$$(C(a,b) + C(a',b) + C(a,b') - C(a',b')) \leqslant 2 \qquad \textbf{(B)} \ ,$$

which can be rewritten as:

$$\left(\lim_{N\to\infty}\sum_{n=1}^{N} s_n\right) \leqslant 2,$$

where $s_n := c(a_n, b_n, b'_n, a'_n)$ and

$$\forall i,j,k,z{:}\mathbb{B} \bullet c(i,j,k,z) := \left(\begin{array}{l} (i+j)_{\mathrm{mod}\,2} + (k+j)_{\mathrm{mod}\,2} \\ +(i+z)_{\mathrm{mod}\,2} - (k+z)_{\mathrm{mod}\,2} \end{array}\right).$$

6.1 Classical inequality

We shall write now the $qGCL$ program for a single run of the classical version of the Gedankenexperiment:

$$B_C := \left(\begin{array}{l} \mathbf{var}\ a,b,a',b'{:}\mathbb{B}, s{:}\mathbb{Z}\bullet \\ \quad a,b,b',a' := (0\square 1, 0\square 1, 0\square 1, 0\square 1); \\ \quad s := c(a,b,b',a') \\ \mathbf{rav} \end{array}\right)$$

where $\mathbb{Z}$ denotes the set of integers. Program B_C can be simplified and abstracted to a more useful program B'_C:

B_C

$=$ prefix notation

$$\begin{array}{l} \mathbf{var}\ a,b,a',b'{:}\mathbb{B}, s{:}\mathbb{Z}\bullet \\ \quad \square\,[(a,b,b',a' := i,j,k,z) \mid i,j,k,z{:}\mathbb{B}]; \\ \quad s := c(a,b,b',a') \\ \mathbf{rav} \end{array}$$

$=$ law S-1

$$\begin{array}{l} \mathbf{var}\ a,b,a',b'{:}\mathbb{B}, s{:}\mathbb{Z}\bullet \\ \quad \square \left[\left(\begin{array}{l} a,b,b',a' := i,j,k,z; \\ s := c(a,b,b',a') \end{array}\right) \mid i,j,k,z{:}\mathbb{B}\right] \\ \mathbf{rav} \end{array}$$

$=$ assignment

$$\begin{array}{l} \mathbf{var}\ a,b,a',b'{:}\mathbb{B}, s{:}\mathbb{Z}\bullet \\ \quad \square \left[\left(\begin{array}{l} a,b,b',a' := i,j,k,z; \\ s := c(i,j,k,z) \end{array}\right) \mid i,j,k,z{:}\mathbb{B}\right] \\ \mathbf{rav} \end{array}$$

$=$ laws D-1,S-1

$$\square\left[\left(\begin{array}{l}\textbf{var}\ a,b,a',b':\mathbb{B},s:\mathbb{Z}\bullet\\ \quad a,b,b',a' := i,j,k,z\,;\\ \quad s := c(i,j,k,z)\\ \textbf{rav}\end{array}\right) \mid i,j,k,z:\mathbb{B}\right]$$

$\sqsupseteq$ law D-3 and $\square$ monotonic

$$\square\left[\left(\begin{array}{l}\textbf{var}\ a,b,a',b':\mathbb{B},s:\mathbb{Z}\bullet\\ \quad s := c(i,j,k,z)\\ \textbf{rav}\end{array}\right) \mid i,j,k,z:\mathbb{B}\right]$$

$=$ laws D-1,S-1

$$\begin{array}{l}\textbf{var}\ a,b,a',b':\mathbb{B},s:\mathbb{Z}\bullet\\ \quad \square\,[(s := c(i,j,k,z)) \mid i,j,k,z:\mathbb{B}]\\ \textbf{rav}\end{array}$$

$=$ introduce B'_C

B'_C

We now calculate $wp.B'_C.(s:\{0,2\})$, which will be a predicate since B'_C does not use any probabilistic choice. We reason:

$wp.B'_C.(s:\{0,2\})$

$=$ $\square$ semantics

$$\bigwedge_{i,j,k,z:\mathbb{B}} \{wp.(s := c(i,j,k,z)).(s:\{0,2\})\}$$

$=$ assignment semantics

$$\bigwedge_{i,j,k,z:\mathbb{B}} \{c(i,j,k,z):\{0,2\}\}$$

$=$ logic

$$\bigwedge_{i,j,k,z:\mathbb{B}} \{(c(i,j,k,z)_{\operatorname{mod}2} = 0) \wedge (0 \leqslant c(i,j,k,z) \leqslant 3)\}$$

$=$ def of c and logic

$$\bigwedge_{i,j,k,z:\mathbb{B}} \left\{(0 \leqslant c(i,j,k,z)) \wedge \left(\begin{array}{l}(i+j)_{\operatorname{mod}2} + (k+j)_{\operatorname{mod}2}\\ +(i+z)_{\operatorname{mod}2} - (k+z)_{\operatorname{mod}2}\end{array}\right)_{\operatorname{mod}2} = 0\right\}$$

$=$ lemma A.2

$$\bigwedge_{i,j,k,z:\mathbb{B}} \{(0 \leqslant c(i,j,k,z)) \wedge (2(i+j))_{\operatorname{mod}2} = 0\}$$

$=$ logic

$$\bigwedge_{i,j,k,z:\mathbb{B}} \{(0 \leqslant c(i,j,k,z))\}$$

$=$ def of c and logic

$$\bigwedge_{i,j,k,z:\mathbb{B}} \{\neg((i+j)_{\mathrm{mod}2} + (i+k)_{\mathrm{mod}2} + (j+z)_{\mathrm{mod}2} < (k+z)_{\mathrm{mod}2})\}$$

$=$ logic

$$\bigwedge_{i,j,k,z:\mathbb{B}} \left\{\neg\left(\begin{array}{lcl} (i+j)_{\mathrm{mod}2} = 0 & \wedge & (i+k)_{\mathrm{mod}2} = 0 \wedge \\ (j+z)_{\mathrm{mod}2} = 0 & \wedge & (k+z)_{\mathrm{mod}2} = 1 \end{array}\right)\right\}$$

$=$ logic

$$\bigwedge_{i,j,k,z:\mathbb{B}} \{\neg((i=j) \wedge (i=k) \wedge (j=z) \wedge (k \neq z))\}$$

$=$ logic

$$\bigwedge_{i,j,k,z:\mathbb{B}} \{\neg((i=j=k=z) \wedge (k \neq z))\}$$

$=$ logic

$true$

The result readily entails that inequality **B** is always satisfied.

6.2 Quantum program

Program B_Q describes the measurement of spin made by two observers along any two directions a and b:

$$B_Q := \left(\begin{array}{l} \mathbf{var}\ \chi{:}q(\mathbb{B}^2), r{:}\mathbb{B}\bullet \\ \quad \chi := \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10})\,; \\ \quad \mathbf{Fin}[\mathcal{O}_{ab}](r, \chi) \\ \mathbf{rav} \end{array}\right)$$

where $\mathcal{O}_{ab}$ is the spin operator along directions a, b and its self-adjoint operator is then $S_a \otimes S_b$. For simplicity we choose a, b to be coplanar therefore, using polar coordinates, they can be described just by two angles θ_a, θ_b. As usual we map the eigenvalues of $\mathcal{O}_{ab}$ onto set $\mathbb{B}$; the eigenvectors of S_a, S_b are (recall $\phi_a = \phi_b = 0$):

$$\forall i{:}\{a,b\} \bullet \quad \chi_i^0 := \begin{pmatrix} \cos\frac{\theta_i}{2} \\ \sin\frac{\theta_i}{2} \end{pmatrix},\ \chi_i^1 := \begin{pmatrix} -\sin\frac{\theta_i}{2} \\ \cos\frac{\theta_i}{2} \end{pmatrix}.$$

The eigenvectors of $S_a \otimes S_b$ are thus:

$$\begin{array}{l} E_{\mathcal{O}_{ab},0} = \{\chi_a^0 \otimes \chi_b^0, \chi_a^1 \otimes \chi_b^1\}, \\ E_{\mathcal{O}_{ab},1} = \{\chi_a^0 \otimes \chi_b^1, \chi_a^1 \otimes \chi_b^0\} \end{array}$$

from which one can readily write the projectors associated to observable $\mathcal{O}_{ab}$.

Using the refinement techniques illustrated in the previous sections we can rewrite program B_Q as:

$$\begin{array}{l} \mathbf{var}\ \chi{:}q(\mathbb{B}^2), r{:}\mathbb{B}\bullet \\ \quad \oplus\left[\left(r, \chi := i, \frac{1}{\sqrt{2}} P^i_{\mathcal{O}_{ab}}(\delta_{01} - \delta_{10})\right) @ \left(i + (-1)^i \sin^2\frac{\theta_b - \theta_a}{2}\right) \mid i{:}\mathbb{B}\right] \\ \mathbf{rav} \end{array}$$

where for the projectors we used the notation introduced beforehand.

Dropping the initialization of χ in the probabilistic choice leads to an abstraction of B_Q, which will be more useful for us:

$$
\begin{array}{ll}
B_Q & \\
= & \text{laws D-2,S-1} \\
\oplus\left[\left(\begin{array}{l}\textbf{var } \chi{:}q(\mathbb{B}^2), r{:}\mathbb{B}\bullet \\ \quad r,\chi := i, \frac{1}{\sqrt{2}}P^i_{\mathcal{O}_{ab}}(\delta_{01}-\delta_{10}) \\ \textbf{rav}\end{array}\right) @ \left(i+(-1)^i\sin^2\frac{\theta_b-\theta_a}{2}\right) \mid i{:}\mathbb{B}\right] & \\
\sqsupseteq & \text{law D-3 and } \oplus \text{ monotonic} \\
\oplus\left[\left(\begin{array}{l}\textbf{var } \chi{:}q(\mathbb{B}^2), r{:}\mathbb{B}\bullet \\ \quad r := i \\ \textbf{rav}\end{array}\right) @ \left(i+(-1)^i\sin^2\frac{\theta_b-\theta_a}{2}\right) \mid i{:}\mathbb{B}\right] & \\
= & \text{law D-2,S-1} \\
\quad\begin{array}{l}\textbf{var } \chi{:}q(\mathbb{B}^2), r{:}\mathbb{B}\bullet \\ \quad \oplus\left[(r := i) @ \left(i+(-1)^i\sin^2\frac{\theta_b-\theta_a}{2}\right) \mid i{:}\mathbb{B}\right] \\ \textbf{rav}\end{array} & \\
= & \text{infix notation} \\
\quad\begin{array}{l}\textbf{var } \chi{:}q(\mathbb{B}^2), r{:}\mathbb{B}\bullet \\ \quad (r := 0) \;{}_{\sin^2\frac{\theta_b-\theta_a}{2}}\!\oplus (r := 1) \\ \textbf{rav}\end{array} &
\end{array}
$$

therefore B_Q can be viewed as a random variable $X{:}\mathbb{B} \to [0,1]$ whose expected value is $E[X] = \cos^2\frac{\theta_b-\theta_a}{2}$.

The rules of quantum theory establish that the correlation $C(a,b)$ is equal to the expected value of observable $\mathcal{O}_{ab}$: therefore $C(a,b) = E[X] = \cos^2\frac{\theta_b-\theta_a}{2}$. Inequality **B** thus becomes:

$$\left(\cos^2\frac{\theta_b-\theta_a}{2}+\cos^2\frac{\theta_{b'}-\theta_a}{2}+\cos^2\frac{\theta_b-\theta_{a'}}{2}+\cos^2\frac{\theta_{b'}-\theta_{a'}}{2}\right) \leqslant 2\ .$$

Assuming now $\theta_a = \theta_b$ (*i.e.* a and b parallel) and $\frac{\theta_{b'}-\theta_a}{2} = \frac{\theta_b-\theta_{a'}}{2} = \phi$, the inequality is:

$$(1+2\cos^2\phi-\cos^2 2\phi) \leqslant 2\ ,$$

which is violated for $0 < \phi < \frac{\pi}{4}$.

7 Conclusions

We have shown how it is possible to formalize various demonstrations of quantum mechanical nonlocality. Recent results assert that almost all two-particle entangled states show nonlocal properties, as Hardy proved [9]. Using *qGCL* it is possible to handle this case, too [21].

Future work might involve updating the definition of quantum procedures in *qGCL* with recent developments in quantum theory, namely superoperators and positively operator valued measures (POVM) [4]; extension to infinite quantum systems is another possible direction.

8 Acknowledgements

The author wishes to thank Jeff Sanders for suggesting that *qGCL* might be used to describe nonlocal quantum phenomena and for reading drafts of this paper.

This work has been supported by a scholarship from the Engineering and Physical Sciences Research Council (UK) and by a scholarship from Università degli Studi di Perugia (Italy).

References

[1] A. Aspect, P. Graingier, and G. Roger. Experimental realization of EPR Gedanken-experiment: A new violation of Bell's inequalities. *Physical Review Letters*, 49:91–94, 1982.

[2] Adriano Barenco. A universal two-bit gate for quantum computation. *Proceeding of the Royal Society of London* A, 449:679–683, 1995.

[3] J.S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[4] Paul Busch, Marian Grabowski, and Pekka J.Lahti. *Operational Quantum Physics*. Lecture Notes in Physics. Springer-Verlag, 2nd edition, 1997.

[5] David Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London*, A425:73–90, 1989.

[6] David Deutsch, Adriano Barenco, and Arthur Ekert. Universality in quantum computation. *Proceedings of the Royal Society of London* A, 449:669–677, 1995.

[7] E. W. Dijkstra. Guarded commands, nondeterminacy and the formal derivation of programs. *CACM*, 18:453–457, 1975.

[8] A. Einstein, B. Podolsky, and N. Rosen. Can quantum mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

[9] Lucien Hardy. Nonlocality for two particles without inequalities for almost all entangled states. *Physical Review Letters*, 71(11):1665–1668, 1993.

[10] C.A.R. Hoare, He Jifeng, and A. Sampaio. Normal form approach to compiler design. *Acta Informatica*, 30:701–739, 1993.

[11] Chris J. Isham. *Lectures on quantum theory.* Imperial College Press, 1997.

[12] He Jifeng, Annabelle McIver, and Karen Seidel. Probabilistic models for the guarded command language. *Science of Computer Programming*, 28:171–192, 1997.

[13] N. David Mermin. Bringing home the atomic world: Quantum mysteries for anybody. *American Journal of Physics*, 49:940–943, 1981.

[14] N. David Mermin. Quantum mysteries revisited. *American Journal of Physics*, 58:731–734, 1990.

[15] Carroll Morgan. *Programming from Specifications.* Prentice-Hall International, 1994.

[16] Carroll Morgan and Annabelle McIver. *pGCL*: formal reasoning for random algorithms. *South African Computer Journal*, 22:14–27, 1999.

[17] Carroll Morgan, Annabelle McIver, and Karen Seidel. Probabilistic predicate transformers. *ACM Transactions on Programming Languages and Systems*, 18(3):325–353, May 1996.

[18] J.W. Sanders and Paolo Zuliani. Quantum programming. *Mathematics of Program Construction, Springer LNCS*, 1837:80–99, 2000.

[19] Benjamin Schumacher. Quantum coding. *Physical Review* A, 51(4):2738–2747, 1995.

[20] John von Neumann. *Mathematical Foundations of Quantum Mechanics.* Princeton University Press, 1955.

[21] Paolo Zuliani. *DPhil Thesis.* Oxford University. In preparation.

A Appendix

A.1 Algebraic programming laws

We list a few algebraic laws which hold for $pGCL$ programs; the semantic models adopted and proofs can be found in [12, 17], for a complete exposition of an algebra of programming for the guarded-command language see [10].

Law (N-1). $P \,\Box\, Q = Q \,\Box\, P$

Law (P-1). $P \;{}_1\!\oplus\; Q = P$

Law (P-2). $P \;{}_r\!\oplus\; Q = Q \;{}_{1-r}\!\oplus\; P$

Law (S-1). $(P \,\Box\, Q) \fatsemi R = (P \fatsemi R) \,\Box\, (Q \fatsemi R)$

Law (S-2). $(P \;{}_r\!\oplus\; Q) \fatsemi R = (P \fatsemi R) \;{}_r\!\oplus\; (Q \fatsemi R)$

Law (A-1). $(x := e) \fatsemi (P \;{}_r\!\oplus\; Q) = (x := e \fatsemi P) \;{}_{r[x \backslash e]}\!\oplus\; (x := e \fatsemi Q)$

In law A-1 $r[x\backslash e]$ denotes the expression obtained replacing all free occurences of x in r by e. In the next two laws D is any data type; in law D-2 variable x must not appear in expression p.

Law (D-1). $\textbf{var}\, x{:}D \bullet (P \sqcap Q) = (\textbf{var}\, x{:}D \bullet P) \sqcap (\textbf{var}\, x{:}D \bullet Q)$

Law (D-2). $\textbf{var}\, x{:}D \bullet (P \;{}_p\!\oplus\; Q) = (\textbf{var}\, x{:}D \bullet P) \;{}_p\!\oplus\; (\textbf{var}\, x{:}D \bullet Q)$

There is also one refinement law which we used in the paper:

Law (D-3). $\textbf{var}\, x{:}D \sqsubseteq (\textbf{var}\, x{:}D \bullet x := e)$

In law D-3 e is any expression of type D, meaning that initialising a variable will make a program more deterministic. The next lemma will also be useful.

Lemma A.1. *If variables $a, b{:}\mathbb{B}$ do not appear in boolean expressions E, F and $E = \neg F$, then:*

$$\left(\begin{array}{l} a := E \sqcap F \,; \\ b := \neg a \end{array} \right) = \left(\begin{array}{l} b := E \sqcap F \,; \\ a := \neg b \end{array} \right).$$

Proof. We reason:

LHS

$=$ nondet assignment

$(a := E \sqcap a := F) \,; b := \neg a$

$=$ law S-1

$(a := E \,; b := \neg a) \sqcap (a := F \,; b := \neg a)$

$=$ exchange assignment

$(b := \neg E \,; a := \neg b) \sqcap (b := \neg F \,; a := \neg b)$

$=$ law S-1 and $E = \neg F$

$(b := F) \sqcap (b := E) \,; a := \neg b$

$=$ law N-1

$(b := E) \sqcap (b := F) \,; a := \neg b$

$=$ nondet assignment

RHS

□

A.2 Quantum-mechanical probabilities

We write here in detail some of the calculations that yield the quantum-mechanical probabilities used in the paper. All the theory we use can be found in Isham's book [11] and in Mermin's original papers [13, 14].

A.2.1 Mermin's two-particle experiment

We need to calculate $\langle \chi, P^0_{\mathcal{O}_{d_a d_b}} \chi \rangle$ for d_a, d_b:$\{u, v, z\}$ and $\chi = \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10})$. Because of the simmetry between the pairs of directions (u, z) and (v, z) and since our orientation in space is arbitrary, we shall only need to compute $\langle \chi, P^0_{\mathcal{O}_{d_a d_b}} \chi \rangle$ for d_a, d_b:$\{u, z\}$.

S_u is the spin operator along direction u; its eigenvalues are $0, 1$ and the eigenvectors:

$$u_0 := \begin{pmatrix} \cos 60 \\ \sin 60 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}, \quad u_1 := \begin{pmatrix} -\sin 60 \\ \cos 60 \end{pmatrix} = \begin{pmatrix} -\frac{\sqrt{3}}{2} \\ \frac{1}{2} \end{pmatrix}.$$

Using the basis formed by the eigenvectors δ_0, δ_1 of S_z, we can write u_0 and u_1 as:

$$u_0 = \left(\frac{1}{2}\delta_0 + \frac{\sqrt{3}}{2}\delta_1\right), \quad u_1 = \left(-\frac{\sqrt{3}}{2}\delta_0 + \frac{1}{2}\delta_1\right).$$

We start computing for directions (z, z):

$$\begin{aligned}
\langle \chi, P^0_{\mathcal{O}_{zz}} \chi \rangle &= \langle \chi, P_{\delta_{00}+\delta_{11}} \chi \rangle \\
&= \langle \chi, \frac{1}{2}(\delta_{00} + \delta_{11}) \langle (\delta_{00} + \delta_{11}), \chi \rangle \rangle \\
&= \langle \chi, \frac{1}{2}(\delta_{00} + \delta_{11}) \langle (\delta_{00} + \delta_{11}), \frac{1}{\sqrt{2}}(\delta_{01} - \delta_{10}) \rangle \rangle \\
&= \langle \chi, \frac{1}{2}(\delta_{00} + \delta_{11}) \cdot 0 \rangle = 0\,.
\end{aligned}$$

A similar calculations shows that $\langle \chi, P^0_{\mathcal{O}_{uu}} \chi \rangle = 0$. We now calculate for directions (u, z); the projector is $P^0_{\mathcal{O}_{uz}} = P_v$ where:

$$v := u_o \otimes \delta_0 + u_1 \otimes \delta_1 = \left(\frac{1}{2}\delta_{00} + \frac{\sqrt{3}}{2}\delta_{01} - \frac{\sqrt{3}}{2}\delta_{01} + \frac{1}{2}\delta_{11}\right),$$

then:

$$\begin{aligned}
\langle \chi, P^0_{\mathcal{O}_{uz}} \chi \rangle &= \langle \chi, \frac{v}{\|v\|^2} \langle v, \chi \rangle \rangle \\
&= \langle \chi, \frac{v}{2} \cdot \frac{1}{\sqrt{2}} \cdot (\frac{\sqrt{3}}{2} + \frac{\sqrt{3}}{2}) \rangle \\
&= \frac{\sqrt{3}}{2\sqrt{2}} \langle \chi, v \rangle = \frac{\sqrt{3}}{4}(\frac{\sqrt{3}}{2} + \frac{\sqrt{3}}{2}) = \frac{3}{4}\,.
\end{aligned}$$

Similarly, $\langle \chi, P^0_{\mathcal{O}_{zu}} \chi \rangle = \frac{3}{4}$.

A.2.2 Mermin's three-particle experiment

We need to calculate $\langle \chi, P^0_{\mathcal{O}_{abc}} \chi \rangle$ for (a, b, c):W (we recall that W is the set of the settings of the three detectors $\{(x, y, y), (y, x, y), (y, y, x), (x, x, x)\}$) and $\chi = \frac{1}{\sqrt{2}}(\delta_{000} - \delta_{111})$.

For $i{:}\mathbb{B}$ we let u_x^i and u_y^i be the eigenvectors of S_x, S_y; we recall that using the basis $\{\delta_0, \delta_1\}$ they can be written as:

$$u_x^0 = \delta_0 + \delta_1 \,, \qquad u_x^1 = \delta_0 - \delta_1 \,,$$
$$u_y^0 = \delta_0 + i\delta_1 \,, \qquad u_y^1 = \delta_0 - i\delta_1 \,.$$

We now calculate for the setting (x, x, x); the projector is $P^0_{\mathcal{O}_{xxx}} = P_v$ where:

$$\begin{aligned} v :=& u_x^0 \otimes u_x^0 \otimes u_x^0 + u_x^0 \otimes u_x^1 \otimes u_x^1 \\ &+ u_x^1 \otimes u_x^1 \otimes u_x^0 + u_x^1 \otimes u_x^0 \otimes u_x^1 \\ =& 2(\delta_{000} + \delta_{111}) \end{aligned}$$

then $\langle \chi, P^0_{\mathcal{O}_{xxx}} \chi \rangle = 0$ and $\langle \chi, P^1_{\mathcal{O}_{xxx}} \chi \rangle = 1$. For the setting (y, x, y) we define:

$$\begin{aligned} v :=& u_y^0 \otimes u_x^0 \otimes u_y^0 + u_y^0 \otimes u_x^1 \otimes u_y^1 \\ &+ u_y^1 \otimes u_x^1 \otimes u_y^0 + u_x^1 \otimes u_x^0 \otimes u_y^1 \\ =& 2(\delta_{000} - \delta_{111}) \end{aligned}$$

then $\langle \chi, P^0_{\mathcal{O}_{yxy}} \chi \rangle = \langle \chi, P_v \chi \rangle = 1$ and $\langle \chi, P^1_{\mathcal{O}_{yxy}} \chi \rangle = 0$. With similar calculations we get $\langle \chi, P^0_{\mathcal{O}_{yyx}} \chi \rangle = 1$ and $\langle \chi, P^0_{\mathcal{O}_{xyy}} \chi \rangle = 1$.

A.3 Modular arithmetic

A simple but useful lemma, whose proof is trivial.

Lemma A.2. *For $a, b, n{:}\mathbb{Z}$ and $n \neq 0$:*

$$(a + b)_{\mathrm{mod}n} = (a_{\mathrm{mod}n} + b_{\mathrm{mod}n})_{\mathrm{mod}n} \,.$$