Representing two binary repeatable measurements on Hilbert space

Tobias Fritz

Max Planck Institute for Mathematics

`fritz@mpim-bonn.mpg.de`

August 18, 2009

Abstract

When do measurements have a quantum-mechanical model? This article this kind of inverse problem for iterated measurements in quantum mechanics and presents a solution of the simplest non-trivial case. Before that, preliminary observations on pre- and postselection reveal some unexpected properties of quantum-mechanical probabilities, which might potentially be tested in experiments. Then, the simplest non-trivial case of the inverse problem, corresponding to two binary repeatable measurements, is analyzed and solved using methods from operator algebras and the theory of moment problems. Also, the quantum region is studied in some truncations. After that, it is shown that the general probabilistic region spans the whole space of probabilities. This undermines the fact that quantum theories are a very special type of general probabilistic theories. The article ends with some remarks on the complexity of the general inverse problem for quantum measurements and an outline of some properties that potential experimental tests of the quantum constraints should have.

1 Introduction

Consider the following situation: an experimenter works with some fixed physical system whose theoretical description is assumed to be unknown. In particular, it is not known whether the system obeys the laws of quantum mechanics or not. Suppose now that the experimenter can do two different types of measurement a and b, each of which has the possible outcomes 0 and 1. In this article, such as system will be referred to as the "black box fig. 1".

The experimenter can conduct several repeated measurements on the same system – like first a, then b, then again a – and also he can conduct many of these repeated measurements on independent copies of the original system by hitting the "`Reset`" button and starting over. In this way, he will obtain his results in terms of estimates for probabilities of the form

$$P_{a,b,a}(1,0,0) \tag{1}$$

which stands for the probability of obtaining the outcomes 1, 0, 0, given that he first measures a, then b, and then again a.

Figure 1: A black box with two binary measurements and an initialization button.
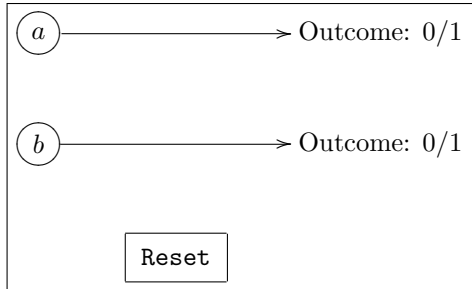
Now suppose that the experimenter finds out that the measurements a and b are always repeatable, in the sense that measuring twice consecutively yields identical results with certainty. In his table of experimentally determined probabilities, this is registered by statements like $P_{b,a,a,b}(0, 1, 0, 0) = 0$.

In a quantum-mechanical description of the system, the repeatable measurements a and b will each be represented by projection operators on some Hilbert space $\mathcal{H}$ and the initial state of the system is given by some state on $\mathcal{H}$; it is irrelevant whether this state is assumed to be pure or mixed, since both cases can be reduced to each other: every pure state is trivially mixed, and a mixed state can be purified by entangling the system with an ancilla. In any case, the probabilities (1) can be calculated from this data by the usual rules of quantum mechanics.

Question 1.1. Which conditions do these probabilities $P.(\cdot)$ have to satisfy in order for a quantum-mechanical description of the system to exist?

Mathematically, this is a certain moment problem in noncommutative probability theory. In its solution, I have tried to be as rigorous as possible. Physically, the constraints turn out to be so unexpected that an intuitive explanation of their presence seems out of reach.

Summary. This article is structured as follows. Section 2 begins by generally studying a binary quantum measurement under the conditions of pre- and postselection. It is found that both outcomes are equally likely, provided that the postselected state is orthogonal to the preselected state. Section 3 goes on by settling notation and terminology for the probabilities in the black box fig. 1 and describes the space of all outcome probability distributions for such a system. The main theorem describing the quantum region within this space is stated and proven in section 4, the largest part of which is solely devoted to the theorem's technical proof; some relevant mathematical background material on moment problems can be found in the appendix A. Section 5 then studies projections of the space of all probabilities and mentions some first results on the quantum region therein; this would mostly be relevant for potential experimental tests. Section 6 goes on by proving that every point in the whole probability space has a model in terms of a general probabilistic theory. As described in section 7, determining the quantum region for a higher number of measurements or a higher number of outcomes should be expected to be very hard. Section 8 mentions some properties that experiments comparing quantum-mechanical models to different general probabilistic models should have. Finally, section 9 briefly concludes the article.

2

Notation and terminology. Quantum-mechanically, a binary repeatable measurement corresponds to a projection operator p. Its negation is written as $\bar{p} \equiv 1 - p$. In order to have a compact index notation for p and $\bar{p}$ at once, I also write $p^1 = p$ and $p^0 = \bar{p} = 1 - p$.

The Pauli matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

will be used in section 4 and in the appendix.

2 Preliminary observations

Before turning to the general case, this section derives some results about the iterated measurement a, b, a and reveals some unexpected constraints for quantum-mechanical models. One may think of the measurements of a in a, b, a as being pre- and postselection, respectively, for the intermediate measurement of b.

So to ask a slightly different question first, how does a general quantum-mechanical binary measurement b behave under conditions of pre- and postselection? Suppose we conduct an experiment which preselects with respect to a state $|\psi_i\rangle$, i.e. it conducts an initial measurement of the projection $|\psi_i\rangle\langle\psi_i|$ and starts over in case of a negative result, and postselects with respect to a state $|\psi_f\rangle\langle\psi_f|$, i.e. it conducts a final measurement of the projection $|\psi_f\rangle\langle\psi_f|$ and starts over from the beginning in case of a negative result. In between the pre- and the postselection, the experimenter measures the binary observable b. For simplicity, the absence of any additional dynamics is assumed.

This kind of situation only makes sense when the final postselection does not always produce a negative outcome, so that the conditional probabilities with respect to pre- and postselection have definite values. This is the case if and only if

$$\langle\psi_i|b|\psi_f\rangle \neq 0, \quad \langle\psi_i|(1-b)|\psi_f\rangle \neq 0,$$

which will be assumed to hold from now on; under the assumption of the following proposition, these two conditions are equivalent.

Proposition 2.1. *In the case that $\langle\psi_i|\psi_f\rangle = 0$, the two outcomes of b have equal probability, independently of any details of the particular quantum-mechanical model:*

$$P\left(b = 0 \;\middle|\; pre = |\psi_i\rangle, post = |\psi_f\rangle\right)$$
$$= \; P\left(b = 1 \;\middle|\; pre = |\psi_i\rangle, post = |\psi_f\rangle\right) = \frac{1}{2}$$

Note that such a binary quantum measurement would yield a perfectly unbiased random number generator.

Proof. The proof of proposition 2.1 is by straightforward calculation. Upon preselection, the system is in the state $|\psi_i\rangle$. The probability of measuring $b = 0$ and successful postselection is given by

$$
\begin{aligned}
|| \, |\psi_f\rangle\langle\psi_f|(1-b)|\psi_i\rangle||^2 &= \langle\psi_i|(1-b)|\psi_f\rangle\langle\psi_f|(1-b)|\psi_i\rangle \\
&= -\langle\psi_i|b|\psi_f\rangle\langle\psi_f|(1-b)|\psi_i\rangle \\
&= \langle\psi_i|b|\psi_f\rangle\langle\psi_f|b|\psi_i\rangle \\
&= || \, |\psi_f\rangle\langle\psi_f|b|\psi_i\rangle||^2
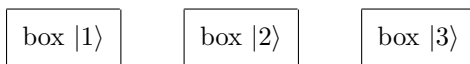\end{aligned}
$$

which equals the probability of measuring $b = 1$ and successful postselection. $\square$

For a concrete example, consider a quantum particle which can be located in either of three boxes $|1\rangle$, $|2\rangle$, and $|3\rangle$, so that the state space is given by

$$
\mathcal{H} = \mathbb{C}^3 = \text{span}\{|1\rangle, |2\rangle, |3\rangle\}
$$

Now let ζ be a third root of unity, such that $1 + \zeta + \zeta^2 = 0$, and use initial and final states as follows:

$$
\text{preselection: } |\psi_i\rangle = \frac{|1\rangle + |2\rangle + |3\rangle}{\sqrt{3}}
$$

$$
\boxed{\text{box } |1\rangle} \qquad \boxed{\text{box } |2\rangle} \qquad \boxed{\text{box } |3\rangle}
$$

$$
\text{postselection: } |\psi_f\rangle = \frac{|1\rangle + \zeta|2\rangle + \zeta^2|3\rangle}{\sqrt{3}}
$$

Then upon opening any box as the intermediate measurement and detecting presence of the particle will locate the particle in that box with a (conditional) probability of *exactly* $1/2$; see [AV07] for the original version of this three-boxes thought experiment, with even more counterintuitive consequences. Possibly such an experiment might be realized using quantum dots as boxes. And possibly a high-precision version of such an experiment – looking for deviations from the quantum prediction of exactly $1/2$ – might be an interesting further experimental test of quantum mechanics. In order to guarantee the crucial assumption of exact orthogonality of initial and final states, one could implement both pre- and postselection via the same von Neumann measurement and select for a final outcome differing from the initial outcome.

A similar calculation as in the proof of proposition 2.1 also shows that the following more general statement is true:

Proposition 2.2. *(a) Given an observable a together with two different eigenvalues $\lambda_0 \neq \lambda_1$ and a projection observable b, the outcome probabilities for b under $(a = \lambda_0)$-preselection and $(a = \lambda_1)$-postselection are equal:*

$$
P_b\left(0 \,\middle|\, a_{\text{pre}} = \lambda_0, a_{\text{post}} = \lambda_1\right) = P_b\left(1 \,\middle|\, a_{\text{pre}} = \lambda_0, a_{\text{post}} = \lambda_1\right) = \frac{1}{2}
$$

(b) The same holds true upon additional preselection before the first measurement of a, and also upon additional postselection after the second measurement of a.

What does this imply for quantum-mechanical models of the black box fig. 1? Given that one measures the sequence a, b, a such that the two measurements of a yield 0 and 1 respectively, then the two outcomes for b have equal probability:

$$\boxed{P_{a,b,a}(0,0,1) = P_{a,b,a}(0,1,1)} \tag{2}$$

Similar relations can be obtained form this equation by permuting $a \leftrightarrow b$ and $0 \leftrightarrow 1$. In words: given that the second measurement of a has a result different from the first, then the intermediate binary measurement of b has conditional probability $1/2$ for each outcome, no matter what the physical details of the quantum system are and what the initial state is. This is trivially true in the case that a and b commute: then, both probabilities in (2) vanish.

3 Probabilities for two binary repeatable measurements

In the situation of fig. 1, the repeatability assumption for both a and b has the consequence that it is sufficient to consider alternating measurements of a and b only. Therefore, all non-trivial outcome probabilities are encoded in the following two stochastic processes:

$$P_{a,b,a,\dots}(\dots)$$

and

$$P_{b,a,b,\dots}(\dots).$$

Both of these expressions are functions taking a finite binary string in $\{0,1\}^*$ as their argument, and returning the probability of that outcome for the specified sequence of alternating measurements. Since total probability is conserved, it is clear that for every finite binary string $r \in \{0,1\}^*$,

$$
\begin{aligned}
P_{a,b,a,\dots}(r) &= P_{a,b,a,\dots}(r,0) + P_{a,b,a,\dots}(r,1) \\
P_{b,a,b,\dots}(r) &= P_{b,a,b,\dots}(r,0) + P_{b,a,b,\dots}(r,1)
\end{aligned}
\tag{3}
$$

In the rest of this article, the probabilities $P_{a,b,a,\dots}$ will be denoted by P_a for the sake of brevity, while similarly P_b stands for the probabilities determining the second stochastic process $P_{b,a,b,\dots}$. A probability assignment for the P_a's and P_b's is called *admissible* whenever the probability conservation laws (3) hold.

4 Classification of probabilities in quantum theories

Now let us assume that the black box fig. 1 does have a quantum-mechanical description and determine the constraints that then hold for the probabilities P_a and P_b.

The final results are presented right now at the beginning, and the rest of the section is then devoted to showing how this theorem can be derived from the mathematical results presented in the appendix.

Given a binary sequence $r \in \{0,1\}^n$, denote the number of switches in r by $s(r)$, i.e. the number of times that a 1 follows a 0 or a 0 follows a 1. Similarly, $s(r, r')$ is the number of switches in the concatenated sequence r, r'. The single letter r and the sequence $r_1, \dots, r_n$ are interchangeable notation.

The overline notation $\bar{r}$ stands for the inverted sequene, i.e. $0 \leftrightarrow 1$ in r. The letter $\mathcal{C}$ denotes the convex subset of $\mathbb{R}^4$ that is defined and characterized in the appendix.

Theorem 4.1. *A quantum-mechanical description of the black box (1) exists if and only if the outcome probabilities satisfy the following constraints:*

- *$P_a(0, r_1, \ldots, r_n)$ only depends on $s(0, r)$; denote this value by*

$$P_a(0, r_1, \ldots, r_n) = F_{a,0}(n, s(0, r)) \quad \forall r.$$

- *$P_a(1, r_1, \ldots, r_n)$ only depends on $s(1, r)$; denote this value by*

$$P_a(1, r_1, \ldots, r_n) = F_{a,1}(n, s(1, r)) \quad \forall r.$$

- *$P_b(0, r_1, \ldots, r_n)$ only depends on $s(0, r)$; denote this value by*

$$P_b(0, r_1, \ldots, r_n) = F_{b,0}(n, s(0, r)) \quad \forall r.$$

- *$P_b(1, r_1, \ldots, r_n)$ only depends on $s(1, r)$; denote this value by*

$$P_b(1, r_1, \ldots, r_n) = F_{b,1}(n, s(1, r)) \quad \forall r.$$

- *The equation*

$$P_a(r) + P_a(\bar{r}) = P_b(r) + P_b(\bar{r})$$

holds for all r.

- *Using the notation*

$$
\begin{aligned}
F_{a,+}(n, s) &= F_{a,1}(n, s) + F_{a,0}(n, s) \\
C_1(n, s) &= \frac{1}{2} \left(F_{a,1}(n, s) - F_{a,0}(n, s) + F_{b,1}(n, s) - F_{b,0}(n, s) \right) \\
C_2(n, s) &= \frac{1}{2} \left(F_{a,1}(n, s) - F_{a,0}(n, s) - F_{b,1}(n, s) + F_{b,0}(n, s) \right),
\end{aligned}
$$

the inequality[1]

$$
\left(\sum_{k=0}^{\infty} (-1)^k \binom{1/2}{k} C_1(n + k - 1, s + k) \right)^2
$$
$$
+ \left(\sum_{k=0}^{\infty} (-1)^k \binom{1/2}{k} C_2(n + k - 1, s) \right)^2 \leq F_{a,+}(n, s)^2
$$

holds for every $n \in \mathbb{N}$ and $s \in \{1, \ldots, n - 1\}$.

- *Using the coefficients*

$$
c_{n,k} = \begin{cases}
(-1)^k \binom{-1/2}{k} & \text{for } k \leq n \\
(-1)^k \binom{-1/2}{k} - (-1)^{k-n} \binom{-1/2}{k-n} & \text{for } k > n
\end{cases}
$$

---

[1]Note that all sums are automatically absolutely convergent since $F_{\cdot, \cdot}(\cdot, \cdot) \in [0, 1]$ and $\sum_{k=0}^{\infty} \left| \binom{1/2}{k} \right| = 1 < \infty$.

and the quantities

$$V_{x,\pm}(n) = \sum_{k=0}^{\infty} c_{n,k} C_1(k,k)$$

$$\pm \sqrt{F_{a,+}(n,n)^2 - \left(\sum_{k=0}^{\infty}(-1)^k \binom{1/2}{k} C_2(n+k-1,n-1)\right)^2}$$

$$V_{z,\pm}(n) = \sum_{k=0}^{\infty} c_{n,k} C_2(k,0)$$

$$\pm \sqrt{F_{a,+}(n,0)^2 - \left(\sum_{k=0}^{\infty}(-1)^k \binom{1/2}{k} C_1(n+k-1,k)\right)^2},$$

the point in $\mathbb{R}^4$ given by

$$\left(\sup_n V_{x,-}(n),\ \sup_n V_{z,-}(n),\ \inf_n V_{x,+}(n),\ \inf_n V_{z,+}(n)\right) \tag{4}$$

has to lie in the convex region $\mathcal{C} \subseteq \mathbb{R}^4$ characterized in proposition A.2.[2]

To begin the proof of this theorem, let $\mathcal{A}_2 = C^*(a,b)$ be the C^*-algebra freely generated by two projections a and b. Then for every quantum-mechanical model of the system, we obtain a unique C^*-algebra homomorphism

$$\mathcal{A}_2 \longrightarrow \mathcal{B}(\mathcal{H})$$

which maps the universal projections to concrete projections on $\mathcal{H}$. Then upon pulling back the black boxes' initial state $|\psi\rangle$ to a C^*-algebraic state on $\mathcal{A}_2$, we can calculate all outcome probabilities via algebraic quantum mechanics on $\mathcal{A}_2$. Conversely, any C^*-algebraic state on $\mathcal{A}_2$ defines a quantum-mechanical model of the two binary observables system by virtue of the GNS construction. Therefore, we will do all further considerations on $\mathcal{A}_2$. In this sense, the states on $\mathcal{A}_2$ are the universal instances of quantum black boxes (1).

$\mathcal{A}_2$ is known [RS89] to be of the form

$$\mathcal{A}_2 \cong \{f : [0,1] \to M_2(\mathbb{C}) \mid f(0),\ f(1) \text{ are diagonal}\}$$

where the universal pair of projections is given by

$$a(t) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \frac{\mathbb{1}_2 + \sigma_z}{2}$$

$$b(t) = \begin{pmatrix} t & \sqrt{t(1-t)} \\ \sqrt{t(1-t)} & 1-t \end{pmatrix} = \frac{1}{2}\mathbb{1}_2 + \sqrt{t(1-t)}\,\sigma_x + \left(t - \frac{1}{2}\right)\sigma_z$$

By the Hahn-Banach extension theorem, the set of states on $\mathcal{A}_2$ can be identified with the set of functionals obtained by restricting the states on the full matrix algebra $\mathscr{C}([0,1], M_2(\mathbb{C}))$ to the

---

[2] In particular, the expressions under the square roots have to be non-negative and the suprema and infima have to be finite.

subalgebra $\mathcal{A}_2$. Hence for the purposes of the proof of theorem 4.1, there is no need to distinguish between $\mathcal{A}_2$ and $\mathscr{C}([0,1], M_2(\mathbb{C}))$.

Now consider a sequence of $n+1$ sequential measurements having the form $a, b, a, \ldots$. The set of outcomes for all measurements taken together is given by the set $\{0,1\}^{n+1}$ of binary sequences $r = (r_i)_{i=0}^n$. Every such outcome r has an associated Kraus operator which is given by

$$H_r = a^{r_0} b^{r_1} a^{r_2} \ldots \tag{5}$$

where the superscripts indicate whether one has to insert the projection a or b itself or its orthogonal complement $\bar{a} = 1 - a$ or $\bar{b} = 1 - b$, respectively. Then the probability of obtaining that outcome is given by the expression

$$\begin{aligned} P_a(r_0, r_1, \ldots, r_n) &= \rho\left(H_r H_r^\dagger\right) \\ &= \rho\left(a^{r_0} b^{r_1} a^{r_2} \ldots a^{r_2} b^{r_1} a^{r_0}\right) \end{aligned} \tag{6}$$

Now follows the main observation which facilitates all further calculations.

Lemma 4.2. *We have the following reduction formulas in $\mathcal{A}_2$:*

$$\begin{array}{ll} aba = ta, & bab = tb \\ a\bar{b}a = (1-t)a, & b\bar{a}b = (1-t)b \\ \bar{a}b\bar{a} = (1-t)\bar{a}, & \bar{b}a\bar{b} = (1-t)\bar{b} \\ \bar{a}\bar{b}\bar{a} = t\bar{a}, & \bar{b}\bar{a}\bar{b} = t\bar{b} \end{array}$$

Proof. Direct calculation. □

As a consequence, one finds that the measurement outcome probabilities (6) have the form

$$P_a(r_0, r_1, \ldots, r_n) = \rho\left(t^{n-s}(1-t)^s a^{r_0}\right)$$

where s is the number of switches in the binary sequence $r_0, \ldots, r_n$; the same clearly applies to the P_b's that determine the outcome probabilities for the measurement sequence $b, a, b, \ldots$. Hence, one necessary condition on the probabilities is the following:

Proposition 4.3. *The probabilities $P_a(r_0, r_1, \ldots, r_n)$ only depend on the number of switches contained in the binary sequence $r_0, \ldots, r_n$. The same holds for the $P_b(r_0, r_1, \ldots, r_n)$.*

A particular instance of this is equation (2).

Remark 4.4. Moreover, this observation is actually a *consequence* of the conditional statement of proposition 2.2(b). Due to that result, it is clear that the equations

$$P_a(r_0, \ldots, r_k, 0, 0, 1, r_{k+3}, \ldots, r_n) = P_a(r_0, \ldots, r_k, 0, 1, 1, r_{k+3}, \ldots, r_n)$$

$$P_a(r_0, \ldots, r_k, 1, 0, 0, r_{k+3}, \ldots, r_n) = P_a(r_0, \ldots, r_k, 1, 1, 0, r_{k+3}, \ldots, r_n)$$

hold. In words: the outcome probability does not change if the position of a switch in the binary string is moved by one. On the other hand, it is clear that any two binary sequences with the same number of switches can be transformed into each other by subsequently moving the position of each switch by one.

Since the dependence on the sequence r is only via its length $n+1$, the number of switches s, and the initial outcome r_0, mention of r will be omitted from now on. Instead, all expressions should be considered as functions of n and s, with $s \in \{0, \ldots, n\}$. The two possible values of the initial outcome r_0 as well as the initial type of measurement are indicated by subscripts:

$$
\begin{aligned}
P_a(0, r_1, \ldots, r_n) &= F_{a,0}(n, s) \\
P_a(1, r_1, \ldots, r_n) &= F_{a,1}(n, s) \\
P_b(0, r_1, \ldots, r_n) &= F_{b,0}(n, s) \\
P_b(1, r_1, \ldots, r_n) &= F_{b,1}(n, s)
\end{aligned}
$$

By the present results, the four functions $F_{\cdot,\cdot}$ can be written as

$$
\begin{aligned}
F_{a,1}(n, s) &= \rho \left(t^{n-s}(1-t)^s a \right) \\
F_{a,0}(n, s) &= \rho \left(t^{n-s}(1-t)^s \bar{a} \right) \\
F_{b,1}(n, s) &= \rho \left(t^{n-s}(1-t)^s b \right) \\
F_{b,0}(n, s) &= \rho \left(t^{n-s}(1-t)^s \bar{b} \right)
\end{aligned}
$$

Though instead of using these sequences of probabilities, the patterns are easier to spot using instead the new variables

$$
\begin{aligned}
F_{a,+}(n, s) &\equiv F_{a,1}(n, s) + F_{a,0}(n, s), & F_{a,-}(n, s) &\equiv F_{a,1}(n, s) - F_{a,0}(n, s) \\
F_{b,+}(n, s) &\equiv F_{b,1}(n, s) + F_{b,0}(n, s), & F_{b,-}(n, s) &\equiv F_{b,1}(n, s) - F_{b,0}(n, s)
\end{aligned}
$$

In these terms, we can write the four equations as

$$
\begin{aligned}
F_{a,+}(n, s) &= \rho \left(t^{n-s}(1-t)^s \right) \\
F_{b,+}(n, s) &= \rho \left(t^{n-s}(1-t)^s \right) \\
F_{a,-}(n, s) &= \rho \left(t^{n-s}(1-t)^s \sigma_z \right) \\
F_{b,-}(n, s) &= \rho \left(t^{n-s}(1-t)^s \left[2\sqrt{t(1-t)}\, \sigma_x + (2t-1)\, \sigma_z \right] \right)
\end{aligned}
$$

Therefore, it is clear that another necessary constraint is that

$$
F_{a,+}(n, s) = F_{b,+}(n, s) \quad \forall n, s
$$

In terms of the probabilities, this translates into

$$
\boxed{P_a(r) + P_a(\bar{r}) = P_b(r) + P_b(\bar{r})}
$$

The first non-trivial instance of this occurs for the case $n = 1$, where we have the equations

$$
\begin{aligned}
P_a(0, 0) + P_a(1, 1) &= P_b(0, 0) + P_b(1, 1) \\
P_a(0, 1) + P_a(1, 0) &= P_b(0, 1) + P_b(1, 0)
\end{aligned}
$$

which also have been noted in [AS01, p. 257/8].

Finally, let us try to extract the conditions that need to be satisfied by the $F_{a,-}$ and $F_{b,-}$. Considering the form of the equations, it seems convenient to introduce the quantities

$$
\begin{aligned}
C_1(n,s) &\equiv \frac{1}{2}\left(F_{a,-}(n,s) + F_{b,-}(n,s)\right) \\
&= \frac{1}{2}\left(F_{a,1}(n,s) - F_{a,0}(n,s) + F_{b,1}(n,s) - F_{b,0}(n,s)\right) \\
C_2(n,s) &\equiv \frac{1}{2}\left(F_{a,-}(n,s) - F_{b,-}(n,s)\right) \\
&= \frac{1}{2}\left(F_{a,1}(n,s) - F_{a,0}(n,s) - F_{b,1}(n,s) + F_{b,0}(n,s)\right)
\end{aligned}
$$

which are highly reminiscient of the CHSH correlations. In these terms,

$$
C_1(n,s) = \rho\left(t^{n-s}(1-t)^s \underbrace{\left[\sqrt{t(1-t)}\,\sigma_x + t\sigma_z\right]}_{\vec{v}_1(t)\cdot\vec{\sigma}}\right)
$$

$$
C_2(n,s) = \rho\left(t^{n-s}(1-t)^s \underbrace{\left[-\sqrt{t(1-t)}\,\sigma_x + (1-t)\sigma_z\right]}_{\vec{v}_2(t)\cdot\vec{\sigma}}\right)
$$

The reason that this is nicer is because now, the two vectors $\vec{v}_1(t)$, $\vec{v}_2(t)$, are orthogonal for each t. Finally, $\vec{v}_1(t)$ and $\vec{v}_2(t)$ can be normalized to get

$$
\begin{aligned}
C_1(n,s) &= \rho\left(t^{n-s+1/2}(1-t)^s\,\vec{n}_1(t)\cdot\vec{\sigma}\right) \\
C_2(n,s) &= \rho\left(t^{n-s}(1-t)^{s+1/2}\,\vec{n}_2(t)\cdot\vec{\sigma}\right)
\end{aligned}
$$

with vectors $\vec{n}_1(t)$, $\vec{n}_2(t)$, that are normalized and orthogonal for each t. Using an appropriate automorphism of $\mathcal{A}_2$ given by conjugation with a t-dependent unitary $U(t) \in SU(2)$, the vectors $\vec{n}_i(t)$ can be rotated in such a way that they coincide with the standard basis vectors $\vec{e}_x$ and $\vec{e}_z$, constant as functions of t.

Then, theorem 4.1 is a consequence of theorem A.3 as applied to

$$
\begin{aligned}
M_1'(n,s) &= F_{a,+}(n,s) \\
M_x'(n,s) &= C_1(n,s) \\
M_z'(n,s) &= C_2(n,s)
\end{aligned}
$$

5 Determining the quantum region in truncations

In actual experiments, only a finite number of the probabilities can be measured. Also, these can realistically only be known up to finite precision due to finite statistics. An even more problematic issue is that perfect von Neumann measurements are impossible to realize and can only be approximated. Here, we ignore the latter two problems and focus on the issue that only a finite number of probabilities are known.

10

Question 5.1. Given numerical values for a finite subset of the probabilities $P.(\cdot)$, how can one decide whether a quantum-mechanical model reproducing these probabilities exists?

Clearly, such a model exists if and only if these probabilities can be extended to a specification of *all* outcome probabilities P_a and P_b satisfying the conditions given in theorem 4.1. However, this observation doesn't seem very useful – how might one decide whether such an extension exists? The problem is that the projection of a convex set (the quantum region) from a higher-dimensional vector space down to a lower-dimensional one can be notoriously hard to describe.

This problem is a close relative of the truncated Hausdorff moment problem (see e.g. [Wi46, ch. III]). In a finite truncation of the Hausdorff moment problem, the allowed region coincides with the convex hull of the moments of the Dirac measures, which are exactly the extreme points in the space of measures. Therefore, the allowed region is the convex hull of an algebraic curve embedded in Euclidean space.

In the present case, it is possible to follow an analogous strategy of first determining the extreme points in the set of states – that is, the pure states on the algebra – then calculate the corresponding points in the truncation, and finally take the convex hull of this set of points. To begin this program, note that the pure states on the algebra are exactly those of the form

$$\mathscr{C}\left([0,1], M_2(\mathbb{C})\right) \longrightarrow \mathbb{C}, \quad f \mapsto \langle \psi | f(t_0) | \psi \rangle$$

where $t_0 \in [0,1]$ is fixed, and $|\psi\rangle$ stands for some fixed unit vector in $\mathbb{C}^2$; this corresponds to integration with respect to a projection-valued Dirac measure on $[0,1]$. Furthermore, since all the algebra elements of interest lie in the subalgebra given by the $M_2(\mathbb{R})$-valued functions – as opposed to $M_2(\mathbb{C})$-valued – the phases of the components of $|\psi\rangle$ are arbitrary, and can therefore be chosen such that $|\psi\rangle$ has real-valued components. This argument shows that $|\psi\rangle$ can be assumed to be given by

$$|\psi\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}.$$

In conclusion, the pure states are parametrized by the numbers $t_0 \in [0,1]$ and $\theta \in [0, 2\pi]$. In any given truncation, this determines an algebraic surface, whose convex hull coincides with the quantum region in that truncation. This reduces the problem to the calculation of the convex hull of an algebraic surface embedded in Euclidean space.

The following theorem is concerned with the infinite-dimensional truncation to all P_a, which means that one simply disregards all probabilities P_b while keeping the P_a.

Theorem 5.2. *A quantum-mechanical model in the P_a truncation exists for an admissible probability assignment if and only if $P_a(r)$ only depends on $s(r)$.*

Proof. It follows from the main theorem (4.1) that this condition is necessary. To see that it is sufficient, recall the equations

$$\begin{aligned} F_{a,+}(n,s) &= \rho\left(t^{n-s}(1-t)^s\right) \\ F_{a,-}(n,s) &= \rho\left(t^{n-s}(1-t)^s\sigma_z\right). \end{aligned}$$

Then upon choosing $M_1(n,s) = F_{a,+}(n,s)$, $M_x(n,s) = 0$ and $M_z(n,s) = F_{a,-}(n,s)$, theorem A.1 applies and shows that such a state ρ can be found as long as the condition

$$|F_{a,-}(n,s)| \leq F_{a,+}(n,s)$$

holds. In terms of the probabilities, this requirement means

$$|F_{a,1}(n,s) - F_{a,0}(n,s)| \leq F_{a,1}(n,s) + F_{a,0}(n,s),$$

which always holds trivially since all probabilities are non-negative. This ends the proof. □

This ends the current treatment of truncations. It is hoped that the future study of truncations will be relevant for experiments.

6 A general probabilistic model always exists

In order to understand as to how far the conditions found are characteristic of quantum mechanics, one should try to determine the analogous requirements for the probabilities in the case of alternative theories different from quantum mechanics and in the case of more general theories having quantum mechanics as a special case. This section deals with the case of general probabilistic theories.

What follows is a brief exposition of the framework of general probabilistic theories and of the possible models for a black box system (1). Afterwards, it will be shown that every assignment of outcome probabilities for the black box system does have a general probabilistic model. Together with the results of the previous sections, this shows that – for systems with two binary measurements – quantum-mechanical models are a very special class of general probabilistic theories.

For the present purposes, a general probabilistic theory is defined by specifying a real vector space V, a non-vanishing linear functional $\mathrm{tr} : V \to \mathbb{R}$, and a convex set of normalized states $\Omega \subseteq V$ such that

$$\mathrm{tr}(\rho) = 1 \quad \forall \rho \in \Omega \tag{7}$$

The cone $\Omega_0 \equiv \mathbb{R}_{\geq 0}\Omega$ is the set of all unnormalized states. By construction,

$$\Omega = \Omega_0 \cap \mathrm{tr}^{-1}(1).$$

Since all that matters for the physics is really Ω_0 and tr on Ω_0, one can assume without loss of generality that Ω_0 spans V,

$$V = \Omega_0 - \Omega_0. \tag{8}$$

Now, an *operation* is a linear map $T : V \to V$ which maps unnormalized states to unnormalized states,

$$T(\Omega_0) \subseteq \Omega_0,$$

and does not increase the trace,

$$\mathrm{tr}(T(\rho)) \leq 1 \quad \forall \rho \in \Omega.$$

For $\rho \in \Omega$, the number $\mathrm{tr}(T(\rho))$ is interpreted as the probability that the operation takes place, given T as one of several alternative operations characteristic of the experiment. In case that T happens, the post-measurement state is given by

$$\rho' \equiv \frac{T(\rho)}{\mathrm{tr}(T(\rho))},$$

where the denominator is just the normalization factor.

Example 6.1. As an example of this machinery, one may take density matrices as normalized states and completely positive maps as operations. This is quantum theory; the usual form of a quantum operation in terms of Kraus operators can be recovered by virtue of the Stinespring factorization theorem.

A repeatable binary measurement is then implemented by two operations $a, \bar{a} : V \to V$ which are idempotent,

$$a^2 = a, \quad \bar{a}^2 = \bar{a},$$

and complementary in the sense that the operation $a + \bar{a}$ preserves the trace. Physically, the operation a takes place whenever the measurement has a positive outcome, whereas $\bar{a}$ happens in the case that the measurement has a negative outcome.

Proposition 6.2. *Under these assumptions, $a\bar{a} = \bar{a}a = 0$.*

Proof. Clearly, $a\bar{a}$ is an operation, and therefore it maps Ω_0 to Ω_0. On the other hand,

$$\operatorname{tr}(\bar{a}a(\rho)) = \operatorname{tr}(a(\rho)) - \operatorname{tr}(aa(\rho)) = 0,$$

which proves $\bar{a}a = 0$ by (7). The other equation works in exactly the same way. $\qquad\square$

The interpretation of this result is that, when a has been measured with a positive outcome, then the opposite result $\bar{a}$ will certainly not occur in the second measurement, and vice versa. Therefore, the measurement of a vs. $\bar{a}$ is repeatable.

In the previous sections, the quantum region was found to be a very small subset of the space of all probabilities. The following theorem shows that this is not the case for general probabilistic theories.

Theorem 6.3. *Given any admissible probability assignment for the P_a's and P_b's, there exists a general probabilistic model that reproduces these probabilities.*

Proof. The idea of the proof is analogous to the characterization of the quantum region done in section 4: to try and construct a universal theory for the black box system, which covers all of the allowed region in probability space at once. In order to achieve category-theoretic universality (an initial object in the appropriate category), one nneds to consider the $\mathbb{R}$-algebra freely generated by formal variables v_a, $v_{\bar{a}}$, v_b, $v_{\bar{b}}$, subject to the relations imposed by the above requirements. Hence the definition is this,

$$\mathcal{A}_{gp} = \Big\langle v_a, v_{\bar{a}}, v_b, v_{\bar{b}} \ \Big| \quad v_a v_{\bar{a}} = v_{\bar{a}} v_a = v_b v_{\bar{b}} = v_{\bar{b}} v_b = 0,$$

$$v_a^2 = v_a, \ v_{\bar{a}}^2 = v_{\bar{a}}, \ v_b^2 = v_b, \ v_{\bar{b}}^2 = v_{\bar{b}} \Big\rangle_{\mathbb{R}\mathtt{Alg}}$$

where the notation indicates that this is to be understood as a definition in terms of generators and relations in the category of unital associative algebras over the field $\mathbb{R}$. The index gp stands for "general probabilistic".

Now an unnormalized state on $\mathcal{A}_{gp}$ is defined to be a linear functional

$$\rho : \mathcal{A}_{gp} \longrightarrow \mathbb{R}$$

13

which is required to be non-negative on all products of generators and the unit 1, and additionally needs to satisfy

$$\rho\left(x(v_a + v_{\overline{a}})\right) = \rho(x), \quad \rho\left(x(v_b + v_{\overline{b}})\right) = \rho(x)$$

for any $x \in \mathcal{A}_{gp}$. The set of unnormalized states Ω_0 is a convex cone in the vector space dual $\mathcal{A}_{gp}^*$. The trace is defined to be

$$\mathrm{tr}(\rho) \equiv \rho(1),$$

so that a state is normalized if and only if $\rho(1) = 1$.

Now for the definition of the operators a, $\overline{a}$, b, $\overline{b}$. Given an unnormalized state $\rho \in \Omega_0$, they produce a new state which is defined as

$$
\begin{aligned}
a(\rho)(x) &\equiv \rho(xv_a) \\
\overline{a}(\rho)(x) &\equiv \rho(xv_{\overline{a}}) \\
b(\rho)(x) &\equiv \rho(xv_b) \\
\overline{b}(\rho)(x) &\equiv \rho(xv_{\overline{b}})
\end{aligned}
$$

Since $v_a^2 = v_a$, it follows that $a^2 = a$, and analogous derivations work for all the other relations required to hold between the a, $\overline{a}$, b, $\overline{b}$.

Now given any initial state ρ and conducting the alternating measurements of a and b, the model predicts outcome probabilities that are given by

$$
\begin{aligned}
P_a(r) &= \rho\left(v_{a^{r_1}} v_{b^{r_2}} v_{a^{r_3}} \ldots\right) \\
P_b(r) &= \rho\left(v_{b^{r_1}} v_{a^{r_2}} v_{b^{r_3}} \ldots\right)
\end{aligned}
\tag{9}
$$

So given any assignment of outcome probabilities P_a, P_b, one can regard the equations (9) as a definition of ρ on products of generators. This ρ extends to a state on $\mathcal{A}_g p$ by linearity, where the equations (6) hold by conservation of probability. This ends the proof. $\qquad\square$

7   Remarks on potential generalizations

It would certainly be desirable to generalize the present results about quantum mechanics to situations involving a higher number of measurements or a higher number of outcomes per measurement or by allowing non-trivial dynamics for the system. I will now describe the corresponding C^*-algebras involved in this which one would have to understand in order to achieve such a generalization.

Consider a "black box" system analogous to (1) on which the experimenter can conduct k different kinds of measurement. Suppose also that the jth measurement has $n_j \in \mathbb{N}$ outcomes, and that again these measurements are repeatable, which again implies the absence of non-trivial dynamics.

A quantum-mechanical observable describing a von Neumann measurement with n possible outcomes is given by a hermitian operator with (up to) n different eigenvalues. Since the eigenvalues are nothing but arbitrary labels of the measurement outcomes, we might as well label the outcomes by the roots of unity $e^{\frac{2\pi i l}{n}}$, $l \in \{0, \ldots, n-1\}$. But then in this case the observable is given by a unitary operator u which satisfies $u^n = 1$. Conversely, given any unitary operator u of order n, we can diagonalize u into eigenspaces with eigenvalues being the roots of unity $e^{\frac{2\pi i l}{n}}$, and therefore we can think of u as being an observable where the n outcomes are labelled by the roots of unity.

14

By this reasoning, the specification of k observables where the jth observable has n_j different outcomes is equivalent to specifying k unitary operators, where the jth operator is of order n_j. Hence, the corresponding universal C^*-algebra is in this case given by the C^*-algebra freely generated by unitaries of the appropriate orders. But this object in turn coincides with the group C^*-algebra

$$C^*(\mathbb{Z}_{n_1} * \ldots * \mathbb{Z}_{n_k})$$

where the group is the indicated free product of finite cyclic groups. One should expect that these C^*-algebras have a very intricate structure in general; for example when $k = 2$ and $n_1 = 2$, $n_2 = 3$, one has the well-known isomorphism $\mathbb{Z}_2 * \mathbb{Z}_3 \cong PSL_2(\mathbb{Z})$, so that one has to deal with the group C^*-algebra of the modular group.

8 Possible experimental tests of quantum mechanics

The results of the previous sections show that the quantum region is certainly much smaller in the space of all probabilities than the general probabilistic region. Therefore, specific experimental tests of the quantum constraints from theorem 4.1 in a finite truncation seem indeed appropriate. However, there is an important caveat: for sufficiently small systems with many symmetries, it might be the case that any general probabilistic model is automatically a quantum theory. For example, when the convex set of states of a general probabilistic theory lives in $\mathbb{R}^3$ together with its usual action of the rotation group $SO(3)$ as symmetries, then it is automatically implied that the system is described by quantum mechanics, since every bounded and rotationally invariant convex set in $\mathbb{R}^3$ is a ball and therefore affinely isomorphic to the quantum-mechanical Bloch ball. This observation shows that some obvious candidates for experimental tests – like a photon sent through two kinds of polarizers – are too small for a successful distinction of quantum theory vs. different general probabilistic theories.

For these reasons, one should try to find systems with many degrees of freedom and few symmetries in order to conceive of experimental tests of quantum mechanics. The quantum dot experiment described in section 2 might be a good starting point for further investigation of these issues.

9 Conclusion

This article was concerned with the simplest non-trivial case of the inverse problem of quantum measurement for iterated measurements: given the probabilities for outcomes of sequences of iterated measurements on a physical systems, under which conditions can there exist a quantum-mechanical model of the system which recovers these probabilities? This question has been answered to the extent that there are several infinite sequences of constraints, all of which are rather unexpected, at least to the author. They show that the quantum region in the space of all probabilities is actually quite small and comparatively low-dimensional. In this sense, quantum-mechanical theories belong to a very specific class. The present results yield no insight on the question why our world should be quantum-mechanical – to the contrary, the conditions in theorem (4.1) are so unituitive and complicated that the existence of a direct physical reason for their presence seems unlikely.

A clearly positive feature of the strict constraints for quantum-mechanical models is that they could facilitate further experimental tests of quantum mechanics.

References

[RS89] Iain Raeburn, Allan M. Sinclair: *The C^*-algebra generated by two projections*, Math. Scand. 65/2 (1989), pp. 278–290.

[AV07] Yakir Aharanov, Lev Vaidman: *The Two-State Vector Formalism: An Updated Review*, Lecture Notes in Physics 734 (2007).

[AS01] Erik M. Alfsen, Frederic W. Shultz: *State spaces of operator algebras*, Birkhäuser (2001).

[Lo86] George G. Lorentz: *Bernstein Polynomials*, Chelsea Publishing Company (1986).

[CF91] Raúl E. Curto, Lawrence A. Fialkow: *Recursiveness, positivity and truncated moment problems*, Houston Journal of Mathematics 17(4), 1991.

[Wi46] David Widder: *The Laplace Transform*, Princeton University Press (1946).

A   Appendix: Two noncommutative moment problems

Let $\mathcal{A} \equiv \mathscr{C}\left([0,1], M_2(\mathbb{C})\right)$ be the C^*-algebra of continuous functions with values in 2×2-matrices.

Theorem A.1. *Given real numbers $M_1(n,s)$, $M_x(n,s)$ and $M_z(n,s)$ for each $n \in \mathbb{N}_0$ and $s \in \{0,\ldots,n\}$, there exists a state ρ on $\mathcal{A}$ that has the moments*

$$
\begin{aligned}
M_1(n,s) &= \rho\left(t^{n-s}(1-t)^s \cdot \mathbb{1}_2\right) \\
M_x(n,s) &= \rho\left(t^{n-s}(1-t)^s \cdot \sigma_x\right) \\
M_z(n,s) &= \rho\left(t^{n-s}(1-t)^s \cdot \sigma_z\right)
\end{aligned}
\tag{10}
$$

if and only if the following conditions hold:

- *probability conservation:*

$$
M_i(n,s) = M_i(n+1,s) + M_i(n+1,s+1) \quad \forall i \in \{1,x,z\}
\tag{11}
$$

- *non-negativity:*

$$
M_1(n,s) \geq \sqrt{M_x(n,s)^2 + M_z(n,s)^2}
\tag{12}
$$

- *normalization:*

$$
M_1(0,0) = 1
\tag{13}
$$

Proof. This proof is an adaptation of the solution of the Hausdorff moment problem as it is outlined in [Wi46, III §2]. Given the state ρ, it follows that (11) holds by $1 = t + (1-t)$. The non-negativity of $M_1(n,s)$ is a consequence of the fact that the function $t^{n-s}(1-t)^s \cdot \mathbb{1}_2$ is a positive element of $\mathcal{A}$. For the second inequality, note that linear combination

$$
c\,\mathbb{1}_2 + r\,\sigma_x + s\,\sigma_z
$$

is a positive matrix if and only if both the determinant and the trace are non-negative, which means that $r^2 + s^2 \leq c^2$ and $c \geq 0$. Hence in this case, the function

$$
t^{n-s}(1-t)^s \cdot (c\,\mathbb{1}_2 + r\,\sigma_x + s\,\sigma_z)
$$

16

is a positive element of $\mathcal{A}$, and the assertion follows by applying ρ to this function and choosing the values

$$r = -M_x(n,s), \quad s = -M_z(n,s), \quad c = \sqrt{M_x(n,s)^2 + M_z(n,s)^2}.$$

The main burden of the proof is to construct a state ρ, given a sequence of moments that satisfies the constraints (11), (12). First of all, (11), (12) and (13) together imply that

$$M_1(n,s) \leq 1 \quad \forall n, s \tag{14}$$

Now denote by $\mathcal{P}$ the real vector space of $\mathbb{R}[t]$-linear combinations of the matrices $\mathbb{1}_2$, σ_x and σ_z. The state ρ will first be constructed on $\mathcal{P}$, which is a subspace of $\mathcal{A}$.

Recall that the Bernstein polynomials [Lo86]

$$B_{n,s}(t) = \binom{n}{s} t^s (1-t)^{n-s}$$

can be used to approximate any continuous function on $[0,1]$ in the sense that the approximants

$$A_n(f)(t) \equiv \sum_{s=0}^{n} f\left(\frac{s}{n}\right) B_{n,s}(t)$$

converge uniformly to f,

$$|f(t) - A_n(f)(t)| < \varepsilon_n \ \forall t \in [0,1], \quad \varepsilon_n \stackrel{n\to\infty}{\longrightarrow} 0.$$

The Bernstein polynomials can be used to construct a sequence of approximating states ρ_n on $\mathcal{P}$. These are defined in terms of the given moments as

$$\rho_n \left(P_1(t)\mathbb{1}_2 + P_x(t)\sigma_x + P_z(t)\sigma_z \right)$$

$$\equiv \sum_{s=0}^{n} \binom{n}{s} \left[P_1\left(\frac{s}{n}\right) M_1(n,s) + P_x\left(\frac{s}{n}\right) M_x(n,s) + P_z\left(\frac{s}{n}\right) M_z(n,s) \right].$$

for any polynomials P_1, P_x and P_z. Although it is hard to directly check convergence of the sequence $(\rho_n)_{n\in\mathbb{N}}$, it is at least clear that the ρ_n are uniformly bounded,

$$\left| \rho_n(P_1(t)\mathbb{1}_2 + P_x(t)\sigma_x + P_z(t)\sigma_z) \right|$$

$$\stackrel{(12)}{\leq} \max_{t\in[0,1]} \left[|P_1(t)| + \sqrt{P_x(t)^2 + P_z(t)^2} \right] M_1(n,s)$$

$$\stackrel{(14)}{\leq} \max_{t\in[0,1]} \left[|P_1(t)| + \sqrt{P_x(t)^2 + P_z(t)^2} \right] \tag{15}$$

$$= \max_{t\in[0,1]} \left\| P_1(t)\mathbb{1}_2 + P_x(t)\sigma_x + P_z(t)\sigma_z \right\|$$

where the norm in the last expression coincides with the C^*-algebra norm on $\mathcal{A}$.

On the other hand, let $\mathcal{P}_n$ be the subspace of $\mathcal{P}$ where the polynomials are of degree up to n. A basis of $\mathcal{P}_n$ is given by the $3n+3$ matrix polynomials

$$B_{n,s}\mathbb{1}_2, \ B_{n,s}\sigma_x, \ B_{n,s}\sigma_z; \quad s \in \{0,\dots,n\}. \tag{16}$$

17

Then the requirements (10) uniquely define a linear functional $\widetilde{\rho}_k : \mathcal{P}_k \to \mathbb{R}$,

$$\begin{aligned}
\widetilde{\rho}_k\left(B_{n,s}\mathbb{1}_2\right) &= M_1(n, n-s) \\
\widetilde{\rho}_k\left(B_{n,s}\sigma_x\right) &= M_x(n, n-s) \\
\widetilde{\rho}_k\left(B_{n,s}\sigma_z\right) &= M_z(n, n-s).
\end{aligned}$$

But now the relations

$$\frac{B_{n,s}}{\binom{n}{s}} = \frac{B_{n+1,s}}{\binom{n+1}{s}} + \frac{B_{n+1,s+1}}{\binom{n+1}{s+1}},$$

in conjunction with the additivity law (11), show that the diagram

commutes for all k. Therefore, the $\widetilde{\rho}_k$ extend to a trial state $\widetilde{\rho} : \mathcal{P} \to \mathbb{R}$, which is now defined on all of $\mathcal{P}$. The problem with $\widetilde{\rho}$ is that it is not obviously bounded.

Therefore, the rest of this proof is devoted to showing that the approximating states converge to the trial state in the weak sense:

$$\rho_k(P) \overset{k \to \infty}{\longrightarrow} \widetilde{\rho}(P) \quad \forall P \in \mathcal{P}.$$

Then (15) implies that $\widetilde{\rho}$ is bounded and $||\widetilde{\rho}|| = 1$. Hence the Hahn-Banach extension theorem shows that $\widetilde{\rho}$ can be extended to a linear functional $\widehat{\rho} : \mathcal{A} \to \mathbb{C}$ with $||\widehat{\rho}|| = 1$. This proves the original assertion by the fact that this is automatically a state as soon as $||\widehat{\rho}|| = \rho(\mathbb{1}) = 1$ holds, and the construction of $\widehat{\rho}$ such that the equations (10) hold for this state.

In order to check this convergence, it is sufficient to consider the values of the states on the basis polynomials (16). And for those, the calculation will be shown only for the first type $B_{n,s}\mathbb{1}_2$, since the other two work in exactly the same way.

$$\widetilde{\rho}\left(B_{n,n-s}(t)\mathbb{1}_2\right) - \rho_k\left(B_{n,n-s}(t)\mathbb{1}_2\right)$$

$$= M_1(n,s) - \sum_{r=0}^{k} \binom{k}{r}\left(\frac{r}{k}\right)^{n-s}\left(1-\frac{r}{k}\right)^s M_1(k,r)$$

$$\overset{(11)}{=} \sum_{r=0}^{k} \left[\binom{k-n}{r-s} - \binom{k}{r}\left(\frac{r}{k}\right)^{n-s}\left(1-\frac{r}{k}\right)^s\right] M_1(k,r)$$

$$= \sum_{r=0}^{k} \left[\frac{\binom{k-n}{r-s}}{\binom{k}{r}} - \left(\frac{r}{k}\right)^{n-s}\left(1-\frac{r}{k}\right)^s\right] \binom{k}{r} M_1(k,r)$$

Therefore using $\sum_{r=0}^{k} \binom{k}{r} M_1(k,r) = M_1(0,0) = 1$,

$$\left|\widetilde{\rho}\left(B_{n,n-s}(t)\mathbb{1}_2\right) - \rho_k\left(B_{n,n-s}(t)\mathbb{1}_2\right)\right| \leq \max_{r=0}^{k} \left|\frac{\binom{k-n}{r-s}}{\binom{k}{r}} - \left(\frac{r}{k}\right)^{n-s}\left(1-\frac{r}{k}\right)^s\right| \qquad (17)$$

18

$$\leq \max_{y\in[0,1]} \left| \frac{\Gamma(k-n+1)}{\Gamma(k+1)} \cdot \frac{\Gamma(ky+1)}{\Gamma(ky-s+1)} \cdot \frac{\Gamma(k(1-y)+1)}{\Gamma(k(1-y)-n+s+1)} - y^{n-s}(1-y)^s \right|$$

This expression trivially vanishes for $y = 0$ and for $y = 1$. For $y \in (0,1)$, all the Gamma function arguments tend to infinity, therefore the formula

$$\lim_{t\to\infty} \frac{\Gamma(t+m+1)}{\Gamma(t+1)} \cdot t^{-m} = 1$$

can be applied in the form

$$\left| \frac{\Gamma(t+m+1)}{\Gamma(t+1)} - t^m \right| < \varepsilon \cdot t^m \quad \forall t \geq t_0(m,\varepsilon)$$

to show that (17) vanishes in the $k \to \infty$ limit. This finally ends the proof. $\qquad\square$

Before studying the next noncommutative moment problem, some preparation is needed. So let $\mathcal{C} \subseteq \mathbb{R}^4$ be the set of points $(x_0, y_0, x_1, y_1) \in \mathbb{R}^4$ with the following property: the rectangle in $\mathbb{R}^2$ that is spanned by (x_0, y_0) as the lower left corner and (x_1, y_1) as the upper right corner has non-empty intersection with the unit disc $\{(x,y) \,|\, x^2 + y^2 \leq 1\}$.

Proposition A.2. $\mathcal{C}$ *is a convex semialgebraic set. A point* (x_0, y_0, x_1, y_1) *lies in* $\mathcal{C}$ *if and only if it satisfies all the following five clauses:*

$$x_0 \leq x_1 \,\wedge\, y_0 \leq y_1$$
$$(x_0 \leq 1 \wedge y_0 \leq 0) \vee (x_0 \leq 0 \wedge y_0 \leq 1) \vee (x_0^2 + y_0^2 \leq 1)$$
$$(x_0 \leq 1 \wedge y_1 \geq 0) \vee (x_0 \leq 0 \wedge y_1 \geq -1) \vee (x_0^2 + y_1^2 \leq 1)$$
$$(x_1 \geq -1 \wedge y_0 \leq 0) \vee (x_1 \geq 0 \wedge y_0 \leq 1) \vee (x_1^2 + y_0^2 \leq 1)$$
$$(x_1 \geq -1 \wedge y_1 \geq 0) \vee (x_1 \geq 0 \wedge y_1 \geq -1) \vee (x_1^2 + y_1^2 \leq 1)$$

Proof. $\mathcal{C}$ is the projection obtained by forgetting the first two coordinates of the points in the set

$$\widetilde{\mathcal{C}} \equiv \left\{ (x, y, x_0, y_0, x_1, y_1) \in \mathbb{R}^6 \,\middle|\, x_0 \leq x \leq x_1,\ y_0 \leq y \leq y_1,\ x^2 + y^2 \leq 1 \right\}.$$

Since $\widetilde{\mathcal{C}}$ is convex semi-algebraic, so is any projection of it, and therefore $\mathcal{C}$.

A description of $\widetilde{\mathcal{C}}$ in terms of linear inequalities is given by

$$x - x_0 \geq 0, \quad -x + x_1 \geq 0$$
$$y - y_0 \geq 0, \quad -y + y_1 \geq 0$$
$$x \cdot \cos\alpha + y \cdot \sin\alpha \leq 1 \quad \forall \alpha \in [0, 2\pi]$$

From this, one obtains the linear inequalities that define $\mathcal{C}$ by taking all these positive linear combinations for which the dummy variables x and y drop out. There are exactly two such combinations that do not use the α-family inequalities, and they are $x_0 \leq x_1$ and $y_0 \leq y_1$. On the other hand, if such a linear combination contains α-family inequalities for at least two different values of α, the inequality cannot be tight, since any non-trivial positive linear combination of the α-family inequalities for different values of α is dominated by a single one with another value of α. Therefore, it suffices to conisder each value of α at a time, and add appropriate multiples of the other inequalities

such that x and y drop out. Since for both x and y and each sign, there is exactly one inequality among the first four that contains that variable with that sign, there is a unique way to replace x by x_0 or x_1 and y by y_0 or y_1. Depending on the value of α, there are four sign combinations to consider, and the result is the following set of inequalities:

$$
\begin{aligned}
x_1 \cdot \cos\alpha + y_1 \cdot \sin\alpha \leq 1 & \quad \forall \alpha \in [0, \pi/2], \\
x_0 \cdot \cos\alpha + y_1 \cdot \sin\alpha \leq 1 & \quad \forall \alpha \in [\pi/2, \pi], \\
x_1 \cdot \cos\alpha + y_0 \cdot \sin\alpha \leq 1 & \quad \forall \alpha \in [\pi, 3\pi/2], \\
x_0 \cdot \cos\alpha + y_0 \cdot \sin\alpha \leq 1 & \quad \forall \alpha \in [3\pi/2, 2\pi].
\end{aligned}
$$

Each of these families of inequalities in turn is equivalent to the corresponding clause above; for example, $\alpha \in [0, \pi/2]$ bounds a region defined by the lines $x_1 = 1$, $y_1 = 1$ and the circular arc in the first quadrant of the x_1-y_1-plane. This region coincides with the one defined by the first of the clauses above. This works in the same way for the other three families. $\qquad \square$

Theorem A.3. *Given real numbers $M_1'(n, s)$, $M_x'(n, s)$ and $M_z'(n, s)$ for each $n \in \mathbb{N}_0$ and $s \in \{0, \ldots, n\}$, there exists a state ρ on $\mathcal{A}$ that has the (integer and half-integer) moments*

$$
\begin{aligned}
M_1'(n, s) &= \rho\left(t^{n-s}(1-t)^s \cdot \mathbb{1}_2\right) \\
M_x'(n, s) &= \rho\left(t^{n-s+1/2}(1-t)^s \cdot \sigma_x\right) \\
M_z'(n, s) &= \rho\left(t^{n-s}(1-t)^{s+1/2} \cdot \sigma_z\right)
\end{aligned}
\tag{18}
$$

if and only if the following conditions hold:

- *probability conservation:*

$$
M_i'(n, s) = M_i'(n+1, s) + M_i'(n+1, s+1) \quad \forall i \in \{1, x, z\}
\tag{19}
$$

- *non-negativity:*

$$
M_1'(n, s) \geq 0
\tag{20}
$$

for all $n \in \mathbb{N}_0$ and $s \in \{0, \ldots, n\}$. Furthermore,[3]

$$
\begin{aligned}
&\left(\sum_{k=0}^{\infty} (-1)^k \binom{1/2}{k} M_x'(n+k-1, s+k)\right)^2 \\
&+ \left(\sum_{k=0}^{\infty} (-1)^k \binom{1/2}{k} M_z'(n+k-1, s-1)\right)^2 \leq M_1'(n, s)^2
\end{aligned}
\tag{21}
$$

for $n \in \mathbb{N}$ and $s \in \{1, \ldots, n-1\}$. Finally, using the coefficients

$$
c_{n,k} = \begin{cases}
(-1)^k \binom{-1/2}{k} & \text{for } k \leq n \\
(-1)^k \binom{-1/2}{k} - (-1)^{k-n} \binom{-1/2}{k-n} & \text{for } k > n
\end{cases}
$$

---

[3]Note that all sums are automatically absolutely convergent since $F_{\cdot,\cdot}(\cdot, \cdot) \in [0, 1]$ and $\sum_{k=0}^{\infty} \left|\binom{1/2}{k}\right| = 1 < \infty$.

and the quantities

$$V_{x,\pm}(n) = \sum_{k=0}^{\infty} c_{n,k} M'_x(k,k)$$

$$\pm \sqrt{M'_1(n,n)^2 - \left(\sum_{k=0}^{\infty}(-1)^k \binom{1/2}{k} M'_z(n+k-1,n-1)\right)^2}$$

$$V_{z,\pm}(n) = \sum_{k=0}^{\infty} c_{n,k} M'_z(k,0)$$

$$\pm \sqrt{M'_1(n,0)^2 - \left(\sum_{k=0}^{\infty}(-1)^k \binom{1/2}{k} M'_x(n+k-1,k)\right)^2}$$

the point in $\mathbb{R}^4$ given by

$$\left(\sup_n V_{x,-}(n), \ \sup_n V_{z,-}(n), \ \inf_n V_{x,+}(n), \ \inf_n V_{z,+}(n)\right) \tag{22}$$

has to lie in $\mathcal{C}$.[4]

- *normalization:*

$$M'_1(0,0) = 1 \tag{23}$$

Proof. It will be shown first that these conditions are necessary. This is immediate for (19), (20) and (23). Furthermore, the (uniformly convergent) binomial expansions

$$\sqrt{t} = \sqrt{1-(1-t)} = \sum_{k=0}^{\infty} \binom{1/2}{k}(-1)^k(1-t)^k$$

$$\sqrt{1-t} = \sum_{k=0}^{\infty} \binom{1/2}{k}(-1)^k t^k$$

can be applied to express most of the integer moments of a given state in terms of the half-integer moments of that state,

$$\rho\left(t^{n-s}(1-t)^s \sigma_x\right) = \sum_{k=0}^{\infty}(-1)^k \binom{1/2}{k} \rho\left(t^{n-s-1/2}(1-t)^{s+k}\sigma_x\right), \quad s \in \{0,\dots,n-1\}$$

$$\rho\left(t^{n-s}(1-t)^s \sigma_z\right) = \sum_{k=0}^{\infty}(-1)^k \binom{1/2}{k} \rho\left(t^{n-s+k}(1-t)^{s-1/2}\sigma_z\right), \quad s \in \{1,\dots,n\}. \tag{24}$$

In the present notation (10) and (18), this reads

$$M_x(n,s) = \sum_{k=0}^{\infty}(-1)^k \binom{1/2}{k} M'_x(n+k-1,s+k), \quad s \in \{0,\dots,n-1\}$$

$$M_z(n,s) = \sum_{k=0}^{\infty}(-1)^k \binom{1/2}{k} M'_z(n+k-1,s-1), \quad s \in \{1,\dots,n\}. \tag{25}$$

---

[4]In particular, the expressions under the square roots have to be non-negative and the suprema and infima have to be finite.

Together with (12), these formulas imply the constraint (21) for all relevant values $s \in \{1, \ldots, n - 1\}$. Given in addition $M_x(0,0) = \rho(\sigma_x)$ and $M_z(0,0) = \rho(\sigma_z)$, the remaining integer moments undetermined by (25) can be calculated as

$$
\begin{aligned}
M_x(n,n) &\overset{(11)}{=} M_x(0,0) - \sum_{k=1}^{n} M_x(k, k-1) \overset{(25)}{=} M_x(0,0) - \sum_{k=0}^{\infty} c_{n,k} M'_x(k, k), \\
M_z(n,0) &\overset{(11)}{=} M_z(0,0) - \sum_{k=1}^{n} M_z(k, 1) \overset{(25)}{=} M_z(0,0) - \sum_{k=0}^{\infty} c_{n,k} M'_z(k, 0).
\end{aligned}
\tag{26}
$$

where the second steps also involve rearrangements of the sums. Since $M_x(n,n)$ is constrained by (12) to have an absolute value of at most

$$
\sqrt{M_1(n,n)^2 - M_z(n,n)^2} = \sqrt{M'_1(n,n)^2 - \left(\sum_{k=0}^{\infty} \binom{1/2}{k} M'_z(n+k-1, n-1)\right)^2},
$$

equation (26) shows that $M_x(0,0)$ has to lie in the interval

$$
[V_{x,-}(n), V_{x,+}(n)]
\tag{27}
$$

for all n; therefore, it also has to lie in the intersection of all these intervals, which is the interval

$$
\left[\sup_n V_{x,-}(n), \inf_n V_{x,+}(n)\right].
$$

Exactly analogous considerations show that $M_z(0,0)$ has to lie in the interval

$$
\left[\sup_n V_{z,-}(n), \inf_n V_{z,+}(n)\right].
$$

Now one concludes that the point (22) has to be in $\mathcal{C}$ by the additional constraint

$$
M_x(0,0)^2 + M_z(0,0)^2 \leq M_1(0,0)^2 = 1.
\tag{28}
$$

For the converse direction, it will be shown that the assumptions imply the existence of moments $M_x(n,s)$ and $M_z(n,s)$ satisfying the hypothesis of theorem A.1 such that the M'_x and M'_z can be recovered as

$$
\begin{aligned}
M'_x(n,s) &= \sum_{k=0}^{\infty} (-1)^k \binom{1/2}{k} M_x(n+k, s+k) \\
M'_z(n,s) &= \sum_{k=0}^{\infty} (-1)^k \binom{1/2}{k} M_z(n+k, s),
\end{aligned}
\tag{29}
$$

and such that the $M_1(n,s)$ coincide with the $M'_1(n,s)$. To begin, use (25) to define $M_x(n,s)$ for $s \in \{0, \ldots, n-1\}$ and $M_z(n,s)$ for $s \in \{1, \ldots, n\}$. As soon as additionally the values for $M_x(0,0)$ and $M_z(0,0)$ are determined, the remaining integer moments are defined by (26). Then it can be verified by direct calculation – treating the cases $s \in \{1, \ldots, n-1\}$ separately from $s = 0$ and $s = n$ – that the equations (29) hold, indpendently of the chosen values for $M_x(0,0)$ and $M_z(0,0)$.

22

It remains to verify that, with these definitions of M_x and M_z, the requirements of theorem (A.1) can be satisfied for appropriate choices of $M_x(0,0)$ and $M_z(0,0)$. The equations (11) easily follow by direct calculation, using (19). Again by the binomial expansions, the second part of (12) is directly equivalent to (21) for $s \in \{1, \ldots, n-1\}$. In the case that $s = n \neq 0$, it holds as long as $M_x(0,0)$ is chosen to lie in the interval (27); a similar statement holds for $s = 0$ and $n > 0$. For $s = n = 0$, the constraint is equivalent to (28) and means that $(M_x(0,0), M_z(0,0))$ has to lie in the unit disk of $\mathbb{R}^2$. By the assumption that (22) lies in $\mathcal{C}$, it follows that a consistent choice for $M_x(0,0)$ and $M_z(0,0)$ that satisfies all these requirements is indeed possible. $\qquad\square$