Precedence and freedom in quantum physics

Lee Smolin

May 17,2012

Contents

Abstract

A new interpretation of quantum mechanics is proposed according to which precedence, freedom and novelty play central roles. This will be based on a modification of the postulates for quantum theory(see Theory #1 discussed below). We argue that quantum mechanics is uniquely characterized as the probabilistic theory in which individual systems have maximal freedom in their responses to experiment, given reasonable axioms for the behavior of probabilities in a physical theory. Thus, to the extent that quantum systems are free(see Free Will Theorem discussion below)), there is a sense in which they are maximally free.

We also propose that laws of quantum evolution arise from a principle of precedence according to which the outcome of a measurement on a quantum system is selected randomly from the ensemble of outcomes of previous instances of the same measurement on the same quantum system. This implies that dynamical laws for quantum systems can evolve as the universe evolves, because new precedents are generated by the formation of new entangled states.

1 Introduction

We are used to thinking that the laws of physics are deterministic and that this precludes the occurrence of genuine novelty in the universe. All that happens is rearrangements of elementary particles with unchanging properties by unchanging laws.

But must this really be the case? We need determinism only in a limited set of circumstances, which is where an experiment has been repeated many times. In these cases we have learned that it is reliable to predict that when we repeat an experiment in the future, which we have done many times in the past, the probability distribution of future outcomes will be the same as observed in the past.

Usually we take this to be explained by the existence of fundamental timeless laws which control all change. But this could be an over-interpretation of the evidence. What we need is only that there be a principle that measurements which repeat processes which have taken place many times in the past yield

the same outcomes as were seen in the past. Such a principle of precedence would explain all the instances where determinism by laws works without restricting novel processes to yield predictable outcomes. There could be at least a small element of freedom in the evolution of novel states without contradicting the application of laws to states which have been produced plentifully in the past.

But are there any truly novel states in nature?

It is fair to say that classical mechanics precludes the existence of genuine novelty, because for certain all that happens is the motion of particles under fixed laws. But quantum mechanics is different, in two ways. First, in quantum mechanics does not give unique predictions for how the future will resemble the past. It gives from past instances only a statistical distribution of possible outcomes of future measurements.

Second, in quantum physics there is the phenomena of entanglement which involves novel properties shared between subsystems which are not just properties of the individual subsystems. The free will theorem of Conway and Kochen(discussed below as *Free Will Theorem*) tells us that in these cases systems respond to measurements in a way that can be considered free, in the sense that the result of an individual measurement on elements of an entangled system could not be predicted by any knowledge of the past.

An entangled state can be novel in that it can be formed from a composition of subsystems into a state never before occurring in the prior history of the universe. This is common for example in biology where natural selection can give rise to novel proteins and sequences of nucleic acids which almost certainly, due to the combinatorial vastness of the number of possibilities, have not existed before.

There is then the possibility that novel states can behave unpredictability because they are without precedent. Only after they have been created enough times to accumulate ample precedent would the behavior of these novel states become lawful.

Hence we can have a conception of law which is sufficient to account for the repeatability of experiments, without restricting novel states from being free from constraints from deterministic laws. In essence the laws evolve with

the states. The first several iterations of a novel state are not determined by any law. Only after sufficient precedent has been established does a law take hold, and only for statistical predictions. Individual outcomes can be largely unconstrained.

Quantum physics allows this possibility because the generic single measurement is not determined by quantum dynamics. Only if the system is prepared in an eigenstate of the measurement being made is the result determined. But these require fine tuning and are hence non-generic. Otherwise quantum dynamics is stochastic so that no outcome of a single generic observation can disagree with predictions of quantum mechanics.

There are aspects of measurements that are not predicted by quantum mechanics which offer scope for genuine novelty and freedom from deterministic evolution. Imagine a double slit experiment with a very weak source of photons. The measurement gives a sequence of positions to which the photons fall on the screen, $x_1, x_2, ..., x_N$. Each individual photon can end up anywhere on the screen. Quantum mechanics predicts the overall statistical ensemble that accumulates after many photons, $\rho(x)$. But it does not, for example, restrict the order by which they fall. Quantum mechanics is equally consistent with a record in which the $x_i{}'$s are permuted, from one random sequence to another.

Macroscopic outcomes could depend on the order of positions, for example, if someone chooses to make a career in science or politics based on whether the $13th$ photon falls to the left or right side of the screen.

The basic idea of the formulation of quantum theory proposed here is that

1. Systems with no precedents have outcomes not determined by prior law.

2. When there is sufficient precedence the outcome of an experiment is determined by making a random selection from the ensemble of prior cases.

3. The outcome of measurements on systems with no or few precedents is as free as possible, in a sense that needs to be defined precisely.

Stated more carefully these become the principles of this approach to quantum theory, to be specified below.

This proposal is a twist on the real ensemble interpretation (Theory #2 discussed below). The principle proposed in the real ensemble interpretation is that whenever probabilities appear in quantum physics they must be relative frequencies within ensembles every element of which really exists.

In the original version of this idea the ensemble associated with a quantum state exists simultaneously with it. In the new version the ensembles exist in the past of the process they influence.

How much precedence is necessary to turn freedom into deterministic dynamics? There must for each system be an answer to this question.

If the first instance of a measurement made on a novel state is undetermined, but the probabilities for outcomes of a measurement with a great deal of precedence is tightly determined, there is, for any system, a number of distinct prior preparations whose statistical distributions of outcomes must be measured to determine, as well as can be done, the distributions of outcomes of measurements made on future iterations of that system. This is the number of degrees of freedom of the system, to be denoted K below(this follows from Theory #1 and Theory #3 discussed below). There is also the dimension or capacity of the system which is the number, N, of outcomes that can be distinguished by measurements on the system (Theories #1 and #3). These numbers and their relation must play a crucial role because they determine when there is sufficient precedent for future cases to be determined as possible.

We show below that there is a precise sense in which quantum kinematics is specified by requiring that K be as large as possible, given N, consistent with a small set of reasonable general axioms. This means that there is the maximal amount of information needed per distinguishable outcome to predict the statistical distribution of outcomes for any experiment. As a result, we can say that the responses of quantum systems to individual measurements are maximally free from the constraints of determinism from prior cases.

To formulate this idea precisely, we can make use of an axiomatic formulation of quantum theory, given by Theory #1 below, which is based on Theory #3 ideas. These theories give four axioms for how probabilities for outcomes behave when systems are combined into composite systems, or subsystems

are projected out of larger systems and proves that they imply quantum mechanics or classical probability theory. To these we will add a new, fifth, axiom which picks out the quantum case. These five postulates define the kinematics of quantum systems.

The hard work needed to show this has already been done by Theory #1. The observation that these five postulates determine quantum theory is a trivial consequence of the earlier work.

Informally stated these five postulates are

1. The state of a composite system is characterized by the statistics of measurements on the individual components.

2. All systems that effectively carry the same amount of information have equivalent state spaces.

3. Every pure state of a system can be transformed into every other by a reversible transformation.

4. In systems that carry one bit of information, all measurements which give non- negative probabilities are allowed by the theory.

5. Quantum systems are maximally free, in that a specification of their statistical state, sufficient for predicting the probabilities for outcome of any future measurement, requires the maximal amount of information, relative to the number of outcomes of an individual measurement.

To these we add a postulate about quantum dynamics. This is the principle of precedence, which, informally stated, says

> **Principle of precedence**: When a quantum process terminating in a measurement has many precedents, which are instances where an identically prepared system was subject to the same measurement in the past, the outcome of the present measurement is deter- mined by picking randomly from the ensemble of precedents of that measurement.

We first review the Free Will Theorem and the three earlier theories and then give a brief sketch of the new interpretation of quantum mechanics, by giving more precise statements of these postulates.

2 Free Will Theorem

2.1 Introduction

Do we really have free will, or, as a few determined folk maintain, is it all an illusion? We don't know, but will prove here that if indeed there exist any experimenters with a modicum of free will, then elementary particles must have their own share of this valuable commodity.

"I saw you put the fish in!" said a simpleton to an angler who had used a minnow to catch a bass. Our reply to an analogous objection would be that we use only a minuscule amount of human free will to deduce free will not only of the particles inside ourselves, but all over the universe.

To be more precise, what we will show is that the particles' response(more precisely still, the universe's response in the neighborhood of the particles) to a certain type of experiment is not determined by the entire previous history of that part of the universe accessible to them. The free will we assume is just that the experimenter can freely choose to make any one of a small number of observations. In addition, we make three physical assumptions in the form of three simple axioms.

The fact that they cannot always predict the results of future experiments has sometimes been described just as a defect of theories extending quantum mechanics. However, if our physical axioms are even approximately true, the free will assumption implies the stronger result, that no theory, whether it extends quantum mechanics or not, can correctly predict the results of future spin experiments. It also makes it clear that this failure to predict is a merit rather than a defect, since these results involve free decisions that the universe has not yet made.

2.1.1 Stating the theorem

We proceed at once to describe our axioms. There exist *particles of total spin 1* upon which one can perform an operation called *measuring the square of the component of spin in a direction w* which always yields one of the answers 0 or 1.

On measuring squared spins. Our assertion that Sx^2, Sy^2, Sz^2 must take

the values $1, 0, 1$ in some order may surprise some physicists, who expect sentences involving definite values for S_x, S_y, S_z to be meaningless, since these operators do not commute. However, for a spin 1 particle their squares do commute.

We can envisage measuring S_x^2, S_y^2, S_z^2 by an electrical version of the Stern-Gerlach experiment, by interferometry that involves coherent recombination of the beams for $S_x = +1$ and $S_x =?1$, or finally by a *spin-Hamiltonian* type of experiment that measures an expression of the form $aS_x^2 + bS_y^2 + cS_z^2$. An example of a spin 1 system is an atom of orthohelium.

We will write $w \to i$ ($i = 0$ or 1) to indicate the result of this operation. We call such measurements for three mutually orthogonal directions x, y, z a triple experiment for the frame (x, y, z).

The SPIN axiom: A triple experiment for the frame (x, y, z) always yields the outcomes $1, 0, 1$ in some order.

We can write this as: $x \to j$, $y \to k$, $z \to l$, where j, k, l are 0 or 1 and $j + k + l = 2$.

It is possible to produce two distantly separated spin 1 particles that are *twinned*, meaning that they give the same answers to corresponding questions.

To produce a twinned pair of spin 1 particles, one forms a pair in *the singleton state*, i.e., with total spin 0. An explicit description of this state is

$$|S_w^a = 1\rangle \left|S_w^b = -1\right\rangle + |S_w^a = -1\rangle \left|S_w^b = 1\right\rangle - |S_w^a = 0\rangle \left|S_w^b = 0\right\rangle$$

This state is independent of the direction w. We remark that $S_w^a (= S_w \otimes I)$ and $S_{w'}^b (= I \otimes S_{w?})$ are commuting operators for any directions w and $w?$.

Such *singleton* states have been achieved experimentally for two spin 1/2 particles separated by more than $10\,km$. Presumably a similar singleton state for distantly separated spin 1 particles will be attained eventually with sufficient technology.

A symmetrical form of the TWIN axiom would say that if the same triple x, y, z were measured for each particle, possibly in different orders, then the

two particles' responses to the experiments in individual directions would be the same. For instance, if measurements in the order x, y, z for one particle produced $x \to 1$, $y \to 0$, $z \to 1$, then measurements in the order y, z, x for the second particle would produce $y \to 0$, $z \to 1$, $x \to 1$. Although we could use the symmetric form for the proof of the theorem, a truncated form is all we need, and will make the argument clearer:

The TWIN axiom: For twinned spin 1 particles, if the first experimenter A performs a triple experiment for the frame (x, y, z), producing the result $x \to j$, $y \to k$, $z \to l$ while the second experimenter B measures a single spin in direction w, then if w is one of x, y, z, its result is that $w \to j, k,$ *or* l, respectively.

The FIN axiom: There is a finite upper bound to the speed with which information can be effectively transmitted.

This is, of course, a well-known consequence of relativity theory, the bound being the speed of light. We will discuss the notion of *information* later in addition we will also give precise meaning we will give to *effectively* later. (It applies to any realistic physical transmission.)

FIN is not experimentally verifiable directly, even in principle (unlike SPIN and TWIN).

Digression on the operational meanings of various terms. Our uses of the terms *spin* 1 *particle* and *squared spin in direction w* seem to refer to certain theoretical concepts. But we only use them to refer to the locations of the spots on a screen that are produced by suitable beams in the above kinds of experiment.

Thus our axioms, despite the fact that they derive from the theories of quantum mechanics and relativity, actually only refer to the predicted macroscopic results of certain possible experiments. Our dismissal of hidden variable theories is therefore much stronger than the previous ones that presuppose quantum mechanics. From a logical point of view this is very important, since any use of quantum mechanical terminology necessarily makes it unclear exactly what is being assumed.

Continuing:

Its real justification is that it follows from relativity and what we call *effective causality*, that effects cannot precede their causes.

We remark that we have made some tacit idealizations in the above preliminary statements of our axioms, and will continue to make them in the initial version of our proof. For example, we assume that the spin experiments can be performed instantaneously, and in exact directions. In later sections, we show how to replace both assumptions and proofs by more realistic ones that take account of both the approximate nature of actual experiments and their finite duration.

In our discussion, we will suppose for simplicity that the finite bound is the speed of light, and use the usual terminology of past and future light-cones, etc. To fix our ideas, we will suppose the experimenter A to be on Earth, while experimenter B is on Mars, at least 5 light-minutes away. We are now ready to state our theorem.

The Free Will Theorem (assuming SPIN, TWIN, and FIN)

> *If the choice of directions in which to perform spin 1 experiments is not a function of the information accessible to the experimenters, then the responses of the particles are equally not functions of the information accessible to them.*

Why do we call this result the Free Will theorem? It is usually tacitly assumed that experimenters have sufficient free will to choose the settings of their apparatus in a way that is not determined by past history. We make this assumption explicit precisely because our theorem deduces from it the more surprising fact that the particles' responses are also not determined by past history. Thus the theorem asserts that if experimenters have a certain property, then spin 1 particles have exactly the same property. Since this property for experimenters is an instance of what is usually called *free will*, we find it appropriate to use the same term also for particles.

We remark that the Free Will assumption, that *the experimenters' choice of directions is not a function of the information accessible to them*, has allowed us to make our theorem refer to the world itself, rather than merely to some theory of the world. However, later we will also produce a modified version that invalidates certain types of theory without using the free will assumption.

One way of blocking no-go theorems that hidden variable theories have proposed is *contextuality* - that the outcome of an experiment depends upon hidden variables in the apparatus. For the triple experiment in SPIN, contextuality allows the particles spin in the z direction (say) to depend upon the frame (x, y, z). However, since the particle's past history includes all its interactions with the apparatus, the Free Will theorem closes that loophole.

2.2 The Proof

We proceed at once to the proof. We first dispose of a possible naive supposition - namely that *the squared spin $\theta(w)$ in direction w* already exists prior to its measurement. If so, the function θ would be defined on the unit sphere of directions, and have the property

(i) that its values on each orthogonal triple would be $1, 0, 1$ in some order.

This easily entails two further properties:

(ii) We cannot have $\theta(x) = \theta(y) = 0$ for any two perpendicular directions x and y;

(iii) for any pair of opposite directions w and $?w$, we have $\theta(w) = \theta(-w)$. Consequently, θ is really defined on $\pm$-*directions*.

We call a function on a set of directions that has all three of these properties a 101-*function*. However, the above naive supposition is disproved by the Kochen-Specker paradox for Peres' 33-direction configuration, namely:

Lemma: There is no 101-function for the ± 33 directions of Figure 1.

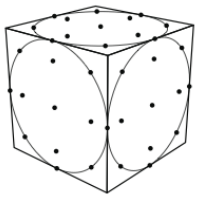

Figure 1: The ± 33 directions are defined by the lines joining the center of the cube to the ± 6 mid-points of the edges and the ± 3 sets of 9 points of the 3×3 square arrays shown inscribed in the incircles of its faces.

Since this merely says that a certain geometric combinatorial puzzle has no solution. We give a short proof below.

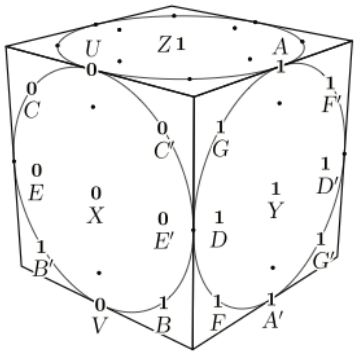

Figure 2: Spin assignments for Peres' 33 directions

Consider Figure 2 above and assume that a 101-function θ is defined on these ± 33 directions. If $\theta(W) = i$, we write $W \to i$. The orthogonalities of the triples and pairs used below in the proof of a contradiction are easily seen geometrically. For instance, in Figure 2, B and C subtend the same angle at the center O of the cube as do U and V, and so are orthogonal. Thus A,B,C form an orthogonal triple. Again, since rotating the cube through a right angle about OZ takes D and G to E and C, the plane orthogonal to D passes through Z,C,E, so that C,D is an orthogonal pair and Z,D,E is an orthogonal triple. We will write *wlog* to mean *without loss of generality*.

The orthogonality of X,Y, Z implies $X \to 0$, $Y \to 1$, $Z \to 1$ (wlog)

The orthogonality of X, A implies $A \to 1$ and similarly $A' \to 1$

The orthogonality of A, B, C implies $B \to 1$, $C \to 0$ (wlog) and similarly $B' \to 1$, $C' \to 0$

The orthogonality of C, D implies $D \to 1$ and similarly $D' \to 1$

The orthogonality of Z, D, E implies $E \to 0$ and similarly $E' \to 0$

The orthogonality of E, F and E, G implies $F \to 1$, $G \to 1$ and similarly $F' \to 1$, $G' \to 1$

The orthogonality of F, F', U implies $U \to 0$

The orthogonality of G, G', V implies $V \to 0$

and since U is orthogonal to V , this is a contradiction that proves the Lemma.

Deduction of The Free Will Theorem

We consider experimenters A and B performing the pair of experiments described in the TWIN axiom on separated twinned particles a and b, and assert that the responses of a and b cannot be functions of all the information available to them.

The contrary *functional hypothesis* is that particle $a's$ response is a function $\theta_a(\alpha)$ of the information α available to it.

In the first instance, we shall suppose that this information is determined by the triple x, y, z together with the information α' that was available just before the choice of that triple, and so is independent of x, y, z. So we can express it as a function

$$\theta_a(x, y, z; \alpha') = \{x \to j, y \to k, z \to l\}$$

[Here and later we use the fixed symbol θ_a for this function, despite a change of its variables (here from α to $x, y, z; \alpha'$)].

We refine this notation to pick out any particular one of the three answers by adjoining a question-mark to the appropriate one of x, y, z; thus:

$$\theta_a(x?, y, z; \alpha') = j$$
$$\theta_a(x, y?, z; \alpha') = k$$
$$\theta_a(x, y, z?; \alpha') = l$$

Under a similar supposition for we express bs responses as a function

$$\theta_b(w; \beta') = \{w \to m\}$$

of the direction w and the information β' available to b before w was chosen, and again, we write this alternatively as

$$\theta_b(w?; \beta') = m$$

The TWIN axiom then implies that

$$theta_b(w?;\beta') = \begin{cases} \theta_a(x?,y,z;\alpha') & \text{if } w = x \\ \theta_a(x,y?,z;\alpha') & \text{if } w = y \\ \theta_a(x,y,z?;\alpha') & \text{if } w = z \end{cases} \qquad (\star)$$

The Free Will assumption now implies that for each direction w and triple of orthogonal directions x, y, z chosen from our set of ± 33, there are values of α' and β' for which every one of the functions in $(\star)$ *is* defined, since it entails that the experimenters can freely choose an x, y, z and w to perform the spin 1 experiments.

Now we defined α' so as to be independent of x, y, z, but it is also independent of w, since there are coordinate frames in which B's experiment happens later than A's. Similarly, β' is independent of x, y, z as well as w.

Now we fix α' and β' and define

$$\theta_0(w) = \theta_b(w?;\beta')$$

and find that

$$\begin{aligned} \theta_a(x?,y,z;\alpha') &= \theta_0(x) \\ \theta_a(x,y?,z;\alpha') &= \theta_0(y) \\ \theta_a(x,y,z?;\alpha') &= \theta_0(z) \end{aligned}$$

Thus θ_0 is a 101-function on the ± 33 directions, in contradiction to the Lemma. So we have proved the theorem under the indicated suppositions.

However, one of the particles responses, say a's, might also depend on some further information bits that become available to it after x, y, z is chosen. If each such bit is itself a function of earlier information about the universe (and x, y, z) this actually causes no problem, as we show in the next section.

We are left with the case in which some of the information used (by a, say) is spontaneous, that is to say, is itself not determined by any earlier information whatever. Then there will be a time t_0 after x, y, z are chosen with the property that for each time $t < t_0$ no such bit is available, but for every $t > t_0$ some such bit is available.

But in this case the universe has taken a free decision at time t_0, because the information about it after t_0 is, by definition, not a function of the information available before t_0! So if a's response really depends on any such spontaneous information-bit, it is not a function of the triple x, y, z and the state of the universe before the choice of that triple.

This completes the proof of the Free Will theorem, except for our ascription of the free decision to the particles rather than to the universe as a whole. We discuss this and some other subtleties in later sections after noting the following variant.

2.3 The Free State Theorem

As we remarked, there is a modification of the theorem that does not need the Free Will assumption. Physical theories since Descartes have described the evolution of a state from an initial arbitrary or *free* state according to laws that are themselves independent of space and time. We call such theories with arbitrary initial conditions *free state theories*.

The Free State theorem (assuming SPIN, TWIN, FIN)

> *No free state theory can exactly predict the results of twinned spin* 1 *experiments for arbitrary triples* x, y, z *and vectors* w*. In fact it cannot even predict the outcomes for the finitely many cases used in the proof.*

This is because our only use of the Free Will assumption was to force the functions θ_a and θ_b to be defined for all of the triples x, y, z and vectors w from a certain finite collection and some fixed values α' and β' of other information about the world. Now we can take these as the given initial conditions.

We will see that it follows from the Free State theorem that no free state theory that gives a mechanism for reduction, and *a fortiori* no hidden variable theory (such as Bohm's) can be made relativistically invariant.

3 Information

Readers may be puzzled by several problems. In the first place, was it legal to split up information in the way we did in the proof? To justify this, we shall

use the standard terminology of information theory, by identifying the truth value of each property of the universe5 with a *bit* of information. **Digression on On Properties** We will describe the state of the universe or any system in it by means of properties. The more usual description in terms of values of physical quantities such as energy, angular momentum, etc. can always be reduced to a set of properties, such as *the energy E lies in the interval* (E_1, E_2). We prefer the more primitive notion of property, because it avoids the possible problematic use of the continuum of real numbers in favor of 1 and 0 (or yes and no), which is more likely to correspond to ultimate facts about the world. More importantly, we have in mind allowing properties that are more general than allowed by values of physical quantities.

Which properties do we allow? In classical particle physics the set of properties is often identified with a Boolean algebra of (Borel) subsets of a phase space, whereas in quantum mechanics this is replaced by a lattice of projection operators on Hilbert space. Perhaps we should also make some such restriction?

No! Our theorem would be weakened, rather than strengthened, by any such restriction. Also, it is important that we make no theoretical assumptions about properties, because we don't want our theorem to depend on any physical theory. Our theorem will only be a statement about the real world, as distinct from some theory of the world, if we refuse to limit the allowed properties in any way. So the answer is: we must allow every possible property!

Continuing:

These truth values are then simply *information*, which therefore can as usual be thought of as a set of bits. We emphasize that we do not assume any structure on the set of properties or put any restriction on the simultaneous existence of properties. The only aspect of information that we use is that it consists of set of bits of information, which we can partition in various ways.

Not all information in the universe is accessible to a particle a. In the light of FIN, information that is space-like separated from a is not accessible to a. The information that is accessible to a is the information in the past light cone of a.

We redefine α' to be all the information used by a that is independent of

x, y, z, and show that in fact any information-bit used by a is a function of α' and x, y, z. For when x, y, z are given, any information-bit $i(x, y, z; \alpha')$ that is a function of x, y, z (and maybe some of the earlier information independent of x, y, z and so in α') is redundant, and can be deleted from the arguments of the function θ_a. To see this, observe that experimenter A need use only certain orthogonal triples

$$(x_1, y_1, z_1), (x_2, y_2 1, z_2), ..., (x_{40}, y_{40}, z_{40})$$

namely the 16 orthogonal triples inside the Peres configuration together with the 24 that are obtained by completing its 24 remaining orthogonal pairs.

Then the information bit $i(x, y, z; \alpha')$ will be one of the particular bits

$$i(x_1, y_1, z_1; \alpha'), i(x_2, y_2 1, z_2; \alpha'), ..., i(x_{40}, y_{40}, z_{40}; \alpha')$$

corresponding to these, and since these bits are not functions of the variables x, y, z, they are part of the information α'.

Another way to say this is that we are replacing the original function θ_a by a new function

$$\theta'_a(x, y, z; \alpha') = \theta_a(x, y, z; \alpha', ..., i(x, y, z; \alpha'), ...)$$

obtained by compounding it with the functions i for each such bit.

3.1 The prompter-actor problem

Any precise formulation of our theorem must cope with a certain difficulty that we can best describe as follows. It is the possibility that spin experiments performed on twinned particles a and b might always cause certain other particles a' and b' to make free decisions(our proof dealt with such decisions in the discussion of *spontaneous information*) of which the responses of a and b are functions. In this context, we may call a' and b' *promptons*, a and b *actons*.

There is obviously no way to preclude this possibility, which is why we said that more precisely, it is the universe that makes the free decision in the neighborhood of the particles. However, we don't usually feel the need for such pedantry, since the important fact is the existence of the free decision

and that it is made near a and b. Let us remind the reader that even the spin 1 particles a and b are already theoretical constructs, and there is no point in further multiplication of theoretical entities. We are really talking of spots on a screen, rather than any kind of particle(we discussed this point earlier in the digression about the *operational meanings of various terms*.

4 The Consistency Problem for Spin Experiments

It cannot be denied that our axioms in combination have some paradoxical aspects. One might say that they violate common sense, because a and b must give the same answers to the same questions even though these answers are not defined ahead of time. But does that mean that the axioms are logically inconsistent? This is by no means a trivial question. Indeed, quantum mechanics and general relativity have been mutually inconsistent for most of their joint lifetime, an inconsistency that heterotic string theory resolved (with great difficulty) only by changing the dimension of space-time!

Even the consistency of quantum mechanics with special relativity is somewhat problematic. Indeed many people have concluded that when the reduction of the state vector as given by von Neumanns *Projection Rule* is added, paradoxes of the EPR kind contradict relativistic invariance. So might our axioms actually be inconsistent? No! We can show this using what we shall call a *Janus model*, a notion that will at the same time help elucidate some puzzling phenomena. Before we do that, we illustrate the idea by giving a Janus model for an artificially simple construction we call *hexagonal physics*.

4.1 A hexagonal universe

The space-time of this physics is a hexagonal tessellation of the plane, with time increasing vertically. An experimenter who is in a given hexagon on day t can only be in one of the two hexagons that abut it from above on day $t+1$, the choice between these two hexagons being left to the experimenter's free will as shown in Figure 3.

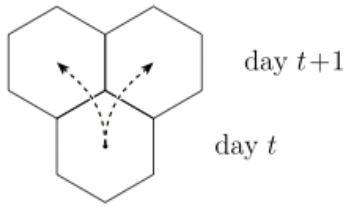

Figure 3: Free will in a hexagonal universe

We suppose that each hexagon has a *spin* whose value 0 or 1 can be determined by an experimenter upon reaching that hexagon at a given day, but not before. This is the analogue of the FIN axiom.

The only other physical law is that the sum of the spins of three hexagons arranged as in Figure 3 is even (i.e. 0 or 2), which is the analogue of SPIN (and, as we shall see, also of TWIN, since it relates the spins of remote hexagons on the same day).

Are these axioms consistent with each other and with the experimenters' limited amount of free will? We can show that the answer is *yes* by introducing an agent, Janus, who will realize them. His realization will also show that the response of the particles is not a function of past history in this little universe, showing that they also exhibit a limited amount of free will according to our definition.

Let us imagine for instance, that two physicists, A and B, both start at the lowest hexagon of Figure 4 on day 0, and that they never happen to perform their experiments at the same instant.

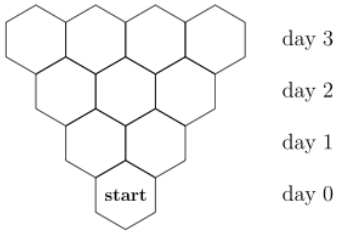

Figure 4:

Janus freely decides the result of the first experiment on any given day, and then uses the SPIN axiom to fill in the results for the other hexagons on that day. For example, if on day 5, A and B are at the far left and right hexagons of Figure 5 respectively, and the outcome for A on day 5 is 1, then Janus fills in the other hexagons for day 5 uniquely as in Figure 5 to fulfill the SPIN axiom.

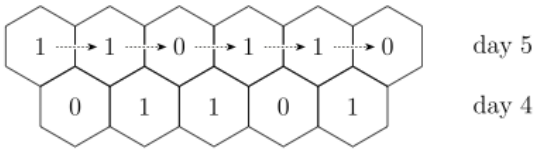

Figure 5:

The fact that Janus decides on the outcome only at the time of the first experiment on a given day shows that indeed neither experimenter can predict the result of an experiment before that day. SPIN is also obeyed since Janus uses it to fill in the rest of the hexagons for that day.

Note that in his realization of hexagonal physics, the speed with which Janus transmits information is not restricted by our analogue of FIN. Although this may seem peculiar, it does not contradict the fact that FIN holds in the model. It is analogous to the standard way of establishing the consistency of non-Euclidean geometry by constructing a model for hyperbolic geometry (which denies the parallel axiom) inside Euclidean geometry (for which that axiom is true). We have also been greatly influenced by the analogous use by others of the Axiom of Choice to construct a model for set theory in which that axiom does not hold.

Also, Janus need not respect the visible left-right symmetry of hexagonal physics. Suppose, for instance that A always moves left, B always moves right, and that they agree to perform their experiments exactly at noon on each day. Then Janus might either use his *left face* by freely deciding the outcome for A and using SPIN to compute the outcome for B, or use his *right face* to do the reverse.

If one reader were to mimic Janus by freely choosing (or throwing a coin) to determine the spin of either all the leftmost hexagons in Figure 4 or all

the rightmost ones, and then use SPIN to fill in the rest, then subsequent readers would not be able to decide which choice the first reader made. We can say that this kind of physics has left-right symmetry even though none of the Janus constructions do. Thus, the Janus models show the consistency of this physics, but cannot be *the* explanation for the physics, since there is both a left and a right Janus model.

Physics often enunciates the principle that scientific theories should ideally have all the symmetries of the facts they explain. Since hexagonal physics has the left-right reflection that its Janus models do not share, they violate this principle. In our view, models that violate this principle are discredited as explanations, but they do have a proper use, which is to provide consistency proofs.

Logicians are accustomed to the fact that assertions inside a model often differ from those outside it. For example, the *straight lines* in Poincare's model for hyperbolic geometry are actually circular arcs, while the *sets without choice functions* inside some models for set theory actually do have choice functions outside it.

In a similar way, since Janus is not himself part of the physics he realizes, he is not himself subject to its laws. His very name might already have suggested that we need no longer believe in him!

4.2 Consistency of our axioms for spin experiments

There is a similar Janus model that establishes the consistency of the real axioms SPIN, TWIN, FIN, together with the Free Will assumption. Janus chooses a coordinate frame and decides his response to the twinned spin-1 experiments of A and B in the order they happen in this frame. How does he do this? The answer is that he uses a truly random coin, or his own free will (!) to produce the outcome 0 or 1, unless this value is already forced by SPIN and TWIN, (i.e., $z \to 0$ forces $y \to 1$, $x \to 1$, while $y \to 1$ forces $z \to 0$, and $x \to j$ for either experimenter forces $x \to j$ for the other). Clearly, it is always possible to obey SPIN and TWIN, and the Free Will assumption holds since neither the decisions of the experimenters nor Januss answers are determined ahead of time.

The possible responses produced by this method are Lorentz invariant, despite the fact that Janus's method manifestly is not. The image of Janus's method under a Lorentz transformation is of course the analogous method for the image coordinate frame. Since Janus's method is causal, this shows that the phenomena appear to be causal from every coordinate frame. The technical language discussed later describes this by saying they are *effectively causal*. It is obvious that the inhabitants of a given Janus model cannot transmit information backward in time, so by symmetry they cannot effectively transmit information superluminally - in other words, FIN holds in the Janus model. (See the discussion of effective notions later).

5 The Consistency of Free Will with Quantum Mechanics

In 1952, David Bohm produced a well-known model for quantum mechanics (including von Neumanns Projection Rule). This is contentious because Bohm's construction (as in fact he was well aware) does not share the relativistic invariance of the physics it *explains*. This means that in our language it must only be what we have called a Janus model, rather than *the* real explanation of the behavior of the world, since its images under Lorentz transformations are different equally good explanations. The Free Will theorem shows in fact that this construction cannot be made relativistic.

Nevertheless, Bohms construction was a great achievement, because it is a Janus model that establishes the consistency of quantum mechanics, including the Projection Rule. In fact we can modify it so as to prove below the strong result that these are also consistent with the free will of particles.

5.1 Exorcising determinism

The main point of hidden variable theories has perhaps been to restore determinacy to physics. Our Free Will theorem is the latest in a line of argument against such theories. However, the situation is not as simple as it seems, since the determinacy of such theories can be conjured out of existence by a simple semantic trick.

For definiteness we shall refer to Bohm's theory, which is the best known

and most fully developed one, although the trick is quite general. According to Bohm, the evolution of a system is completely determined by certain real numbers (his *hidden variables*), whose initial values are not all known to us.

What we do know about these initial values may be roughly summed up by saying that they lie in a set S_0 (more precisely, they will also have a probability distribution P_0, which we temporarily ignore). An experiment might conflict with some of the initial values, and so enable us to shrink the set S_0, say to S_t at time t. The *exorcism trick* is just to regard the whole set S_t of current possibilities, rather than any supposed particular point of S_0, as all that actually exists at time t.

On this view, as t increases, S_t steadily shrinks, not, as Bohm would say, because we have learned more about the position of the initial point, but perhaps because the particles have made free choices. In the more precise version(later), the probability distribution P_0 on the set S_0 will be successively refined to more and more concentrated distributions P_t as the time t increases.

Bohm's theory so exorcised, has become a non-deterministic theory, which, however, still gives exactly the same predictions! In fact, the exorcised form of Bohm's theory is consistent with our assertion that particles have free will. We need only suppose once again that a Janus uses appropriate truly random devices to give the probability distributions P_t. If he does so, then the responses of the particles in our spin experiments, for instance, will not be determined ahead of time, and so they will be exhibiting free will, in our sense.

As it stands, Bohm's theory visibly contradicts FIN. But since the effects it produces are just those of quantum mechanics, they are in fact Lorentz invariant. The exorcised form of Bohm's theory therefore performs the service of proving the consistency of quantum mechanics (including the Projection Rule) with FIN and the Free Will property of particles.

6 Relativistic Forms of Concepts

The usual formulations of causality and transmission of information involve the intuitive notions of space and time. Since our axiom FIN is a consequence

of relativity, we must analyze these ideas so as to put them into relativistically invariant forms, which we shall denote by prefixing the adjective *effective*.

(i) *Effective causality.* The notion of causality is problematic even in classical physics, and has seemed even more so in relativity theory. This is because a universally accepted property of causality is that effects never precede their causes, and in relativity theory time order is coordinate-frame dependent.

A careful analysis, however, shows that the proper relativistic notion of causality is really no more problematic than the classical one. This is because all we have the right to demand is that *the universe should appear causal from every coordinate frame.* We call this property *effective causality.*

The Janus models that *explained* our twinned spin experiments are causal, and therefore show that the phenomena are compatible with effective causality. (The same is true of the spin EPR experiment.)

The situation is admittedly odd, since what is a cause in the Janus explanation for one frame becomes an effect in that for another. However, effective causality has the following nice properties:

(1) No observer can distinguish it from *real* causality (whatever that means).

(2) By definition, it is Lorentz invariant.

(3) It is the strongest possible notion of causality that *is* Lorentz invariant.

(4) It is provably compatible with SPIN,TWIN,FIN, and the Free Will assumption.

(ii) *Effective transmission of information.* There is a similar problem of extending the notion of transmission of information to the relativistic case.

Obviously, we cannot invariantly say that *information is transmitted from a to b* if a and b are space-like separated, since then b is earlier than a in some coordinate frames. If information is really transmitted from a to b, then this will appear to be so in all coordinate frames,

which we shall express by saying that *information is effectively transmitted from a to b.*

Many physicists believe that some kinds of information really are transmitted instantaneously. We will discuss the fallacious argument that suggests this in the next section.

(iii) *Effective semi-localization* A similar definition can help us understand where the *free will* decision we have found is exercised. We shall say that a phenomenon is *effectively located in a certain (not necessarily connected) region of space-time* just when this appears to be so in every coordinate frame.

Then it is clear that we cannot describe the outcome 00 or 11 to one of our twinned spin 1 experiments as *having been determined near a*, since in some frames it was known earlier near b. We can, however, say that choice of 00 or 11 is effectively located in some neighborhood of the pair a, b (i.e., a pair of neighborhoods about a and b). We encapsulate the situation by describing the decision as *effectively semi-localized.*

As we already remarked in the Introduction, our assertion that *the particles make a free decision* is merely a shorthand form of the more precise statement that *the Universe makes this free decision in the neighborhood of the particles.*

It is only for convenience that we have used the traditional theoretical language of particles and their spins. The operational content of our theorem, discussed in the *digression on operational meaning of various terms* earlier, is that real macroscopic things such as the locations of certain spots on screens are not functions of the past history of the Universe. From this point of view it would be hard to distinguish between the pair of statements italicized above.

We summarize our other conclusions:

(1) *What happens is effectively causal.*

(2) *No information is effectively transmitted in either direction between a and b.*

(3) *The outcome is effectively semi-localized at the two sites of measurement.*

Our definitions of the *effective* notions have the great advantage of making these three assertions obviously true. Although they are weaker than one might wish, it is also obvious that they are in fact the strongest assertions of their type that are relativistically invariant.

Warning - *effective so-and-so*, although it is relativistically invariant, is not the same thing as *invariant so-and-so*. It would be inappropriate, for instance, to describe the Janus explanations of our twinned spin experiments as *invariantly causal*, since what is a cause in one frame becomes an effect in another. The effective notions are more appropriately described as the invariant semblances of the original ones. *Effective causality*, although it is indeed a relativistically invariant notion, is not *invariant causality* - it has merely the appearance of causality from every coordinate frame.

We close this section by emphasizing the strange nature of semi-localization. We might say that the responses of the particles are only *semi-free*; in a manner of speaking, each particle has just *half a mind*, because it is yoked to the other. However, we continue to call their behavior *free* in view of the ironic fact that it is only this yoking that has allowed us to prove that they have any freedom at all!

What happens is paradoxical, but the Janus models, even though we don't believe them, show that it is perfectly possible; and experiments that have actually been performed confirm it. So we must just learn to accept it, as we accepted the earlier paradoxes of relativity theory.

7 On Relativistic Solecisms

Many physicists believe that certain kinds of information (*quantum information* or *phase information*) really are transmitted instantaneously. Indeed, this might almost be described as the orthodox view, since it follows from a (careless) application of the standard formalism of quantum mechanics.

We shall explain the fallacious argument that leads to this conclusion for the *spin EPR* case of a pair A, B of spin $1/2$ particles in the singleton state

$\left|\uparrow_z^A\right\rangle \left|\downarrow_z^B\right\rangle - \left|\downarrow_z^A\right\rangle \left|\uparrow_z^B\right\rangle$. It says that *when the measurement of A in direction z yields spin up, the state is changed by applying the projection operator $P_z \otimes I$ to the singleton state, which annihilates the second term, so that the state becomes $\left|\uparrow_z^A\right\rangle \left|\downarrow_z^B\right\rangle$, in which B is spin down.*

The word *becomes* in this statement is then misinterpreted to mean *changes at the instant of measurement*, even though this is, of course, relativistically meaningless. However, all that is really asserted is that if this measurement finds A to be spin up, then if and when a similar measurement is also performed on B, B will be found to be spin down.

The assertion that *B is spin down* (made after A has been found to be spin up) is grammatically incorrect. We call it a *relativistic solecism*. It is important to avoid making such mistakes, since they can lead to genuine errors of understanding. How can we do so?

One easy trick is to use the correct tense for such assertions, which is often the *future perfect* (*will have*). A grammatically correct version is that if and when *both* measurements have been performed, they will have found that A was spin up if and only if they will have found B to be spin down. This is a Lorentz invariant way of stating exactly the same facts.

Figure 6 describes the situation.

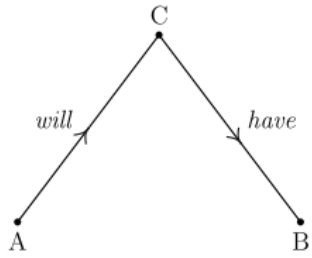

Figure 6: A concludes what B *will have* found

An observer C whose past light cone contains both experiments can legitimately say that *A found spin up, B spin down*. However, A can only say that *if the B measurement has been performed, it will have found spin down*. In this, the *will* looks forward from A to C, while the *have* looks backward from C to B.

Notice that this makes no mention of the relativistically non-existent notion of *instantaneity*, and that (consequently) it works equally well for frames in which the B measurement precedes the A one. In fact, it is independent of frame. The avoidance of relativistic solecisms is a valuable habit to cultivate!

7.1 A Modest proposal

This line of thought naturally leads us to recommend our *Modest Proposal* for the interpretation of states in quantum mechanics. According to this, what is usually called the state is merely a predictor (with probabilities) of what will happen if various experiments are performed(we note that despite the commonly held view among physicists that the ray in Hilbert space contains more information than probabilities of outcomes, Gleason's theorem shows that we can uniquely characterize rays by these probabilities). Even when the prediction is that some assertion has probability 1, that assertion is still contingent on the appropriate experiment being performed.

Thus if a triple experiment has found $x \to 1$, $y \to 1$, $z \to 0$, we certainly know that $S_x^2 = S_y^2 = 1$, but many physicists would say that *we also know* $S_w^2 = 1$ *for any other direction* w *perpendicular to* z (since the probability predicted for this assertion is 1). More modestly, we would say only that *if a measurement is made in direction* w*, it will find* $S_w^2 = 1$.

To say, in these circumstances, that S_w^2 is already 1, is, in our view, to be guilty of a simple confusion. After all, one does not say that an astronomical event like an eclipse has already happened as soon as it has been predicted with certainty.

We revert to the spin EPR case discussed above, supposing that a measurement of A at time t produces *spin up*, giving $\left|\uparrow_x^A\right\rangle \left|\downarrow_z^B\right\rangle$ for the state of the pair, and $\left|\downarrow_z^B\right\rangle$ for the state of B. Then we allow ourselves to say that A *is spin up*, since the measurement has actually been performed, but not that B *is spin down* at time t.

If the appropriate measurement of B is actually performed at time t, it of course produces *spin down*. But (supposing that A and B are 5 light-minutes apart), it will equally produce *spin down* if it is instead performed 1 minute hence, at time $t+1$, while if it was performed already at time $t?1$, it already

did produce that answer. Nothing about B changed at time t.

Those who would say more might not make any mistaken predictions, but their opinions about what happens are not consistent with relativity theory, unlike our more modest ones. As with our discussion of effective notions, careful speech pays off - our assertions are obviously both true and relativistically invariant, while stronger ones are not.

8 The Free Will Theorem is Robust

Our first versions of SPIN and TWIN were tacitly idealized; we now remove some of this idealization. In practice, we expect to find deviations from these axioms, for instance because the vectors x, y, z will only be nominally, or approximately, orthogonal, rather than exactly so; similarly w will at best be only only nominally parallel to one of them, and again, the twinned pair might only be nominally in the singlet state. Also, the two theories of quantum mechanics and special relativity from which we derived our axioms, might only be approximately true. In fact, general relativity is already a more exact theory than special relativity. However, we may safely assume:

SPIN': If we observe the squared spin in three nominally orthogonal directions, then the probability of a *canonical outcome* (i.e., j, k, l are $1, 0, 1$ in some order) is at least $1 - \epsilon_s$.

TWIN': If w, nominally in the same direction as x or y or z, yields the value m, then the probability that m equals the appropriate one of j, k, l is at least $1 - \epsilon_t$.

Then following the argument of the theorem, we define a function $\theta_1(w)$ of direction that behaves like a 101-function in all but a proportion $3\epsilon_t + \epsilon_s$ of cases. For if w is nominally the same as y (say), we deduce as before that

$$\theta_a(x, y?, z; \alpha') = k =_{\epsilon_t} m = \theta_b(w?; \beta')$$

where $=_{\epsilon_t}$ means *is equal to except in a proportion ϵ of cases.*.

Now if we fix on any possible values for α' and β' (which exist by the Free Will assumption) and define $\theta_1(w)$ to be $\theta_b(w?; \beta')$, we find

$$(\theta_1(x), \theta_1(y), \theta_1(z)) =_{3\epsilon_t} (j, k, l) =_{\epsilon_s} 1, 0, 1$$

in some order.

But the Lemma shows in fact that any function of direction must fail to have the 101-property for at least one of 40 particular orthogonal triples (the 16 orthogonal triples of the Peres configuration and the triples completed from its remaining 24 orthogonal pairs), so we have a contradiction unless $3\epsilon_t + \epsilon_s \geq 1/40$.

How big may we expect the epsilons to be? I am not an experimentalist, but believe that the errors in angle will dominate the other errors, so that the upper bounds we shall obtain by estimating them conservatively can be relied upon.

Let us assume that x, y, z make angles α, β, γ with each other in cyclic order. We can now use the standard quantum mechanical techniques given below to determine *upper bounds for the epsilons.*.

Suppose we make a sequence of measurements of properties with corresponding projections $P_1, ..., P_n$ on a system in a pure state ϕ. Then the probability that the properties all hold is

$$\langle P_n \cdots P_1\phi, P_n \cdots P_1\phi\rangle = \langle \phi, P_1 \cdots P_n \cdots P_1\phi\rangle = tr(P_1 \cdots P_n \cdots P_1 P_\phi)$$

where P_ϕ is the projection onto the ray of ϕ. This becomes $tr(P_1 \cdots P_n \cdots P_1\rho)$ if the system is in a mixed state given by the density operator ρ.

In our case, for SPIN' we have $n = 3$ and $\rho = I/3$, since we give equal weight to each of the properties P_x, P_y, P_z that the squared spin is 0 in the nominal directions x, y, z. The the probability of 000 for P_x, P_y, P_z is

$$\begin{aligned} tr(P_xP_yP_zP_yP_xI/3) &= tr(|x\rangle\langle x|\,|y\rangle\langle y|\,|z\rangle\langle z|\,|y\rangle\langle y|\,|x\rangle\langle x|)/3 \\ &= \frac{1}{3}\cos^2\alpha\cos^2\gamma \end{aligned}$$

Similarly, the probability of 010 is

$$tr(P_x(I-P_y)P_z(I-P_y)P_xI/3) = (\cos^2\beta + \cos^2\alpha\cos^2\gamma - 2\cos\alpha\cos\beta\cos\gamma)/3$$

We thus obtain as the sum of five such expressions:

$$(2\cos^2\alpha + 2\cos^2\beta + 2\cos^2\gamma - 4\cos\alpha\cos\beta\cos\gamma + \cos^2\alpha\cos^2\gamma)/3$$

for the probability of a noncanonical result when we observe directions x, y, z in that order. If α, β, γ are all in the interval $[\pi/2 - \delta, \pi/2 + \delta]$, this gives

$$\epsilon_s \leq (6\delta^2 + 4\delta^3 + \delta^4)/3$$

Again, if w makes an angle ϕ with one of x, y, z, then the probability for the non-canonical result01 or 10 is $2(\sin^2 \phi)/3$, so if ϕ is in the interval $[-\delta, \delta]$, then $\epsilon_t \leq 2\delta^2/3$. Thus,

$$3\epsilon_t + \epsilon_s \leq 4\delta^2 + (4\delta^3 + \delta^4)/3$$

which is $\leq 1/800$ if $\delta \leq 1$ degree. Also, for TWIN', we have $n = 2$ and $\rho = I/3$. Observations of a spin 1 particle (or two twinned particles) in two directions w, w' at angle ϕ give outcomes 10 or 01 with probability

$$tr(P_w(I - P_{w'})P_w I/3) + tra((I - P_w)P_{w'}(I - P_w)I/3) = \frac{2}{3}\sin^2 \phi$$

All of this means that the non-canonical observations $000, 100, 010, 001, 111$ for SPIN and $01, 10$ for TWIN can be expected to occur less than once in 800 experiments, rather than at least once in every 40 experiments, as implied by the functional hypothesis. A more reasonable bound for δ might be 1 minute, giving the upper bound 1/2900000 for the probability of these non-canonical results.

We remarked above that the change from special to general relativity made no difference to our results - now is a good time to explain why. The main difference between the two theories is that in a curved space-time one should replace *same direction* by *directions related by parallel transport* in the TWIN axiom. However, near the solar system, the curvature of space-time is so small that it was extremely hard even to detect, so that any additional angular errors caused by the special relativistic approximation will be utterly negligible compared to the 1 degree or 1 minute we have assumed.

The same comment applies to the possible replacement of either general relativity or quantum mechanics by some putatively more accurate theory, provided this preserves the truth of SPIN' and TWIN' for some sufficiently small epsilons.

9 Historical remarks

In the 1960s the KochenSpecker (K-S) paradox and the Bell Inequality appeared independently, both showing that certain types of hidden variable theories are at variance with the predictions of quantum mechanics. The K-S paradox showed that the so-called *non-contextual* hidden variable theories are impossible, while the Bell Inequality implied instead that those that satisfy *Bell locality* are impossible. In the 1970s, Kochen showed via an EPR-type twinning experiment for two spin 1 particles that in fact Bell locality implied the non-contextuality condition.

The advantage of the K-S theorem over the Bell theorem is that it leads to an outright contradiction between quantum mechanics and the hidden variable theories for a single spin experiment, whereas the Bell theorem only produces the wrong probabilities for a series of experiments. It has not been possible to derive a version of the Free Will theorem from Bells inequalities.

The (untwinned) K-S paradox is very robust. There have also been improvements on the number of directions needed for the K-S theorem. The original version used 117 directions. The smallest known at present is a 31-direction set. Subsequently, Peres found the more symmetric set of 33 that we have used here because it allows a simpler proof than the 31-direction one.

In 1989, Greenberger, Horne and Zeilinger gave a new version of Kochen's 1970's form of the K-S paradox. They use three spin 1/2 particles in place of our two spin 1 ones, and show that the Bell locality assumption leads to an outright contradiction to quantum predictions, without probabilities. We could prove the Free Will theorem using GHZ's spin 1/2 triplets instead of our spin 1 twins. The advantages of doing so are

(i) It shows that spin 1/2 particles are just as much free agents as are our spin-1 ones.

(ii) The argument leading to a contradiction is simpler.

(iii) A version of the experiment has actually been carried out.

Nevertheless, we have given the twinned spin 1 version for the following reasons:

(i) The twinned spin 1 experiment was suggested by Kochen already in the 1970's.

(ii) Conceptually, it is simpler to consider two systems instead of three.

(iii) The K-S argument in its present version with 33 directions is now also very simple.

(iv) An experiment with particles remote enough to verify the Free Will theorem will probably be realized more easily with pairs than with triples.

The experiments we described in discussing our theorem are so far only *gedanken-experiments*. This is because our Free Will assumption requires decisions by a human observer, which current physiology tells us takes a minimum of 1/10 of a second. During such a time interval light will travel almost $20,000$ miles, so the experiment cannot be done on Earth.

It is possible to actually do such experiments on Earth if the human choices are replaced by computer decisions using a pseudo-random generator, as has already been done for the EPR spin experiment - and suggested for the GHZ experiment.

This delegation of the experimenter's free choice to a computer program, still leads to a Free Will theorem if we add the assumption that the particles are not privy to the details of the computer program chosen. Note however that replacing the human choice by a pseudo-random number generator does not allow us to dispense with the Free Will assumption since free will is used in choosing this generator! The necessity for the Free Will assumption is evident, since a determined determinist could maintain that the experimenters were forced to choose the computer programs they did because these were predetermined at the dawn of time.

10 The Theory of Ghirardi, Rimini and Weber

Ghirardi, Rimini and Weber have proposed a theory [GRW] that attempts to explain the reduction of the state in quantum mechanics by an underlying mechanism of stochastic *hits*. Their theory, as it stands, is visibly not

relativistically invariant, but they hope to find a relativistic version. We quote:

> *It is appropriate to stress two facts: the problem is still an open and a quite stimulating and difficult one. However there seems to be some possibility of carrying it on consistently.*

The Free Will theorem shows that this hope cannot be realized, if we reject as fantastic the possibility that the *hits* that control the particles' behavior also completely determine the experimenters' actions.

This is because the response of particle a, say(or perhaps the possible free decision (*prompton*) at an earlier time t_0 that prompted this response-see earlier proof of the theorem.), may depend only on hits in its past light cone, which (if they physically exist) have already been incorporated in the information α and β accessible to it. However, our proof of the Free Will theorem shows that the particles response is not a function of this information.

Because the argument is rather subtle, we re-examine the relevant part of the proof in detail.

Let α_0 be the information from the hits that influences the behavior of particle a. Then by FIN, α_0 cannot depend on the direction w since in some frames this direction is only determined later. It may depend on x, y, z, but, as our earlier discussion, we can write it as a function of x, y, z, and the information α_0' contained in it that is not a function of x, y, z.

Similarly the information β_0 from the hits that influence particle b's behavior must already be independent of x, y, z, and can be written as a function of w and the information β_0' it contains that is not a function of w. We see that this *hit* information α_0' and β_0' causes no problems - it is just a part of the information α' and β' already treated in our proof.

Not only does this cover classically correlated information, such as signals from Alpha Centauri, but it also shows that subtle non-local correlations between the hits at a and b cannot help. We can even let both particles be privy to all the information in α' and β'. The only things we cannot do are to let a be influenced by w or b by x, y, z (so breaking FIN), or to let the hits that control the particles' behavior also completely determine the experimenters' choice of directions, contradicting our Free Will assumption.

10.1 Randomness can't help

The problem has been thought to lie in determinism:

> *Taking the risk of being pedantic, we stress once more that from our point of view the interest of Gisin's theorem lies in the fact that it proves that if one wants to consider nonlinear modifications of quantum mechanics one is forced to introduce stochasticity and thus, in particular, the dynamics must allow the transformations of ensembles corresponding to pure cases into statistical mixtures.*

However, our argument is valid whether the hits are strictly determined (the case already covered by Gisin) or are somehow intrinsically stochastic. In either case, the GRW theory implies that the reduction is determined by the hits and so contradicts the Free Will theorem.

To see why, let the stochastic element in a putatively relativistic GRW theory be a sequence of random numbers (not all of which need be used by both particles). Although these might only be generated as needed, it will plainly make no difference to let them be given in advance. But then the behavior of the particles(or of the appropriate *promptons*) in such a theory would in fact be a function of the information available to them (including this stochastic element) and so its explanation of our twinned spin experiment would necessarily involve superluminal transmission of information between a and b. From a suitable coordinate frame this transmission would be backward in time, contradicting causality.

It is true that particles respond in a stochastic way. But this stochasticity of response cannot be explained by putting a stochastic element into any reduction mechanism that determines their behavior, because this behavior is not in fact determined by any information (even stochastic information!) in their past light cones.

10.2 Summary

We can summarize the argument by saying first, that the information (whether stochastic or not) that the hits convey to a and b might as well be the same, so long as it is not to break FIN by telling b about x, y, z or a about w, and second, that then it might as well have been given in advance. Of course it

is possible to let the particles' behavior be a function of *promptons*, but this merely passes the buck - even if we call these promptons *hits*, *they* must be of a kind that cannot be determined by previous history, even together with stochastic information.

The same argument shows, again assuming the experimenters' free will, that no relativistically invariant theory can provide a mechanism for reduction, because that would determine a particles behavior, contradicting the fact that it is still free to make its own decision. Moreover, we have seen that the Free Will assumption is not needed for free state theories: *relativistically invariant theories that purport to provide answers at least to all our proposed triple experiments cannot also provide a mechanism for reduction.*

This prevents not only GRW, but any scientific theory of this traditional free state type, from providing a relativistically invariant mechanism for reduction, even without the Free Will assumption. The theories that purport to do so must deny one of SPIN, TWIN, FIN.

We remark that Albert and Vaidman [AV] have made another objection to GRW - that its explanation of the Stern-Gerlach experiment does not produce sufficiently fast reduction. Ghirardis response places part of the reduction quite literally in the eye of the beholder, which however leads to the concordance problem of the next section (in its acute form).

11 Philosophical Remarks Related to the Free Will Theorem

11.1 On Free Will

Let us first discuss the Free Will assumption itself. What if it is false, and the experimenter is not free to choose the direction in which to orient his apparatus? We first show by a simple analogy that a universe in which every choice is really Hobson's choice is indeed logically possible. Someone who takes a friend to see a movie he has himself already seen experiences a kind of determinacy that the friend does not. Similarly, if what we are experiencing is in fact *a second showing of the universe movie*, it is deterministic even if *the first showing* was not.

It follows that we cannot *prove* our Free Will assumption - determinism, like solipsism, is logically possible. Both the non-existence of free agents in determinism and the external world in solipsism are rightly conjured up by philosophers as consistent if unbelievable universes to show the limits of what is possible, but we discard them as serious views of our universe.

It is hard to take science seriously in a universe that in fact controls all the choices experimenters think they make. Nature could be in an insidious conspiracy to *confirm* laws by denying us the freedom to make the tests that would refute them. Physical induction, the primary tool of science, disappears if we are denied access to random samples. It is also hard to take seriously the arguments of those who according to their own beliefs are deterministic automata!

We have defined *free will* to be the opposite of *determinism* despite the fact that since Hume some philosophers have tried to reconcile the two notions - a position called *compatibilism*. In our view this position arose only because all the physics known in Hume's day was deterministic, and it has now been outmoded for almost a century by the development of quantum mechanics.

However, for the purposes of this discussion, we can bypass this hoary discussion, simply by saying that the only kind of free will we are discussing, for both experimenters and particles, is the active kind of free will that can actually affect the future, rather than the compatibilists' passive variety that does not.

11.2 Free versus Random?

Although we find ourselves unable to give an operational definition of either *free* or *random*, we have managed to distinguish between them in our context, because free behavior can be twinned, while random behavior cannot (a remark that might also interest some philosophers of free will). Ghirardi remarked that it follows from Gisin's theorem that their *hits* must involve a stochastic element in order to make the GRW theory relativistically invariant. We have shown that what the hits really need is some freedom (to be precise, that they must be at least semi-free). It is for reasons including these that we prefer to describe our particles' behavior as *free* rather than *random*, *stochastic*, or *indeterminate*.

11.3 Interpretation of Quantum Mechanics

We next describe our own thoughts on the interpretation of Quantum Mechanics, which have been informed by the Free Will theorem even when not strictly implied by it.

We first dismiss the idea, still current in popular accounts although long discounted by most physicists, that a conscious mind is necessary for reduction. It should suffice to say that there has never been any evidence for this opinion, which arose only from the difficulty of understanding the reduction, but has never helped to solve that problem. The evidence against it is the obvious Concordance Problem - if reduction is in the mind of the observer, how does it come about that the reductions produced by different observers are the same? This problem is particularly acute for our proposed type of experiment, in which the fact that one observer is on Earth and the other on Mars causes relativistic difficulties.

Von Neumann's *Cut Theorem* has sometimes been used to support this belief, since it shows that any single observer can explain the facts by imagining he performs the reduction, but used in the other direction it actually proves that there can be no evidence for this belief, since the facts are equally explained by supposing the cut takes place outside him. The belief is akin to solipsism and has the same drawbacks - it does not respect the symmetry that the facts are invariant under interchange of observers.

11.4 Textural Tests

What, then, causes the reduction to take place? The Cut Theorem shows that current quantum mechanics, being linear, cannot itself decide this question. We believe that the reduction is a real effect that will only be explained by a future physics, but that current experiments are already informative. Every experimentalist knows that it is in fact extremely difficult to maintain coherence - it requires delicate experiments like those of Mach-Zehnder interferometry. Consideration of such experiments has led us to believe that the criterion that decides between wave-like and corpuscular behavior is what we may call the *texture* of the surroundings. Roughly speaking, only sufficiently *smooth* textures allow it to behave as a wave, while *rough* ones force it to become a particle.

Exactly what this means depends on the circumstances in a way that we do not pretend to understand. Thus in the interferometric context, the half-silvered beam-splitters permit wave-like behavior, so count as smooth, while detectors force the collapse to a particle, i.e., are rough.

However, the Free Will Theorem tells us something very important, namely that although a *rough* texture forces *some* decision to be made, it does not actually choose which decision that is. We may regard such a texture as a tribunal that may require a particle to answer, but may not force it to make any particular answer. A future theory may reasonably be expected to describe more fully exactly which *textures* will cause reductions, but the Free Will Theorem shows that no such theory will correctly predict the results of these reductions:

Textural tests may demand but not command.

11.5 Closing remarks

It is our belief that the assumptions underlying the earlier disproofs of hidden variables remain problematic. They involve questionable notions such as *elements of reality*, counterfactual conditionals, and the resulting unphysical kinds of locality. Indeed, in his careful analysis of these theories, Redhead produces no fewer than ten different varieties of locality.

One advantage of the Free Will theorem is that by making explicit the necessary Free Will assumption, it replaces all these dubious ideas by a simple consequence, FIN, of relativity. A greater one is that it applies directly to the real world rather than just to theories. It is this that prevents the existence of local mechanisms for reduction.

The world it presents us with is a fascinating one, in which fundamental particles are continually making their own decisions. No theory can predict exactly what these particles will do in the future for the very good reason that they may not yet have decided what this will be! Most of their decisions, of course, will not greatly affect things - we can describe them as mere ineffectual flutterings, which on a large scale almost cancel each other out, and so can be ignored. I strongly believe, however, that there is a way our brains prevent some of this cancellation, so allowing us to integrate what remains and producing our own free will.

The mere existence of free will already has consequences for the philosophy of general relativity. That theory has been thought by some to show that *the flow of time* is an illusion. We quote only one of many distinguished authors to that effect: *The objective world simply is, it does not happen* (Hermann Weyl). It is remarkable that this common opinion, often referred to as the *block universe* view, has come about merely as a consequence of the usual way of modeling the mathematics of general relativity as a theory about the curvature of an eternally existing arena of space-time. In the light of the Free Will theorem this view is mistaken, since the future of the universe is not determined. Theodore Roosevelt's decision to build the Panama Canal shows that free will moves mountains, which implies, by general relativity, that even the curvature of space is not determined. The stage is still being built while the show goes on.

Einstein could not bring himself to believe that *God plays dice with the world*, but perhaps we could reconcile him to the idea that *God lets the world run free*.

12 Theory #1- Information-theoretic postulates for quantum theory

12.1 Introduction

By all standards, quantum theory is one of the most successful theories of physics. It provides the basis of particle physics, chemistry, solid state physics, and it is of paramount importance for many technological achievements. So far, all experiments have confirmed its universal validity in all parts of our physical world. Unfortunately, quantum theory is also one of the most mysterious theories of physics.

In the text books, quantum theory is usually introduced by stating several abstract mathematical postulates: *States are unit vectors in a complex Hilbert space; probabilities are given by the Born rule; the Schrodinger equation describes time evolution in closed systems*, to name just some of them. As many students recognize - and experienced researchers over years of use sometimes tend to forget - these postulates seem arbitrary and do not have a clear meaning. It is true that they work very well and are in accordance with

experiments, but *why are they true?* How come that nature is described by these counterintuitive laws of complex Hilbert spaces?

What at first sight seems to be a physically vacuous, philosophical question is in fact of high relevance to theoretical physics, in particular for *attempts to generalize quantum theory*. There have been several attempts in the past to construct natural modifications of quantum theory - either to set up experimental tests of quantum physics, or to adapt it in a way which allows for easier unification with general relativity. However, modification of quantum theory turned out to be a surprisingly difficult task.

A historical example is given by Weinberg's non- linear modification of quantum theory. Only a few months after his proposal was published, Gisin demonstrated that the resulting theory has an unexpected poisonous property: it allows for superluminal signaling. It can be shown in general that other proposals of this kind must face similar fate. It seems as if the usual postulates of quantum theory are intricately intertwined, in a way such that modification of one postulate makes the combination of the others collapse into a physically meaningless - or at least problematic - theory.

In this section, we propose a way to overcome this situation: we consider four natural information-theoretic postulates that have a clear physical meaning, which when taken together, turn out to be equivalent to the usual postulates of quantum theory. In particular, these postulates do not refer to complex numbers, Hilbert spaces, or operators, but use only notions which make sense in terms of classical probability. They can loosely be stated as follows:

1. The state of a composite system is characterized by the statistics of measurements on the individual components.

2. All systems that effectively carry the same amount of information have equivalent state spaces.

3. Every pure state of a system can be transformed into every other by continuous reversible time evolution.

4. In systems that carry one bit of information, all measurements which give non-negative probabilities are allowed by the theory.

Below, we show how to derive the usual formalism of quantum theory from these postulates. Surprisingly, the complex numbers and Hilbert spaces pop

out even though they are not mentioned in the postulates. This will also allow us to gain a better understanding of the usual quantum formalism, and resolve some of the mystery around ad hoc postulates like the Born rule.

Our result suggests an obvious method to obtain natural modifications of quantum theory: *drop one of the postulates that we propose, and work out mathematically what the resulting set of theories looks like.* In contrast to the usual formulation of quantum theory, we know for sure that the resulting alternative theories exist and are consistent - for example, they do not allow for superluminal signaling as in Weinberg's approach. In a way, those theories are *quantum theory's closest cousins*: they are not necessarily formulated in terms of Hilbert spaces, but they are physically and conceptually as close to quantum theory as possible.

As the simplest possible modification, suppose we drop the word *continuous* from Postulate 3 - that is, we allow for discrete reversible time evolution. Unsurprisingly, another solution in addition to quantum theory appears: in this additional theory, states are (discrete) probability distributions, and reversible time evolution is given by permutations of outcomes. This is exactly *classical probability theory* in the discrete case. It turns out to be the unique additional solution in this case.

This modern approach to reconstruction was pioneered by Hardy (see Theory #2). Clearly, the attempt to axiomatize quantum theory dates back much further, including attempts by Birkhoff and von Neumann, Mackey, or Ludwig. From a more mathematical angle, there has been extensive work on classifying the state spaces of operator algebras.

Every axiomatization has its own benefits. We think that the main advantage of this work - as described below - is its *parsimony*: our postulates are rather weak, possibly even close to optimal. Thus, one may expect that dropping one or two of the postulates will allow us to discover other theories that share many interesting features with quantum theory, but still describe a different kind of physics.

12.2 What do we mean by *quantum theory*?

When talking about axiomatizing quantum theory, there is sometimes confusion about what we actually mean by it. The term *quantum theory* arouses association with many different aspects of physics that are usually treated in quantum mechanics text books, such as particles, the hydrogen atom, three-dimensional position and momentum space and many other things.

However, a more careful definition should apply here. As an analogy, consider the theory of statistical mechanics. This theory consists of an application of probability theory to mechanics, which means in particular that abstract probability theory can be studied detached from statistical physics - and this has been done in mathematics for a very long time.

Similarly, we can consider quantum mechanics to be a combination of an abstract probabilistic theory - *quantum theory* - and classical mechanics. Abstract quantum theory can be studied detached from its mechanical realization; the main difference to the previous example lies in the historical fact that the development of quantum mechanics preceded that of abstract quantum theory. In this terminology, we understand by emphquantum theory the statement that

- states are vectors (or density matrices) in a complex Hilbert space
- probabilities are computed by the Born rule or the trace rule
- the possible reversible transformations are the unitaries,
- measurements are described by projection operators, and thus observables are given by self-adjoint matrices.

The *classical mechanics* part, on the other hand, determines the type of Hilbert space to consider (such as $L^2(\mathbb{R}^3)$), the choice of *Hamiltonians* H which generate the time evolution, $U(t) = exp(iHt)$, and the choice of initial states of that time evolution. This conceptual distinction has proven particularly useful in the development of quantum information theory. It seems that this distinction was always implicit when expressing the desire to *quantize* any classical physical theory, that is, to combine it with abstract quantum theory.

Thus, since we are aiming for a reconstruction of abstract quantum theory,

we will not refer to position, momentum, or Hamiltonians in this discussion. Instead, we only use the notions of abstract probability theory: of events, happening with certain probabilities, and of transformations modifying the probabilities. Furthermore, we restrict our analysis to finite-dimensional systems: we argue that the main mystery is why to have a complex Hilbert space at all. If this is understood in finite dimensions, it seems only a small conceptual (though possibly mathematically challenging) step to guess the correct infinite-dimensional generalizations.

Since we presuppose probabilities as given, we also do not address the question where these probabilities come from. Hence we also ignore the question about what happens in a quantum measurement, and all other interpretational mysteries encompassing the formulation of quantum theory. Instead, we restrict ourselves to ask how the mathematical formalism of quantum theory can be derived from simpler postulates, and what possible modifications of it we might hope to find in nature. Summarizing:

Questions that we would like to address:

- How can we understand (that is, derive) the complex Hilbert space formalism from simple assumptions on probabilities?
- What other probabilistic theories are conceptually closest to quantum theory?

Questions that we do *not* address:

- What is *probability*?
- The measurement problem: What happens to a state during/after a measurement?
- How can we *interpret* quantum mechanics?

In order to formulate our postulates, we work with a simple and general framework encompassing all conceivable ways to formulate physical theories of probability: this is the framework of generalized probabilistic theories.

12.3 Generalized Probabilistic Theories

Classical probability theory (abbreviated CPT henceforth) is used to describe processes which are not deterministic. Classical probability theory (abbreviated CPT henceforth) is used to describe processes which are not deterministic. This is achieved by assuming a particular mathematical structure: a probability space with a unique fixed probability measure, which is used to assign probabilities to all random variables. The framework of generalized probabilistic theories generalizes this approach in a simple way. We will now give a brief introduction to this framework, built on general considerations of what constitutes an experiment in physics.

In order to set up a common picture, we consider Figure 7

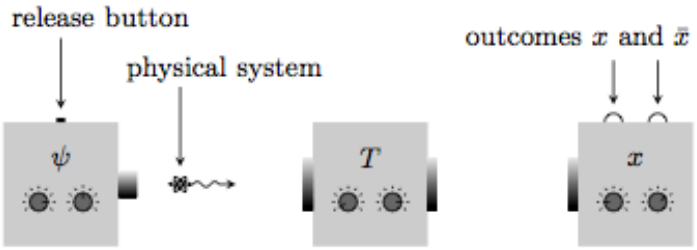

Figure 7: General experimental set up. From left to right there are the preparation, transformation and measurement devices. As soon as the release button is pressed, the preparation device outputs a physical system in the state specified by the knobs. The next device performs the transformation specified by its knobs (which in particular can be *do nothing*). The device on the right performs the measurement specified by its knobs, and the outcome (x or $\bar{x}$) is indicated by the corresponding light.

as the model for what constitutes a physical experiment. This is just an illustration: the events that we describe are arbitrary, and may as well be natural processes that happen without human or technological intervention.

The main idea (Figure 1) is that physical systems can cause objective events - for example clicks of detectors. We say that two systems are in the *same state* ω if all outcome probabilities of all possible measurements are the same. In order to test this empirically, we always assume that we can prepare a phys-

ical system in a given state as often as we want. That is, we may think of a *preparation device* which produces a physical system in a particular state.

12.3.1 A. States and measurements

Single outcomes of measurements are called *effects*, and are denoted by uppercase letters such as E. The probability of obtaining outcome E, if measured on state ω, will be denoted $E(\omega)$. This way, effects become maps from states to probabilities in $[0, 1]$.

What can we say about the set of all possible states ω in which a given system can be prepared? Suppose we have two preparation devices; one of them prepares the system in some state ω, the other one prepares it in some state ϕ. Then we can use these devices to construct a new device, which tosses a coin, and then prepares either state ω with probability $p \in [0, 1]$, or state ϕ with probability $1 - p$. We denote this new state by

$$\omega' := p\omega + (1 - p)\phi$$

Clearly, if we apply a measurement on ω', we get outcome E with probability

$$E(\omega') = pE(\omega) + (1 - p)E(\phi)$$

Thus, by this construction, we see that states ω become elements of an affine space(an affine space is what is left of a vector space after you've forgotten which point is the origin), and effects E are affine maps. The set of all possible states - called the *state space* $\mathcal{S}$ - will be a subset of this affine space. We have just seen that $\omega \in \mathcal{S}$ and $\phi \in \mathcal{S}$ imply $p\omega + (1 - p)\phi \in \mathcal{S}$ if $0 \leq p \leq 1$; that is, state spaces are convex sets(let S be a vector space over the real numbers, or, more generally, some ordered field. This includes Euclidean spaces. A set C in S is said to be convex if, for all x and y in C and all t in the interval $[0, 1]$, the point $(1 - t)x + ty$ is in C. In other words, every point on the line segment connecting x and y is in C).

In principle, state spaces can be infinite-dimensional (and in fact, in many physical situations, they are). However, in this discussion, we will only consider finite-dimensional state spaces. Then, states ω are determined by finitely many coordinates, and we may use this to construct a more concrete representation of states. Denote the dimension of a state space $\mathcal{S}$ by

d. Then, by choosing d affinely independent(an affine combination is a linear combination in which the sum of the coefficients is 1 - just as members of a set of vectors are linearly independent if none is a linear combination of the others, so also they are affinely independent if none is an affine combination of the others) effects $E_1, ..., E_d$, the probabilities $E_1(\omega), ..., E_d(\omega)$ determine ω uniquely. We now use the representation

$$\omega = \begin{pmatrix} 1 \\ E_1(\omega) \\ E_2(\omega) \\ \vdots \\ E_d(\omega) \end{pmatrix} = \begin{pmatrix} 1 \\ \omega_1 \\ \omega_2 \\ \vdots \\ \omega_d \end{pmatrix} \in \mathcal{S} \subset (R)^{d+1} \tag{1}$$

The choice of $E_1, ..., E_d$ is arbitrary, subject only to the restriction that they are affinely independent. We call a set of effects with this property *fiducial*, and we refer to $E_1(\omega), ..., E_d(\omega)$ as *fiducial outcome probabilities*. The component $\omega_0 := 1$ has been introduced for calculational convenience: it allows us to write the affine effects E as *linear* functionals on the larger space $(R)^{d+1}$. It will also turn out to be particularly useful in calculations involving composite state spaces.

In the following, we will assume that state spaces $\mathcal{S}$ are topologically closed and bounded, i.e. compact(a topological space is compact if every open cover of X has a finite subcover. In other words, if X is the union of a family of open sets, there is a finite subfamily whose union is X. A subset A of a topological space X is compact if it is compact as a topological space with the relative topology (i.e., every family of open sets of X whose union contains A has a finite subfamily whose union contains A). The extremal points of the convex set $\mathcal{S}$ will be called *pure states*; these are states ω which cannot be written as mixtures $p\varphi + (1-p)\varphi'$ of other states $\varphi \neq \varphi'$ with $0 < p < 1$. It follows from the compactness of $\mathcal{S}$ that every state can be written as a convex combination of at most $d+1$ pure states.

Measurements with n outcomes are described by a collection of n effects $E_1, E_2, ..., E_n$ with the property $E_1(\omega) + E_2(\omega) + ... + E_n(\omega) = 1$ for all states ω. This ex- presses the fact that outcome i happens with probability $E_i(\omega)$, and the total probability is one. Note that two effects E and F can only be part of the same measurement if $E(\omega) + F(\omega) \leq 1$ for all states ω. Sets of fiducial effects (as introduced above) do not necessarily have this

property. A single effect E is always part of a measurement with two outcomes E and $\bar{E}$, where $\bar{E}(\omega) := 1 - E(\omega)$.

Figure 8 gives some examples of convex state spaces.

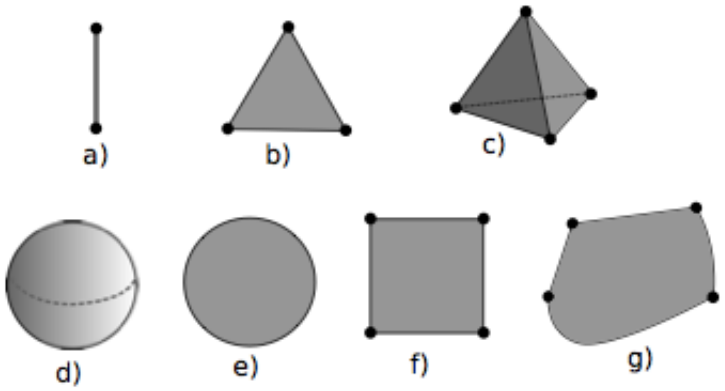

Figure 8: Examples of convex state spaces: a) is a classical bit, b) and c) are classical 3- and 4-level systems, d) is a quantum bit, e) is the projection of a qubit, f) and g) are neither classical nor quantum. Note that quantum n-level systems for $n \geq 3$ are not balls.

First, consider a classical bit, which is described within CPT. We can think of a coin which shows either heads or tails; in general, it can be in one of those configurations with some probability. The probability p of showing heads determines the state uniquely, since the tails probability must be $1 - p$. Thus, $p \in [0, 1]$ is a fiducial probability; recalling (1), we can represent states as $\omega = [1, p]^T$. This yields a one-dimensional state space, with two pure states $[1, 0]^T$ and $[1, 1]^T$, corresponding to coins which deterministically show heads or tails. It is depicted in Figure 8a.

Similarly, classical $n-$level systems have states which correspond to probability distributions $p_1, ..., p_n$. Since $p_n = 1 - (p_1 + p_2 + ... + p_{n-1})$, the numbers $p_1, ..., p_{n-1}$ are fiducial outcome probabilities, yielding states $\omega = [1, p_1, ..., p_{n-1}]^T$. Geometrically, the resulting state spaces are simplices. They are depicted in Figure 8b) and c) for $n = 2$ and $n = 3$.

Quantum systems look very different: as it is well- known, states of quantum $2-$level systems, i.e. qubits, can be parametrized by a vector $\vec{r} \in \mathbb{R}^3$ with

$|\vec{r}| \leq 1$, such that every density matrix can be written $\rho = (\mathbf{1} + \vec{r} \cdot \vec{\sigma})/2$, with $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ the Pauli matrices. Thus we can use the vector $[1, r'_x, r'_y, r'_z]^T$ to represent states, where $r'_i := (1 + r_i)/2$ is the probability to measure *spin up* in $i-$direction. This state space is the famous (slightly reparametrized) Bloch ball, cf. Figure 8d).

Figure 8e) shows a state space which is a projection of the Bloch ball: it corresponds to the effective state space that we obtain if, for some reason, spin measurements in $z-$direction are physically impossible to implement, with states $\omega = [1, r'_x, r'_y]^T$. The square state space in Figure 8f) describes a system for which there exist two independent effects, say X and Y, that can yield probabilities $X(\omega)$ and $Y(\omega)$ in $[0, 1]$ arbitrarily and independently from each other. States will be of the form $\omega = [1, \omega_x, \omega_y]^T$,with $\omega_x = X(\omega)$ and $\omega_y = Y(\omega)$.

Consider the two yes-no-measurements which correspond to the effects X and Y; we can interpret these as spin measurements in two orthogonal directions, with *yes*-outcome X or Y for *spin up*, and *no*-outcome $\bar{X}$ or $\bar{Y}$ for *spin down*. If we perform either one of these measurements on the state in the square $\omega = (1, 1, 1)$, then we will get the *yes*-outcome with unit probability - and this is true for both measurements. If we consider the analogous measurements on the circle state space, we see that the corresponding behavior becomes impossible: if one of the spin measurements yields outcome *yes* with certainty, then the other spin measurement must give outcome *yes* with probability $1/2$. This follows from $r_x^2 + r_y^2 \leq 1$.

Thus, the circle state space shows a form of *complementarity*, which is not present in the square state space. As this example illustrates, the state space of a physical system can tell us everything about its information-theoretic properties. Given a description of the state space $\mathcal{S}$, we can also determine the set of all linear functionals which map states to the unit interval $[0, 1]$, that is, the candidates for possible effects. However, not all of them may be possible to implement in physics: maybe some of them are *forbidden*, similarly as superselection rules forbid some superpositions in quantum mechanics. Therefore, to every given state space $\mathcal{S}_A$, there is a set of *allowed effects* which are interpreted as those that can actually be physically performed.

We introduce some notions which will be useful later: A set of states $\omega_1, ..., \omega_n$ is called *distinguishable* if there is a measurement with outcomes represented by effects $E_1, ..., E_n$, such that $E_i(\omega_j) = \delta_{ij}$, which is 1 if $i = j$ and 0 otherwise. The interpretation is that we can build a device which perfectly distinguishes the different states ω_j. Given a physical system A, we define the capacity N_A as the maximal size of any set of distinguishable states $\omega_1, ..., \omega_n \in \mathcal{S}_A$. A measurement which is able to distinguish N_A states (that is, as much as possible) will be called *complete*.

For a quantum state space, N_A equals the dimension of the underlying complex Hilbert space. We also use the notation $K_A := dim(\mathcal{S}_A) + 1$; this is the dimension of the sur- rounding linear space that carries $\mathcal{S}_A$. For a qubit, for example, we have $N_A = 2$, but $K_A = 4$. In quantum theory, $K_A = N_A^2$ equals the number of independent real parameters in a density matrix (dropping normalization). In classical probability theory, we always have $K_A = N_A$.

12.3.2 B. Transformations

A transformation is a map T which takes a state to another state. Which transformations are actually possible is a question of physics. However, there are certain minimal assumption that every transformation must necessarily satisfy in order to be physically meaningful in the context of convex state spaces. First, transformations must respect probabilistic mixtures - that is,

$$T(p\omega + (1-p)\varphi) = pT(\omega) + (1-p)T(\varphi)$$

This is because both sides of the equation can be interpreted as the result of randomly preparing ω or φ (with probabilities p respectively $1-p$) and applying the transformation T. Thus, transformations (from one system to itself) are linear maps which map a state space $\mathcal{S}$ into itself.

If both T and $T^{?1}$ are physically allowed transformations, we call T *reversible*. The set of reversible transformations on a state space $\mathcal{S}_A$ is a group $\mathcal{G}_A$. For physical reasons, we assume that $\mathcal{G}_A$ is topologically closed, hence a compact group (it may be a finite group). A topological group is a group G together with a topology on G such that the group's binary operation and the group's inverse function are continuous functions with respect to the topology. A topological group is a mathematical object with both an algebraic structure and a topological structure. Thus, one may perform algebraic operations, because of the group structure, and one may talk about continuous functions,

because of the topology. A compact group is a topological group whose topology is compact. Compactness is not easy to describe precisely in an intuitive manner; in some sense it says that the topology allows the space to be considered as *small* (compactness is a kind of topological counterpart to finiteness of sets), even though as a set it may be quite large. Moreover, more intuitive characterizations of compactness are often dependent on additional properties of the topological space to be valid; the following description assumes the space is a metric space, so that "closeness" of points has meaning. Then compactness means that whenever one chooses infinitely many sample points from the space, some of the samples must eventually get arbitrarily close to at least one point of the space. This could be because some point is itself sampled infinitely many times (as would necessarily happen if the space were finite), but a more significant possibility is that the point itself is not in the sample, but that any neighborhood of the point, however small, does contain infinitely many sample points.

Reversible transformations map a state space bijectively(a map is called bijective if it is both one-to-one and onto itself - hence they are symmetries of the state space. For example, in quantum theory, reversible transformations are the unitary conjugations, $\rho \mapsto U\rho U^\dagger$. In the Bloch ball representation of the qubit (as in Figure 8d)), these maps are represented as rotations, such that the group of reversible transformations is isomorphic to SO(3).

However, as this example also shows, not all symmetries are automatically allowed reversible transformations: a reflection in the Bloch ball is a symmetry, but it is not an allowed transformation (in the density matrix picture, it would correspond to an anti-unitary map).

In summary, for what follows, a physical system A is specified by three mathematical objects: the state space $\mathcal{S}_A$, the group of reversible transformations $\mathcal{G}_A$ (which is a compact subgroup of all symmetries of $\mathcal{S}_A$), and a set of physically allowed effects. The latter will not be given a particular notation, but we assume that the set of allowed effects is topologically closed. For obvious physical reasons, if E is an allowed effect and $T \in \mathcal{G}_A$, then $E \circ T$ is an allowed effect; similarly, convex combinations of allowed effects are allowed.

12.3.3 C. Composite systems

If we are given two physical systems A and B, we would like to define a composite system AB which is also a physical system in the sense described above, with its own state space $\mathcal{S}_{AB}$, group of reversible transformations $\mathcal{G}_{AB}$, and set of allowed effects.

In contrast to quantum theory, the framework of general probabilistic theories allows many different possible composites for two given systems A and B. Every possible composite AB has a set of minimal physical assumptions that it must satisfy:

- If $\omega_A \in \mathcal{S}_A$ and $\omega_B \in \mathcal{S}_B$ are two local states,then there is a distinguished state $\omega_A\omega_B \in \mathcal{S}_{AB}$ which is interpreted as the result of preparing ω_A and ω_B independently on the subsystems A and B.

- If E_A and E_B are local allowed effects on A and B, then there is a distinguished allowed effect E_AE_B on AB which is interpreted as measuring E_A on A and E_B on B independently, yielding the total probability that outcome E_A happens on system A, and outcome E_B happens on system B.

- This intuition is mathematically expressed by demanding that

  $$E_AE_B(\omega_A\omega_B) = E_A(\omega_A)E_B(\omega_B)$$

  where both E_AE_B and $\omega_A\omega_B$ are affine in both arguments. This also formalizes the physical assumption that the temporal order of the local preparations respectively measurements is irrelevant.

From the previous point, we can infer that we can represent independent local preparations $\omega_A\omega_B$ and measurement outcomes E_AE_B by tensor products:

$$E_AE_B \equiv E_A \otimes E_B \quad , \quad \omega_A\omega_B \equiv \omega_A \otimes \omega_B$$

Consider the joint state space $\mathcal{S}_{AB}$, which is contained in a linear space AB. We have inferred that

$$A \otimes B \subseteq AB$$

For the dimensions of these spaces, we obtain

$$K_AK_B \leq K_{AB}$$

Now consider two different measurements (for simplicity with two outcomes) $E_B, \bar{E}_B := \mathbf{1}_B - E_B$ and $F_B, \bar{F}_B := \mathbf{1}_B - F_B$ where $\mathbf{1}_B$ denotes the trivial effect on system B which yields unit probability on every normalized state. We can think of an agent *Bob*, holding system B, who may decide freely (say, randomly in a way which is uncorrelated with A) whether to perform measurement $E_B, \bar{E}_B$ or $F_B, \bar{F}_B$.

Suppose that *Alice* (holding system A) performs some measurement after Bob has chosen and performed his measurement on a bipartite state ω_{AB}. The marginal probability that she obtains (not knowing Bob's outcome) is the same in both cases:

$$\begin{aligned} E_A \otimes \mathbf{1}_B(\omega_{AB}) &= E_A \otimes E_B(\omega_{AB}) + E_A \otimes \bar{E}_B(\omega_{AB}) \\ &= E_A \otimes F_B(\omega_{AB}) + E_A \otimes \bar{F}_B(\omega_{AB}) \end{aligned}$$

The same holds with the roles of A and B reversed. We have recovered the *no-signalling property*: Bob cannot send information to Alice merely by choosing his local measurement (and vice versa). Moreover, we have proven that Alice locally observes the *reduced state* $\omega_A := Id_A \otimes \mathbf{1}_B(\omega_{AB})$ (note that Id_A is a linear transformation, while $\mathbf{1}_B$ is a linear functional). This state is uniquely characterized by the equation

$$E_A(\omega_A) = E_A \otimes \mathbf{1}_B(\omega_{AB})$$

or all functionals (in particular, all allowed effects) E_A.

For physically meaningful composites AB, we should demand that reduced states ω_A, ω_B of all bipartite states $\omega^{AB} \in \mathcal{S}_{AB}$ are valid local states themselves. Instead, we will demand something which is stronger and contains this as a special case. Suppose that Alice and Bob share ω^{AB} and Bob performs a measurement and obtains outcome E_B. Knowing this outcome leaves a *conditional* state $\omega_A^{E_B}$ at Alices side, which by elementary probability theory satisfies

$$E_A(\omega_A^{E_B}) = \frac{E_A \otimes E_B(\omega_{AB})}{\mathbf{1}_A \otimes E_B(\omega_{AB})} \tag{2}$$

We demand that $\omega_A^{E_B} \in \mathcal{S}_A$ for all allowed effects E_B and all $\omega_{AB} \in \mathcal{S}_{AB}$. The reduced state ω_A can be written

$$\omega_A = \lambda \omega_A^{E_B} + (1-\lambda)\omega_A^{\bar{E}_B}$$

with $\lambda = \mathbf{1}_A \otimes E_B(\omega_{AB})$; thus, $\omega_A \in \mathcal{S}_A$ by convexity.

In some situations, this condition is automatically satisfied, namely if all effects on A and B are allowed (recall that not all effects need to be physically possible to implement; above, we have discussed that possibly only a subset of effects might be physically allowed). The proof will also illustrate that the *cone of unnormalized states* is a useful concept.

Lemma 1. *Suppose that A and B are state spaces such that all effects are allowed. Then, the inclusion of conditional states in the local state spaces follows directly from the fact that the composite state space AB contains all product states and effects.*

Proof. Define the *cone of unnormalized states* A_+ on A by

$$A_+ := \{\lambda\omega_A \,|\, \omega_A \in \mathcal{S}_A, \lambda \geq 0\}$$

Since $\mathbf{1}_A(\lambda\omega) = \lambda$ for $\omega \in \mathcal{S}_A$, a vector $\omega \in A_+$ is a normalized state, i.e., $\omega \in \mathcal{S}_A$, iff $\mathbf{1}_A(\omega_A) = 1$.

The *cone of unnormalized effects* is

$$A^+ := \{\lambda E_A \,|\, E_A(\omega_A) \in [0,1] \text{ for all } \omega_A \in \mathcal{S}_A\}$$

Since we have said that all effects are allowed, every linear map $E_A : A \to \mathbb{R}$ with $E_A(\omega) \in [0,1]$ is an allowed effect. The set A_+ contains all multiples of those. Both sets A_+ and A^+ are *closed convex cones*, where *cones* refers to the fact that if x is in the set, then λx is also in the set for all $\lambda \geq 0$.

It is now easy to see that A^+ is the *dual cone* $(A_+)^*$ of A_+, where

$$(A_+)^* \equiv \{E : A \to \mathbb{R} \,|\, E(\omega) \geq 0 \text{ for all } \omega \in A^+\}$$

Since $(A_+)^{**} = A_+$, we get also that A_+ is the dual cone of A^+; in other words,

$$A_+ = \{\omega \in A \,|\, E(\omega) \geq 0 \text{ for all } E \in A^+\}$$

Recall the definition of the conditional state in (2). It follows directly from this definition that $E_A(\omega_A^{E_B}) \geq 0$ for all allowed effects E_A, hence for all $E_A \in A^+$. But then, we must have $\omega_A^{E_B} \in A_+$. Since $\mathbf{1}_A(\omega_A^{E_B}) = 1$, we get $\omega_A^{E_B} \in \mathcal{S}_A$. The same reasoning holds for B instead of A. □

Our state spaces also carry a group of reversible transformations. If $G_A \in \mathcal{G}_A$ is a reversible transformation on A, and $G_B \in \mathcal{G}_B$ one on B, it is physically clear that we should be able to accomplish both transformations locally independently; i.e., $G_A \otimes G_B \in \mathcal{G}_{AB}$. We will assume that composite state spaces satisfy this condition. One of our postulates below will be the postulate of *local tomography*(quantum tomography or quantum state tomography is the process of reconstructing the quantum state (density matrix) for a source of quantum systems by measurements on the systems coming from the source). This is an additional condition on composites AB which is sometimes, but not always imposed in the framework of general probabilistic theories: It states that

> *global states are uniquely determined by the statistics of local measurement outcomes.*

That is, if ω_{AB} and φ_{AB} are global states in $\mathcal{S}_{AB}$, then $E_A \otimes E_B(\omega_{AB}) = E_A \otimes E_B(\varphi_{AB})$ implies that $\omega_{AB} = \varphi_{AB}$. But the part of AB which is *seen* by product effects $E_A \otimes E_B$ is exactly $A \otimes B$. That is, the postulate of local tomography is equivalent to $AB = A \otimes B$, and thus to

$$K_{AB} = K_A K_B$$

Thus, we get some kind of *tensor product rule* for composite state spaces, including $\mathbf{1}_{AB} = \mathbf{1}_A \otimes \mathbf{1}_B$. Note that this is not as strong as the tensor product rule of quantum theory (which specifies the global states uniquely, giving the local Hilbert spaces). Classical probability theory satisfies this rule as well. Suppose that A is a classical bit, and B is a classical 3−level system. Then the composite AB is classical 6−level system, i.e. $K_{AB} = 6$, while $K_A = 2$ and $K_B = 3$. We get $K_{AB} = K_A K_B$, which is equivalent to local tomography.

To see that we are still far beyond quantum theory, suppose that A and B are both the square state space from Figure 8f). Then, define the global state space $\mathcal{S}_{AB}$ as the set of all vectors $x \in AB$ with $E_A \otimes E_B(x) \in [0, 1]$ for all effects E_A and E_B, and $\mathbf{1}_A \otimes \mathbf{1}_B(x) = 1$ (normalization). It turns out that this state space contains so-called *PR-box states* that violate the Bell-CHSH inequality by more than any quantum states. The set of states $\mathcal{S}_{AB}$ itself turns out to be the eight-dimensional *no-signalling polytope*(in elementary geometry, a polytope is a geometric object with flat sides, which exists in

any general number of dimensions) for two parties with two measurements and two outcomes each. The fact that these state spaces can have stronger non-locality than quantum theory has been extensively studied and is a main reason for the popularity of general probabilistic theories in quantum information.

It is also important to keep in mind that the conditions above do *not* determine the composite state space $\mathcal{S}_{AB}$ uniquely, even if $\mathcal{S}_A$ and $\mathcal{S}_B$ are given. For example, if $\mathcal{S}_A$ and $\mathcal{S}_B$ are quantum state spaces, then the usual composite quantum state space is a possible composite $\mathcal{S}_{AB}$, but there are other possibilities: one of them is to define $\mathcal{S}_{AB}$ as the set of unentangled global states. It satisfies all conditions mentioned above.

12.3.4 D. Equivalent state spaces

In classical physics, choosing a different inertial coordinate system does not alter the physical predictions of Newtonian mechanics. A similar statement is true for convex states spaces.

Consider a system A, given by a state space $\mathcal{S}_A$, a group of transformations $\mathcal{G}_A$, and some allowed effects. Suppose that B is another system, and suppose that there is an invertible linear map $L : A \to B$ (where now A and B denote the linear spaces carrying the state spaces) such that

- $\mathcal{S}_B = L(\mathcal{S}_A)$
- E_A is an allowed effect on A if and only if $E_A \circ L^{-1}$ is an allied effect on B
- $\mathcal{G}_B = L \circ \mathcal{G}_A \circ L^{-1}$

Then the systems A and B are physically indistinguishable from each other - they describe the same type of system, just parametrized in different ways. We will then call A and B equivalent. This notion is obviously an equivalence relation.

An example of two equivalent state spaces is given by a qubit B and the three-ball A. That is, the set of states $\mathcal{S}_B$ is the set of $2 \times 2-$density matrices, with the unitaries (acting by conjugation) as the group of reversible transformations $\mathcal{G}_B$. The state space A is defined as the set of states $\omega = [1, \vec{r}]^T$, where

$\vec{r}$ s a vector with Euclidean norm $|\vec{R}| \leq 1$ (as in Figure 8d)); the group of transformations is $\mathcal{G}_A = SO(3)$. The corresponding linear map establishing the equivalence is $L(\omega) := (r_0 \cdot \mathbf{1} + \vec{r} \cdot \vec{\sigma})/2$ where r_0 denotes the first component of ω.

Thus, in our endeavour to derive quantum theory, all we have to do is to prove that all state spaces satisfying our postulates are equivalent to quantum state spaces.

12.4 The Postulates

In this section, we describe our postulates and explain their physical meaning. We start with an axiom on composite state spaces that has already been mentioned in Subsection C above:

Postulate 1 (Local tomography). The state of a composite system AB is completely characterized by the statistics of measurements on the subsystems A, B.

The name *local tomography* comes from the interpretation that state tomography on composite systems can be done by performing local measurements and subsequently comparing the outcomes to uncover correlations. As already mentioned, this postulate is equivalent to $K_{AB} = K_A K_B$, where K_A denotes the number of degrees of freedom needed to specify an unnormalized state on A.

Our second postulate formalizes a property of physics that physicists intuitively take for granted, and that is in fact used very often in performing real experiments. Imagine some physical three-level system (that is, with three perfectly distinguishable states and no more: $N = 3$) that we can access in the lab (it might be quantum, classical, or describable within another theory). Now suppose that, for some reason, we have a situation where we never find the system in the third of the three distinguishable configurations on performing a measurement.

To have a concrete example, consider a quantum system that consists of three energy levels which can be occupied by a single particle. Suppose the system is constructed such that the third energy level is actually never occupied

(maybe because the corresponding energy is too high).

The consequence that we expect is the following: We effectively have a two-level system. This is definitely true for quantum theory, and classical probability theory, but it is not necessarily true for other generalized probabilistic theories. In general, for any number of levels (perfectly distinguishable states) N, we expect to have a corresponding state space $\mathcal{S}_N$. And the collection of states $\omega \in \mathcal{S}_N$ which has probability zero to be found in the $N-$th level upon measurement should be equivalent to $\mathcal{S}_{N-1}$.

In actual physics, this property is used all the time: We apply *effective descriptions* of physical systems, by ignoring impossible configurations. Qubits manufactured in the lab usually actually correspond to two levels of a system with much more energy levels, set up in a way such that the additional energy levels have probability close to zero to be occupied.

One may argue that physics would be in severe trouble if this property did not hold: we would then possibly have to take into account unobservable potential configurations even if they are never seen. They would modify the resulting state space that we actually observe. The following *subspace postulate* formalizes this idea. It is actually somewhat stronger than our discussion motivates: it also implies that, for every N, there is a unique type of $N-$level system $\mathcal{S}_N$.

The notions of complete measurements and equivalent state spaces were defined earlier in Subsections A and D.

Postulate 2 (Equivalence of subspaces). *Let $\mathcal{S}_N$ and $\mathcal{S}_{N-1}$ be systems with capacities N and $N-1$, respectively. If $E_1, ..., E_N$ is a complete measurement on $\mathcal{S}_N$, then the set of states $\omega \in \mathcal{S}_N$ with $E_N(\omega) = 0$ is equivalent to $\mathcal{S}_{N-1}$.*

The notion of equivalence needs some discussion. Postulate 2 states the equivalence of $\mathcal{S}_{N-1}$ and

$$\mathcal{S}'_{N-1} := \{\omega \in \mathcal{S}_N \,|\, E_N(\omega) = 0\} \tag{3}$$

Denote the real linear space which contains $\mathcal{S}_N$ by V_N; define V_{N-1} analogously, and set $V'_{N-1} := span(\mathcal{S}'_{N-1})$. Equivalence means first of all that there is an invertible linear map $L : V_{N-1} \to V'_{N-1}$ such that $L(\mathcal{S}_{N-1}) = \mathcal{S}'_{N-1}$. But

it also means that transformations and measurements on one of them can be implemented on the other. We now describe in more detail what this means.

Every effect E on $\mathcal{S}_N$ defines an effect on $\mathcal{S}'_{N-1}$ by restricting it to the corresponding linear space, resulting in $E_N \restriction V'_{N-1}$. Equivalence implies that the resulting set of effects is in one-to-one correspondence with the set of effects on $\mathcal{S}_{N-1}$, as described earlier in Subsection D.

The transformations on $\mathcal{S}'_{N-1}$ are defined analogously. To be more specific, define $\bar{\mathcal{G}}'_{N-1}$ as the set of transformations in $\mathcal{S}_N$ that preserve $\mathcal{S}'_{N-1}$ (or, equivalently, V'_{N-1}):

$$\bar{\mathcal{G}}'_{N-1} := \{T \in \mathcal{G}_N \,|\, T\mathcal{S}'_{N-1} = \mathcal{S}'_{N-1}\}$$

The set of reversible transformations $\mathcal{G}'_{N-1}$ is defined as the restriction of all these transformations to $\mathcal{S}'_{N-1}$ (or rather, as linear maps, to V'_{N-1}):

$$\mathcal{G}'_{N-1} = \{T \restriction V'_{N-1} \,|\, T \in \bar{\mathcal{G}}'_{N-1}\}$$

Equivalence means that

$$\mathcal{G}'_{N-1} = L \circ \mathcal{G}_{N-1} \circ L^{-1}$$

Concretely, if $U \in \mathcal{G}_{N-1}$ is any reversible transformation on a state space of capacity $N-1$, then the transformation $\tilde{U} := L \circ U \circ L^{-1}$ is a reversible transformation on $\mathcal{S}'_{N-1}$, i.e., $\tilde{U} \in \mathcal{G}'_{N-1}$. As such, it can be written $\tilde{U} = T \restriction \mathcal{S}'_{N-1}$ for some reversible transformation $T \in \mathcal{G}_N$.

It is important to note that *we don't have full information on* T - that is, our postulate does not specify T uniquely, given $\tilde{U}$. By definition, T preserves $\mathcal{S}'_{N-1}$ and therefore the subspace V'_{N-1}, but we do not know how it acts on the complement of that subspace - it might act as the identity there, or it might have a non-trivial action. Postulate 2 does not specify this. In general, there may (and will) be different T which implement the same $\tilde{U}$ on the subspace.

Using Postulate 2 iteratively, we see that state spaces of smaller capacity are included (in the sense described above) in those of larger capacity; symbolically,

$$\mathcal{S}_1 \subsetneq \mathcal{S}_2 \subsetneq \mathcal{S}_3 \subsetneq .....$$

Our next postulate describes the idea that any actual physical theory of probabilities must allow for ample possibilities of reversible time evolution. In situations where *no information is lost* - assuming that this situation applies to closed systems -, these systems A must evolve reversibly, that is, according to some subgroup of the group of reversible transformation $\mathcal{G}_A$. Clearly, if this group is trivial (contains only the identity), physics becomes *frozen*: no reversible time evolution is possible at all.

Postulate 3 proclaims a minimal amount of transformational richness for reversible time evolution: as a minimal requirement, it states that the group of reversible transformations should at least act transitively on the pure states. That is, if we prepare a pure state ω, and φ is another (desired) pure state on the same state space, then there should be a reversible transformation T which maps ω to φ:

Postulate 3 (Symmetry). *For every pair of pure states $\omega, \varphi \in \mathcal{S}_A$, there is a reversible transformation $T \in \mathcal{G}_A$ such that $T\omega = \varphi$.*

It is easy to see that Postulate 3 is actually true for quantum theory: every pure state can be mapped to every other by some unitary. This example also shows that Postulate 3 is rather weak: in quantum theory, even tuples of perfectly distinguishable pure states $\omega_1, ..., \omega_n$ can be mapped to other tuples $\varphi_1, ..., \varphi_n$ by suitable unitaries. This is a much higher degree of symmetry than what is directly demanded by Postulate 3.

There is one postulate remaining. As we discussed earlier in Subsection A, given some state space $\mathcal{S}_A$, not all effects (i.e. linear functionals on A which are non-negative on $\mathcal{S}_A$) may be physically allowed. Similarly as for superselection rules, it might be true that some effects are impossible to implement (an example would be a state space that allows only noisy measurements, and no outcome whatsoever occurs with probability zero).

In order for our axiomatization to work, we need to postulate that this strange behavior does not happen: that is, all mathematically well-defined effects correspond in fact to allowed measurement outcomes. As it turns out, it is sufficient to postulate this for a $2-$level system $\mathcal{S}_2$ (i.e. a generalized bit) only. In combination with the other postulates, it follows then for all other state spaces.

Postulate 4 (All measurements allowed). *All effects on $\mathcal{S}_2$ are outcome probabilities of possible measurements.*

From a mathematical point of view, this postulate could also be regarded as a background assumption: structurally, it says that the class of considered theories is the class of models where the effects are automatically taken as the dual of the states. In other words, it means that whenever we refer to *measurements* in the other postulates, we actually refer to collections of effects without considering the possibility that additional physical conditions might prevent their implementation. It is interesting to note that Postulate 4 can be replaced by a different formulation. It refers to *completely mixed states*, which are states that are in the relative interior of the convex set of states:

Postulate 4' If a state is not completely mixed, then there exists at least one state that can be perfectly distinguished from it.

12.5 How Quantum Theory Follows from the Postulates

We are now ready to carry out the reconstruction of quantum theory (QT) from the postulates. As it turns out, there will be another solution to Postulates 1.-4., which is classical probability theory (CPT). By this we mean the theory where the states are finite probability distributions, and the reversible transformations are the permutations. Figure 8a)-c) shows what classical probability distributions look like in terms of convex sets: they are simplices.

Therefore, we will now prove the following theorem:

Theorem 1 (Main Result). *The only general probabilistic theories, satisfying Postulates 1.-4. above, are equivalent to one of the following two theories:*

- **Classical probability theory (CPT):** *The state space is the set of probability distributions,*

$$\mathcal{S}_N = \{(p_1, ..., p_N) \,|\, p_i \geq 0, \sum_i p_i = 1\}$$

and the reversible transformations $\mathcal{G}_N$ are the per- mutations on $\{1, ..., N\}$.

- **Quantum theory (QT):** *The state space $\mathcal{S}_N$ is the set of density matrices on $N-$dimensional complex Hilbert space,*

$$\mathcal{S}_N = \{\rho \in \mathbb{C}^{N\times N} \mid \rho \geq 0, Tr\rho = 1\}$$

and the group of reversible transformations $\mathcal{G}_N$ is the projective unitary group, that is, the set of maps $\rho \mapsto U\rho U^{-1}$ with $U^\dagger U = \mathbf{1}$.

In both cases, all effects must be allowed. Working out the set of effects (that is, linear functionals on states yielding values between 0 and 1), one easily recovers the usual measurements of CPT and QT. In this discussion, we will not give the full reconstruction but will only try to give an easily accessible summary of the reconstruction, its main ideas, and some interesting observations in the course of the argument.

Before starting to do this, let us discuss a simple observation regarding Theorem 1. In order to rule out CPT - and hence to single out QT uniquely - we can tighten Postulate 3 by replacing it with the following modification:

Postulate 3C (Continuous symmetry.) *For every pair of pure states $\omega, \varphi \in \mathcal{S}_A$, there is a continuous family of reversible transformations $\{G_t\}_{t\in[0,1]}$ such that $G_0\omega = \omega$ and $G_1\omega = \varphi$.*

In other words, every pure state can be *continuously moved* into every other pure state. A statement like this is expected to be true in physical systems with continuous reversible time evolution - which is the case that seems to be true, to good approximation, in our universe. The consequence is:

The only general probabilistic theory that satisfies Postulates 1, 2, 3C, and 4, is quantum theory (QT).

12.5.1 A. Why bits are balls

In QT, the state space of a 2−level system (that is, a generalized bit, or qubit, $\mathcal{S}_2$) is a three-dimensional ball, the Bloch ball. In CPT, the (classical) bit instead is a line segment, as shown in Figure 8. In fact, this is a ball, too: it is a one-dimensional unit ball. However, quantum $N-$level systems with $N \geq 3$ are not balls: they contain mixed states in their topological

boundary(the boundary of a subset S of a topological space X is the set of points which can be approached both from S and from the outside of S - more precisely, it is the set of points in the closure of S, not belonging to the interior of S).

We will now show that all theories satisfying our postulates must have Euclidean ball states spaces as generalized bits. The dimension of this ball will not be determined yet; this will be done later on.

Our argument proceeds in two steps: first, we show that the state space $\mathcal{S}_2$ cannot have lines in its boundary; that is, we exclude the fact that $\mathcal{S}_2$ has proper faces as in the left picture of Figure 9. Using convex geometry language, we prove that $\mathcal{S}_2$ is strictly *convex*.

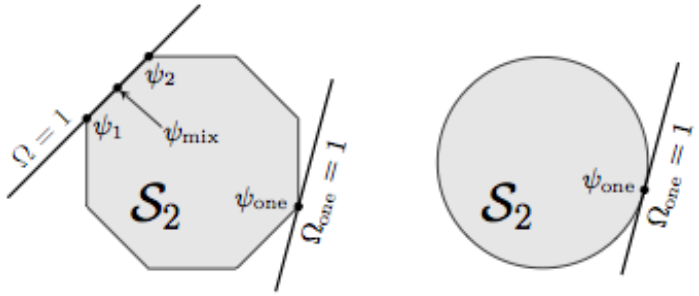

Figure 9: Like every compact convex set, the bit state space $\mathcal{S}_2$ contains pure states ω_e that are exposed - that is, there is an effect E_e such that ω_e is the unique state where this effects attains value 1. Due to Postulate 2, this proves that $\mathcal{S}_1$ contains a single state only. Now suppose $\mathcal{S}_2$ had lines in its boundary, as in the left picture. Then we would analogously find another effect E that attains value 1 on a non-trivial face. Consequently, Postulate 2 would tell us that $\mathcal{S}_1$ contains infinitely many states - a contradiction. Thus, $\mathcal{S}_2$ must be strictly convex as in the right picture. Euclidean ballness follows from group representation theory.

As a second step, we show that the symmetry property, Postulate 3, enforces $\mathcal{S}_2$ to be a Euclidean ball. The reason for this comes from group representation theory: since the group of transformations acts linearly, there is an inner product such that all transformations are orthogonal with respect to it.

Lemma 2. *The state space of the generalized bit $\mathcal{S}_2$ is strictly convex.*

Proof. Consider any effect E with $0 \leq E(\omega) \leq 1$ for all states $\omega \in \mathcal{S}_2$. Then this effect belongs to a two-outcome measurement (as defined earlier in Subsection A), consisting of the two effects E and $\mathbf{1} - E$. It is important to understand that the level sets $\{x \,|\, E(x) = c\}$ are hyperplanes(a hyperplane of an $n-$dimensional space is a flat subset with dimension $n-1$ - by its nature, it separates the space into two half spaces) of codimension(difference between dimension of space and subspace) 1, due to linearity of E. This is true for all state spaces $\mathcal{S}$. On the other hand, given some hyperplane, we can construct a corresponding effect E (with some freedom of offset and scaling) that has this hyperplane as its level set.

Like every compact convex set, $\mathcal{S}_2$ has at least one pure state ω_e which is exposed - that is, there is a hyperplane which touches the convex set only in ω_e and in no other point. Thus, we can construct an effect E_e such that the corresponding hyperplane is $\{x \,|\, E_e(x) = 1\}$, i.e., $E_e(\omega) = 1$, and $min_{\omega \in \mathcal{S}_2} E_e(\omega) = 0$. But then, $(E_e, \mathbf{1} - E_e)$ distinguishes two states perfectly, which is the maximal number for a bit - in other words, this is a *complete measurement*.

Now Postulate 2 says that

$$\begin{aligned} \{\omega \in \mathcal{S}_2 \,|\, (\mathbf{1} - E_e)(\omega) = 0\} &= \{\omega \in \mathcal{S}_2 \,|\, E_e(\omega) = 1\} \\ &= \{\omega_e\} \simeq \mathcal{S}_1 \end{aligned}$$

In other words, $\mathcal{S}_1$ is a trivial state space which contains only a single state. Now suppose that $\mathcal{S}_2$ would have lines in its boundary, and therefore non-trivial faces, as depicted on the left-hand side of Figure 9. Then we would find a supporting hyperplane that touches $\mathcal{S}_2$ in infinitely many states. Constructing a corresponding effect E and repeating the argument from above, we would analogously argue that $\mathcal{S}_1$ must contain infinitely many states. This is a contradiction. □

Balls do not have lines in their boundary, but there are many other strictly convex sets - for example, imagine a droplet-like figure. However, Postulate 3 says that there is lots of symmetry in the state space $\mathcal{S}_2$: all pure states (which we now know means all states in the topological boundary) are connected by reversible transformations.

From this, one can prove that

Lemma 3. *The state space $\mathcal{S}_2$ is equivalent to a Euclidean ball (of some dimension $d_2 := K_2 - 1$).*

Recall that we denote the dimension of the set of unnormalized states in $\mathcal{S}_N$ by K_N; therefore, the set of normalized states has dimension $K_N - 1$. We will not prove Lemma 3 here, but only sketch where it comes from. An important notion turns out to be the *maximally mixed state*. On any state space $\mathcal{S}_N$, define μ_N as a mixture over the group of transformations,

$$\mu_N := \int_{\mathcal{G}_N} G\omega \, dG$$

where $\omega \in \mathcal{S}_N$ is any pure state. This is an integral over the invariant measure of the group(). It follows from the connectedness of all pure states (Postulate 3) that μ_N does not depend on the choice of the pure state ω. Moreover, μ_N turns out to be the unique state which is invariant with respect to all reversible transformations,

$$G\mu_N = \mu_N \quad \text{for all } G \in \mathcal{G}_N$$

All states $\omega \in \mathcal{S}_N$ span an affine space of dimension $K_N - 1$. We can now consider μ_N to be the origin of that affine space(remember - an affine space or affine linear space is a vector space that has forgotten its origin); then, reversible transformations $G \in \mathcal{G}_N$ act linearly; they preserve the origin. By group representation theory, there is an inner product on that space which is invariant with respect to all reversible transformations. As a consequence, all pure states have the same norm with respect to this inner product. In the case of a bit, i.e., $N = 2$, this yields a sphere, containing all pure states, with the maximally mixed state μ_N as the center of the ball.

12.5.2 B. The multiplicativity of capacity

So far, we know that of we combine two state space A and B, the joint state space has dimension $K_{AB} = K_A K_B$ - this is due to Postulate 1, local tomography, as discussed earlier in Subsection C. However, we do not yet know whether the same equality is true for capacity N. An important step in the derivation of quantum theory is to prove this. As it turns out, a key insight is that the maximally mixed state must be multiplicative: if we have

two state spaces A and B, then the maximally mixed state on the composite system AB (assuming our postulates) is

$$\mu_{AB} = \mu_A \otimes \mu_B$$

This is easily proved from the fact that μ_{AB} must in particular be invariant with respect to all local reversible transformations, leaving $\mu_A \otimes \mu_B$ as the only possibility.

A further key lemma is the following: **Lemma 4.** *If there are perfectly distinguishable pure states $\omega_1, ..., \omega_n \in \mathcal{S}_N$ that average to the maximally mixed state, i.e.,*

$$\mu_N = \frac{1}{n} \sum_{i=1}^{n} \omega_i$$

then $n = N$.

Proof. Clearly, $N \geq n$, since N is the maximal number of perfectly distinguishable states. On the other hand, let $\varphi_1, ..., \varphi_n$ be a set of perfectly distinguishable pure states on $\mathcal{S}_N$, and $E_1, ..., E_N$ the corresponding effects, i.e., $E_i(\omega_j) = \delta_{ij}$. Since $1 = \sum_{i=1}^{n} E_I(\mu_N)$, there must be some k such that $E_k(\mu_N) \leq 1/N$. By Postulate 3, there is a reversible transformation $G \in \mathcal{G}_N$ with $G\omega_i = \varphi_k$. Thus

$$\begin{aligned} \frac{1}{N} \geq E_k(\mu_N) = E_k \circ G(\mu_N) &= \frac{1}{n} \sum_{i=1}^{n} E_k \circ G(\omega_i) \\ &\geq \frac{1}{n} E_k \circ G(\omega_1) = \frac{1}{n} \end{aligned}$$

Thus, we also have $N \leq n$, proving the claim. □

In quantum theory, the maximally mixed state on an $N-$dimensional Hilbert space is the density matrix

$$\mu_N = \frac{\mathbf{1}_N}{N} = \frac{1}{N} \sum_{i=1}^{N} |\psi_i\rangle \langle\psi_i|$$

if $|\psi_1\rangle, ..., |\psi_N\rangle$ denotes an orthonormal basis of $\mathbb{C}^N$ - that is, if these are pure states that are perfectly distinguishable. This is in agreement with Lemma

4. Moreover, we can prove that an analogous formula holds for every theory satisfying our Postulates 1.-4.:

Lemma 5. *For every N, there are N pure perfectly distinguishable states $\omega_1, ..., \omega_N \in \mathcal{S}_N$ such that*

$$\mu_N = \frac{1}{N} \sum_{i=1}^{N} \omega_i$$

We only sketch the proof here: For $N = 1$, the statement is trivially true, since $\mathcal{S}_1$ contains only a single state. For $N = 2$, we know that $\mathcal{S}_N$ is a Euclidean ball, with the maximally mixed state in the center. Thus, taking ω_1 and ω_2 as two antipodal points on the ball (say, north and south pole), we get

$$\mu_2 = \frac{1}{2}(\omega_1 + \omega_2)$$

and these states are perfectly distinguishable by an analogue of a quantum spin measurement. Now suppose we combine k of these generalized bit state spaces $\mathcal{S}_2$ into a joint state space, $\mathcal{S}_2^{\otimes k} := \mathcal{S}_2 \otimes .... \otimes \mathcal{S}_2$. Then the maximally mixed state on the resulting state space is

$$\mu_{\mathcal{S}_2^{\otimes k}} = \mu_2 \otimes ..... \otimes \mu_2 = \frac{1}{2^k} \sum_{i_1,...,i_k=1,2} \omega_{i_1} \otimes .... \otimes \omega_{i_k}$$

Since in locally tomographic composites, products of pure states are pure, the $\omega_{i_1} \otimes .... \otimes \omega_{i_k}$ are all pure states, and they are perfectly distinguishable by product measurements. Thus, Lemma 4 shows that the capacity of $\mathcal{S}_2^{\otimes k}$ must be $N_{\mathcal{S}_2^{\otimes k}} = 2^k$. This proves Lemma 5 for all N which are a power of two. For all other N, the lemma is proved by using the fact that $\mathcal{S}_N$ is embedded in some $\mathcal{S}_2^{\otimes k}$ for some k large enough due to Postulate 2, and then constructing the maximally mixed state on $\mathcal{S}_N$ in a clever way from that on $\mathcal{S}_2^{\otimes k}$.

Now we can just tensor together the equations

$$\mu_{N_A} = \frac{1}{N_A} \sum_{i=1}^{N_A} \omega_i^A \quad \text{and} \quad \mu_{N_B} = \frac{1}{N_B} \sum_{i=1}^{N_B} \omega_i^B$$

and we obtain

$$\mu_{N_A B} = \mu_{N_A} \otimes \mu_{N_B} = \frac{1}{N_A N_B} \sum_{i=1}^{N_A} \sum_{j=1}^{N_B} \omega_i^A \otimes \omega_j^B$$

and Lemma 4 tells us that capacity must be multiplicative:

Lemma 6. $N_AB = N_AN_B$

Why is this equation so important? As noticed by Hardy, it allows us to draw a surprising conclusion. Every state space $\mathcal{S}N$ has unnormalized dimension K_N. Since $K_AB = K_AK_B$ and $N_AB = N_AN_B$ for all state spaces A and B due to our postulates, we get the following facts:

- The function $N \mapsto K_N$ mapsnaturalnumbersto natural numbers, and is strictly increasing due to Postulate 2.
- It satisfies $K_{N_1,N_2} = K_{N_1}K_{N_2}$, and $K_1 = 1$

These simple conditions imply that there must be an integer $r \geq 1$ such that

$$K_N = N^r \tag{4}$$

Now recall that the dimension of the bit state space (which is a Euclidean ball) is $d_2 := K_2 - 1$. It follows that

$$d_2 \in \{1, 3, 7, 15, 31, ...\}$$

since $K_2 = 2^r$ for some $r \in \mathbb{N}$. Thus, we see in particular that the bit state space is an *odd*-dimensional Euclidean ball. The next subsection will deal with the case $d_2 = 1$; as we will see, this case corresponds to classical probability theory.

C. How to get classical probability theory (CPT)

Suppose that $d_2 = K_2 - 1$; that is, the generalized bit is a one-dimensional ball, as shown in Figure 8. A line segment like this describes a classical bit. What can we say about $N-$level systems for $N \geq 3$ in this case? Equation (4) tells us that the parameter r must be $r = 1$, and thus

$$K_N = N$$

for all N, not only for $N = 2$.

Choose N perfectly distinguishable pure states $\omega_1, ..., \omega_N \in \mathcal{S}_N$ and $E_1, ..., E_N$ the corresponding effects with $E_i(\omega_j) = \delta_{ij}$ as well as $\sum_i E_i = \mathbf{1}$. It is easy

to see that the states must be linearly independent; since $K = N$, they span the full unnormalized state space.

Thus, every state ω can be written $\omega = \sum_{i=1}^{N} \alpha_i \omega_i$ with $\alpha_i \in \mathbb{R}$ and $\sum_i \alpha_i = \mathbf{1}(\omega) = 1$. But then, $E_j(\omega) = \alpha_j \geq 0$, and so this decomposition of ω is in fact a convex decomposition.

In other words, the full state space $\mathcal{S}_N$ is a convex combination of $\omega_1, ..., \omega_N$ - that is, a classical simplex as in Figure 8a)c). These are exactly the state spaces of CPT. Moreover, since for $N = 2$, we can permute the two pure states due to Postulate 3. We can use the subspace postulate, that is, Postulate 2, to conclude that every pair of pure states on $\mathcal{S}_N$ can be interchanged. These transpositions generate the full permutation group, which must thus be the group of reversible transformations $\mathcal{G}_N$. We have therefore proven the following:

> *In the case $d_2 = 1$, we get classical probability theory as the unique solution of Postulates 1.-4.*

D. The curious 7-dimensional case

Let us now consider the remaining cases, i.e. the cases where the dimension of the Euclidean bit ball is $K_2 - 1 \in \{3, 7, 15, 31, ...\}$. The generalized bit carries a group of reversible transformations $\mathcal{G}_2$; by our background assumptions mentioned earlier in Subsection B, this must be a topologically closed matrix group. Closed subgroups of Lie groups are Lie groups; therefore, $\mathcal{G}_2$ is itself a Lie group. Since it maps the unit ball into itself, it must be a subgroup of the orthogonal group.

Denote by $\mathcal{G}_2^0$ the connected component(a connected space is a topological space that cannot be represented as the union of two or more disjoint nonempty open subsets - the maximal connected subsets (ordered by inclusion) of a nonempty topological space are called the connected components of the space) of $\mathcal{G}_2$ containing the identity matrix. We have

$$\mathcal{G}_2^0 \subseteq SO(d_2)$$

We know from Postulate 3 that for every pair of pure states $\omega, \varphi \in \mathcal{S}_2$, there is a reversible transformation $T \in \mathcal{G}_2$ with $T\omega = \varphi$. In other words, $\mathcal{G}_2$ acts transitively(a group G acts transitively on a set S if for any $x, y \in S$, there

is some $g \in G$ such that $gx = y$) on the unit sphere, that is, the surface of the unit ball. It can be shown that this implies that $\mathcal{G}_2^0$ is itself transitive on the unit sphere.

At first sight, it seems that this enforces $\mathcal{G}_2^0$ to be the full special orthogonal group $SO(d_2)$, but this intuition is easily seen to be wrong. For example, the group of $4 \times 4-$matrices

$$\left\{ \begin{pmatrix} re\, U & im\, U \\ -im\, U & re\, U \end{pmatrix} \middle| U \in SU(2) \right\}$$

acts transitively on the surface of the $4-$dimensional unit ball, even though it is a proper subgroup of $SO(4)$. The set of all compact connected Lie matrix groups which act transitively on the unit sphere has been classified. In general, there are many possibilities. Fortunately, however, we have additional information: we know that the bit ball has odd dimension $d_2 := K_2 - 1$. It turns out that there remain only two possibilities:

- If $d_2 \neq 7$, then $\mathcal{G}_2^0 = SO(d_2)$
- If $d_2 = 7$, then $\mathcal{G}_2^0$ is either $SO(7)$ or of the form MG_2M^{-1}, where M is a fixed orthogonal matrix, and G_2 is the fundamental representation of the exceptional Lie group G_2.

In fact, $d_2 = 7$ appears in our list of possible dimensions of the bit ball, because $7 = 2^3 - 1$. In our endeavor to derive quantum theory from Postulates 1.-4., we will have to show that all the cases $d_2 \in \{7, 15, 31, ...\}$ violate at least one postulate. Thus, we see that the case $d_2 = 7$ has to be (and is) treated separately.

The appearance of $d_2 = 7$ as a special case seems like an almost unbelievable coincidence. Is there some deeper significance to this case? Might there be some interesting unknown theory waiting to be discovered which has $7-$dimensional balls as bits and the exceptional Lie group G_2 as the analogue of local unitaries? We do not know.

12.5.3 Subspace structure and 3-dimensionality

Having discussed the case of classical probability theory with bit ball dimension $d_2 = 1$, the remaining cases are

$$d_2 \in \{3, 7, 15, 31, ...\}$$

We will now show that all dimensions $d_2 \geq 7$ are incompatible with the postulates, leaving only the case $d_2 = 3$ - that is, the Bloch ball of quantum theory. For the rest of this section, we ignore the special case $d_2 = 7$ with $\mathcal{G}_2^0 = MG_2M^{-1}$ and G_2 the exceptional Lie group; it can be ruled out by an analogous argument.

In the following, we will parametrize the single bit state space as

$$\mathcal{S}_2 = \left\{ \begin{pmatrix} 1 \\ \hat{\omega} \end{pmatrix} \,\middle|\, \hat{\omega} \in \mathbb{R}^{d_2}, \|\hat{\omega}\| \leq 1 \right\}$$

The maximally mixed state becomes $\mu = (1, 0)^T$. Let $n := (1, 0, ..., 0)^T$, then we have two pure states $\omega_1 := (1, n)^T$ and $\omega_2 := (1, -n)^T$, corresponding to the north and south pole of the ball. These states are pure, and they are perfectly distinguished by the measurement consisting of the two effects (for $\omega \in \mathcal{S}_2$)

$$E_1(\omega) := (1 + \langle \hat{\omega}, n \rangle)/2$$
$$E_2(\omega) := (1 - \langle \hat{\omega}, n \rangle)/2$$

We know that if we combine two bits into a joint state space, we obtain a state space of capacity four:

$$\mathcal{S}_4 = \mathcal{S}_2 \otimes \mathcal{S}_2$$

Thus, the product states $\omega_i \otimes \omega_j$ with $i, j = 1, 2$ represent four perfectly distinguishable states in $\mathcal{S}_4$, and the corresponding product effects $E_i \otimes E_j$ constitute a complete measurement. Recall, however, that the joint state space that we sloppily denoted $\mathcal{S}_2 \otimes \mathcal{S}_2$ is not fully known so far - all we know is that the surrounding linear space is the tensor product of the local spaces. At this stage, we do not yet have a complete description of the set of all global states $\mathcal{S}_4$.

Using the subspace postulate twice, i.e. Postulate 2, we obtain that the set of states ω with $(E_1 \otimes E_1 + E_2 \otimes E_2)(\omega) = 1$ is again equivalent to a single bit. This turns out to be a surprisingly restrictive requirement that we are now going to exploit. Denote this set of states by F (it is a face of the state space $\mathcal{S}_4$), then

$$F = \{\omega \in \mathcal{S}_4 \,|\, (E_1 \otimes E_1 + E_2 \otimes E_2)(\omega) = 1\} \simeq \mathcal{S}2$$

In the following, we will label the two bits by indices A and B for convenience. The group $\mathcal{G}_2^0 = SO(d_2)$ contains a subgroup $\mathcal{G}_2^s$ which leaves the axis containing north and south pole invariant, i.e.

$$\mathcal{G}_2^s := \{G \in \mathcal{G}_2 \,|\, G\omega_1 = \omega_1 \text{ and } G\omega_2 = \omega_2\} \simeq SO(d_2 - 1)$$

If $R \in SO(d_2 - 1)$, then its action as an element of $\mathcal{G}_2^s$ is

$$\left(1, \omega^{(1)}, ..., \omega^{(d_2)}\right)^T \mapsto \left(1, \omega^{(1)}, R\left(\omega^{(2)}, ..., \omega^{(d_2)}\right)\right)^T$$

Suppose we apply one transformation of this kind on each part of a bipartite state ω locally; that is, a transformation $G_A \otimes G_B$ with $G_A, G_B \in \mathcal{G}_2^s$. Then we have $(E_1 \otimes E_1 + E_2 \otimes E_2)(\omega) = 1$ if and only if $(E_1 \otimes E_1 + E_2 \otimes E_2)(G_A \otimes G_B)(\omega) = 1$. Thus, this transformation leaves the face F invariant:

$$(G_A \otimes G_B)F = F$$

We know that the dimension of the linear span of F is $d_2 + 1$, since it is equivalent to $\mathcal{S}_2$. We will now explore in more detail how the transformations $G_A \otimes G_B$ act on the face F. In particular, we are interested in the structure of invariant subspaces.

First, consider a single bit. Its unnormalized states are carried by a real vector space $A = \mathbb{R}^{d_2+1}$ that we can decompose in the following way:

$$A = \mathbb{R} \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \oplus \mathbb{R} \cdot \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \oplus A'$$

where A' denotes the set of all vectors with first two components zero.Since $\mu = (1, 0, ..., 0)^T$ and $G\mu = \mu$, as well as $\omega_1 = (1, 1, 0, ..., 0)^T$ and $G\omega_1 = \omega_1$ for all $G \in \mathcal{G}_2^s$, these three subspaces are all invariant.

Consequently, the vector space which carries two bits, $AB \equiv A \otimes B$, contains the subspace $A' \otimes B'$ which is invariant with respect to all transformations $G_A \otimes G_B$ for $G_A, G_B \in \mathcal{G}_2^s$. This defines an action of $SO(d_2 - 1) \times SO(d_2 - 1)$ on the subspace $A' \otimes B'$.

With a bit of work, one can show that the face F contains at least one state

ω which has non-zero overlap with $A' \otimes B'$. Denote the projection of that vector onto this subspace by $\omega_{A'\otimes B'}$. We know that every $(G_A \otimes G_B)(\omega)$ is a valid state in the face F, and its component in the aforementioned subspace is $(G_A \otimes G_B)(\omega_{A'\otimes B'})$. Now imagine we apply all the local transformations $G_A \otimes G_B$ to the vector $\omega_{A'\otimes B'}$, and we are interested in the orbit - that is, in the set of all vectors that we can generate this way.

If $d_2 \geq 4$, then the group $SO(d_2?1)$ has a nice property in terms of group representation theory: It is irreducible. That is, its action on $\mathbb{C}^{d_2-1}$ does not leave any non-trivial subspaces invariant. This allows us to draw an important conclusion: it implies that the product group $SO(d_2-1) \times SO(d_2-1)$ is also irreducible. But then, the orbit $(G_A \otimes G_B)(\omega_{A'\otimes B'})$ must span the full space $A' \otimes B'$, which has dimension $(d_2-1)^2$ - this is a very large orbit. In fact, it is too large for the subspace postulate: above, we have concluded from Postulate 2 that the span of the face F (which is preserved by those local transformations) must have dimension d_2+1, which is less than $(d_2-1)^2$ if $d_2 > 3$. Thus, we obtain a contradiction: if the bit ball has dimension $d_2 \in \{7, 15, 31, ...\}$, it is impossible to combine two bits into a joint state space which satisfies all our postulates.

As it turns out, this is not true if $d_2 = 3$: the group $SO(d_2-1) = SO(2)$ leaves the span of $(1, i)^T$ invariant; that is, $SO(2)$ is reducible. Thus, this case is not ruled out by the reasoning above. In group-theoretic terms, this reducibility is related to the fact that $SO(2)$ is Abelian. In other words, *the fact that rotations commute in* $3-1$ *dimensions can be seen as a possible reason of the fact that the Bloch ball is* $3-$*dimensional.*

Lemma 7. *The dimension of the bit ball must be* $d_2 = 3$.

We have thus uncovered a group-theoretic explanation why the smallest non-trivial quantum systems have three mutually incompatible, independent components and not more. Due to Postulate 4, we can find all possible measurements on this state space: all effects (that is, linear functionals) which yield probabilities in the interval $[0, 1]$ correspond to outcome probabilities of possible measurements. It is easy to see that these effects are in one-to-one correspondence with the quantum measurements (POVMs) on a single qubit.

Furthermore, we know that the group of reversible transformations contains

$SO(3)$, the rotations of the Bloch ball, which correspond to the unitary transformations on a qubit. At this point, however, we do not yet know whether $\mathcal{G}_2 = SO(3)$ or $\mathcal{G}_2 == O(3)$.

12.5.4 F. Quantum theory on N-level systems for $N \geq 3$

In the previous section, we have derived quantum theory for single bits. It remains to show that our postulates also predict quantum theory for all $N-$level systems with $N \geq 3$. As before, we only sketch the main proof ideas.

For a single bit in state $(1, \hat{\omega})^T$, we can obtain the usual representation as a density matrix by applying a linear map $L : \mathbb{R}^4 \to \mathbb{C}_{sa}^{2\times 2}$, where the latter symbol denotes the real vector space of self-adjoint complex $2 \times 2-$matrices. This map L is defined by linear extension of

$$L(\omega) := (\mathbf{1} + \hat{\omega} \cdot \vec{\sigma})/2$$

where $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ denotes the Pauli matrices. The representation that we obtain (applying L in a suitable way to effects and transformations as well) is equivalent in the sense of Subsection D to the Bloch ball representation.

If we have the state space $\mathcal{S}_4 = \mathcal{S}_2 \otimes \mathcal{S}_2$ of two bits, we can use the map $L \otimes L$ to represent states $\omega \in \mathcal{S}_4$ by self-adjoint $4 \times 4-$matrices $L \otimes L(\omega)$. Recall that we have constructed a face F of $\mathcal{S}_4$ in the previous subsection. Analyzing F in a bit more detail, one can show that it contains a family of pure states ω_u, where $u \in [0, \pi)$, which are mapped by $L \otimes L$ onto

$$L \otimes L(\omega_u) = |\psi_u\rangle \langle\psi_u|$$

where

$$|\psi_u\rangle = \cos\frac{u}{2} |0\rangle \langle 0| + \sin\frac{u}{2} |1\rangle \langle 1|$$

for some orthonormal basis $\{|0\rangle, |1\rangle\}$. This is an entangled quantum state with Schmidt coefficients $\cos(u/2)$ and $\sin(u/2)$. Choosing u appropriately, they can attain any value between 0 and 1. Thus, by applying local unitaries (which corresponds to the $SO(3)-$rotations of the local balls), we can generate all pure quantum states.

Denoting $\mathcal{S}_4' := L \otimes L(\mathcal{S}_4)$, we have proven the following:

Lemma 8. *$\mathcal{S}'_4$ contains all pure $2-$qubit quantum states as pure states.*

The next step is somewhat tricky: we have to show that there are no further (non-quantum) states in $\mathcal{S}'_4$. The idea is to show that all quantum effects are allowed effects on $\mathcal{S}'_4$. Then, if there were additional non-quantum states in $\mathcal{S}'_4$, some of these effects would give negative probabilities, which is impossible.

We know that the product effects are allowed on $\mathcal{S}_4$. Applying the transformation $L \otimes L$, some of the corresponding effects in $\mathcal{S}'_4$ are the maps

$$\rho \mapsto Tr(P_1 \otimes P_2 \rho)$$

where P_1 and P_2 are one-dimensional projectors. If $T \in \mathcal{G}_4$ is any reversible transformation on $\mathcal{S}_4$, denote the corresponding transformation on $\mathcal{S}'_4$ by $T' \in \mathcal{G}'_4$. It maps states ρ to $T'(\rho)$. Suppose we could show the equation

$$Tr(P_1 \otimes P_2 T'(\rho)) = Tr((T')^{-1}(P_1 \otimes P_2)\rho) \tag{5}$$

Then we would be done: due to Postulate 3, transformations $T' \in \mathcal{G}'_4$ can map every pure product state to every other pure state, in particular, to every pure entangled quantum state. This way, $(T')^{-1}$ in (5) would generate all entangled quantum effects from the product effect $P_1 \otimes P_2$. This is exactly what we want.

When would eq. (5) hold? Up to a factor $1/4$, the map $L^{\otimes 2}$ is an isometry (a distance-preserving map): for all $x, y \in \mathbb{R}^4 \otimes \mathbb{R}^4$, we have

$$Tr\left(L^{\otimes 2}(x) L^{\otimes 2}(y)\right) = \frac{1}{4}\langle x, y \rangle$$

Thus, translating eq. (5) from $\mathcal{S}'_4$ back to $\mathcal{S}_4$, the corresponding equation is

$$\langle E_1 \otimes E_2, T\omega \rangle = \langle T^{-1}(E_1 \otimes E_2), \omega \rangle$$

This is satisfied if $T^T = T^{-1}$ for all $T \in \mathcal{G}_4$. In fact, we have

Lemma 9. *All reversible transformations $T \in \mathcal{G}_4$ act as orthogonal matrices on $\mathbb{R}^4 \otimes \mathbb{R}^4$*

The proof of this lemma is non-trivial and somewhat surprising: it uses

Schur's Lemma from group representation theory, together with the fact that there exist certain kinds of SWAP and CNOT operations on two bits. These operations are constructed by using Postulate 2.

Due to Lemma 9, all the above argumentation becomes solid: eq. (5) is valid, and we get

Lemma 10. *$\mathcal{S}_4'$ is the set of $2-$qubit quantum states, and the allowed effects are the quantum effects.*

So what about the transformations? First of all, we know that that the transformation group of a single bit must be $SO(3)$ - it cannot be $O(3)$, because local reflections would correspond to partial transposition which generates negative eigenvalues on entangled states. Furthermore, every transformation $T \in \mathcal{G}_4$ is a linear isometry on the set of self-adjoint $4 \times 4-$matrices that maps the set of density matrices into itself.

According to Wigners Theorem, only unitary and anti-unitary maps satisfy this. However, due to Wigners normal form, anti-unitary maps generate reflections in some Bloch ball faces of the state space, which is impossible due to Postulate 2.

So $\mathcal{G}_4$ is a subgroup of the unitary group. Due to Postulate 3, it maps some pure product state to an entangled state. In other words, $\mathcal{G}_4$ contains an entangling unitary, and also all local unitaries. It is a well-known fact from quantum computation that these transformations generate the full unitary group.

We have thus shown

Lemma 11. *The group of reversible transformations $\mathcal{G}_2'$ on two bits corresponds to the unitary conjugations, i.e., the maps $\rho \mapsto U\rho U^\dagger$ with $U \in SU(4)$.*

It is now clear that what we did for two bits can also be done for n bits. Since every $\mathcal{S}_N$ is contained in some $\mathcal{S}_{2^n}$ for n large enough, we can use the subspace postulate to conclude that every state space $\mathcal{S}_N$ is equivalent to the quantum $N-$level state space.

12.6 Conclusions and Outlook

We have shown that the Hilbert space formalism of quantum theory can be reconstructed from four natural, information-theoretic postulates. We hope that this reconstruction - together with other recent axiomatizations - contributes to a better understanding of quantum theory, and sheds some light on some of the mysterious aspects of its formalism, such as the appearance of complex numbers or unitaries.

One of the main motivations for this discussion, as mentioned earlier, was to search for *quantum theory's closest cousins*: dropping one or two of the axioms, and working out the remaining set of theories, should yield interesting alternative probabilistic theories that are conceptually close to quantum theory, but not described by the Hilbert space formalism. These theories make different physical predictions that can be tested experimentally.

What is the status of the search for those theories? Currently, it seems that there are two natural ways to proceed. The first possibility is to drop the subspace postulate (Postulate 2), because it is in a way the strongest and most complicated postulate. This raises the question what other theories (in addition to quantum theory and classical probability theory) have the properties of local tomography and pure-state transitivity, given that all effects are outcomes of allowed measurements?

In the case where the local systems are balls and the transformation groups are assumed to be continuous, quantum theory is still the only solution for two binary systems. In fact, there is currently no known example of a theory which satisfies the remaining three postulates and is not a part of quantum theory. This suggests the conjecture that the results of this discussion remain basically valid if the subspace axiom is dropped.

A second possibility is to drop local tomography, i.e. Postulate 1. Then it seems that indeed further theories appear as solutions, in particular state spaces of Jordan algebras. It is an interesting open problem to work out this idea rigorously, and to classify all state spaces that appear in addition to quantum theory.

13 Theory #2 - Quantum Theory From Five Reasonable Axioms

13.1 Introduction

Quantum theory, in its usual formulation, is very abstract. The basic elements are vectors in a complex Hilbert space. These determine measured probabilities by means of the well known trace formula - a formula which has no obvious origin. It is natural to ask why quantum theory is the way it is. Quantum theory is simply a new type of probability theory. Like classical probability theory it can be applied to a wide range of phenomena. However, the rules of classical probability theory can be determined by pure thought alone without any particular appeal to experiment (though, of course, to develop classical probability theory, we do employ some basic intuitions about the nature of the world). Is the same true of quantum theory? Put another way, could a $19th$ century theorist have developed quantum theory without access to the empirical data that later became available to his $20th$ century descendants? In this paper it will be shown that quantum theory follows from five very reasonable axioms which might well have been posited without any particular access to empirical data. We will not recover any specific form of the Hamiltonian from the axioms since that belongs to particular applications of quantum theory (for example - a set of interacting spins or the motion of a particle in one dimension). Rather we will recover the basic structure of quantum theory along with the most general type of quantum evolution possible. In addition we will only deal with the case where there are a finite or countably infinite number of distinguishable states corresponding to a finite or countably infinite dimensional Hilbert space. We will not deal with continuous dimensional Hilbert spaces.

The basic setting we will consider is one in which we have preparation devices, transformation devices, and measurement devices. Associated with each preparation will be a state defined in the following way:

> **The state** associated with a particular preparation is defined to be (that thing represented by) any mathematical object that can be used to determine the probability associated with the outcomes of any measurement that may be performed on a system prepared by the given preparation.

Hence, a list of all probabilities pertaining to all possible measurements that could be made would certainly represent the state. However, this would most likely over-determine the state. Since most physical theories have some structure, a smaller set of probabilities pertaining to a set of carefully chosen measurements may be sufficient to determine the state. This is the case in classical probability theory and quantum theory. Central to the axioms are two integers K and N which characterize the type of system being considered.

- The *number of degrees of freedom*, K, is defined as the minimum number of probability measurements needed to determine the state, or, more roughly, as the number of real parameters required to specify the state.

- The dimension, N, is defined as the maximum number of states that can be reliably distinguished from one another in a single shot measurement.

We will only consider the case where the number of distinguishable states is finite or countably infinite. As will be shown below, classical probability theory has $K = N$ and quantum probability theory has $K = N^2$ (note we do not assume that states are normalized).

The five axioms for quantum theory (to be stated again, in context, later) are

Axiom 1 *Probabilities.* Relative frequencies (measured by taking the proportion of times a particular outcome is observed) tend to the same value (which we call the probability) for any case where a given measurement is performed on a ensemble of n systems prepared by some given preparation in the limit as n becomes infinite.

Axiom 2 *Simplicity.* K is determined by a function of N (i.e. $K = K(N)$) where $N = 1, 2, ...$ and where, for each given N, K takes the minimum value consistent with the axioms.

Axiom 3 *Subspaces.* A system whose state is constrained to belong to an M dimensional subspace (i.e. have support(subset of the domain of a function where it is non-zero valued) on only M of a set of N possible distinguishable states) behaves like a system of dimension M.

Axiom 4 *Composite systems.* A composite system consisting of subsystems A and B satisfies $N = N_A N_B$ and $K = K_A K_B$

Axiom 5 *Continuity.* There exists a continuous reversible transformation on a system between any two pure states of that system.

The first four axioms are consistent with classical probability theory but the fifth is not (unless the word *continuous* is dropped). If the last axiom is dropped then, because of the simplicity axiom, we obtain classical probability theory (with $K = N$) instead of quantum theory (with $K = N^2$). It is very striking that we have here a set of axioms for quantum theory which have the property that if a single word is removed - namely the word *continuous* in Axiom 5 - then we obtain classical probability theory instead.

The basic idea of the proof is simple. First we show how the state can be described by a real vector, $\mathbf{p}$, whose entries are probabilities and that the probability associated with an arbitrary measurement is given by a linear function, $\mathbf{r}\cdot\mathbf{p}$, of this vector (the vector $\mathbf{r}$ is associated with the measurement). Then we show that we must have $K = N^r$ where r is a positive integer and that it follows from the simplicity axiom that $r = 2$ (the $r = 1$ case being ruled out by Axiom 5). We consider the $N = 2, K = 4$ case and recover quantum theory for a two dimensional Hilbert space. The subspace axiom is then used to construct quantum theory for general N. We also obtain the most general evolution of the state consistent with the axioms and show that the state of a composite system can be represented by a positive operator on the tensor product of the Hilbert spaces of the subsystems. Finally, we show obtain the rules for updating the state after a measurement.

This discussion is organized in the following way. First we will describe the type of situation we wish to consider (in which we have preparation devices, state transforming devices, and measurement de- vices). Then we will describe classical probability theory and quantum theory. In particular it will be shown how quantum theory can be put in a form similar to classical probability theory. After that we will forget both classical and quantum probability theory and show how they can be obtained from the axioms.

Others have set up axiomatic formulations of quantum theory. Much of this work is in the quantum logic tradition. The advantage of the present discussion is that there are a small number of simple axioms, these axioms

can easily be motivated without any particular appeal to experiment, and the mathematical methods required to obtain quantum theory from these axioms are very straightforward (essentially just linear algebra).

13.2 Setting the Scene

We will begin by describing the type of experimental situation we wish to consider (see Figure 10).

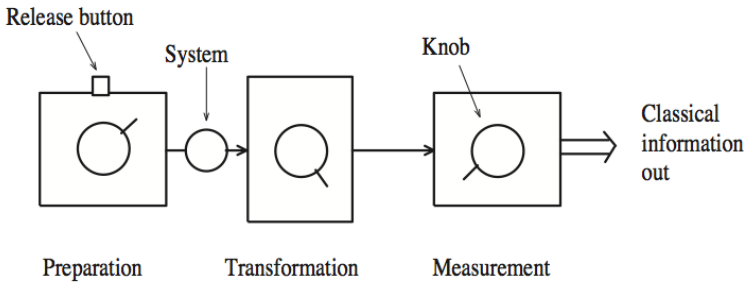

Figure 10: The situation considered consists of a preparation device with a knob for varying the state of the system produced and a release button for releasing the system, a transformation device for transforming the state (and a knob to vary this transformation), and a measuring apparatus for measuring the state (with a knob to vary what is measured) which outputs a classical number.

An experimentalist has three types of device. One is a preparation device. We can think of it as preparing physical systems in some state. It has on it a number of knobs which can be varied to change the state prepared. The system is released by pressing a button. The system passes through the second device. This device can transform the state of the system. This device has knobs on it which can be adjusted to effect different transformations (we might think of these as controlling fields which effect the system). We can allow the system to pass through a number of devices of this type. Unless otherwise stated, we will assume the transformation devices are set to al- low the system through unchanged. Finally, we have a measurement apparatus. This also has knobs on it which can be adjusted to determine what measurement is being made. This device outputs a classical number. If no system is incident on the device (i.e., because the button on the preparation device was

not pressed) then it outputs a 0 (corresponding to a null outcome). If there is actually a physical system incident (i.e., when the release button is pressed and the transforming device has not absorbed the system) then the device outputs a number l where $l = 1$ *to* L (we will call these non-null outcomes). The number of possible classical outputs, L, may depend on what is being measured (the settings of the knobs).

The fact that we allow null events means that we will not impose the constraint that states are normalized. This turns out to be a useful convention. It may appear that requiring the existence of null events is an additional assumption. However, it follows from the subspace axiom that we can arrange to have a null outcome. We can associate the non-null outcomes with a certain subspace and the null outcome with the complement subspace. Then we can restrict ourselves to preparing only mixtures of states which are in the non-null subspace (when the button is pressed) with states which are in the null subspace (when the button is not pressed).

The situation described here is quite generic. Although we have described the set up as if the system were moving along one dimension, in fact the system could equally well be regarded as remaining stationary whilst being subjected to transformations and measurements. Furthermore, the system need not be localized but could be in several locations. The transformations could be due to controlling fields or simply due to the natural evolution of the system. Any physical experiment, quantum, classical or other, can be viewed as an experiment of the type described here.

13.3 Probability measurements

We will consider only measurements of probability since all other measurements (such as expectation values) can be calculated from measurements of probability. When, in this discussion, we refer to a measurement or a probability measurement we mean, specifically, a measurement of the probability that the outcome belongs to some subset of the non-null outcomes with a given setting of the knob on the measurement apparatus. For example, we could measure the probability that the outcome is $l = 1$ or $l = 2$ with some given setting.

To perform a measurement we need a large number of identically prepared

systems.

A measurement returns a single real number (the probability) between 0 and 1. It is possible to perform many measurements at once. For example, we could simultaneously measure [the probability the outcome is $l = 1$] and [the probability the outcome is $l = 1$ or $l = 2$] with a given knob setting.

13.4 Classical Probability Theory

A classical system will have available to it a number, N, of distinguishable states. For example, we could consider a ball that can be in one of N boxes. We will call these distinguishable states the basis states. Associated with each basis state will be the probability, p_n, of finding the system in that state if we make a measurement. We can write

$$\mathbf{p} = \begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ \vdots \\ p_N \end{pmatrix} \tag{1}$$

This vector can be regarded as describing the state of the system. It can be determined by measuring N probabilities and so $K = N$. Note that we do not assume that the state is normalized (otherwise we would have $K = N?1$).

The state $\mathbf{p}$ will belong to a convex set S. Since the set is convex it will have a subset of extremal states. These are the states

$$\mathbf{p}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \mathbf{p}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \mathbf{p}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad \text{etc.} \tag{2}$$

and the state

$$\mathbf{p}_{null} = \mathbf{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{3}$$

The state $\mathbf{0}$ is the null state (when the system is not present). We define the set of pure states to consist of all extremal states except the null state. Hence, the states in (2) are the pure states. They correspond to the system definitely being in one of the N distinguishable states. A general state can be written as a convex sum of the pure states and the null state and this gives us the exact form of the set S. This is always a polytope (a shape having flat surfaces and a finite number of vertices).

We will now consider measurements. Consider a measurement of the probability that the system is in the basis state n. Associated with this probability measurement is the vector $\mathbf{r}_n$ having a 1 in position n and 0s elsewhere. At least for these cases the measured probability is given by

$$p_{meas} = \mathbf{r} \cdot \mathbf{p} \tag{4}$$

However, we can consider more general types of probability measurement and this formula will still hold. There are two ways in which we can construct more general types of measurement:

1. We can perform a measurement in which we decide with probability λ to measure $\mathbf{r}_A$ and with probability $1-\lambda$ to measure $\mathbf{r}_B$. Then we will obtain a new measurement vector $\lambda\mathbf{r}_A + (1-\lambda)\mathbf{r}_B$.

2. We can add the results of two compatible probability measurements and therefore add the corresponding measurement vectors.

An example of the second is the probability measurement that the state is basis state 1 or basis state 2 is given by the measurement vector $\mathbf{r}_1 + \mathbf{r}_2$. From linearity, it is clear that the formula (4) holds for such more general measurements.

There must exist a measurement in which we simply check to see that the system is present (i.e. not in the null state). We denote this by $\mathbf{r}^I$. Clearly

$$\mathbf{r}^I = \sum_n \mathbf{r}_n = \begin{pmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \tag{5}$$

Hence $0 \leq \mathbf{r}^I \cdot \mathbf{p} \leq 1$ with normalized states saturating the upper bound.

With a given setting of the knob on the measurement device there will be a certain number of distinct non-null outcomes labeled $l = 1$ *to* L. Associated with each outcome will be a measurement vector $\mathbf{r}_l$. Since, for normalized states, one non-null outcome must happen we have

$$\sum_{l=1}^{L} \mathbf{r}_l = \mathbf{r}^I \tag{6}$$

This equation imposes a constraint on any measurement vector. Let allowed measurement vectors $\mathbf{r}$ belong to the set R. This set is clearly convex (by virtue of 1. above). To fully determine R first consider the set R^+ consisting of all vectors which can be written as a sum of the basis measurement vectors, $\mathbf{r}_n$, each multiplied by a positive number. For such vectors $\mathbf{r} \cdot \mathbf{p}$ is necessarily greater than 0 but may also be greater than 1. Thus, elements of R^+ may be too long to belong to R. We need a way of picking out those elements of R^+ that also belong to R. If we can perform the probability measurement $\mathbf{r}$ then, by (6) we can also perform the probability measurement $\bar{\mathbf{r}} \equiv \mathbf{r}^I - \mathbf{r}$. Hence

$$\text{if and only if } \ \mathbf{r}, \bar{\mathbf{r}} \in R^+ \quad \text{and} \quad \mathbf{r} + \bar{\mathbf{r}} = \mathbf{r}^I \quad \text{then} \quad \mathbf{r}, \bar{\mathbf{r}} \in R \tag{7}$$

This works since it implies that $\mathbf{r} \cdot \mathbf{p} \leq 1$ for all $\mathbf{p}$ so that $\mathbf{r}$ is not too long.

Note that the Axioms 1 to 4 are satisfied but Axiom 5 is not since there are a finite number of pure states. It is easy to show that reversible transformations take pure states to pure states (see later). Hence a continuous reversible transformation will take a pure state along a continuous path through the pure states which is impossible here since there are only a finite number of pure states.

13.5 Quantum Theory

Quantum theory can be summarized by the following rules

> **States:** The state is represented by a positive (and therefore Hermitian) operator $\hat{\rho}$ satisfying $0 \leq tr(\hat{\rho}) \leq 1$.

Measurements: Probability measurements are represented by a positive operator $\hat{A}$. If $\hat{A}_l$ corresponds to outcome l where $l = 1$ *to* L then

$$\sum_{l=1}^{L} \hat{A}_l = \hat{I} \tag{8}$$

Probability formula: The probability obtained when the measurement $\hat{A}$ is made on the state $\hat{\rho}$ is

$$p_{meas} = tr(\hat{A}\hat{\rho}) \tag{9}$$

Evolution: The most general evolution is given by the superoperator \$

$$\hat{\rho} = \$(\hat{\rho}) \tag{10}$$

where \$

- Does not increase the trace.
- Is linear.
- Is completely positive.

This way of presenting quantum theory is rather condensed. The following notes should provide some clarifications

1. It is, again, more convenient not to impose normalization. This, in any case, more accurately models what happens in real experiments when the quantum system is often missing for some portion of the ensemble.

2. The most general type of measurement in quantum theory is a POVM (positive operator valued measure). The operator $\hat{A}$ is an element of such a measure.

3. Two classes of superoperator are of particular interest. If \$ is reversible (i.e. the inverse $\$^{-1}$ both exists and belongs to the allowed set of transformations) then it will take pure states to pure states and corresponds to unitary evolution. The von Neumann projection postulate takes the state $\hat{\rho}$ to the state $\hat{P}\hat{\rho}\hat{P}$ when the outcome corresponds to the projection operator $\hat{P}$. This is a special case of a superoperator evolution in which the trace of $\hat{\rho}$ decreases.

4. It has been shown by Krauss that one need only impose the three listed constraints on \$ to fully constrain the possible types of quantum evolution. This includes unitary evolution and von Neumann projection as already stated, and it also includes the evolution of an open system (interacting with an environment). It is sometimes stated that the superoperator should preserve the trace. However, this is an unnecessary constraint which makes it impossible to use the superoperator formalism to describe von Neumann projection.

5. The constraint that \$ is completely positive imposes not only that \$ preserves the positivity of $\hat{\rho}$ but also that of $\$_A \otimes \hat{I}_B$ acting on any element of a tensor product space also preserves positivity for any dimension of B.

This is the usual formulation. However, quantum theory can be recast in a form more similar to classical probability theory. To do this we note first that the space of Hermitian operators which act on a N dimensional complex Hilbert space can be spanned by N^2 linearly independent projection operators $\hat{P}_k$ for $k = 1$ to $K = N^2$. This is clear since a general Hermitian operator can be represented as a matrix. This matrix has N real numbers along the diagonal and $\frac{1}{2}N(N-1)$ complex numbers above the diagonal making a total of N^2 real numbers. An example of N^2 such projection operators will be given later.

Define

$$\hat{\mathbf{P}} = \begin{pmatrix} \hat{P}_1 \\ \hat{P}_2 \\ \vdots \\ \hat{P}_K \end{pmatrix} \tag{11}$$

Any Hermitian matrix can be written as a sum of these projection operators times real numbers, i.e. in the form $\mathbf{a} \cdot \hat{\mathbf{P}}$ where $\mathbf{a}$ is a real vector ($\mathbf{a}$ is unique since the operators $\hat{P}_k$ are linearly independent). Now define

$$\mathbf{p}_S = tr(\hat{\mathbf{P}}\hat{\rho}) \tag{12}$$

Here the subscript S denotes *state*. The $k\,th$ component of this vector is equal to the probability obtained when $\hat{P}_k$ is measured on $\hat{rho}$. The vector $\mathbf{p}_S$ contains the same information as the state $\hat{rho}$ and can therefore be

regarded as an alternative way of representing the state. Note that $K = N^2$ since it takes N^2 probability measurements to determine $\mathbf{p}_S$ or, equivalently $r\hat{ho}$. We define $\mathbf{r}_M$ through

$$\hat{A} = \mathbf{r}_M \cdot \hat{\mathbf{P}} \tag{13}$$

The subscript M denotes *measurement*. The vector $\mathbf{r}_M$ is another way of representing the measurement $\hat{A}$. If we substitute (13) into the trace formula (9) we obtain

$$p_{meas} = \mathbf{r}_M \cdot \mathbf{p}_S \tag{14}$$

We can also define

$$\mathbf{p}_M = tr(\hat{A}\hat{\mathbf{P}}) \tag{15}$$

and $\mathbf{r}_S$ by

$$\hat{\rho} = \hat{\mathbf{P}} \cdot \mathbf{r}_S \tag{16}$$

Using the trace formula (9) we obtain

$$p_{meas} = \mathbf{p}_M \cdot \mathbf{r}_S = \mathbf{r}_M^T D \mathbf{r}_S \tag{17}$$

where T denotes transpose and D is the $K \times K$ matrix with real elements given by

$$D_{ij} = tr(\hat{P}_i \hat{P}_j) \tag{18}$$

or we can write $D = tr(\hat{\mathbf{P}}\hat{\mathbf{P}}^T)$. From (14,17) we obtain

$$\mathbf{p}_S = D\mathbf{r}_S \tag{19}$$

and

$$\mathbf{p}_M = D^T \mathbf{r}_M \tag{20}$$

We also note that

$$D = D^T \tag{21}$$

though this would not be the case had we chosen different spanning sets of projection operators for the state operators and measurement operators. The inverse D^{-1} must exist (since the projection operators are linearly independent). Hence, we can also write

$$p_{meas} = \mathbf{p}_M^T D^{-1} \mathbf{p}_S \tag{22}$$

The state can be represented by an $\mathbf{r}-$type vector or a $\mathbf{p}-$type vector as can the measurement. Hence the subscripts M and S were introduced. We will

sometimes drop these subscripts when it is clear from the context whether the vector is a state or measurement vector. We will stick to the convention of having measurement vectors on the left and state vectors on the right as in the above formulae. We define $\mathbf{r}^I$ by

$$\hat{I} = \mathbf{r}^I \cdot \hat{\mathbf{P}} \tag{23}$$

This measurement gives the probability of a non-null event. Clearly we must have $0 \leq \mathbf{r}^I \cdot \mathbf{p} \leq 1$ with normalized states saturating the upper bound. We can also define the measurement which tells us whether the state is in a given subspace. Let $\hat{I}_W$ be the projector into an M dimensional subspace W. Then the corresponding $\mathbf{r}$ vector is defined by $\hat{I}_W = \mathbf{r}^{I_W} \cdot \hat{\mathbf{P}}$. We will say that a state $\mathbf{p}$ is in the subspace W if

$$\mathbf{r}^{I_W} \cdot \mathbf{p} = \mathbf{r}^I \cdot \mathbf{p} \tag{24}$$

so it only has support in W. A system in which the state is always constrained to an $M-$dimensional subspace will behave as an $M-$dimensional system in accordance with Axiom 3.

The transformation $\hat{\rho} \to \$(\hat{\rho})$ of $\hat{\rho}$ corresponds to the following transformation for the state vector $\mathbf{p}$:

$$\begin{aligned}
\mathbf{p} &= tr(\hat{\mathbf{P}}\hat{\rho}) \\
&\to tr(\hat{\mathbf{P}}\$(\hat{\rho})) \\
&= tr(\hat{\mathbf{P}}\$(\hat{\mathbf{P}}^T D^{-1}\mathbf{p})) \\
&= Z\mathbf{p}
\end{aligned}$$

where equations (16,19) were used in the third line and Z is a $K \times K$ real matrix given by

$$Z = tr(\hat{\mathbf{P}}\$(\hat{\mathbf{P}})^T)D^{-1} \tag{25}$$

(we have used the linearity property of \$). Hence, we see that a linear transformation in $\hat{\rho}$ corresponds to a linear transformation in $\mathbf{p}$. We will say that $Z \in \Gamma$.

Quantum theory can now be summarized by the following rules

States: The state is given by a real vector $\mathbf{p} \in S$ with N^2 components.

Measurements: A measurement is represented by a real vector $\mathbf{r} \in R$ with N^2 components.

Probability formula: The measured probability if measurement $\mathbf{r}$ is performed on state $\mathbf{p}$ is

$$p_{meas} = \mathbf{r} \cdot \mathbf{p}$$

Evolution: The evolution of the state is given by $\mathbf{p} \rightarrow Z\mathbf{p}$ where $Z \in \Gamma$ is a real matrix.

The exact nature of the sets S, R and Γ can be deduced from the equations relating these real vectors and matrices to their counterparts in the usual quantum formulation. We will show that these sets can also be deduced from the axioms. It has been noticed by various other authors that the state can be represented by the probabilities used to determine it.

There are various ways of choosing a set of N^2 linearly independent projections operators $\hat{P}_k$ which span the space of Hermitaan operators. Perhaps the simplest way is the following. Consider an $N-$dimensional complex Hilbert space with an orthonormal basis set $|n\rangle$ for $n = 1$ *to* N. We can define N projectors

$$|n\rangle \langle n| \tag{26}$$

Each of these belong to one-dimensional subspaces formed from the orthonormal basis set. Define

$$|mn\rangle_x = \frac{1}{\sqrt{2}}(|m\rangle + |n\rangle)$$

$$|mn\rangle_y = \frac{1}{\sqrt{2}}(|m\rangle + i\,|n\rangle)$$

for $m < n$. Each of these vectors has support on a two-dimensional subspace formed from the orthonormal basis set. There are $\frac{1}{2}N(N-1)$ such two-dimensional subspaces. Hence we can define $N(N-1)$ further projection operators

$$|mn\rangle_x \langle mn| \quad \text{and} \quad |mn\rangle_y \langle mn| \tag{27}$$

This makes a total of N^2 projectors. It is clear that these projectors are linearly independent. Each projector corresponds to one degree of freedom. There is one degree of freedom associated with each one-dimensional subspace n, and a further two degrees of freedom associated with each two-dimensional subspace mn. It is possible, though not actually the case in

quantum theory, that there are further degrees of freedom associated with each three-dimensional subspace and so on. Indeed, in general, we can write

$$K = Nx_1 + \frac{1}{2!}N(N-1)x_2 + \frac{1}{3!}N(N-1)(N-2)x_3 + ... \quad (28)$$

We will call the vector $\mathbf{x} = (x_1, x_2, ...)$ the *signature* of a particular probability theory. Classical probability theory has signature $\mathbf{x}_{Classical} = (1, 0, 0, ...)$ and quantum theory has signature $\mathbf{x}_{Quantum} = (1, 2, 0, 0, ...)$. We will show that these signatures are respectively picked out by Axioms 1 to 4 and Axioms 1 to 5. The signatures $\mathbf{x}_{Reals} = (1, 1, 0, 0, ...)$ of real Hilbert space quantum theory and $\mathbf{x}_{Quaternions} = (1, 4, 0, 0, ...)$ of quaternionic quantum theory are ruled out.

If we have a composite system consisting of subsystem A spanned by $\hat{P}_i^A$ $(i = 1\ to\ K_A)$ and B spanned by $\hat{P}_j^B$ $(j = 1\ to\ K_B)$ then $\hat{P}_i^A \otimes \hat{P}_j^B$ arelinearlyinde- pendent and span the composite system. Hence, for the composite system we have $K = K_A K_B$. We also have $N = N_A N_B$. Therefore Axiom 4 is satisfied.

The set S is convex. It contains the null state 0 (if the system is never present) which is an extremal state. Pure states are defined as extremal states other than the null state (since they are extremal they cannot be written as a convex sum of other states as we expect of pure states). We know that a pure state can be represented by a normalized vector $|\psi\rangle$. This is specified by $2N - 2$ real parameters (N complex numbers minus overall phase and minus normalization). On the other hand, the full set of normalized states is specified by $N^2 - 1$ real numbers. The surface of the set of normalized states must therefore be $N^2 - 2$ dimensional. This means that, in general, the pure states are of lower dimension than the the surface of the convex set of normalized states. The only exception to this is the case $N = 2$ when the surface of the convex set is $2-$dimensional and the pure states are specified by two real parameters. This case is illustrated by the Bloch sphere. Points on the surface of the Bloch sphere correspond to pure states.

In fact the $N = 2$ case will play a particularly important role later so we will now develop it a little further. There will be four projection operators

spanning the space of Hermitian operators which we can choose to be

$$\hat{P}_1 = |1\rangle \langle 1| \tag{29}$$

$$\hat{P}_2 = |2\rangle \langle 2| \tag{30}$$

$$\hat{P}_3 = (\alpha |1\rangle + \beta |2\rangle)(\alpha^* \langle 1| + \beta^* \langle 2|) \tag{31}$$

$$\hat{P}_4 = (\gamma |1\rangle + \delta |2\rangle)(\gamma^* \langle 1| + \delta^* \langle 2|) \tag{32}$$

where $|\alpha|^2 + |\beta|^2 = 1$ and $|\gamma|^2 + |\delta|^2 = 1$. We have chosen the second pair of projections to be more general than those defined in (27) above since we will need to consider this more general case later. We can calculate D using (18)

$$D = \begin{pmatrix} 1 & 0 & 1-|\beta|^2 & 1-|\delta|^2 \\ 0 & 1 & |\beta|^2 & |\delta|^2 \\ 1-|\beta|^2 & |\beta|^2 & 1 & |\alpha\gamma^* + \beta\delta^*|^2 \\ 1-|\delta|^2 & |\delta|^2 & |\alpha\gamma^* + \beta\delta^*|^2 & 1 \end{pmatrix} \tag{33}$$

We can write this as

$$D = \begin{pmatrix} 1 & 0 & 1-a & 1-b \\ 0 & 1 & a & b \\ 1-a & a & 1 & c \\ 1-b & b & c & 1 \end{pmatrix} \tag{34}$$

where a and b are real with $\beta = \sqrt{a} exp(i\phi_3)$, $\delta = \sqrt{b} exp(i\phi_4)$, and $c = |\alpha\gamma^* + \beta\delta^*|^2$. We can choose α and γ to be real (since the phase is included in the definition of β and δ). It then follows that

$$\begin{aligned} c = 1 - a - b + 2ab \\ + 2\cos(\phi_4 - \phi_3)\sqrt{ab(1-a)(1-b)} \end{aligned} \tag{35}$$

Hence, by varying the complex phase associated with α,β, γ and δ we find that

$$c_- < c < c_+ \tag{36}$$

where

$$c_\pm \equiv 1 - a - b + 2ab \pm 2\sqrt{ab(1-a)(1-b)} \tag{37}$$

This constraint is equivalent to the condition $Det(D) > 0$. Now, if we are given a particular D matrix of the form (34) then we can go backwards to

the usual quantum formalism though we must make some arbitrary choices for the phases. First we use (35) to calculate $\cos(\phi_4 - \phi_3)$. We can assume that $0 \leq \phi_4 - \phi_3 \leq \pi$ (this corresponds to assigning i to one of the roots of $sqrt{-}1$). Then we can assume that $\phi_3 = 0$. This fixes ϕ_4. An example of this second 1 choice is when we assign the state $\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ (this has real coefficients) to spin along the x direction for a spin half particle. This is arbitrary since we have rotational symmetry about the z axis. Having calculated ϕ_3 and ϕ_4 from the elements of D we can now calculate α,β, γ and δ and hence we can obtain $\hat{\mathbf{P}}$. We can then calculate $\hat{\rho}$, $\hat{A}$ and \$ from $\mathbf{p}$, $\mathbf{r}$, and Z and use the trace formula. The arbitrary choices for phases do not change any empirical predictions.

13.6 Basic Ideas and the Axioms

We will now forget quantum theory and classical probability theory and rederive them from the axioms. In this section we will introduce the basic ideas and the axioms in context.

13.6.1 Probabilities

As mentioned earlier, we will consider only measurements of probability since all other measurements can be reduced to probability measurements. We first need to ensure that it makes sense to talk of probabilities. To have a probability we need two things. First we need a way of preparing systems (in Figure 10 this is accomplished by the first two boxes) and second, we need a way of measuring the systems (the third box in Figure 10). Then, we measure the number of cases, n_+, a particular outcome is observed when a given measurement is performed on an ensemble of n systems each prepared by a given preparation. We define

$$prob_+ = \lim_{n\to\infty} \frac{n_+}{n} \tag{38}$$

In order for any theory of probabilities to make sense $prob_+$ must take the same value for any such infinite ensemble of systems prepared by a given preparation. Hence, we assume

Axiom 1 Probabilities. *Relative frequencies (measured by taking the proportion of times a particular outcome is observed) tend to the same value (which*

we call the probability) for any case where a given measurement is performed on an ensemble of n systems prepared by some given preparation in the limit as n becomes infinite.

With this axiom we can begin to build a probability theory.

Some additional comments are appropriate here. There are various different interpretations of probability: as frequencies, as propensities, the Bayesian approach, etc. As stated, Axiom 1 favors the frequency approach. However, it it equally possible to cast this axiom in keeping with the other approaches. In this discussion we are principally interested in deriving the structure of quantum theory rather than solving the interpretational problems with probability theory and so we will not try to be sophisticated with regard to this matter. Nevertheless, these are important questions which deserve further attention.

13.6.2 The state

We can introduce the notion that the system is described by a state. Each preparation will have a state associated with it. We define the state to be (that thing represented by) any mathematical object which can be used to determine the probability for any measurement that could possibly be performed on the system when prepared by the associated preparation. It is possible to associate a state with a preparation because Axiom 1 states that these probabilities depend on the preparation and not on the particular ensemble being used. It follows from this definition of a state that one way of representing the state is by a list of all probabilities for all measurements that could possibly be performed. However, this would almost certainly be an over-complete specification of the state since most physical theories have some structure which relates different measured quantities. We expect that we will be able to consider a subset of all possible measurements to determine the state. Hence, to determine the state we need to make a number of different measurements on different ensembles of identically prepared systems. A certain minimum number of appropriately chosen measurements will be both necessary and sufficient to determine the state. Let this number be K. Thus, for each setting, $k = 1$ *to* K, we will measure a probability p_k with an appropriate setting of the knob on the measurement apparatus. These K

probabilities can be represented by a column vector $\mathbf{p}$ where

$$\mathbf{p} = \begin{pmatrix} p_1 \\ p_2 \\ p_3 \\ \vdots \\ p_K \end{pmatrix} \tag{39}$$

Now, this vector contains just sufficient information to determine the state and the state must contain just sufficient information to determine this vector (otherwise it could not be used to predict probabilities for measurements). In other words, the state and this vector are interchangeable and hence we can use $\mathbf{p}$ as a way of representing the state of the system. We will call K the number of degrees of freedom associated with the physical system. We will not assume that the physical system is always present. Hence, one of the K degrees of freedom can be associated with normalization and therefore $K \geq 1$.

13.6.3 Fiducial measurements

We will call the probability measurements labeled by $k = 1$ *to* K used in determining the state the *fiducial measurements*. There is no reason to suppose that this set is unique. It is possible that some other fiducial set could also be used to determine the state.

13.6.4 Measured probabilities

Any probability that can be measured (not just the fiducial ones) will be determined by some function f of the state $\mathbf{p}$. Hence,

$$p_{meas} = f(\mathbf{p}) \tag{40}$$

For different measurements the function will, of course, be different. By definition, measured probabilities are between 0 and 1.

$$0 \leq p_{meas} \leq 1$$

This must be true since probabilities are measured by taking the proportion of cases in which a particular event happens in an ensemble.

13.6.5 Mixtures

Assume that the preparation device is in the hands of Alice. She can decide randomly to prepare a state $\mathbf{p}_A$ with probability λ or a state $\mathbf{p}_B$ with probability $1-\lambda$. Assume that she records this choice but does not tell the person, Bob say, performing the measurement. Let the state corresponding to this preparation be $\mathbf{p}_C$. Then the probability Bob measures will be the convex combination of the two cases, namely

$$f(\mathbf{p}_C) = \lambda f(\mathbf{p}_A) + (1-\lambda) f(\mathbf{p}_B) \tag{41}$$

This is clear since Alice could subsequently reveal which state she had prepared for each event in the ensemble providing two sub-ensembles. Bob could then check his data was consistent for each subensemble. By Axiom 1, the probability measured for each subensemble must be the same as that which would have been measured for any similarly prepared ensemble and hence (41) follows.

13.6.6 Linearity

Equation (41) can be applied to the fiducial measurements themselves. This gives

$$\mathbf{p}_C = \lambda \mathbf{p}_A + (1-\lambda)\mathbf{p}_B \tag{42}$$

This is clearly true since it is true by (41) for each component.

Equations (41,42) give

$$f(\lambda \mathbf{p}_A + (1-\lambda)\mathbf{p}_B) = \lambda f(\mathbf{p}_A) + (1-\lambda) f(\mathbf{p}_B) \tag{43}$$

This strongly suggests that the function $f(\cdot)$ is linear. This is indeed the case and a proof is given in Appendix 1. Hence, we can write

$$p_{meas} = \mathbf{r} \cdot \mathbf{p} \tag{44}$$

The vector $\mathbf{r}$ is associated with the measurement. The $k\,th$ fiducial measurement is the measurement which picks out the $k\,th$ component of $\mathbf{p}$. Hence, the fiducial measurement vectors are

$$\mathbf{r}^1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \mathbf{r}^2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \mathbf{r}^3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad \text{etc.} \tag{45}$$

13.6.7 Transformations

We have discussed the role of the preparation device and the measurement apparatus. Now we will discuss the state transforming device (the middle box in Figure 10). If some system with state $\mathbf{p}$ is incident on this device its state will be transformed to some new state $\mathbf{g}(\mathbf{p})$. It follows from Eqn (41) that this transformation must be linear. This is clear since we can apply the proof in the Appendix 1 to each component of $\mathbf{g}$. Hence, we can write the effect of the transformation device as

$$\mathbf{p} \to Z\mathbf{p} \tag{46}$$

where Z is a $K \times K$ real matrix describing the effect of the transformation.

13.6.8 Allowed states, measurements, and transformations

We now have states represented by $\mathbf{p}$, measurements represented by $\mathbf{r}$, and transformations represented by Z. These will each belong to some set of physically allowed states, measurements and transformations. Let these sets of allowed elements be S,R and Γ. Thus,

$$\mathbf{p} \in S \tag{47}$$

$$\mathbf{r} \in R \tag{48}$$

$$Z \in \Gamma \tag{49}$$

We will use the axioms to determine the nature of these sets. It turns out (for relatively obvious reasons) that each of these sets is convex.

13.6.9 Special states

If the release button on Figure 10 is never pressed then all the fiducial measurements will yield 0. Hence, the null state $\mathbf{p}_{null} = \mathbf{0}$ can be prepared and therefore $\mathbf{0} \in S$.

It follows from (42) that the set S is convex. It is also bounded since the entries of $\mathbf{p}$ are bounded by 0 and 1. Hence, S will have an extremal set $S_{extremal}$ (these are the vectors in S which cannot be written as a convex sum of other vectors in S). We have $\mathbf{0} \in S_{extremal}$ since the entries in the vectors $\mathbf{p}$ cannot be negative. We define the set of pure states S_{pure} to be the set

of all extremal states except **0**. Pure states are clearly special in some way. They represent states which cannot be interpreted as a mixture. A driving intuition in this work is the idea that pure states represent definite states of the system.

13.6.10 The identity measurement

The probability of a non-null outcome is given by summing up all the non-null outcomes with a given setting of the knob on the measurement apparatus (see Figure 10). The non-null outcomes are labeled by $l = 1$ *to* L.

$$p_{non-null} = \sum_{l=1}^{L} \mathbf{r}_l \cdot \mathbf{p} = \mathbf{r}^I \cdot \mathbf{p} \tag{50}$$

where $\mathbf{r}_l$ is the measurement vector corresponding to outcome l and

$$\mathbf{r}^I = \sum_{l=1}^{L} \mathbf{r}_l \tag{51}$$

is called the identity measurement.

13.6.11 Normalized and unnormalized states

If the release button is never pressed we prepare the state **0**. If the release button is always pressed (i.e., for every event in the ensemble) then we will say $\mathbf{p} \in S_{norm}$ or, in words, that the state is normalized. Unnormalized states are of the form $\lambda\mathbf{p} + (1 - \lambda)\mathbf{0}$ where $0 \leq \lambda < 1$. Unnormalized states are therefore mixtures and hence, all pure states are normalized, that is

$$S_{pure} \subset S_{norm}$$

We define the normalization coefficient of a state $\mathbf{p}$ to be

$$\mu = \mathbf{r}^I \cdot \mathbf{p} \tag{52}$$

In the case where $\mathbf{p} \in S_{norm}$ we have $\mu = 1$.

The normalization coefficient is equal to the proportion of cases in which the release button is pressed. It is therefore a property of the state and cannot

depend on the knob setting on the measurement apparatus. We can see that $\mathbf{r}^I$ must be unique since if there was another such vector satisfying (52) then this would reduce the number of parameters required to specify the state contradicting our starting point that a state is specified by K real numbers. Hence $\mathbf{r}^I$ is independent of the measurement apparatus knob setting.

13.6.12 Basis states

Any physical system can be in various states. We expect there to exist some sets of normalized states which are distinguishable from one another in a single shot measurement (were this not the case then we could store fixed records of information in such physical systems). For such a set we will have a setting of the knob on the measurement apparatus such that each state in the set always gives rise to a particular outcome or set of outcomes which is disjoint from the outcomes associated with the other states. It is possible that there are some non-null outcomes of the measurement that are not activated by any of these states. Any such outcomes can be added to the set of outcomes associated with, say, the first member of the set without effecting the property that the states can be distinguished. Hence, if these states are $\mathbf{p}_n$ and the measurements that distinguish them are $\mathbf{r}_n$ then we have

$$\mathbf{r}_m \cdot \mathbf{p}_n = \delta_{mn} \quad \text{where} \quad \sum_n \mathbf{r}_n = \mathbf{r}^I \tag{53}$$

The measurement vectors $\mathbf{r}_n$ must add to $\mathbf{r}^I$ since they cover all possible outcomes. There may be many such sets having different numbers of elements. Let N be the maximum number of states in any such set of distinguishable states. We will call N the *dimension*. We will call the states $\mathbf{p}_n$ in any such set *basis states* and we will call the corresponding measurements $\mathbf{r}_n$ *basis measurements*. Each type of physical system will be characterized by N and K. A note on notation: In general we will adopt the convention that the subscript n ($n = 1$ *to* N) labels basis states and measurements and the superscript k ($k = 1$ *to* K) labels fiducial measurements and (to be introduced later) fiducial states. Also, when we need to work with a particular choice of fiducial measurements (or states) we will take the first n of them to be equal to a basis set. Thus, $\mathbf{r}^k = \mathbf{r}_k$ for $k = 1$ *to* N.

If a particular basis state is impure then we can always replace it with a pure state. To prove this we note that if the basis state is impure we can write it

as a convex sum of pure states. If the basis state is replaced by any of the states in this convex sum this must also satisfy the basis property. Hence, we can always choose our basis sets to consist only of pure states and we will assume that this has been done in what follows.

Note that $N = 1$ is the smallest value N can take since we can always choose any normalized state as $\mathbf{p}_1$ and $\mathbf{r}_1 = \mathbf{r}^I$.

13.6.13 Simplicity

There will be many different systems having different K and N. We will assume that, nevertheless, there is a certain constancy in nature such that K is a function of N. The second axiom is

Axiom 2 Simplicity. *K is determined by a function of N (i.e., $K = K(N)$) where $N = 1, 2, ...$ and where, for any given N, K takes the minimum value consistent with the axioms.*

The assumption that $N = 1, 2, ...$ means that we assume nature provides systems of all different dimensions. The motivation for taking the smallest value of K for each given N is that this way we end up with the simplest theory consistent with these natural axioms. It will be shown that the axioms imply $K = N^r$ where r is an integer. Axiom 2 then dictates that we should take the smallest value of r consistent with the axioms (namely $r = 2$). However, it would be interesting either to show that higher values of r are inconsistent with the axioms even without this constraint that K should take the minimum value, or to explicitly construct theories having higher values of r and investigate their properties.

13.6.14 Subspaces

Consider a basis measurement set $\mathbf{r}_n$. The states in a basis are labeled by the integers $n = 1$ *to* N. Consider a subset W of these integers. We define

$$\mathbf{r}^{I_W} = \sum_{n \in W} \mathbf{r}_n \tag{54}$$

Corresponding to the subset W is a subspace which we will also call W defined by

$$\mathbf{p} \in W \quad \text{iff} \quad \mathbf{r}^{I_W} \cdot \mathbf{p} = \mathbf{r}^I \cdot \mathbf{p} \tag{55}$$

Thus, **p** belongs to the subspace if it has support only in the subspace. The dimension of the subspace W is equal to the number of members of the set W. The complement subset $\overline{W}$ consists of the the integers $n = 1$ *to* N not in W. Corresponding to the subset $\overline{W}$ is the subspace $\overline{W}$ which we will call the complement subspace to W. Note that this is a slightly unusual usage of the terminology *subspace* and *dimension* which we employ here because of the analogous concepts in quantum theory. The third axiom concerns such subspaces.

Axiom 3 Subspaces. *A system whose state is contrained to belong to an M dimensional subspace behaves like a system of dimension M.*

This axiom is motivated by the intuition that any collection of distinguishable states should be on an equal footing with any other collection of the same number distinguishable states. In logical terms, we can think of distinguishable states as corresponding to a propositions. We expect a probability theory pertaining to M propositions to be independent of whether these propositions are a subset or some larger set or not.

One application of the subspace axiom which we will use is the following: If a system is prepared in a state which is constrained to a certain subspace W having dimension N_W and a measurement is made which may not pertain to this subspace then this measurement must be equivalent (so far as measured probabilities on states in W are concerned) to some measurement in the set of allowed measurements for a system actually having dimension N_W.

13.6.15 Composite systems

It often happens that a preparation device ejects its system in such a way that it can be regarded as being made up of two subsystems. For example, it may emit one system to the left and one to the right (see Figure 11). We will label these subsystems A and B. We assume

Axiom 4 Composite systems. *A composite system consisting of two subsystems A and B having dimension N_A and N_B respectively, and number of degrees of freedom K_A and K_B respectively, has dimension $N = N_A N_B$ and number of degrees of freedom $K = K_A K_B$.*

We expect that $N = N_A N_B$ for the following reasons. If subsystems A and

B have N_A and N_B distinguishable states, then there must certainly exist $N_A N_B$ distinguishable states for the whole system. It is possible that there exist more than this but we assume that this is not so. We will show that the relationship $K = K_A K_B$ follows from the following two assumptions

- If a subsystem is in a pure state then any joint probabilities between that subsystem and any other subsystem will factorize. This is a reasonable assumption given the intuition (mentioned earlier) that pure states represent definite states for a system and therefore should not be correlated with anything else.

- The number of degrees of freedom associated with the full class of states for the composite system is not greater than the number of degrees of freedom associated with the separable states. This is reasonable since we do not expect there to be more entanglement than necessary.

Note that although these two assumptions motivate the relationship $K = K_A K_B$ we do not actually need to make them part of our axiom set (rather they follow from the five axioms). To show that these assumptions imply $K = K_A K_B$ consider performing the $i\,th$ fiducial measurement on system A and the $j\,th$ fiducial measurement on system B and measuring the joint probability p_{ij} that both measurements have a positive outcome. These joint probabilities can be arranged in a matrix $\tilde{p}_{AB}$ having entries p_{ij}. It must be possible to choose K_A linearly independent pure states labeled $\mathbf{p}_A^{k_A}$ ($k_A = 1\ to\ K_A$) for subsystems A, and similarly for subsystem B. With the first assumption above we can write $\tilde{p}_{AB}^{k_A k_B} = \mathbf{p}_A^{k_A}(\mathbf{p}_B^{k_B})^T$ when system A is prepared in the pure state $\mathbf{p}_A^{k_A}$ and system B is prepared in the pure state $\mathbf{p}_B^{k_B}$. It is easily shown that it follows from the fact that the states for the subsystems are linearly independent that the $K_A K_B$ matrices $\tilde{p}_{AB}^{k_A k_B}$ are linearly independent. Hence, the vectors describing the correspond- ing joint states are linearly independent. The convex hull(the convex hull or convex envelope for a set X of points in the Euclidean plane or Euclidean space is the minimal convex set containing X) of the end points of $K_A K_B$ linearly independent vectors and the null vector is $K_A K_B$ dimensional. We cannot prepare any additional *product* states which are linearly independent of these since the subsystems are spanned by the set of fiducial states considered. Therefore, to describe convex combinations of the separable states requires $K_A K_B$ degrees of freedom and hence, given the second assumption above, $K = K_A K_B$.

It should be emphasized that it is not required by the axioms that the state of a composite system should be in the convex hull of the product states. Indeed, it is the fact that there can exist vectors not of this form that leads to quantum entanglement.

13.7 The continuity axiom

Now we introduce the axiom which will give us quantum theory rather than classical probability theory. Given the intuition that pure states represent definite states of a system we expect to be able to transform the state of a system from any pure state to any other pure state. It should be possible to do this in a way that does not extract information about the state and so we expect this can be done by a reversible transformation. By reversible we mean that the effect of the transforming device (the middle box in Figure 10) can be reversed irrespective of the input state and hence that $Z^{?1}$ exists and is in Γ. Furthermore, we expect any such transformation to be continuous since there are generally no discontinuities in physics. These considerations motivate the next axiom.

Axiom 5 Continuity. *There exists a continuous reversible transformation on a system between any two pure states of the system.*

By a continuous transformation we mean that one which can be made up from many small transformations only infinitesimally different from the identity. The set of reversible transformations will form a compact Lie group (compact because its action leaves the components of $\mathbf{p}$ bounded by 0 and 1 and hence the elements of the transformation matrices Z must be bounded).

If a reversible transformation is applied to a pure state it must necessarily output a pure state. To prove this assume the contrary. Thus, assume $Z\mathbf{p} = \lambda\mathbf{p}_A + (1-\lambda)\mathbf{p}_B$ where $\mathbf{p}$ is pure, Z^{-1} exists and is in Γ, $0 < \lambda < 1$, and the states $\mathbf{p}_{AB}$ are distinct. It follows that $\mathbf{p} = \lambda Z^{-1}\mathbf{p}_A + (1-\lambda)Z^{-1}\mathbf{p}_B$ which is a mixture. Hence we establish proof by contradiction.

The infinitesimal transformations which make up a reversible transformation must themselves be reversible. Since reversible transformations always transform pure states to pure states it follows from this axiom that we can transform any pure state to any other pure state along a continuous trajec-

tory through the pure states. We can see immediately that classical systems of finite dimension N will run into problems with the continuity part of this axiom since there are only N pure states for such systems and hence there cannot exist a continuous trajectory through the pure states. Consider, for example, transforming a classical bit from the state 0 to the state 1. Any continuous transformation would have to go through an infinite number of other pure states (not part of the subspace associated with our system). Indeed, this is clear given any physical implementation of a classical bit. For example, a ball in one of two boxes must move along a continuous path from one box (representing a 0) to the other box (representing a 1). Deutsch has pointed out that for this reason, the classical description is necessarily approximate in such situations whereas the quantum description in the analogous situation is not approximate. We will use this axiom to rule out various theories which do not correspond to quantum theory (including classical probability theory).

Axiom 5 can be further motivated by thinking about computers. A classical computer will only employ a finite number of distinguishable states (usually referred to as the memory of the computer - for example 10 GB). For this reason it is normally said that the computer operates with finite resources. However, if we demand that these bits are described classically and that transformations are continuous then we have to invoke the existence of a continuous infinity of distinguishable states not in the subspace being considered. Hence, the resources used by a classically described computer performing a finite calculation must be infinite. It would seem extravagant of nature to employ infinite resources in performing a finite calculation.

13.8 The Main Proofs

In this section we will derive quantum theory and, as an aside, classical probability theory by dropping Axiom 5. The following proofs lead to quantum theory

1. Proof that $K = N^r$ where $r = 1, 2, ...$

2. Proof that a valid choice of fiducial measurements is where we choose the first N to be some basis set of measurements and then we choose 2 additional measurements in each of the $\frac{1}{2}N(N-1)$ two-dimensional subspaces (making a total of N^2).

3. Proof that the state can be represented by an $\mathbf{r}-$type vector.

4. Proof that pure states must satisfy an equation $\mathbf{r}^T D\mathbf{r} = 1$ where $D = D^T$.

5. Proof that $K = N$ is ruled out by Axiom 5 (though leads to classical probability theory if we drop Axiom 5) and hence that $K = N^2$ by the Axiom 2.

6. We show that the $N = 2$ case corresponds to the Bloch sphere and hence we obtain quantum theory for the $N = 2$ case.

7. We obtain the trace formula and the conditions imposed by quantum theory on $\hat{\rho}$ and $\hat{A}$ for general N.

8. We show that the most general evolution consistent with the axioms is that of quantum theory and that the tensor product structure is appropriate for describing composite systems.

9. We show that the most general evolution of the state after measurement is that of quantum theory (including, but not restricted to, von Neumann projection).

13.8.1 Proof that $K = N^r$

In this section we will see that $K = N^r$ where r is a positive integer. It will be shown in Section 13.8.5 that $K = N$ (i.e., when $r = 1$) is ruled out by Axiom 5. Now, as shown in Section 13.8.5, quantum theory is consistent with the Axioms and has $K = N^2$. Hence, by the simplicity axiom (Axiom 2), we must have $K = N^2$ (i.e., $r = 2$).

It is quite easy to show that $K = N^r$. First note that it follows from the subspace axiom (Axiom 3) that $K(N)$ must be a strictly increasing function of N. To see this consider first an N dimensional system. This will have $K(N)$ degrees of freedom. Now consider an $N+1$ dimensional system. If the state is constrained to belong to an N dimensional subspace W then it will, by Axiom 3, have $K(N)$ degrees of freedom. If it is constrained to belong to the complement 1 dimensional subspace then, by Axiom 3, it will have at least one degree of freedom (since K is always greater than or equal to 1). However, the state could also be a mixture of a state constrained to $W$with

some weight λ and a state constrained to the complement one dimensional subspace with weight $1-\lambda$. This class of states must have at least $K(N)+1$ degrees of freedom (since λ can be varied). Hence, $K(N+1) \geq K(N)+1$. By Axiom 4 the function $K(N)$ satisfies

$$K(N_A N_B) = K(N_A)K(N_B) \tag{56}$$

Such functions are known in number theory as *completely multiplicative*. It is shown in Appendix 2 that all strictly increasing completely multiplicative functions are of the form $K = N^\alpha$. Since K must be an integer it follows that the power, α, must be a positive integer. Hence

$$K(N) = N^r \quad \text{where} \quad r = 1, 2, 3, ... \tag{57}$$

The signatures (see earlier discussion) associated with $K = N$ and $K = N^2$ are $\mathbf{x} = (1, 0, 0, ...)$ and $\mathbf{x} = (1, 2, 0, 0, ...)$ respectively. It is interesting to consider some of those cases that have been ruled out. Real Hilbert spaces have $\mathbf{x} = (1, 1, 0, ...)$ (consider counting the parameters in the density matrix). In the real Hilbert space composite systems have more degrees of freedom than the product of the number of degrees of freedom associated with the subsystems (which implies that there are necessarily some degrees of freedom that can only be measured by performing a joint measurement on both subsystems). Quaternionic Hilbert spaces have $\mathbf{x} = (1, 4, 0, ...)$. This case is ruled out because composite systems would have to have less degrees of freedom than the product of the number of degrees of freedom associated with the subsystems. This shows that quaternionic systems violate the principle that joint probabilities factorize when one (or both) of the subsystems is in a pure state. We have also ruled out $K = N^3$ (which has signature $\mathbf{x} = (1, 6, 6, 0, 0, ...)$) and higher r values. However, these cases have only been ruled out by virtue of the fact that Axiom 2 requires we take the simplest case. It would be interesting to attempt to construct such higher power theories or prove that such constructions are ruled out by the axioms even without assuming that K takes the minimum value for each given N.

The fact that $x_1 = 1$ (or, equivalently, $K(1) = 1$) is interesting. It implies that if we have a set of N distinguishable basis states they must necessarily be pure. After the one degree of freedom associated with normalization has been counted for a one dimensional subspace there can be no extra degrees of freedom. If the basis state was mixed then it could be written as a convex

sum of pure states that also satisfy the basis property. Hence, any convex sum would would satisfy the basis property and hence there would be an extra degree of freedom.

13.8.2 Choosing the fiducial measurements

We have either $K = N$ or $K = N^2$. If $K = N$ then a suitable choice of fiducial measurements is a set of basis measurements. For the case $K = N^2$ any set of N^2 fiducial measurements that correspond to linearly independent vectors will suffice as a fiducial set. However, one particular choice will turn out to be especially useful. This choice is motivated by the fact that the signature is $\mathbf{x} = (1, 2, 0, 0, ...)$. This suggests that we can choose the first N fiducial measurements to correspond to a particular basis set of measurements $\mathbf{r}_n$ (we will call this the fiducial basis set) and that for each of the $\frac{1}{2}N(N-1)$ two-dimensional fiducial subspaces W_{mn} (i.e., two-dimensional subspaces associated with the $m\,th$ and $n\,th$ basis measurements) we can chose a further two fiducial measurements which we can label $\mathbf{r}_{mnx}$ and $\mathbf{r}_{mny}$ (we are simply using x and y to label these measurements). This makes a total of N^2 vectors. It is shown in Appendix 3.4 that we can, indeed, choose N^2 linearly independent measurements $(\mathbf{r}_n, \mathbf{r}_{mnx}, \mathbf{r}_{mny})$ in this way and, furthermore, that they have the property

$$\mathbf{r}_{mnx} \cdot \mathbf{p} = 0 \quad \text{if} \quad \mathbf{p} \in \overline{W}_{mn} \tag{58}$$

where $\overline{W}_{mn}$ is the complement subspace to W_{mn}. This is a useful property since it implies that the fiducial measurements in the W_{mn} subspace really do only apply to that subspace.

13.8.3 Representing the state by r

Till now the state has been represented by $\mathbf{p}$ and a measurement by $\mathbf{r}$. However, by introducing fiducial states, we can also represent the measurement by a $\mathbf{p}-$type vector (a list of the probabilities obtained for this measurement with each of the fiducial states) and, correspondingly, we can describe the state by an $\mathbf{r}-$type vector. For the moment we will label vectors pertaining to the state of the system with subscript S and vectors pertaining to the measurement with subscript M (we will drop these subscripts later since it will be clear from the context which meaning is intended).

Fiducial states

We choose K linearly independent states, $\mathbf{p}_S^k$ for $k = 1\ to\ K$, and call them fiducial states (it must be possible to choose K linearly independent states since otherwise we would not need K fiducial measurements to determine the state). Consider a given measurement $\mathbf{r}_M$. We can write

$$p_M^k = \mathbf{r}_M \cdot \mathbf{p}_S^k \tag{59}$$

Now, we can take the number p_M^k to be the $k\,th$ component of a vector. This vector, $\mathbf{p}_M$, is related to $\mathbf{r}_M$ by a linear transformation. Indeed, from the above equation we can write

$$\mathbf{p}_M = C\mathbf{r}_M \tag{60}$$

where C is a $K \times K$ matrix with l, k entry equal to the $l\,th$ component of $\mathbf{p}_S^k$. Since the vectors $\mathbf{p}_S^k$ are linearly independent, the matrix C is invertible and so $\mathbf{r}_M$ can be determined from $\mathbf{p}_M$. This means that $\mathbf{p}_M$ is an alternative way of specifying the measurement. Since p_{meas} is linear in $\mathbf{r}_M$, which is linearly related to $\mathbf{p}_M$ it must also be linear in $\mathbf{p}_M$. Hence we can write

$$p_{meas} = \mathbf{p}_M \cdot \mathbf{r}_S \tag{61}$$

where the vector $\mathbf{r}_S$ is an alternative way of describing the state of the system. The $k\,th$ fiducial state can be represented by an $\mathbf{r}-$type vector, $\mathbf{r}_S^k$, and is equal to that vector which picks out the $k\,th$ component of $\mathbf{p}_M$. Hence, the fiducial states are

$$\mathbf{r}_S^1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \mathbf{r}_S^2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \mathbf{r}_S^3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \quad \text{etc.} \tag{62}$$

A useful bilinear form for p_{meas}

The expression for p_{meas} is linear in both $\mathbf{r}_M^k$ and $\mathbf{r}_S^k$. In other words, it is a bilinear form and can be written

$$p_{meas} = \mathbf{r}_M^T D \mathbf{r}_S \tag{63}$$

where superscript T denotes transpose, and D is a $K \times K$ real matrix (equal, in fact, to C^T).The k, l element of D is equal to the probability measured when the $k\,th$ fiducial measurement is performed on the $l\,th$ fiducial state (since, in the fiducial cases, the $\mathbf{r}$ vectors have one 1 and otherwise 0s as components). Hence,

$$D_{lk} = (\mathbf{r}_M^l)^T D \mathbf{r}_S^k \tag{64}$$

D is invertible since the fiducial set of states are linearly independent.

Vectors associated with states and measurements

There are two ways of describing the state: Either with a $\mathbf{p}-$type vector or with an $\mathbf{pr}-$type vector. From (44, 63) we see that the relation between these two types of description is given by

$$\mathbf{p}_S = D\mathbf{r}_S \tag{65}$$

Similarly, there are two ways of describing the measurement: Either with an $\mathbf{r}-$type vector or with a $\mathbf{p}-$type vector. From (61,63) we see that the relation between the two ways of describing a measurement is

$$\mathbf{p}_M = D^T \mathbf{r}_M \tag{66}$$

(Hence, C in equation (60) is equal to D^T).

Note that it follows from these equations that the set of states/measurements $\mathbf{r}_{S,M}$ is bounded since $\mathbf{p}_{S,M}$ is bounded (the entries are probabilities) and D is invertible (and hence its inverse has finite entries).

13.8.4 Pure states satisfy $\mathbf{r}^T D \mathbf{r} = 1$

Let us say that a measurement *identifies* a state if, when that measurement is performed on that state, we obtain probability one. Denote the basis measurement vectors by $\mathbf{r}_{Mn}$ and the basis states (which have been chosen to be pure states) by $\mathbf{p}_{Sn}$ where $n = 1\ to\ N$. These satisfy $\mathbf{r}_{Mn} \cdot \mathbf{p}_{Sn} = \delta_{mn}$. Hence $\mathbf{r}_{Mn}$ identifies $\mathbf{p}_{Sn}$.

Consider an apparatus set up to measure $\mathbf{r}_{M1}$. We could place a transformation device, T, in front of this which performs a reversible transformation. We would normally say that that T transforms the state and then $\mathbf{r}_{M1}$ is

measured. However, we could equally well regard the transformation device T as part of the measurement apparatus. In this case some other measurement $\mathbf{r}$ is being performed. We will say that any measurement which can be regarded as a measurement of $\mathbf{r}_{M1}$ preceded by a reversible transformation device is a pure measurement. It is shown in Appendix 3.7 that all the basis measurement vectors $\mathbf{r}_{Mn}$ are pure measurements and, indeed, that the set of fiducial measurements of Section 13.8.2 can all be chosen to be pure.

A pure measurement will identify that pure state which is obtained by acting on $\mathbf{p}_{S1}$ with the inverse of T. Every pure state can be reached in this way (by Axiom 5) and hence, corresponding to each pure state there exists a pure measurement. We show in Appendix 3.5 that the map between the vector representing a pure state and the vector representing the pure measurement it is identified by is linear and invertible.

We will now see that not only is this map linear but also that, by appropriate choice of the fiducial measurements and fiducial states, we can make it equal to the identity. A convex structure embedded in a $K-$dimensional space must have at least $K+1$ extremal points (for example, a triangle has three extremal points, a tetrahedron has four, etc.). In the case of the set S, one of these extremal points will be $\mathbf{0}$ leaving at least K remaining extremal points which will correspond to pure states (recall that pure states are extremal states other than $\mathbf{0}$). Furthermore, it must be possible to choose a set of K of these pure states to correspond to linearly independent vectors (if this were not possible then the convex hull would be embedded in a lower than K dimensional space). Hence, we can choose all our fiducial states to be pure. Let these fiducial states be $\mathbf{r}_S^k$. We will choose the $k\,th$ fiducial measurement $\mathbf{r}_M^k$ to be that pure measurement which identifies the $k\,th$ fiducial state. These will constitute a linearly independent set since the map from the corresponding linearly independent set of states is invertible.

We have proven (in Appendix 3.5) that, if $\mathbf{r}_M$ identifies $\mathbf{r}_S$, there must exist a map

$$\mathbf{r}_S = H\mathbf{r}_M \tag{67}$$

where H is a $K \times K$ constant matrix. In particular this is true for the fiducial states and fiducial measurements:

$$\mathbf{r}_S^k = H\mathbf{r}_M^k \tag{68}$$

However, the fiducial vectors have the special form given in (45,62), namely zeros everywhere except for the $k\,th$ entry. Hence, the map H is equal to the identity. This is true because we have chosen the fiducial measurements to be those which identify the fiducial states. Since these vectors are related by the identity map we will drop the M and S subscripts in what follows, it being understood that the left most vector corresponds to the measurement apparatus and the right most vector corresponds to the state. *Thus the measurement r identifies the state* $\mathbf{r}$ *(i.e. given by the same vector) if* $\mathbf{r}$ *is pure.* Hence,

$$\mathbf{r}^T D\mathbf{r} = 1 \tag{69}$$

for pure states (and pure measurements). This equa- tion is very useful since will help us to find the pure states. It is shown in Appendix 3.6 that $D = D^T$.

It is shown in Appendix 3.7 that the fiducial measurements $\mathbf{r}_n$, $\mathbf{r}_{mix}$, and $\mathbf{r}_{mny}$ are pure. They will identify a set of pure states represented by the same vectors $\mathbf{r}_n$, $\mathbf{r}_{mix}$, and $\mathbf{r}_{mny}$ which we take to be our fiducial states. The first N fiducial states, $\mathbf{r}_n$, are then just the basis states and it follows from (58) that the remaining basis states, $\mathbf{r}_{mix}$, and $\mathbf{r}_{mny}$ are in the corresponding W_{mn} subspaces.

13.8.5 Ruling out the $K = N$ case

Consider the $K = N$ case. There will be $K = N$ fiducial vectors which we can choose to be equal to the basis vectors. From equation (64) we know that the lk element of D is equal to the measured probability with the $k\,th$ fiducial state and the $l\,th$ fiducial measurement. Since the fiducial vectors correspond to basis vectors this implies that D is equal to the identity. The pure states must satisfy

$$\mathbf{r}^T D\mathbf{r} = 1 \tag{70}$$

We also have $\mathbf{p} = D\mathbf{r}$ (equation (65)). Given that D is equal to the identity in this case we obtain

$$\sum_{k=1}^{N} (p^k)^2 = 1 \tag{71}$$

where p^k is the $k\,the$ component of $\mathbf{p}$. However,

$$0 \leq p^k \leq 1 \tag{72}$$

Normalization implies that

$$\sum_{k=1}^{N} p^k = 1 \tag{73}$$

The solutions of (71), (72), (73) have one p_k equal to 1 and all the others are equal to 0. In other words, the only pure vectors are the basis vectors themselves which corresponds to classical probability theory. This forms a discrete set of vectors and so it is impossible for Axiom 5 (the continuity axiom) to be satisfied. Hence, we rule out such theories. However, if Axiom 5 is dropped then, by Axiom 2, we must take $K = N$. This necessarily corresponds to classical probability theory for the following reasons. We can choose our $K(= N)$ fiducial measurements to be the basis measurements $\mathbf{r}_n$. Then the basis states must be represented by vectors with zero's in all positions except the $n\,th$ position. All states must have normalization coefficient less than or equal to 1. Hence, all states can be written as a convex combination of the basis states and the null state. This means that only the basis states are pure states. Hence, we have classical probability theory.

13.8.6 The Bloch sphere

We are left with $K = N^2$ (since $K = N$ has been ruled out by Axiom 5). Consider the simplest non-trivial case $N = 2$ and $K = 4$. Normalized states are contained in a $K - 1 = 3$ dimensional convex set. The surface of this set is two-dimensional. All pure states correspond to points on this surface. The four fiducial states can all be taken to be pure. They correspond to a linearly independent set. The reversible transformations that can act on the states form a compact Lie Group. The Lie dimension (number of generators) of this group of reversible transformations cannot be equal to one since, if it were, it could not transform between the fiducial states. This is because, under a change of basis, a compact Lie group can be represented by orthogonal matrices. If there is only one Lie generator then it will generate pure states on a circle. But the end points of four linearly independent vectors cannot lie on a circle since this is embedded in a two-dimensional subspace. Hence, the Lie dimension must be equal to two. The pure states are represented by points on the two-dimensional surface. Furthermore, since the Lie dimension of the group of reversible transformations is equal to two it must be possible to transform a given pure state to any point on this surface. If we can find

this surface then we know the pure states for $N = 2$. This surface must be convex since all points on it are extremal. We will use this property to show that the surface is ellipsoidal and that, with appropriate choice of fiducial states, it can be made spherical (this is the Bloch sphere).

The matrix D can be calculated from equation (64)

$$D_{ij} = (\mathbf{r}^i)^T D \mathbf{r}^j$$

As above, we will choose the fiducial measurements to be those pure measurements which identify the fiducial states (these also being taken to be pure). Hence, D will have $1'$s along the diagonal. We choose the first two fiducial vectors to be basis vectors. Hence, D has the form

$$D = \begin{pmatrix} 1 & 0 & 1-a & 1-b \\ 0 & 1 & a & b \\ 1-a & a & 1 & c \\ 1-b & b & c & 1 \end{pmatrix} \tag{74}$$

The two $0'$s follow since the first two vectors are basis vectors (i.e., $(\mathbf{r}^2)^T D \mathbf{r}^2 = 0$ and $(\mathbf{r}^2)^T D \mathbf{r}^1 = 0$). The $1-a$ and a pair above the diagonal follow from normalization since

$$1 = (\mathbf{r}^I)^T D \mathbf{r}^i = (\mathbf{r}^1)^T D \mathbf{r}^i + (\mathbf{r}^2)^T D \mathbf{r}^i \tag{75}$$

The $1-b$ and b pair follow for similar reasons. The matrix is symmetric and this gives all the terms below the diagonal.

We will not show that the constraints on the elements of D are the same as in quantum theory (discussed in Section 13.8.5). Define

$$\mathbf{v} = \begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 - r_1 \\ r_3 \\ r_4 \end{pmatrix} \tag{76}$$

Thus,

$$\mathbf{r} = C\mathbf{v} \tag{77}$$

where

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{78}$$

Hence $\mathbf{r}^T D\mathbf{r}' = \mathbf{v}^T C^T DC\mathbf{v}'$. From (74) we obtain

$$F \equiv C^T DC = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 1 & a & b \\ 1 & a & 1 & c \\ 1 & b & c & 1 \end{pmatrix} \tag{79}$$

Now $\mathbf{r}^I = \mathbf{r}_1 + \mathbf{r}_2 = (1,1,0,0)^T$. The corresponding $\mathbf{v}$ type vector is, using (76), $\mathbf{v}^I = (1,0,0,0)^T$. Assume that $\mathbf{r}$ is normalized to μ and $\mathbf{r}'$ is normalized to μ'. Then

$$\mu = \mathbf{v}^I F\mathbf{v} = 2v_0 + \sum_{i=1}^{3} v_i \tag{80}$$

and similarly for μ'. For normalized states $\mu = 1$. If $\mathbf{v}^I F\mathbf{v}'$ is multiplied out and (80) is used to eliminate v_0 (and a similar equation is used to eliminate v_0') then we obtain

$$p_{meas} = \mathbf{r}^T D\mathbf{r}' = \vec{v}^T A\vec{v}' + \mu\mu'/2 \tag{81}$$

where

$$\vec{v} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} r_2 - r_1 \\ r_3 \\ r_4 \end{pmatrix} \tag{82}$$

and

$$A = \begin{pmatrix} \frac{1}{2} & a - \frac{1}{2} & b - \frac{1}{2} \\ a - \frac{1}{2} & \frac{1}{2} & c - \frac{1}{2} \\ b - \frac{1}{2} & c - \frac{1}{2} & \frac{1}{2} \end{pmatrix} \tag{83}$$

All the pure states will be normalized. Furthermore, they will satisfy $\mathbf{r}^T D\mathbf{r} = 1$ or

$$\vec{v}^T A\vec{v} = \frac{1}{2} \tag{84}$$

This equation defines a two dimensional surface T embedded in three dimensions. For example, if $a = b = c = \frac{1}{2}$ then we have a sphere of radius 1 (this is, in fact, the Bloch sphere). If A has three positive eigenvalues then T will be an ellipsoid. If A has one or two negative eigenvalues then T will be a hyperboloid (if A has three negative eigenvalues then there cannot be any real solutions for $\vec{v}$). An equal mixture of the two basis states $\frac{1}{2}\mathbf{r}_1 + \frac{1}{2}\mathbf{r}_2$ corresponds to $\vec{v} = (0,0,0)^T$. Thus, the origin is in the set of allowed states. An ellipsoid represents a convex surface with the origin in its interior. On the

other hand, the curvature of a hyperboloid is such that it cannot represent a convex surface with the origin on the interior and so cannot represent points in the set of pure vectors. Thus we require that T has three positive eigenvalues. A necessary condition for A to have all positive eigenvalues is that $det(A) > 0$. We have three variables a, b and c. The condition $det(A) = 0$ is satisfied when

$$c = c_{\pm} \equiv 1 - a - b + 2ab \pm 2\sqrt{ab(1-a)(1-b)} \tag{85}$$

Note, we get the same conditions on c if we solve $det\, D = 0$. We know the case with $a = b = c = \frac{1}{2}$ corresponds to a sphere. This falls between the two roots in equation (85). The sign of the eigenvalues cannot change unless the determinant passes through a root as the parameters are varied. Hence, all values of a, b, c satisfying

$$c_- < c < c_+ \tag{86}$$

must correspond to three positive eigenvalues and hence to an ellipsoid. Values outside this range correspond to some negative eigenvalues (this can be checked by trying a few values). Hence, (86) must be satisfied. This agrees with quantum theory (see (36)). Therefore, we have obtained quantum theory from the axioms for the special case $N = 2$. As detailed in Section 13.8.5, if we are given D we can go back to the usual quantum formalism by using D to calculate $\hat{\mathbf{P}}$ (making some arbitrary choices of phases) and then using the formulae in that section (equations (13) and (16)) to obtain $\hat{\rho}$ for the state and $\hat{A}$ for the measurement.

If T is ellipsoidal it is because we have made a particular choice of fiducial projectors $\hat{P}_k$. We can choose a different set to make T spherical. Since the choice of fiducial vectors is arbitrary we can, without any loss of generality, always take T to be spherical with $a = b = c = \frac{1}{2}$. Hence, without loss of generality, we can always put

$$D = \begin{pmatrix} 1 & 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & 1 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & 1 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 1 \end{pmatrix} \tag{87}$$

for the $N = 2$ case.

Since we have now reproduced quantum theory for the $N = 2$ case we can say that

- Pure states can be represented by $|\psi\rangle\langle\psi|$ where $|\psi\rangle = u|1\rangle + v|2\rangle$ and where u and v are complex numbers satisfying $|u|^2 + |v|^2 = 1$.
- The reversible transformations which can transform one pure state to another can be seen as rotations of the Bloch sphere, or as the effect of a unitary operator $\hat{u}$ in $SU(2)$.

This second observation will be especially useful when we generalize to any N.

13.8.7 General N

It quite easy now to use the N =2 result to construct the case for general N using Axiom 3 (the subspace axiom). We will use the $N = 3$ case to illustrate this process. For this case $K = 9$ and so we need 9 fiducial vectors which we will choose as in Section 13.8.2. Thus, we choose the first 3 of these to be the fiducial basis vectors. There are 3 two-dimensional fiducial subspaces. Each of these must have a further two fiducial vectors (in addition to the basis vectors already counted). As in Section 13.8.2 we will label the two fiducial vectors in the mn subspace as mnx and mny. We will choose the following order for the fiducial states

$$1, 2, 3, 12x, 12y, 13x, 13y, 23x, 23y,$$

This provides the required 9 fiducial vectors. These fiducial vectors can represent pure states or pure measurements. The matrix D is a 9×9 matrix. However, each two-dimensional fiducial subspace must, by Axiom 3, behave as a system of dimension 2. Hence, if we take those elements of D which correspond to an $N = 2$ fiducial subspace they must have the form given in equation (87). We can then calculate that for $N = 3$

$$D = \begin{pmatrix} 1 & 0 & 0 & h & h & h & h & 0 & 0 \\ 0 & 1 & 0 & h & h & 0 & 0 & h & h \\ 0 & 0 & 1 & 0 & 0 & h & h & h & h \\ h & h & 0 & 1 & h & q & q & q & q \\ h & h & 0 & h & 1 & q & q & q & q \\ h & 0 & h & q & q & 1 & h & q & q \\ h & 0 & h & q & q & h & 1 & q & q \\ 0 & h & h & q & q & q & q & 1 & h \\ 0 & h & h & q & q & q & q & h & 1 \end{pmatrix}$$

where $h = 1/2$ and, as we will show, $q = 1/4$. All the $0'$s are because the corresponding subspaces do not overlap (we are using property (58)). The q's correspond to overlapping subspaces. Consider for example, the $D_4 6$ term. This is given by $\mathbf{r}_{12x}^T D \mathbf{r}_{13x}$ which is the probability when $\mathbf{r}_{12x}$ is measured on the state $\mathbf{r}_{13x}$. If states are restricted to the 13 fiducial subspace then, by Axiom 3, the system must behave as a two-dimensional system. In this case, the mea- surement $\mathbf{r}_{12x}$ corresponds to some measurement in the 13 fiducial subspace. Since it has support of $1/2$ on the 1 basis state and support of 0 on the 3 basis state this measurement must be equivalent to the measurement $\frac{1}{2}\mathbf{r}_1$ (though only for states restricted to the 13 fiducial subspace). But $\mathbf{r}_1^T D \mathbf{r}_{13x} = 1/2$ and hence $\mathbf{r}_{12x}^T D \mathbf{r}_{13x} = 1/4$. We can use a similar procedure to calculate D for any N. Once we have this matrix we can convert to the usual quantum formalism as we did in the $N = 2$ case. The projection operators which give rise to this D are, up to arbitrary choices in phase, those in equations (26) and (27) (these arbitrary choices in phase correspond to fixing the gauge). Hence, we obtain $\hat{\mathbf{P}}$. Using the results of Section 13.8.5, we obtain

$$\hat{\rho} = \hat{\mathbf{P}} \cdot \mathbf{r} \tag{88}$$

for a state represented by $\mathbf{r}$, and

$$\hat{A} = \mathbf{r} \cdot \hat{\mathbf{P}} \tag{89}$$

or a measurement represented by $\mathbf{r}$. Hence, we obtain

$$p_{meas} = tr(\hat{A}\hat{\rho}) \tag{90}$$

which is shown to be equivalent to $p_{meas} = \mathbf{r} \cdot \mathbf{p}$ in section 5. We now need to prove that the restrictions from quantum theory on $\hat{A}$ and $\hat{\rho}$ from the axioms.

Both $\hat{\rho}$ and $\hat{A}$ must be Hermitian since $\mathbf{r}$ is real. The basis state $\mathbf{r}_1$ is represented by $|1\rangle\langle 1|$. We showed above that we can apply any unitary rotation $U \in SU(2)$ for the $N = 2$ case. It follows from Axiom 3 and the results of the previous section that if we apply an reversible transformation in a two-dimensional fiducial subspace on a state which is in that two-dimensional subspace the effect will be given by the action of a unitary operator acting in that subspace. Thus imagine we prepare the state $|1\rangle\langle 1|$. Let the basis states be $|n\rangle\langle n|$ (where $n = 1\, to\, N$). Perform the rotation U_{12} in the 12 subspace. This transforms the state to $U_{12}|1\rangle\langle 1|U_{12}^\dagger$. Now redefine the basis states to be $|1'\rangle\langle 1'| = U_{12}|1\rangle\langle 1|U_{12}^\dagger$, $|2'\rangle\langle 2'| = U_{12}|2\rangle\langle 2|U_{12}^\dagger$, and $|n\rangle\langle n|$ for $n \neq 1, 2$

(it is shown in Appendix 3.3 that a reversible transformation in a subspace can be chosen to leave basis states not in that subspace unchanged). Next, we consider a rotation $U_{1'3}$ in the $1'3$ subspace. The state will only have support in this subspace and so Axiom 3 can be applied again. The basis states can be redefined again. This process can be repeated. In this way it is easy to prove we can generate any state of the form

$$\hat{\rho} = |\Psi\rangle \langle\Psi| \tag{91}$$

where

$$|\Psi\rangle = \sum_{n=1}^{N} c_n |n\rangle \tag{92}$$

and $\sum_n |c_n|^2 = 1$ (this is most easily proven by starting with the target state and working backwards). These transformations are reversible and hence all the states generated in this way must be pure. Now, since we have shown that these states exist, all mea- surements performed on these states must be non- negative. That is

$$tr(\hat{A} |\Psi\rangle \langle\Psi|) \geq 0 \quad \text{for all} \quad |\Psi\rangle \tag{93}$$

Hence, we obtain the positivity condition for the operators $\hat{A}$ associated with measurements. For each state, $\mathbf{r}$, there exists a pure measurement represented by the same vector, $\mathbf{r}$, which identifies the state. Hence, since the state $|\Psi\rangle \langle\Psi|$ exists, it follows from (88,89) that measurements of the form

$$\hat{A} = |\Psi\rangle \langle\Psi| \tag{94}$$

exist. Therefore, all states $\hat{\rho}$ must satisfy

$$tr(|\Psi\rangle \langle\Psi| \hat{\rho}) \geq 0 \quad \text{for all} \quad |\Psi\rangle \tag{95}$$

Hence we have proved the positivity condition for states.

We have $\hat{I} = \mathbf{r}^I \cdot \hat{\mathbf{P}}$ since the first N elements of $\mathbf{r}^I$ are equal to 1 and the remainder are 0, and the first N elements of $\hat{\mathbf{P}}$ are projectors corresponding to a basis. Hence, the trace condition (that $0 \leq tr(\hat{\rho}) \leq 1$) follows simply from the requirement $0 \leq \mathbf{r}^I \cdot \mathbf{p} \leq 1$.

The most general measurement consistent with the axioms can be shown to be a POVM. A set of measurements $\mathbf{r}_l$ that can be performed with a given knob setting on the measurement apparatus must satisfy $\sum_l \mathbf{r}_l = \mathbf{r}^I$. Using (89), this corresponds to the constraints $\sum_l \hat{A}_l = I$ as required.

13.8.8 Transformations

It was shown in Section 5 that the transformation Z on $\mathbf{p}$ is equivalent to the transformation \$ on $\hat{\rho}$ where

$$Z = tr(\hat{\mathbf{P}}\$(\hat{\mathbf{P}})^T)D^{-1}) \tag{96}$$

To discuss the constraints on transformations we need to consider composite systems. Figure 11 shows a preparation apparatus producing a system made up of subsystems A and B such that A goes to the left and B goes to the right.

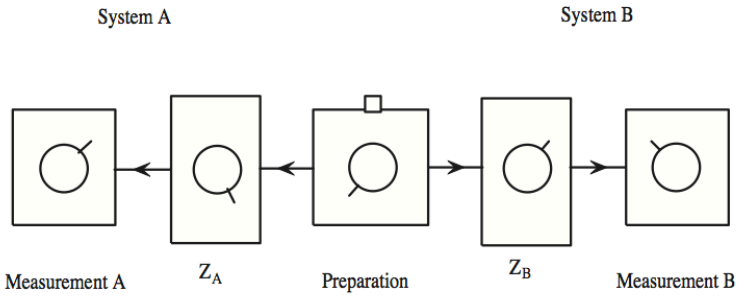

Figure 11: The preparation device here prepares a system in the form of two subsystems which go to the left and the right.

These subsystems then impinge on measurement apparatuses after passing through transformations devices which perform transformations Z_A and Z_B. This set up can be understood to be a special case of the more generic setup shown in Figure 10 (there is no stipulation in the case of Figure 10 that the measurement apparatus or any of the other apparatuses be located only in one place). Assume the transformation devices are initially set to leave the subsystems unchanged. From Axiom 4 we know that there are $K_A K_B$ fiducial measurements. As discussed in Section 5, the space of positive operators for the composite system is spanned by $\hat{P}_i^A \otimes \hat{P}_j^B$ where $\hat{P}_i^A$ $(i = 1\ to\ K_A)$ is a fiducial set for A and $\hat{P}_j^B$ $(j = 1\ to\ K_B)$ is a fiducial set for B. It is shown in Appendix 4 that (as we would expect) the projector $\hat{P}_i^A \otimes \hat{P}_j^B$ corresponds (i) to preparing the $i\,th$ fiducial state at side A and the $j\,th$ fiducial state at side B when the operator is regarded as representing a state, and (ii) to measuring the joint probability of obtaining a positive outcome

at both ends when the $i\,th$ fiducial measurement is performed at side A and the $j\,th$ fiducial measurement is performed at side B when the operator is regarded as representing a measurement. Hence, one choice of fiducial measurements is where we simply perform the $i\,th$ fiducial measurement on A and the $j\,th$ fiducial measurement on B and measure the joint probability p_{ij}. The probabilities p_{ij} could be put in the form of a column vector p_{AB}. However, for discussing transformations, it is more convenient to put them in the form of a $K_A \times K_B$ matrix, $\tilde{p}_{AB}$, having ij entry p_{ij}. It is easy to convert between these two ways of describing the state. We could regard both the preparation apparatus and measurement apparatus B as a preparation apparatus preparing states of subsystem A. If we perform the $j\,th$ fiducial measurement on system B and take only those cases where we obtain a positive result for this measurement preparing the null state otherwise then the resulting state of system A will be given by a vector equal to the $j\,th$ column of $\tilde{p}_{AB}$ (since these probabilities are equal to the probabilities that would be obtained for the fiducial measurements on A with this preparation). Hence, the columns of $\tilde{p}_{AB}$ must transform under Z_A. Similarly, the rows of $\tilde{p}_{AB}$ must transform under Z_B. Hence, when the transformation devices in Figure 11 are active, we have

$$\tilde{p}_{AB} \to Z_A \tilde{p}_{AB} Z_B^T \tag{97}$$

If the state is represented by $\tilde{r}_{AB}$ where

$$\tilde{p}_{AB} = D_A \tilde{r}_{AB} D_B^T \tag{98}$$

then this equation becomes

$$\tilde{r}_{AB} = X_A \tilde{r}_{AB} X_B^T \tag{99}$$

where

$$X_A = D_A^{-1} Z_A D_A \tag{100}$$

and similarly for B. It is easy to see that this is the correct transformation equation in quantum theory (we have dropped the A and B superscripts).

$$\begin{aligned} p_{AB}^{ij} &\rightarrow tr[\hat{P}_i \otimes \hat{P}_j \$_A \otimes \$_B(\hat{\rho})] \\ &= tr[\hat{P}_i \otimes \hat{P}_j \$_A \otimes \$_B(\sum_k \hat{P}_k \otimes \hat{P}_l r^{kl})] \\ &= \sum_{kl} tr[\hat{P}_i \otimes \hat{P}_j \$_A(\hat{P}_k) \otimes \$_B(\hat{P}_l)] r^{kl} \\ &= \sum_{kl} tr[\hat{P}_i \$_A(\hat{P}_k)] r_{AB}^{kl} tr[\hat{P}_j \$_B(\hat{P}_k)] \end{aligned} \tag{101}$$

which, using (96), gives (97) and (99). The steps in (101) can be read backwards. Hence, from (97), we obtain the tensor product structure for describing composite systems.

We will say that Z_A is completely positive iff

$$\tilde{p}_{AB} \rightarrow Z_A \tilde{p}_{AB} \tag{102}$$

maps all allowed states of the composite system AB to states which are also allowed states for any dimension N_B. The only constraint on transformation matrices Z is that they transform states in S to states in S. This means that probabilities must remain bounded by 0 and 1. Hence,

1. Z must not increase the normalization coefficient of states.

2. Z must be completely positive.

Condition 2 is necessary since any system could always be a subsystem of some larger system. The transformations deduced from the axioms are subject to the equivalent constraints for \$ listed in Section 5. They preserve Hermiticity since the transformation matrix Z is real (and hence **p**p remains real). They do not increase the trace (point 1. above). They are linear and they must be completely positive (point 2. above). Hence, the most general type of transformation consistent with the axioms is the most general transformation of quantum theory. As noted in section 5, this gives us unitary evolution and von Neumann projection as special cases.

13.8.9 The state after a measurement

It is possible that, after a measurement, a quantum system emerges from the measurement apparatus. In such cases the measurement apparatus is also behaving as a transformation apparatus. We can think of the state as emerging into a different channel for each measurement outcome. Associated with each outcome, l, of the measurement will be a certain transformation, $Z_l \in \Gamma$, on the state. he probability of any given outcome will not, in general, be equal to 1. Hence, the transformation must reduce the normalization coefficient associated with the state to a value consistent with the probability of obtaining that outcome. This condition is

$$\mathbf{r}^I \cdot Z_l \mathbf{p} = \mathbf{r}_l \cdot \mathbf{p} \quad \text{for all} \quad \mathbf{p} \in S \tag{103}$$

Furthermore, we can consider all these channels taken together. In this case the effective transformation is given by $\sum_l Z_l$. It is necessary that this also belongs to the allowed set of transformations, Γ, and that it does not change the normalization coefficient associated with the state. This second condition can be written

$$\left(\sum_l Z_l \right)^T \mathbf{r}^I = \mathbf{r}^I \tag{104}$$

This is equivalent to constraint

$$tr \sum_l \$(\hat{\rho}) = tr(\hat{\rho}) \quad \text{for all} \quad \hat{\rho} \tag{105}$$

Since completely positive operators can be written as $\$(\hat{\rho}) = \sum_l \hat{M}_l \hat{\rho} \hat{M}_l^\dagger$ this equation can be shown to be equivalent to

$$\sum_l \hat{M}_l^\dagger \hat{M}_l = \hat{I} \tag{106}$$

which is the usual quantum constraint on superoperators associated with measurements.

The two equations (103,104) which constrain the possible transformations of the state after measurement apply equally well to classical probability theory. This may suggest a new approach to the measurement problem in quantum theory.

13.9 Infinite dimensional spaces

There are two types of infinite dimensional space - countable and continuous dimensional. The countable infinite dimensional spaces are accounted for by these axioms since such systems are characterized by the property that any finite subspace obeys quantum theory. It is not so clear what the status of continuous dimensional spaces is. Such spaces can always be modeled arbitrarily well by a countable infinite dimensional Hilbert space. However, there are certain mathematical subtleties associated with the continuous case which we have not considered here. Nevertheless, it is clear that the classical continuous case violates the axioms even though there are continuous paths between states since the continuity axiom (Axiom 5) must also apply to finite subspaces (by Axiom 3) and for these there are no continuous transformations.

While continuous dimensional spaces play a role in some applications of quantum theory it is worth ask- ing whether we expect continuous dimensional spaces to appear in a truly fundamental physical theory of nature. Considerations from quantum gravity suggest that space is not continuous at the planck scale and that the amount of information inside any finite volume is finite implying that the number of distinguishable states is countable. Given the mathematical difficulties that appear with continuous dimensional Hilbert spaces it is also natural to ask what our motivation for considering such spaces was in the first place. Consider a classical particle which can move along a straight line. If where were not a continuous infinity of distinguishable positions for the particle then the only way the particle could move would be to jump from one position to the next. It is because we do not like such discontinuities in physics that we imagine that there is a continuous infinity of distinct positions along the line. However, in quantum theory it is no longer the case that the particle would need to jump and hence the main motivation for considering the continuous dimensional case no longer pertains.

If we do, nevertheless, consider continuous dimensional spaces then there is an interesting respect in which the quantum case is superior to the classical case. Consider again a particle which can move along a straight line. Every point on the line represents a distinguishable state for the particle. Take three points A, B, and C along this line where B is between A and

C. In classical theory, if the particle is to move continuously through the state space from A to C it must pass through point B. However, to move continuously from A to B it need not pass through C. Hence, the pairs AB and AC are on an unequal footing. In quantum theory a particle can pass directly from the point A to the point C without going through the points in between along a continuous trajectory in the state space simply by going along the Bloch sphere corresponding to this two-dimensional subspace (such transformations do not occur in practice since Hamiltonians contain only local terms). Hence, the pairs AB and AC are on an equal footing. We can regard statements like *the particle is at point* B as logical propositions. It is a very desirable property that pairs of propositions should be on an equal footing. Thus, in this respect, quantum theory is superior.

On the other hand, even in the quantum case, continuous dimensional spaces appear to have a topological relationship between infinitesimally displaced distinguishable states which is different to the topological relationship between finitely displaced distinguishable states. This is hard to reconcile with the notion that any pair of distinguishable states are on an equal footing and may be further support for the case against giving continuous dimensional spaces a role in any fundamental theory of nature.

13.10 Discussion

We have shown that quantum theory follows from five very natural axioms. If Axiom 5 (or even just the word *continuous* in Axiom 5) is dropped we obtain classical probability theory instead. It is classical probability theory that must have *jumps*. If a $19\,th$ century ancestor of Schrodinger had complained about dammed classical jumps then he might have attempted to derive a continuous theory of probability and arrived at quantum theory. Quantum theory is, in some respects, both superior to and more natural than classical probability theory (and therefore classical theories in general) since it can describe evolution for finite systems in a continuous way. Since nature is quantum, not classical, it is to be expected that quantum theory is ultimately the more reasonable theory.

There are many reasons to look for better axiomatic formulations of quantum theory.

- Aesthetics. A theory based on reasonable axioms is more appealing.

- A set of reasonable axioms provides us with a deeper conceptual understanding of a theory and is therefore more likely to suggest ways in which we could extend the domain of the theory or modify the axioms in the hope of going beyond quantum theory (for example, to develop quantum gravity).
- This approach puts a different slant on the interpretation of quantum theory (see discussion below).
- Since the formulation of quantum theory here is closer to classical probability theory than the standard formulation, this may motivate new applications and new treatments of the theory of quantum information.

There are various ways in which this work has a bearing on interpretational matters. First, if we re- ally believe these axioms to be reasonable then they would also apply to hidden variables and it would follow that the hidden variable substructure must look like quantum theory. We could not then use hidden variables to solve the measurement problem (since this relies on being able to give the hidden variables a classical probability interpretation). Second, we see here how successful a purely instrumentalist approach is in obtaining the structure of quantum theory. Whilst this need not contradict beliefs held by the realist since he would anyway expect quantum theory to be consistent with instrumentalist argumentation, it does require some explanation. And, third, we obtain that the most general evolution is that of a superoperator. This is capable of taking pure states to mixed states. Hence, collapse interpretations of quantum theory could be incorporated into this structure.

Appendix 1

We will prove that the property

$$f(\lambda \mathbf{p}_A + (1-\lambda)\mathbf{p}_B) = \lambda f(\mathbf{p}_A) + (1-\lambda) f(\mathbf{p}_B) \tag{107}$$

where $\lambda \geq 0$, implies that

$$f(\mathbf{p}) = \sum_\alpha a_\alpha f(\mathbf{p}_\alpha) \tag{108}$$

where

$$\mathbf{p} = \sum_\alpha a_\alpha \mathbf{p}_\alpha \tag{109}$$

if

$$\mathbf{p}_\alpha, \mathbf{p} \in S \quad \text{for all} \quad \alpha$$

for all a_α where S is the set of allowed $\mathbf{p}$. First note that putting $\mathbf{p}_A = 0$ gives

$$f(\lambda \mathbf{p}) = \lambda f(\mathbf{p}) \tag{110}$$

for $0 \leq \lambda \leq 1$. We can write $\gamma = 1/\lambda$ and $\mathbf{p}'' = \mathbf{p}/\lambda$. Then we obtain

$$f(\gamma \mathbf{p}'') = \gamma f(\mathbf{p}'') \tag{111}$$

where $1 \leq \gamma$. Hence

$$f(v\mathbf{p}) = v f(\mathbf{p}) \tag{112}$$

if $v \geq 0$. This only follows from (107) if $\mathbf{p}, v\mathbf{p} \in S$. However, if this is not the case, then the equation does not correspond to any physical situation. Hence, we are free to impose that (112) is true for all $\mathbf{p}$. In those cases where $\mathbf{p}, v\mathbf{p} \in S$ is not satisfied the equation has no physical significance anyway.

Let f_I pertain to that measurement that simply checks to see that a non-null result has been recorded (we call this the identity measurement). We will write $f_I(\mathbf{p}) = \mu$. We define the normalized state $\tilde{\mathbf{p}}$ by $\mu\tilde{\mathbf{p}} = \mathbf{p}$ such that $f_I(\tilde{\mathbf{p}}) = 1$ (using (112)).

We can normalize each of the states in (109) such that

$$\mu\tilde{\mathbf{p}} = \sum_\alpha a_\alpha \mu_\alpha \tilde{\mathbf{p}}_\alpha \tag{113}$$

We are free to choose the fiducial measurement corresponding to the first component of the state vector $\mathbf{p}$ to be the identity measurement. Hence, reading off the first component from (113) we obtain

$$\mu = \sum_\alpha a_\alpha \mu_\alpha \tag{114}$$

Let $\alpha \in A_\pm$ if a_α is $\pm$ve and define

$$\nu = \mu + \sum_{\alpha \in A_-} |a_\alpha| \mu_\alpha = \sum_{\alpha \in A_+} a_\alpha \mu_\alpha \tag{115}$$

We can rearrange (113)

$$\frac{\mu}{\nu}\tilde{\mathbf{p}} + \sum_{\alpha\in A_-} \frac{|a_\alpha|\mu_\alpha}{\nu}\tilde{\mathbf{p}} = \sum_{\alpha\in A_+} \frac{a_\alpha\mu_\alpha}{\nu}\tilde{\mathbf{p}} \tag{116}$$

Each coefficient is positive and the coefficients on each side add to 1. Hence we can apply (107)

$$\frac{\mu}{\nu}f(\tilde{\mathbf{p}}) + \sum_{\alpha\in A_-} \frac{|a_\alpha|\mu_\alpha}{\nu}f(\tilde{\mathbf{p}}) = \sum_{\alpha\in A_+} \frac{a_\alpha\mu_\alpha}{\nu}f(\tilde{\mathbf{p}}) \tag{117}$$

Rearranging this using (112) gives (108) as required.

We see that (108) holds whenever the arguments of f in each term correspond to physical states. If these arguments do not all correspond to physical states then the equation does not correspond to any physical situation. For mathematical simplicity we will impose that (108) still holds in such cases.

Appendix 2

In this appendix we show that any strictly increasing function having the completely multiplicative property

$$K(mn) = K(m)K(n) \tag{118}$$

where n takes only positive integer values, is of the form $K(n) = n^\alpha$. First put $m = n = 1$ into(118). We obtain that $K(1) = 0, 1$. Put $m = 1$ into (118). If $K(1) = 0$then $K(n) = 0$for all n. But this is not strictly increasing. Hence we must have $K(1) = 1$. The argument n can be factorized into primes: $n = p_1^{k_1}p_2^{k_2}....$ where p_i is the ith primes and the k_i's are integers. It follows from the completely multiplicative property that

$$K(n) = \prod_i K^{k_i}(p_i) \tag{119}$$

Hence, the function $K(n)$ is completely determined by its values at the primes. Now consider two primes p and q.Define α by

$$K(p) = p^\alpha \tag{120}$$

Note that $K(p) > 1$ since $K(n)$ is a strictly increasing function and hence $\alpha > 0$. Define a by

$$K(q) = aq^\alpha \tag{121}$$

Introduce the integer t which we will allow to take any positive value. Then define s by

$$p^s > q^t > p^{s-1} \tag{122}$$

From the fact that $K(n)$ is strictly increasing we have

$$K(p^s) > K(q^t) > K(p^{s-1}) \tag{123}$$

Hence,

$$p^{\alpha s} > a^t q^{\alpha t} > p^{\alpha(s-1)} \tag{124}$$

Define $\tilde{s}$ by

$$p^{\tilde{s}} = q^t \tag{125}$$

Comparing with (122) we have

$$\tilde{s} + 1 > s > \tilde{s} > s - 1 > \tilde{s} - 1 \tag{126}$$

Hence, (124) gives

$$p^{\tilde{s}+1} > a^t q^{\alpha t} > p^{\alpha(\tilde{s}-1)} \tag{127}$$

(we have used the fact that $\alpha > 0$). Using (125) we obtain

$$p^{\alpha} > a^t > p^{-\alpha} \tag{128}$$

This must be true for all t. However, a^t can only be bounded from above and below if $a = 1$. Hence, $K(q) = q^{\alpha}$. This applies to any pair of primes, p and q, and hence $K(n) = n^{\alpha}$. **Appendix 3**

In this appendix we will prove a number of related important results some of which are used in the main part of the paper.

The set of reversible transformations is represented by the set, $\Gamma^{reversible}$, of invertible matrices Z in Γ whose inverses are also in Γ. These clearly form a representation of a group. In fact, since, by Axiom 5, this group is continuous and the vectors $\mathbf{p}$ generated by the action of the group remain bounded, $\Gamma^{reversible}$ is a representation of a compact Lie group. It can be shown that all real representations of a compact Lie group are equivalent (under a basis change) to a real orthogonal representation. Let us perform such a basis change. Under this basis change assume that $Z \in \Gamma$ is transformed to $Y \in \Omega$ and $\mathbf{p}_S \in S$ is transformed to $\mathbf{q} \in Q$. The formula $p_{meas} = \mathbf{r} \cdot \mathbf{p}$ becomes

$$p_{meas} = \mathbf{s} \cdot \mathbf{q} \tag{129}$$

where $\mathbf{s}$ now represents the measurement (and is obtainable from $\mathbf{r}$ by a basis change). If a transformation device is present then we have

$$p_{meas} = \mathbf{s}^T Y \mathbf{q} \tag{130}$$

We can regard Y as transforming the state or, alternatively, we can regard it as part of the measurement apparatus. In this case we have $\mathbf{s} \to Y^T \mathbf{s}$. If we now restrict our attention to reversible transformations then $Y \in \Omega^{reversible}$. Therefore, with this representation, both states $\mathbf{q}$ and measurements $\mathbf{s}$ are acted on by elements of $\Omega^{reversible}$.

A3.1

In this Appendix section we will prove that

$$Z_W^T \mathbf{r}^{I_W} = \mathbf{r}^{I_W} \quad \text{for all} \quad Z_W \in \Gamma_W^{reversible} \tag{131}$$

where $\mathbf{r}^{I_W}$ is the identity measurement for the subspace Wn and $\Gamma_W^{reversible}$ is the set of reversible transformations which map states in the subspace W to states in W - such transformations must exist by Axiom 3. We can work in the basis for which the transformations are orthogonal introduced above. Then we wish to prove

$$Y_W^T \mathbf{s}^{I_W} = \mathbf{s}^{I_W} \quad \text{for all} \quad Y_W \in \Omega_W^{reversible} \tag{132}$$

Working in this basis we can write any state in the subspace W as

$$\mathbf{q} = a\mathbf{s}^{I_W} + \mathbf{x} \tag{133}$$

where $\mathbf{x}$ is orthogonal to $\mathbf{s}^I$. The normalization of this state is fixed by a. Let K_W be the number of degrees of freedom associated with the subspace W. Once the normalization coefficient has been fixed there are $K_W - 1$ degrees of freedom left corresponding to the $K_W - 1$ dimensions of the vector space orthogonal to $\mathbf{s}^{I_W}$ for states in W which is spanned by possible $\mathbf{x}$. There must be at least one direction in this vector space for which both $\mathbf{x}$ and $\gamma\mathbf{x}$ where $\gamma \neq 1$, are permissible vectors (corresponding to allowed states). To see this assume the contrary. Thus assume that for each direction $\mathbf{x}/|\mathbf{x}|$ there is only one allowed length of vector. Such a constraint would remove one degree of freedom leaving $K_W - 2$ degrees of freedom which contradicts our starting point that there are $K_W - 1$ degrees of freedom associated with states with a

particular normalization coefficient. Consider such an $\mathbf{x}$ for which $\gamma\mathbf{x}$ is also permissible. Now

$$\mathbf{s}^{I_W} \cdot Y_W\mathbf{q} = \mathbf{s}^{I_W} \cdot \mathbf{q} \tag{134}$$

since the reversible transformation Y_W does not change the normalization coefficient of the state and $\mathbf{q}$ is in W both before and after the transformation. Using (133) this becomes

$$a\mathbf{s}^{I_W} \cdot Y_W\mathbf{s}^{I_W} + \mathbf{s}^{I_W} \cdot Y_W\mathbf{x} = a\mathbf{s}^{I_W} \cdot \mathbf{s}^{I_W} \tag{135}$$

This equation must also apply when $\mathbf{x}$ is replaced by $\gamma\mathbf{x}$.

$$a\mathbf{s}^{I_W} \cdot Y_W\mathbf{s}^{I_W} + \gamma\mathbf{s}^{I_W} \cdot Y_W\mathbf{x} = a\mathbf{s}^{I_W} \cdot \mathbf{s}^{I_W} \tag{136}$$

Subtracting these two equations tells us that the second term on the LHS vanishes. Hence

$$\mathbf{s}^{I_W} \cdot Y_W\mathbf{s}^{I_W} = \mathbf{s}^{I_W} \cdot \mathbf{s}^{I_W} \tag{137}$$

Now, the transformation Y_W is orthogonal and hence length preserving and thus (132) follows.

It follows that

$$Y^T\mathbf{s}^I = \mathbf{s}^I \quad \text{for all} \quad Y \in \Omega^{reversible} \tag{138}$$

where $\mathbf{s}^I$ is the identity measurement in this new basis (written as $\mathbf{r}^I$ in the usual basis). This property is to be expected since reversible transformations leave the normalization coefficient of a state unchanged.

A3.2

It is clearly the case that

$$Z_W\mathbf{p} \in W \quad \text{if} \quad \mathbf{p} \in W \quad \text{and} \quad Z_W \in \Gamma_W^{reversible} \tag{139}$$

It is also the case that

$$Z_W\mathbf{p} \in \overline{W} \quad \text{if} \quad \mathbf{p} \in \overline{W} \quad \text{and} \quad Z_W \in \Gamma_W^{reversible} \tag{140}$$

where $\overline{W}$ is the complement subspace of W. This follows immediately since $\mathbf{p} \in \overline{W}$ iff $\mathbf{r}^{I_W} \cdot \mathbf{p} = 0$. But if this is true then, since $Z_W^T\mathbf{r}^{I_W} = \mathbf{r}^{I_W}$, it is also true that $\mathbf{r}^{I_W} \cdot Z_W\mathbf{p} = 0$. Hence, $Z_W\mathbf{p} \in \overline{W}$.

A3.3

We will now prove that we can choose Z_W such that $Z_W \mathbf{P}_n = \mathbf{P}_n$ for $n \in \overline{W}$. Define $W'(m)$ to be the set containing all the elements of W plus the first m elements of $\overline{W}$. Consider only states constrained to the subspace $W'(1)$ and consider the set $\Gamma^{reversible}_{W'(1)}$ of W?(1) reversible transformations which map states in $W'(1)$ back into $W'(1)$. The subspace W is a subspace of $W'(1)$. Hence, by Axiom 3, there must exist a subset of $\Gamma^{reversible}_{W'(1)}$ which map states in W back into W. By the result in A3.2 these transformations must leave the basis state $\mathbf{p}_{m_1}$ unchanged (where m_1 is the first entry of $\overline{W}$) since this is the only normalized state in $W'(1)$ and the complement of W. We can now run the same argument taking $W'(2)$ to be our system and so on. In this way we establish that we can find a transformations Z_W which have the desired property.

A3.4

In this appendix subsection we show that one possible choice of fiducial measurements are those identified in Section 13.8.2. Consider the set $\Gamma^{reversible}_{mn}$ of reversible transformations that transform states in the subspace W_{mn} to states in the same subspace (where W_{mn} is the subspace associated with the $m\,th$ and the $n\,th$ basis vectors). It follows from the property established in A3.2 that

$$\mathbf{r}_n^T Z_{mn} \mathbf{p} = 0 \quad \text{if} \quad \mathbf{p} \in \overline{W}_{mn} \tag{141}$$

We can regard the transformation device as part of the measurement apparatus (rather than regarding it as acting on the state). In this case we have

$$\mathbf{r}_n \rightarrow Z_{mn}^T \mathbf{r}_n \tag{142}$$

We can choose two particular transformations Z_{mnx} and Z_{mny} to provide us with the two extra needed fiducial measurements, $\mathbf{r}_{mnx}$ and $\mathbf{r}_{mny}$ respectively, for each two-dimensional subspace. The vectors $\mathbf{r}_m$, $\mathbf{r}_n$, $\mathbf{r}_{mnx}$, and $\mathbf{r}_{mny}$ must be linearly independent. It follows from the fact that, for this subspace, the group of transformations is equivalent, under a basis change, to the full group of orthogonal rotations in three dimensions that we can choose Z_{mnx} and Z_{mny} such that this is the case. From (141) we have

$$\mathbf{r}_{mnx} \cdot \mathbf{p} = 0 \quad \text{if} \quad \mathbf{p} \in \overline{W}_{mn} \tag{143}$$

and similarly for $\mathbf{r}_{mny}$.

We will now prove that the N^2 vectors chosen in this way are linearly independent. We can do this by showing that each measurement yields information about the state that none of the others do. First, the vectors $\mathbf{r}_n$ are linearly independent of each other since there exists a vector (namely $\mathbf{p}_m$) having non-zero overlap with any given $\mathbf{r}_m$ which has zero overlap with all the other $\mathbf{r}_n$. Now we add two fiducial vectors, $\mathbf{r}_{mnx}$ and $\mathbf{r}_{mny}$, to each two-dimensional subspace W_{mn} that are, by construction, linearly independent of the basis vectors already in that subspace. Since the fiducial measurements pertaining to one such two-dimensional subspace yield no information about states in any other non-overlapping two-dimensional subspace (because of (143))they must be linearly independent of the fiducial measurements in those non-overlapping subspaces. What about over-lapping two-dimensional subspaces? Consider per-forming the measurement $\mathbf{r}_{mnx}$ on $\mathbf{p}$ in $W_{mn'}$ where $n' \neq n$. Since $\mathbf{p}$ is in $W_{mn'}$ it follows from Axiom 3 that the measurement $\mathbf{r}_{mnx}$ must be equivalent to some measurement in this subspace (though only for states in this subspace). Now, if the state is actually the basis state $\mathbf{p}_{n'}$ then zero probability would be recorded. This means that the measurement $\mathbf{r}_{mnx}$, when regarded as a measurement on $W_{mn'}$ is actually equivalent to a measurement just on the one-dimensional subspace W_m. Hence, $\mathbf{r}_{mnx}$ does not yield any information about states in the subspace $W_{mn'}$ that is not given by $\mathbf{r}_m$ and therefore the measurements $\mathbf{r}_{mn'x}$ and $\mathbf{r}_{mn'y}$ are linearly independent of it. Hence, the N^2 fiducial measurements are all necessary to determine the state and are therefore linearly independent.

A3.5

In this appendix subsection we show that the map between a pure state and that pure measurement identifying it is linear and invertible (recall that pure measurements are defined to be those measurements which can be obtained by acting on the basis measurement $\mathbf{r}_1$ with a reversible transformation). Using the basis for which reversible transformations are orthogonal (see introduction to this appendix) we can put

$$\mathbf{q} = a\mathbf{s}^I + \mathbf{u} \tag{144}$$

for the state, and

$$\mathbf{s} = b\mathbf{s}^I + \mathbf{v} \tag{145}$$

for the measurement where $\mathbf{u}$ and $\mathbf{v}$ are orthogonal to $\mathbf{s}^I$. Since $Y^T\mathbf{s}^I = \mathbf{s}^I$ and since the group of reversible transformations, $\Omega^{reversible}$, is orthogonal it follows that $Y\mathbf{s}^I = \mathbf{s}^I$. Hence, transformations only effect the components of $\mathbf{q}$ and $\mathbf{s}$ orthogonal to $\mathbf{s}^I$. Using $p_{meas} = \mathbf{r} \cdot \mathbf{p} = \mathbf{s} \cdot \mathbf{q}$ we obtain

$$p_{meas} = k + \mathbf{v} \cdot \mathbf{u} \tag{146}$$

where $k = ab\mathbf{s}^I \cdot \mathbf{s}^I$.

Now assume that the pure measurement represented by $\mathbf{s}$ identifies the pure state represented by $\mathbf{s}$. Then $k + \mathbf{u} \cdot \mathbf{v} = 1$. This probability cannot be increased by any transformation device. Hence,

$$\mathbf{v}^T Y \mathbf{u} \leq \mathbf{v}^T \mathbf{u} \quad \text{for all} \quad Y \in \Omega^{reversible} \tag{147}$$

Since the orthogonal transformation Y is length preserving it would appear that the only way to satisfy this condition is if $\mathbf{v}$ is parallel to $\mathbf{u}$. This is indeed the case and is proven at the end of this appendix sub- section. Hence, we can say that the state $\mathbf{q} = a\mathbf{s}^I + \mathbf{u}$ is identified by the measurement $\mathbf{s} = b\mathbf{s}^I + c\mathbf{u}$. Now apply this result to the basis state $\mathbf{q}_1$ (this corresponds to $\mathbf{p}_1$) and the basis measurement $\mathbf{s}_1$ (this corresponds to $\mathbf{r}_1$). Let C be the linear map that performs scalar multiplication by a factor μ in the $\mathbf{s}^I$ direction and by a factor ν in the subspace orthogonal to $\mathbf{s}^I$. We can apply C to $\mathbf{q}$ and C^{-1} to $\mathbf{s}$ such that $\mathbf{s}_1\mathbf{q}_1 = \alpha\mathbf{s}^I + \beta\mathbf{u}_1$ by appropriate choice of the factors μ and ν. The maps C and C^{-1} commute with the orthogonal transformations $\Omega^{reversible}$. Hence, in general, the pure state $\mathbf{q} = \alpha\mathbf{s}^I + Y\beta\mathbf{u}_1$ identified by the pure measurement $\mathbf{s} = \alpha\mathbf{s}^I + Y\beta\mathbf{u}_1$ (i.e. represented by the same vector) as $YY^T = I$. Since the basis change and the maps C and C^{-1} are all linear and invertible it follows that the map from pure states to the pure measurements identifying them is linear and invertible.

As promised, we will now prove that $\mathbf{v}$ is parallel to $\mathbf{u}$ when a pure measurement $\mathbf{s}$ identifies a pure state $\mathbf{q}$. First consider the basis measurement $\mathbf{s}_1$ and the basis state $\mathbf{q}_1$ it identifies. Let V_{mn} be the vector space spanned by the fiducial measurement vectors $\mathbf{s}_m$, $\mathbf{s}_n$, $\mathbf{s}_{mnx}$, and $\mathbf{s}_{mny}$ associated with the mn subspace. It follows from A3.4 that these vector spaces span the full N^2 dimensional vector space. The state $\mathbf{q}_1$ can have no projection into the vector space V_{mn} if $m, n \neq 1$ (since $\mathbf{s} \cdot \mathbf{q}_1 = 0$ for $\mathbf{s}$ associated with the mn subspace). Let $\tilde{V}$ be the vector space spanned by the vector spaces V_{1n} for

$n = 1\,to\,N$. It follows from the fact that $\mathbf{q}_1$ has no projection into V_{mn} for $m, n \neq 1$ that $\mathbf{q}_1$ is in $\tilde{V}$. Now the vector $\mathbf{s}^I = \sum_n \mathbf{s}_n$ is clearly in $\tilde{V}$. Let $\tilde{V}'$ be the vector space in $\tilde{V}$ orthogonal to $\mathbf{s}^I$. We can write $\mathbf{q}_1 = a\mathbf{s}^I + \mathbf{u}_1$ where $\mathbf{u}_1$ is in the vector space $\tilde{V}'$. Similarly, we can write $\mathbf{s}_1 = b\mathbf{s}^I + \mathbf{v}_1$. Define V'_{1n} as the vector space spanned by the fiducial measurement vectors $\mathbf{v}_1$, $\mathbf{v}_n$, $\mathbf{v}_{1nx}$, and $\mathbf{v}_{1ny}$ associated with the subspace $1n$. The vector spaces V'_{1n} for $n = 1\,to\,N$ span $\tilde{V}'$. Consider orthogonal transformations Y_{1n} which leave states in the $1n$ subspace. They will also transform measurements pertaining to the $1n$ subspace to measurements still pertaining to this subspace (and thus still in $V'1n$). Since $\mathbf{v}_1$ and $Y_{1n}^T\mathbf{v}_1$ are both in $V'1n$ we can write (147) as

$$\mathbf{v}_1^T Y_{1n} \mathbf{u}_1^{1n} \leq \mathbf{v}_1^T \mathbf{u}_1^{1n} \tag{148}$$

where $\mathbf{u}_1^{1n}$ is the component of $\mathbf{u}_1$ in $V'1n$. The vector space $V'1n$ is three dimensional and the action of the group of orthogonal transformations in the $1n$ subspace on $\mathbf{u}_1$ is to sweep out a sphere (since these transformations are length preserving). Hence, condition (148) can only be satisfied for all rotations Y_{1n} if $\mathbf{u}_1^{1n}$ is parallel to $\mathbf{v}_1$. The vector spaces $V'1n$ span all of $\tilde{V}'$ and hence $\mathbf{u}_1$ has no component which is perpendicular to $\mathbf{v}_1$. This means that $\mathbf{v}_1$ is parallel to $\mathbf{u}_1$. We complete the proof by noting that a general pure measurement can be written $\mathbf{v} = Y\mathbf{v}_1$ and identifies the pure state $\mathbf{u} = Y\mathbf{u}_1$.

A3.6

It is easy to prove that $D = D^T$. We chose a set of pure fiducial states and we chose the fiducial measurements to be the set of pure measurements that identify these states. Hence, if we represent the fiducial states by a set of vectors $\mathbf{q}^l$ then, as proven in A3.5, we can represent the fiducial measurements by the the same vectors $\mathbf{s}^k = \mathbf{q}^k$. The matrix element D_{kl} is equal to the probability when the $k\,th$ fiducial measurement is performed on the $l\,th$ fiducial state. This is equal to $\mathbf{q}^k \cdot \mathbf{q}^l$ and hence $D = D^T$.

A3.7

Now we will show that the basis measurements $\mathbf{r}_n$ are all pure and, therefore, that all the fiducial measurements of A3.4 are pure. Consider first the case where $N = 2$. Then $K = 4$. The normalized states (and hence pure states) live in a three dimensional space (since we can eliminate one variable by normalization). Hence, orthogonal transformations can be regarded as rotations

about an axis. We can write the basis states as

$$\mathbf{q}_1 = \alpha \mathbf{s}^I + \beta \mathbf{u}_1 \tag{149}$$

$$\mathbf{q}_2 = \alpha \mathbf{s}^I - \beta \mathbf{u}_1 \tag{150}$$

This follows since there exists a continuous orthogonal transformation which takes $\mathbf{q}_1$ to $\mathbf{q}_2$. This can be regarded as a rotation around a great circle. The orthogonal state $\mathbf{q}_2$ must correspond to the opposite point on the circle where $\mathbf{u} = -\mathbf{u}_1$ since this is the point at which $\mathbf{s}_1 \cdot \mathbf{q}$ stops decreasing and starts increasing again. Now, we have already that

$$\mathbf{s}_1 = \alpha \mathbf{s}^I + \beta \mathbf{u}_1 \tag{151}$$

We have not yet proven that $\mathbf{s}_2$ (corresponding to $\mathbf{r}_2$) is pure. However, we know that $\mathbf{s}_1 + \mathbf{s}_2 = \mathbf{s}^I$ so we can write

$$\mathbf{s}_2 = \alpha' \mathbf{s}^I - \beta \mathbf{u}_1 \tag{152}$$

with $\alpha + \alpha' = 1$. It then follows from $\mathbf{s}_1 \cdot \mathbf{q}_2 = \mathbf{s}_2 \cdot \mathbf{q}_1 = 0$ that $\alpha = \alpha' = 1/2$. Hence, $\mathbf{s}_2$ is pure.This proof can be applied to the general N case by considering only a two dimensional subspace. It follows from Axiom 3 that there must exist a set of invertible transformations which transform states in the $1n$ subspace to states in the same subspace. As shown in A3.1, these leave $\mathbf{s}^{I_{W_{1n}}}$ invariant (this is the identity measurement vector for the $1n$ subspace). Hence, we can replace $\mathbf{s}^I$ by $\mathbf{s}^{I_{W_{1n}}}$ throughout the above proof if we are only considering transformations in this subspace. It follows that we can transform $\mathbf{s}_1$ to $\mathbf{s}_n$ and hence the basis measurements are all pure.

Hence we can transform $\mathbf{s}_1$ to any $\mathbf{s}_{mnx}$ by first transforming by a reversible transformation to $\mathbf{s}_n$ and then applying the reversible transformation of A3.4 to obtain $\mathbf{s}_{mnx}$. Similar remarks apply to $\mathbf{s}_{mny}$.

Appendix 4

In this appendix we will show that the projector $\hat{P}_i^A \otimes \hat{P}_j^B$ can correspond to the measurement of the joint probability of obtaining a positive outcome for fiducial measurements i at A and j at B, and to the state when the $i\,th$ fiducial state is prepared at A and the $j\,th$ fiducial state is prepared at B. First, note that we can prepare $N_A N_B$ distinguishable states for the

composite system by preparing basis state m at A and basis state n at B. Since the composite system has $N = N_A N_B$ this represents a complete set of basis states. Further, since $K(1) = 1$ all basis states must be pure (as noted at the end of Section 13.8.1). Hence, we can choose these basis states to correspond to the basis states of our Hilbert space $|mn\rangle$ or, equivalently, $|m\rangle \otimes |n\rangle$. As operators these basis states are $\hat{P}_m^A \otimes \hat{P}_n^B$ where $m(n)$ only runs over the first $N_A(N_B)$ values (the remaining values corresponding to the other fiducial projectors).

Now consider the N_B dimensional subspace with basis states $|1\rangle \otimes |n\rangle$ ($n = 1\,to\,N_B$). This subspace corresponds to the case where system A is prepared in basis state 1 and system B is prepared in any state. A full set of fiducial projectors can be formed for this subspace. These will take the form $\hat{P}_1^A \otimes \hat{P}_l^B$ where $l = 1\,to\,K_B$ (i.e., runs over the all values, not just the basis labels). We can do the same for the case where basis state 2 is prepared at A. Then we have the fiducial projectors $\hat{P}_2^A \otimes \hat{P}_l^B$ for the subspace $2n$ ($n = 1\,to\,N_B$). Indeed, we can do this for the general case in which the basis state m is prepared at A. Now consider the pure state $\hat{P}_1^A \otimes \hat{Q}^B$ where $\hat{Q}^B$ is some arbitrary projector at B. This state is in the $1n$ ($n = 1\,to\,N_B$) subspace and we can perform the fiducial measurements $\hat{P}_1^A \otimes \hat{P}_l^B$ in this subspace to fully characterize this state. The probabilities obtained in making these fiducial measurements will be the same as if we prepared the state $\hat{P}_2^A \otimes \hat{Q}^B$ and made the fiducial measurements $\hat{P}_2^A \otimes \hat{P}_l^B$ and hence this corresponds to the same preparation at B. Hence, in general the projector $\hat{P}_m^A \otimes \hat{Q}^B$ corresponds to preparing the basis state $\hat{P}_m$ at A and the general pure state $\hat{Q}^B$ at B. Now consider the subspace spanned by the projectors $\hat{P}_m^A \otimes \hat{Q}^B$ ($m = 1\,to\,N_A$) in which we prepare $\hat{Q}^B$ at B. A fiducial set for this subspace is $\hat{P}_k^A \otimes \hat{Q}^B$ where $k = 1\,to\,K_A$. If these fiducial measurements are made on a state $\hat{R}^A \otimes \hat{Q}^B$ where $\hat{R}^A$ is a projector at A then we would get the same results as if the fiducial measurements $\hat{P}_k^A \otimes \hat{Q}'^B$ were made on the state $\hat{R}^A \otimes \hat{Q}'^B$. Hence, in both cases the preparation at A is the same. Thus, the pure state $\hat{R}^A \otimes \hat{Q}^B$ corresponds to the case where a particular pure state $\hat{R}^A$ is is prepared at A and the pure state $\hat{Q}^B$ is prepared at B. An analogous argument to that above can be used to show that, regarded as a measurement, the projector $\hat{R}^A \otimes \hat{Q}^B$ corresponds to measuring the joint probability with setting $\hat{R}$ at the end A and setting $\hat{Q}$ at end B. Applied to the fiducial projectors, $\hat{P}_k^A \otimes \hat{P}_l^B$, this proves our result.

14 New postulates for quantum theory

We give two sets of postulates, the first, which pick out the kinematical framework and the second, which specifies dynamics.

14.1 Definitions

We need a number of definitions, in most cases more information is found from Theories #1 and #2, from where these definitions are taken.

- The universe at a given time consists of a number of systems, S_I.
- Systems are labeled by their constituents and preparation.

  New systems can be formed from old systems in three ways.

- New systems can be formed by combinations of existing systems, or composition.
$$S_{12} = S_1 \cup S_2 \tag{153}$$
- Systems may also be prepared by projection, which is subjecting them to a filter that picks out a subset of possible measurement outcomes.
- Systems may also be altered by evolution in time, with or without external influences. This is also called transformation.

  Composition increases the set of possible outcomes of measurements, projection reduces it and evolution leaves the number fixed.

- **Capacity:** For a given system, there is a number N, called the capacity by, which is the number of possible outcomes of a given single measurement made on the system.
- **Degrees of freedom:** The minimal amount of information needed to completely determine the statistical distribution of outcomes of any experiment on the system is K real parameters.
- **Statistical state:** The state of a system S can be specified by a list of K probabilities, $\rho = (p_1, p_2, ..., p_K)$ which are complete in the sense that the probabilities of any measurement made on S can be computed from the p_a. The space of states, S_S is convex and compact, because

the probabilities are bounded by $0 \leq p_a \leq 1$. A state is a mixture if it can be written as a statistical mixture of two other states,

$$p_a = xp_a^1 + (1-x)p_a^2 \tag{154}$$

for a probability $0 \leq x \leq 1$. A state is pure if it cannot be so expressed.

- **Measurement** is a map $E : \rho \to R$ which corresponds to a possible experiment. A set of complete measurements is N measurements that suffice to pick out uniquely one of the N possible outcomes of a measurement.

14.2 Kinematical postulates for quantum theory

For the kinematical framework we work in the tradition of operational axioms for quantum theory pioneered by Hardy. We find it most useful to use a set of postulates proposed by Theory #1, which gives four postulates for quantum theory.

To emphasize the role of freedom in quantum physics I would like to propose a modification of their postulates which modify one and add one additional, so that we have the following system of five postulates.

- **Postulate1: Local tomography.** The state of a composite system AB is completely characterized by the statistics of measurements on the subsystems A and B.

- **Postulate2: Equivalence of subspaces.** Let S_N and S_{N-1} be systems with capacities N and $N-1$, respectively. If $E_1, ..., E_N$ is a complete measurement on S_N, then the set of states $\omega \in S_N$ with $E_N(\omega) = 0$ is equivalent to S_{N-1}. Physically this means that if two quantum systems of the same capacity are equivalent even if one arises by reduction from a larger system.

- **Postulate3: Symmetry.** For every pair of pure states $\omega, \phi \in S_A$, there is a reversible transformation T such that $T \cdot \omega = \phi$.

- **Postulate4: All measurements allowed.** All probability measures on S_2 (that is, maps from S_2 to the interval $[0, 1]$ are outcome probabilities of possible measurements.

- **Postulate5: The principle of maximal freedom.** The amount of information needed to predict the statistical distribution of outcomes of any experiment on a system S should be as large as possible, given N. Thus, K should increase with N by a fixed function, which grows as fast as possible, consistent with the other axioms.

We note that Postulates 1 to 4 are given by Theory #1. Note that we use a version of Postulate 3 that does **not** specify the transformations are continuous. The only thing new is the fifth postulate. The fact that these five postulates together pick out quantum theory uniquely follows trivially from Theorem 1 of Theory #1 which asserts that the first four postulates have two realizations, classical probability theory and quantum theory. Postulate 5 then trivially picks out quantum theory, for which $K = N^2 - 1$ over classical probability theory for which $K = N$.

14.3 Dynamical postulates for quantum theory

We begin by postulating a real ensemble within which probabilities for quantum systems are defined as relative frequencies.

- **Definition:** The *precedents* of a quantum system S is the ensemble, $E(S)$ of systems with the same constituents and preparation (including transformations) in the past. The ensemble of *precedents of a measurement*, M, consists of copies of the processes with the same constituents, preparation and measurement in the past. $M(E, S)$ is the ensemble of outcomes of these measurements.

  We also need to specify how the formalism applies to experiment. This is through a

- **Principle of correspondence:** The statistical state ρ of a quantum system, S, is a description of the ensemble of its precedents. It is measured by constructing an ensemble and measuring the probability distributions of the outcomes of K distinct experiments on them.

  Now we are ready to state the dynamical principle of quantum physics.

- **Postulate 6: Precedence:** The outcome of a measurement, M, on a system, S, is a randomly chosen member of $M(E, S)$, the ensemble of outcomes of past instances of that measurement on identically prepared systems, in the case that the number of such precedents is large.

What if a system has no precedents? This can occur if an entangled state is formed for the first time. Then it is a novel state and we apply

- **The principle of freedom in the absence of precedent:** A quantum system, S, may have no precedent. Then the outcome of a measurement M on it is not determined by any prior knowledge of the state of the universe.

A system may have aspects that have precedence without being determined totally. For example, the possible outcomes of a measurement on a novel system are still constrained by symmetries. They are also constrained by the conservation laws that follow from symmetries including energy.

What happens in between, when the number of precedents is non-zero but small. This requires a novel principle, about which I only have a few preliminary remarks to offer in the next section. A question we can answer now is how many instances are necessary to go between the principle of freedom and the principle of precedence? We note that K is a measure of how many precedents are necessary before the statistical distributions of the outcome of any experiment are determined. Hence, K is a measure of the freedom of quantum systems. This is specified by postulate 5.

This means that quantum systems are maximally free because a maximal number of prior cases is needed to establish enough precedence to predict as we as can be done the result of any measurement. To put this another way, it takes a maximal amount of information to be able to predict or foresee how the system will respond to anything it might encounter.

The fact that K is large compared to N reflects the fact that a density matrix, which could arise as the description of the state of a subsystem entangled within a larger system, requires much more information to specify, then a pure state. This means that there are many more ways a system may be entangled within a larger system than can be distinguished by a single measurement. This accords a great freedom to quantum systems because it means that they can have properties that are only expressed by measuring statistical distributions over many repeated experiments. Our result means that quantum mechanics is the case where this freedom is maximal given a set of reasonable axioms.

15 How precedence builds up

The action of the principle of precedence has to be restricted to cases in which the number of precedents of a measurement is large. Otherwise, the first result with no precedence would be chosen randomly and that result would be the sole precedent for the second result, which would imply that all future measurements would repeat the first random choice. To avoid this a different principle is required while the precedents build up an ensemble which fills out the elements of a density matrix. One intriguing suggestion is that nature tries to induct from the first randomly chosen results the simplest possible rule. This can be understood as saying that it is more efficient for nature to store a simple rule to generate the ensemble of outcomes than it is to store the whole ensemble of outcomes itself. This leads to a hypothesis that nature chooses the simplest rule, in the sense of algorithmic information theory, which accounts for the first small number of precedents. Such a principle of a simplest rule contrasts interestingly with the principle that the state requires as much information as possible to specify.

This suggests that the laws of nature are the result of a minimalization, not of an action, but of the information needed to express a rule that propagates future cases from past cases. So rather than a principle of least action we will formulate dynamics as a principle of least information.

There is of course a difficulty with the idea that the laws of nature are as simple as possible, which is that they aren't. Free theories are simpler than interacting theories because it takes less information to specify linear laws then it does non-linear laws. But a linear world would have no interactions and so no relations to define properties of subsystems. So perhaps the principle that the world is relational forces it to be interacting. Then we require the simplest possible non-linear law. That is easy to satisfy: the simplest non-linear equations are quadratic. Remarkably, both general relativity and Yang-Mills theory can be expressed as quadratic equations through Plebanskis trick of adding auxiliary variables. This basically follows from the fact that gauge couplings modify linear field equations by the addition of a quadratic term coupling matter with the gauge field. Further, it is possible to conjecture that there may be a universal expression which unifies interacting gauge and gravitational theories, in which the fundamental dynamics expressed by a quadratic law. We can also consider the hypothesis that the

state and the dynamical law are unified at a fundamental level, in such a way that the distinction between them is emergent and approximate. From this perspective the law that must be minimal is the one that evolves the state and dynamics together(see later).

16 Discussion

This proposal shows that, at the very least, we do not need to postulate timeless laws of nature to explain the success of physics as a predictive science. A weaker notion in which laws evolve through the accumulation of precedence suffices. The important thing is that this idea is testable, by the construction and study of entangled quantum states which are novel in the sense that they can reasonably be presumed not to have been produced in the history of the universe. If one can construct such states, one can study their evolution and possibly observe the evolution of novel precedents.

One can ask whether the freedom quantum systems have described here means that hidden variables theories are impossible? The answer is no, nothing could contradict the possibility of non-local, context dependent, hidden variables theories because several examples already exist, such as deBrogle-Bohm. We have been concerned here with quantum mechanics as a description of small subsystems of the universe. There could very well be a non-quantum theory that describes the whole universe, truncations of which to small subsystems yield quantum mechanics. The freedom attributed to quantum systems could then be understood as being determined by information about the relations of subsystems to the whole which is lost when one truncates the cosmological theory to extract the behavior of small subsystems.

Someone might object that this interpretation of quantum theory takes the notion of copy, or similar preparation or measurement, as a primitive. This is true. But one should not have to apologize for the use of such primitives in an operational approach to quantum mechanics which, otherwise, takes notions of measurement to be primitives. One might however, still ask how a system knows what its precedents are? This is like asking how an elementary particle knows which laws of nature apply to it. The postulate that general timeless laws act on systems as they evolve in time requires a certain set of metaphys-

ical presuppositions. The hypothesis given here, that instead systems evolve by copying the responses of precedents in their past, requires a different set of metaphysical presuppositions. Either set of presuppositions can appear strange, or natural, depending on ones metaphysical preconceptions. The only scientific question is which sets of metaphysical preconceptions lead to hypotheses which are confirmed by experiment.

An important part of any package of metaphysical presuppositions is the relationship of laws of nature to time. A timeless law cannot refer explicitly to the present or past, because those are thought to be subjective distinctions. The formulation of quantum mechanics proposed here refers explicitly to the past and present and so only makes sense within a framework in which the distinctions between past, present and future are held to be real and objective. This makes it possible to discuss objectively notions of laws evolving in time.

Finally, some will ask whether there are any implications for whether human beings or animals have freedom to make choices not completely determined by the past. This might arise by the generation of novel entangled states in neural processes. Of course, allowing the possibility for novelty is not sufficient. What would be necessary to realize the idea would be to discover that the outcomes of neural processes are influenced by quantum dynamics of large molecules with entangled states, so that the lack of determinism of quantum processes is reflected in human choices and actions. This could very easily fail to be the case. Resolving this kind of question remains a goal for the future.

17 Unification of the state with the dynamical law

17.1 Introduction

Physics has for most of its history been primarily concerned with finding out what the laws of nature are. While we still do not have a completely unified theory of physics, our understanding of the laws of nature has advanced to the point where we are not only interested in what the laws are, but why these are the laws, and not others. This problem has become urgent since

the discovery of the landscape of string theories. The hope that a theory that unifies gravity and the standard model of particle physics would be unique, in a way that leads to unique predictions for beyond the standard model physics, seems difficult to sustain in the face of a vast or infinite number of apparently equally consistent string vacua. Even if one is not confident that string theory is the right framework for unification, no framework has appeared which would answer the why these laws question.

The realization that we would sooner or later have to explain how and why the laws we observe governing our universe were chosen is not new. The issue was emphasized by John Wheeler, but the concern is much older and goes back to Leibnizs Principle of Sufficient Reason. As the American pragmatist philosopher Charles Sanders Pierce wrote in 1893, nothing is so needing of rational explanation than laws of nature. Pierce goes on to say,

> To suppose universal laws of nature capable of being apprehended by the mind and yet having no reason for their special forms, but standing inexplicable and irrational, is hardly a justifiable position. Uniformities are precisely the sort of facts that need to be accounted for. Law is par excellence the thing that wants a reason. Now the only possible way of accounting for the laws of nature, and for uniformity in general, is to suppose them results of evolution.

In contemporary work, all the present attempts to understand how laws may have been chosen from a landscape of possible laws evoke, in one way or another, the notion that the effective low energy laws change on cosmological time scales. This includes eternal inflation and cosmological natural selection. It is notable that both require a notion of time to give meaning to the evolution of effective laws. In cosmological natural selection a time is required to count generations and give sense to an ensemble of universes on the landscape at a fixed time, in eternal inflation it appears necessary to impose a measure which is related to a notion of time on the multiverse.

There is a view that laws have to evolve in a physically real, non-emergent time, in order to have a scientific explanation of why these laws. This discussion explores a suggestion made in these views, which is that the evolution of laws implies a breakdown of the distinction between law and state. Another way to say this is that there is an enlarged notion of state - a metastate - which codes information needed to specify both an effective law and an ef-

fective state, that the effective law acts on. The whole metastate evolves in time, and the distinction between effective law and effective state can only be made for certain time scales. How long these time scales are, as well as the effective laws, are determined by the initial metastate. The effective laws evolve with the state, but they evolve slowly, compared to other information captured by the state.

Hence, on short time scales, and to a certain approximation, one can distinguish a slowly varying effective law which generates faster evolution of an approximate state. On longer time scales the more precise picture is that there is a notion of a meta-state, which codes both the effective law and the effective state.

The purpose of this discussion is to present a simple matrix model where this idea is realized. But in realizing this idea we have to confront an issue that arises in any scenario in which laws of physics evolve. In both cosmological natural selection and eternal inflation there is posited a dynamical mechanism whereby a population of regions of the universe with different laws evolves, giving rise to an evolving distribution on a landscape, or space of laws, $\mathcal{L}$. The evolution of laws on the landscape is then driven by a *metalaw*. Even if not precisely specified, this metalaw becomes a key part of the explanation of why these laws.

In the case of cosmological natural selection, the metalaw is approximate and effective and involves small random changes in the parameters of the standard model. This is analogous to an effective dynamics for evolution of phylogeny in biology. In the case of eternal inflation the metalaw is tunneling from false vacua with amplitudes given by string theory.

However, these scenarios have a weak point. The postulation of metadynamics on the landscape is a scientific hypothesis. How is it to be justified? If there is no principle which determines the law, it is not likely there will be a principle which determines the metalaw. And how is the proposed metalaw to be tested? One can easily imagine different hypotheses for the action of metalaws on the spaces of observable parameters. How are these to be compared, when we see in our past at best one instance of the metalaws acting? Someone may claim that the evolution on the landscape is driven by some fundamental version of string theory. Someone else may claim the evolution

on the landscape is fundamentally stochastic (and why not - so is quantum theory?) and driven only by a simple set of rules. How are we to determine scientifically which is right?

Worse, we may have to postulate some metalandscape of metalaws on which a meta-meta-law acts to govern the choice of the metalaw. There is clearly a danger of an infinite regress here.

On the other hand, if one does not specify a metalaw one explains nothing. We call this the *metalaws dilemma*.

It is important to have a precise idea of what is going wrong when we encounter this kind of dilemma. Normally in physics we specify a theory in two steps. First we specify the configuration or a phase space, $\mathcal{C}$, which is a timeless space of possible configurations a system may have at one time. Then we specify the laws of motion, which generates the possible lawful trajectories of the system on $\mathcal{C}$. If we append to this the landscape of possible laws we have two timeless configuration spaces: that of configurations and that of laws.

This formulation of laws of nature can be called the Newtonian paradigm because it is the basic framework of laws of motion introduced by Newton. The Newtonian paradigm is also the framework for modern quantum mechanics, quantum field theory, and general relativity. In each case there is a timeless space of states acted on by a timeless law.

The Newtonian paradigm is the proper setting for most of physics, which concerns small subsystems of the universe. But when we attempt to scale it up to a description of the universe as a whole it leads to unanswerable questions such as why these laws and not others and what caused the initial conditions. No theory formulated within the Newtonian paradigm can answer these questions because it takes the laws and initial conditions as inputs. When we attempt to invent a theory of evolution on a landscape of theories, but stay within the Newtonian paradigm, we end up with puzzles and paradoxes.

Part of the problem is the following. The Newtonian paradigm is based on a strict separation of the roles of law and initial conditions. This is justified by the fact that we can operationally distinguish the influence of the choice of

laws from the choice of initial conditions, by doing experiments many times varying the initial conditions. Operationally, what we mean by a law is some feature of the evolution which is invariant or conserved when we vary the initial conditions. So the experimental context that gives meaning to theories formulated in the Newtonian paradigm is the study of small subsystems of the universe, where we can repeat an experiment as many times as needed.

In cosmology there is only a single history, so we lose the ability to do an experiment over and over again, while varying the initial conditions. So we have no operational way to absolutely distinguish the influence of the choice of laws from the choice of initial conditions. When we attempt to impose the Newtonian paradigm on the interpretation of cosmological data, and ask questions that assume a strict separation between the role of law and the role of initial conditions, we end up asking confused questions that have no clear answers.

We call this running into the *cosmological fallacy*, which is the mistake of extending a method that is designed to study small subsystems of the universe that come in many copies to the universe as a whole. To usefully apply a theory in the Newtonian paradigm to a system we require data from many repetitions of an experiment to give operational meaning to its basic terms, and in particular, to separate out the role of laws from initial conditions. But in the cosmological case, the data does not allow that distinction to be made (The multiverse seems at first to be a way to avoid this, because it makes our universe one out of many and so appears to reproduce the context needed to make sense of the separation between law and initial condition. This however, cannot succeed so long as we have no data about the other universes, because there is still no operational basis for the distinction between law and initial conditions. The only exception, is special cases where each universe in the ensemble shares a property - then one can check the theory by seeing if our universe has that property. This is the strategy of cosmological natural selection. It also leads to a single prediction for eternal inflation, which is that all universes in the multiverse have $k =?1$).

It is probably wiser to not impose a paradigm for dynamical law on the cosmological data that is based on a distinction that cannot be made within that data. That is, once we lose the ability to distinguish the role of law and initial conditions in the data, because we have just one case in cosmology, we

are probably going to make more progress if we search for a framework for physical theory that does not rely on the distinction between law and initial condition being absolute.

What is then needed is a new paradigm for dynamics on a cosmological scale. In this new framework, the absolute distinction between laws and states, or laws and initial conditions, which underlies the Newtonian paradigm can be transcended. That distinction will be seen to be an artifact of descriptions of small subsystems of the universe, and breaks down on cosmological time scales. The challenge is to introduce such a framework without falling into a vicious circle or the metalaws dilemma. The purpose of this discussion is to explore one possible form that such a new approach to cosmological dynamics may take.

A possible resolution to these conundra is that there could be a notion of universality of metalaws, analogous to universality in the theory of computation. The idea is that any metalaw which could serve as such is equivalent to any other. Computation is universal because any computer can emulate any other exactly. We could propose that any metalaw worthy of that name can emulate any other, because they will lead to the same predictions for the evolution of laws.

In this discussion, however, we propose a model for an approach to the metalaws dilemma, which is that the distinction between states and laws breaks down. This new proposal is realized in a simple matrix model. Instead of timeless law determining evolution on a timeless space of states, we have a single evolution which cannot be precisely broken down into law and state. Formally, what this means is to embed the configuration space of states, $\mathcal{C}$ and the landscape parameterizing laws, $\mathcal{L}$ into a single meta-configuration space, $\mathcal{M}$. The distinction between law and state must then be both approximate and dependent on initial conditions.

There is, it must be granted, an evolution rule on $\mathcal{M}$, but we can choose an evolution rule that is almost entirely fixed by some natural assumptions. The remaining freedom is, we conjecture, accounted for by the principle of universality, as just described. Because the complexity of the effective law is now coded into the state, the meta-law can be very simple, because all it has to do is to generate a sequence of matrices, in which the differences from one

to the next are small. The metalaw dilemma is addressed by showing that the form of this rule is almost completely fixed by some natural assumptions, with the remaining freedom plausibly accounted for by universality.

In this model of a metatheory, the metastate is captured in a large matrix, X, which we take to be antisymmetric and valued in the integers. It might describe a labeled graph. The metalaw is a simple algorithm that yields a sequence of matrices, X_n. The rule is that X_n is gotten by adding to a linear combination of $X_{n?1}$ and $X_{n?2}$ their commutator $[X_{n?1}, X_{n?2}]$. Given the first two matrixes, X_0 and X_1, the sequence is determined. This is more like a simple instruction in computer science than a law of physics, and we are able to argue it is almost unique, given a few simple conditions.

That almost unique evolution rule acts on a configuration space of matrices, whose interpretation depends on a separation of time scales. For certain initial configurations - there will be a long time scale, T_{Newton} such that, for times shorter than T_{Newton}, the dynamics can be approximately described by a fixed law acting on a fixed space of states. Both that law and that state are coded into the X_n. But for longer times everything evolves, laws and states together, and it is impossible to cleanly separate what part of the evolution is changes in law and what part is changes in state. Furthermore, which information in $\mathcal{M}$ evolves slowly, and goes into the specification of the approximate time independent law, and which evolves fast, and goes into the description of the time dependent state, is determined by the initial conditions.

So the question of *why these laws* becomes subsumed into the question of *why these initial conditions* in a metatheory. This does not yet solve the problem of explaining the particular features of the standard model and its parameters, but it gives a new methodology and strategy with which to search for the answer.

Starting from the standard model, one might move in the direction of a metatheory by elevating all parameters to degrees of freedom. This is something like what happens in the string landscape. Here we make a simple model in which the meta-state is a large sparse matrix, perhaps representing the connections on a graph.

In the next section we describe a simple model which illustrates these ideas and show how it leads, for short time scales, to an approximate distinction between an effective law which governs the evolution of a state.

17.2 A minimal evolution rule

We are interested in the most minimal evolution rule we can imagine which combines the theory and the state. Let us specify the meta-state by an $N \times N$ antisymmetric matrix of integers, $(X_n)_{ab} = -(X_n)_{ba}$. We will consider the dimension N to be large. The n refers to a succession of times, $n = 0, 1, 2, ...$ also labeled by integers. $(X_n)_{ab}$ might be taken to describe an adjacency matrix of a weighted, directed, graph, whose edges are labeled by integers. This accords with the expectation that the fundamental variables in physics be relational.

The idea is that there will be an evolution rule which specifies the series of matrices, given initial choices. The choice of this evolution rule is fixed by the following ideas.

1. The evolution rule should mimic second order differential equations, as these are basic to the dynamics of physical systems. So two initial conditions should be required to generate the evolution. We should then need to specify X_0 and X_1 to generate the sequence. We are then interested in rules of the form.

$$X_n = \mathcal{F}(X_{n-1}, X_{n-2}) \tag{1}$$

2. The changes should be small from matrix to matrix, at least given suitable initial conditions. This is needed so that there can be a long time scale on which some of the information in the matrixes are slowly varying. This makes it possible to extract a notion of slowly varying law, acting on a faster varying state. So we will ask that

$$X = \mathcal{F}(X, X) \tag{2}$$

3. We require that the evolution rule be non-linear, because non-linear laws are needed to code interactions in physics. But we can always use the basic trick of matrix models of introducing auxiliary variables, by expanding the matrix, in order to lower the degree of non-linearity. This

accords with the fact that the field equations of general relativity and Yang-Mills theory can, by the use of auxilary variables, be expressed as quadratic equations(for example in the Plebanski action). The simplest non-linear evolution rule will then suffice, so we *require a quadratic evolution rule.*

4. Time reversal invariance, at least at the linear level.

A simple evolution rule that realizes these is

$$X_n = 2X_{n-1} - X_{n-2} + [X_{n?1}, X_{n?2}] \tag{3}$$

This rule is not unique, but it is nearly so. It is easy to derive the general rule satisfying the four requirements just mentioned.

The rule (1) can only have a linear term and a quadratic term. The quadratic term must be a function of X_{n-1} and X_{n-2} that vanishes when they are equal and is antisymmetric. The unique term that does this is the commutator $[X_{n?1}, X_{n?2}]$. When the commutator vanishes there is only a linear term which by (2) must be equal to a linear integral combination of X_{n-1} and X_{n-2}. The general evolution rule satisfying the first three requirements is then

$$X_n = aX_{n-1} + (1-a)X_{n-2} + g[X_{n?1}, X_{n?2}] \tag{4}$$

where a and g must be integers to keep the coefficients of X_n integers.

We pick $a = 2$ and $g = 1$ to get (3). The justification for the choice of the linear term is time reversal invariance. With this choice (3) can be written as

$$\Delta^2 X_n = X_n + X_{n-2} - 2X_{n-1} = [X_{n?1}, X_{n?2}] \tag{5}$$

The linear term, $\Delta^2 X_n$ s invariant under a time reversal transformation around a time $n-1$, given by

$$X_{n-1+\hat{a}} \leftrightarrow X_{n-1-\hat{a}} \tag{6}$$

under which $\Delta^2 X_n \to \Delta^2 X_n$.

The whole dynamics is approximately invariant under a related transformation $X_{n-1+\hat{a}} \leftrightarrow -X_{n-1-\hat{a}}$. An exactly time invariant version of dynamics would be $X_n = 2X_{n-1} - X_{n-2} + [X_n, X_{n?2}]$, but this is much harder to evolve.

Here is a way to understand how state and law are combined under this evolution rule. Let us call the *Hamiltonian at time n*,

$$H_n = X_{n-2} \tag{7}$$

and define the *state at time n* to be

$$\rho = X_n - X_{n-1} \tag{8}$$

We can define the rate of change of the state as

$$\Delta\rho_n = \rho_n - \rho_{n-1} = \Delta^2 X_n \tag{9}$$

Then the evolution rule (3) is expressed as

$$\Delta\rho_n = [\rho_{n-1}, H_n] \tag{10}$$

Thus it appears that the matrix we call H_n is generating evolution on the state called ρ. Another equivalent way to express the evolution is

$$\Delta^2\rho_n = [\Delta\rho_{n-1}, X_{n-2}] \tag{11}$$

17.2.1 Quasi-Hamiltonian evolution

Equations (9,10) holds at all time steps. But this is not really Heisenberg evolution because the operator we are calling the Hamiltonian evolves as the state evolves. But, as we will now show, if we choose the initial conditions so ρ is in a certain sense small compared to H, then the H evolves more slowly than ρ and so for short times it appears as if the state is evolving with respect to a fixed Hamiltonian, so that (8,10) are, for a finite time, well approximated by a Heisenberg-like equation of motion,

$$\Delta\rho_n = [\rho_{n-1}, H_0] \tag{12}$$

To show this we introduce a norm on matrices $\|X\|$ which is equal to the number of non-zero entries. Then, if $p(X)$ is the probability that a matrix element is non-zero, then

$$p(X) = \frac{\|X\|}{N(N-1)/2} \tag{13}$$

Pick an arbitrary time and call it $n = 0$. Call

$$X_0 = H_0 \quad , \quad \rho_1 = A \tag{14}$$

Then define

$$\dot{A} = [A, H_0],\ \ddot{A} = [\dot{A}, H_0],\ \cdots\ A^{(p)} = [A^{(p-1)}, H_0] \tag{15}$$

17.2.2 The first steps

Let us follow the first few steps of evolution

$$\begin{aligned}
X_0 &= H_0 & \rho_1 &= A \\
X_1 &= H_0 + A & \rho_2 &= A + \dot{A} \\
X_2 &= H_0 + 2A + \dot{A} & \rho_3 &= A + 2\dot{A} + \ddot{A} + [\dot{A}, A] \\
X_3 &= H_0 + 3A + 3\dot{A} + \ddot{A} + [\dot{A}, A] & \rho_4 &= A + 3\dot{A} + 3\ddot{A} + A^{(3)} + [\dot{A}, A] \\
& & & \quad + [\ddot{A}, A] + [2\dot{A} + \ddot{A} + [\dot{A}, A], 2A + \dot{A}] \\
X_4 &= H_0 + 4A + 6\dot{A} + 4\ddot{A} + A^{(3)} & & \\
& \quad + 2[\dot{A}, A] + [\ddot{A}, A] & & \\
& \quad + [2\dot{A} + \ddot{A} + [\dot{A}, A], 2A + \dot{A}] & & \qquad (16)
\end{aligned}$$

Clearly terms are rapidly proliferating. To make sense of them, begin by noting that there are two kinds of terms in the ρ_ns. First there are terms that involve single powers of $A^{(p)}$. These come from commutators with H_0 and can be considered to be the effect of evolution with a fixed hamiltonian, H_0. Then there are terms involving commutators of two or more $A^{(p)}$. These register the effect of the changing evolution law. As we will now show, there are natural choices of H_0 and A such that the latter remain unimportant for a large number of time steps.

17.2.3 Norms and probabilities

Let us pick $X_0 = H_0$ to be a random matrix chosen from the ensemble with

$$p(H_0) = \frac{1}{N} \qquad (17)$$

so that it corresponds to the critical region in random graph theory of a graph which is minimally connected. Then

$$\|H_0\| = N \qquad (18)$$

We will pick A to have a norm of order unity, so that X_1 differs from $X_0 = H_0$ by just a few entries or links. Then

$$\|A\| = M \in O(1) \quad \text{so that} \quad p(A) \approx \frac{M}{N^2} \qquad (19)$$

Let us assume that there are no further correlations between H_0 and A so that,

$$p(\dot{A}) = Np(A)p(H_0) \approx \frac{M}{N^2} \tag{20}$$

so that

$$\|\dot{A}\| \approx M \tag{21}$$

It then follows that all the

$$\|A^{(p)}\| \approx M \tag{22}$$

Notice that because these $A^{(p)}$ are so sparse

$$p([A, \dot{A}]) = p([A^{(p)}, A^{(q)}]) = np(A)^2 = \frac{M}{N^3} \tag{23}$$

Hence the norm of these commutators is

$$\|[A^{(p)}, A^{(q)}]\| = \frac{M}{N} \ll 1 \tag{24}$$

This means that there are no entries in most of these commutators.

17.2.4 Breakdown of the distinction between law and state

Now after n evolution steps we will have a time dependent Hamiltonian $H_n = X_{n-2}$ of the form

$$H_n = H_0 + \delta H_n \tag{25}$$

where the time dependent part has the form,

$$\delta H_n = \delta H_n(M) + \delta H_n(M^2) + \cdots \tag{26}$$

where (M^p) signifies the terms of order M^p. The leading term collects terms of order M which come from commutators of the form $[A^{(p)}, H_0]$.

$$\delta H_n(M) = \sum_{p=1}^{n-3} c_p A^{(p)} \tag{27}$$

Here the c_p are integer coefficients.

Any one of the $A^{(p)}$ terms likely has no effect on the evolution of the ρ's,

but there are n of them so δH_n will start to be significant when n is large enough. Hence, ignoring the $O(M^2)$ terms, we have

$$p(\delta H_n(M)) = mN\frac{M}{N^2}\frac{1}{N} = \frac{nM}{N^2} \tag{28}$$

These will be negligible compared to the terms in H_0 if

$$\frac{p(\delta H_n(M))}{p(H_0)} = \frac{nM}{N} < 1 \tag{29}$$

so the approximation in which we neglect the terms in $\delta H_n(M)$ is good as long as

$$n < \frac{N}{M} \tag{30}$$

We can reach the same conclusion by computing the ratio of $p(A^{(p)})$ to $p([A^{(p)}, A^{(q)}])$.

Similarly we can compute the importance of the order M^2 terms in δH_n. These come from commutators of the form $[A^{(p)}, A^{(q)}]$. Any one of these is most likely vanishing, but ?there are n^2 of them.

We have

$$p(\delta H_n(M)) = n^2 N\left(\frac{M}{N^2}\right)^2 = \frac{n^2M^2}{N^3} \tag{31}$$

These can be neglected relative to the entries in H_0 so long as

$$\frac{p(\delta H_n(M^2))}{p(H_0)} = \frac{n^2M^2}{N^2} < 1 \tag{32}$$

which leads us to the same condition (30). Indeed, the order M^q terms in δH_n comes from ??$q-1$ commutators of factors $A^{(p)}$ for $p < q$, so these have probabilities

$$p(\delta H_n(M^q)) = n^q N^{q-1}\left(\frac{M}{N^2}\right)^q = \frac{n^qM^q}{N^{q+1}} \tag{33}$$

These are each negligible compared to the matrix elements of H_0 so long as (30) holds. One can also show this for the sum (26). Assuming the matrices are random so that the commutators are uncorrelated in the limit of large N

we can write,

$$\begin{aligned} p(\delta H_n) &= p(\delta H_n(M)) + p(\delta H_n(M^2) + \cdots) \\ &= \frac{1}{N}\left\{\frac{nM}{N} + \left(\frac{nM}{N}\right)^2 + \cdots\right\} \\ &< \frac{1}{N}\left\{\sum_{q=1}^{\infty}\left(\frac{nM}{N}\right)^q\right\} = \frac{1}{N}\frac{\frac{nM}{N}}{1-\frac{nM}{N}} \end{aligned} \tag{34}$$

Hence

$$\frac{p(\delta H_n)}{p(H_0)} < \frac{\frac{nM}{N}}{1-\frac{nM}{N}} \tag{35}$$

which is small so long as (30) holds. This means that the Hamiltonian evolution law (12) is a good approximation to the exact dynamics so long as (30) holds.

17.3 Conclusions

In the introduction of this discussion we argued for that a cosmological theory must be formulated in a way in which the usual distinction between dynamics and state, or between kinematics and dynamics, breaks down. In the rest of this discussion we illustrated these ideas with a simple toy model. In it we addressed the problem of what determines the meta-law by which effective laws evolve by specifying four simple properties that almost completely determine it. We conjecture that the remaining freedom is unimportant, because there may be a principle of universality among the remaining choices, in the sense that the predictions made by each of them can be mapped to each other.

There remain of course open questions, among which are to demonstrate this conjecture of universality.